ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 5, Issue 2, Februray 2016

Deterring Selfish Nodes Using Account - Aided Reputation Management System in MANETs

Irin Sherly. S[1], Divya.S[2], Kalpana Devi.B.S[3], Nimishambigai.M[4]

Assistant Professor, Dept of IT, Panimalar Institute of Technology, Chennai, Tamilnadu, India[1]

U.G. Student, Department of IT, Panimalar Institute of Technology, Chennai, Tamilnadu, India[2]

U.G. Student, Department of IT, Panimalar Institute of Technology, Chennai, Tamilnadu, India[3]

U.G. Student, Department of IT, Panimalar Institute of Technology, Chennai, Tamilnadu, India[4]

ABSTRACT: Achieving cooperation and deterring selfish behaviors are significant for proper happening of mobile ad hoc networks (MANETs) . For this purpose, most previous efforts entrust on either reputation systems or price systems.Nodes in both systems can be perverse while still being considered honorable. Also, information transfer amid mobile nodes in reputation systems and acclaim circulation in price systems expend symbolic resources. This paper presents a hierarchical Account-aided Reputation Management system (ARM) to effortlessly and adequately provide assistance incentives. ARM builds a hierarchical locality-alive distributed hash table (DHT) frameworkwhich globally collects all node reputation information in the system which can then be used to calculate more factual reputation and detect anomalistic reputation information. Also, ARM blends reputation and price systems by enabling higher-reputed nodes to pay less for their earned services. Theoretical analysis exhibits the properties of ARM. Simulation outcomes show that ARM exceed the individual reputation system and price system in terms of adequacy and effortless of providing assistance incentives and impeding selfish behaviors.

KEYWORDS: Mobile ad hoc networks, price systems, reputa-tion systems.

I. INTRODUCTION

A MOBILE ad hoc network (MANET) is an assemblage of mobile nodes with less fixed infrastructure or centralized management. A MANET is expected to associate thousands or even millions of mobile nodes for universal communication in the future. Nodes here interact with each other by routing data through relay nodes in a multihop manner. Thus, reliable communication is critical to the proper happening of MANETs.

MANETs are particularly vulnerable to selfish behaviors due to the individualized nature of nodes. Selfish nodes tend not to forward data in order to save resources. The presence of only a few misbehaving nodes can hysterically impede the performance of the absolute system [1]. Current main methods to deal with the challenge: reputation systems and price systems. However, existing reputation systems and price systems are neither adequately efficient nor adequately effective. By insufficient efficiency, the methods aggravate the resource -efficiency problem in MANETs by engrossing already sparse resources. The accuracy of node reputation can be negatively affected by false information including falsified, conspiratorial, and misreported information. Falsified information is reported by a misbehaving node inorder to purposely increase/decrease others' reputations. Conspiratorial information is generated by colluders that report high reputations for each other to raise their own reputations and report low reputations for others to decline their reputations. Misreported information in this paper means low reputations for cooperative nodes who cannot offer high -quality transportation service due to injurious network conditions such as background intervention. In this paper, we only focus on these three kinds of false information though there are many other kinds.

In most current reputation systems [1]–[9], a node collects locally generated node feedback and accumulate it to yield the global reputation values (R) for others based on cyclic information exchanges among neighbors. The node

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 5, Issue 2, Februray 2016

whose reputation is below a predefined threshold $(\mathcal{T})$ is considered selfish and put into a blacklist.This paper aims to handle the problems in reputation systems and prices systems for more effective assistance incentives. A fierce challenge is how to efficiently and coordinately tag on the two systems to avoid the problems in the individual systems, ensuring they can be attained to their fullest capacities. Therefore, in this paper, we focus on system design to handle this challenge, which is different from our theoretical work in [15].

We propose a hierarchical Account-aided Reputation Management system (ARM), that coordinately blends a reputation system and a price system to effectively and efficiently deter and detect selfish behaviors.

ARM selects low-mobility and trustworthy nodes as reputation managers (managers in short), constructs them into a locality- aware DHT infrastructure, and coordinately integrates a reputation system and a price system through the framework.

Specifically, ARM consists of three components:

- *A locality-aware DHT infrastructure*. The infrastructure efficiently compiles node reputation and transaction information for effective reputation and account management. Experimental results show that even when including the maintenance overhead in node mobility, ARM still propagates a lower overhead than current reputation and price systems.
- *Reputation management*. Entrusting on the collected globalinformation by DHT, ARM effectively finds false information and accurately determines node reputation. Also, ARM avoids cyclic information exchange, the storage and computing load of each node in the system.

- *Reputation-adaptive account management*. ARM treatsnodes with disimilar reputations differently and also prevents nodes from having fraudulent benefits. Especially, a higher-reputed node pays a lower price while a lower-reputed node pays a higher price for service. Also, a high-reputed node obtains more credits than a low-reputed node for the same forwarding service. Using the DHT, ARM has no virtual credits circling in the network and erradicates the implementation intricacy.

In ARM, *uncooperative and reputed* nodes in reputation system can be determined based on their deficit accounts and *un-cooperative and wealthy* nodes in price system can be determinedas they rapidlyreach $R<\mathcal{T}$. Also, because a cooperative node pays less for the service, the credits earned by a node in a low-traffic area can preserve its requests. As a result, our reputation system for MANETs can more efficiently effectivelyencourage cooperation incentives and deter selfish behavior and misbehaviors.

II. RELATED WORK

In this section, we present the related work about reputation systems and price systems in MANETs. Reputation systems can be divided into two categories: direct observation [16]–[18] and indirect observation [1]–[9] methods. In the former, nodes autonomusly assess their neighbors' reputations based on their direct interactions. To increment the routing accuracy, Conti *et al.* [16] proposed a reliability indexing mechanism, in which each node manage its in/out traffic based on the reliability index value related with the neighbor through which the packet is forwarded .Liu *et al.* [17] proposed to extend the scope of the behavior observation from one hop to two hops. Jaramillo *et al.* [18] showed that the punishment policy in reputation systems always results in a retaliation situation where identified selfish nodes never cooperate again, declinging the throughput of cooperative users. They proposed aexaminig strategy to avoid the retaliation situation. However, because the node behaviors that each node can observe are restricted, exclusively depending on direct observations may enhance the selfish and misbehaving node detection time.In the indirect observation, nodes periodically share their noted reputation information with others. The works in [1] and [2] use the techniques of *watchdog* and *pathrater*. The *Watchdog* in a node accurately listens to the transferenceof the next node in the path in order to determine misbehaviors. The *Pathrater* in a node keeps the valuation of other nodes to avoid interaction with uncooperative nodes in the transmission. Anantvalee and Wu [4] introduced a new type of node called

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 5, Issue 2, Februray 2016

suspicious nodes, which will be further enquired to see if they tend to behave selfishly with two reputation thresholds.Refaei*et al.* [5] introduced a time- slotted approach to allow the evaluation function to instantly and accurately capture changes in node behavior. Also, they use a orderlyprobability ratio to differentiate between cooperative and misbehaving neighbors by monitoring their misbehaving probabilities. The indirect observation based reputation systems decrement the selfish and misbehaving node detection time. However,the malicious nodes may report false information about other nodes, which may decrease selfish node detection reliability.

In order to decrease the number of false ratings, Bucheggeret *al.* [6] proposed a Bayesian prediction mechanism to increase system robustness related to falsely dispersed information. Mundingeret *al.* [7] built a stochastic process to calculate the behavior of the nodes in the system and derive a mean normal differential equation for misreport detection. Luo*et al.* [8] built a fuzzy logic based on only partial reputation information that may not be quite reliable. However, all these methods use complex machine learning and statistical algorithms for selfish and misbehaving node detection, which provokes high computational costs of the mobile nodes.The periodical transfers of the observations lead to high communication overhead. Taking advantage of the DHT structure, ARM efficiently and more aptly calculated the global reputation of the nodes with less overhead. By calculating the deviation of the reputation ratings among average ratings, the selfish and misbehaving nodes can be easily identified with low computational costs. There are many other reputation system works that especially deter misreporting, fake IDs, and free-riding as represented in our previous work [19]. ARM only aims on eliminating the aforementioned falsified, conspiratorial and misreported information when formulating node global reputation values. Price systems [10]–[14] provide incentives for cooperation by using micro payments. In the credit-based system in [11], when a node forwards a message, it keeps a receipt and uploads it to the credit clearance service for credits. Crowcrof*et al.* [12] proposed a traffic price approach, in which the earnings for message forwarding relies not only on the energy consumption of the transmission, but also on the congestion level of the relaying node. A number of works have been proposed to elevate the cooperation among nodes based on game theory [13], [15], [20]–[21]. Since these works focus on theoretical algorithm design, they did not give details on the system designARM focuses on the reputation system design and aims to enhance the system efficiency and effectiveness by coordinately organising the reputation system and price systemthrough a DHT-based infrastructure.

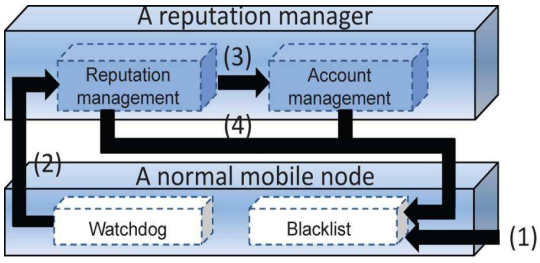


Fig. 1. Overview of the ARM system..

Unlike current price systems , ARM uses an account management mechanism that transparently processes the credit accounts of the nodes based on the node transactions.

III.DESIGN OF THE ARM MANAGEMENT

A. Overview

ARM chooses a number of trustworthy and low-mobility nodes as reputation managers. The reputation managers comprise a locality - aware DHT for efficient operations of ARM. As shown in Fig. 1, each normal mobile node has a *watchdog* [3], [4] to monitor and report the behaviors of itsneighbors to managers.The managers have dual functions: reputation management and account management. Each manager formulates the reputations and increases/decreases the credits in the reports of the mobile nodes for which it is censurable. Nodes with reputations below the threshold are considered as uncooperative nodes. Managers indicate mobile nodes about uncooperative nodes and put into blacklists.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 5, Issue 2, Februray 2016

The blacklisted nodes' forwarding requests are ignored by others.In ARM, a high-reputed node pays less credits while a low-reputed node pays more credits in a forwarding service transaction, thus effectively providing incentives for cooperation among nodes.

B. Assumptions of the Network

In this paper, we consider the scenario of MANETs with normal or relatively large network size and area size that have no centralized dedicated servers in the network. Therefore, we form trustable and relatively stable nodes into a DHT for efficient reputation management. We use the DHT infrastructure for two reasons: 1) given a node's ID, DHT's Insert(ID, object) function can forward the reputation or transaction reports on this node to its manager, and DHT's Lookup(ID) function can forward the reputation or account query to this node's manager; and 2) these two functions have $O(\log N)$ time complications and each node maintains $O(\log N)$ neighbors, which achieves greater scalability. Without the DHT infrastructure, each manager must have a record for each node's mapped manager, which is not adaptable in a large-scale MANET.

Thus, we consider some mobile nodes in the MANET have dual-mode interfaces. As more nodes add up in the network, the nodes with high reputations and low mobility can be slowly selected as reputation manager and added into the DHT. The selected reputation managers can be awarded with virtual credits to recoup their contribution and provide incentives for nodes to become the reputation managers. The reputation messages exchanged among managers are of small size and delay-tolerant compared to data messages. Managers use the low-power interface for data transference. For reputation data transmission, they can use the high- power interface .

C. Locality-Aware DHT Infrastructure

Fig. 2 illustrates the hierarchical structure of ARM. The higher level is a DHT network composed of managers, and the lower level is composed of normal mobile nodes. A DHT partitions ownership of a set of objects among participating nodes and efficiently route messages to the unique owner of any given object. Each object or node is assigned an ID.The DHT has two main functions, Insert(ID,object) and Lookup(ID), to store an object to a node responsible for the ID and to recover the object. ARM constructs a locality-aware DHT where logical proximity matches the physical proximity in reality. In this way, the packet routing path in the overlay is persistent with the packet routing path in the physical topology.To construct a locality-aliveDHT, the physical topology should also be a Hamiltonian cycle [23]

1) Locality-Aware DHT Infrastructure Construction:

Fig. 3 shows an example of a physical topology and its related logical topology in ARM. In a logical topology, the distance between nodes' IDs represents their logical distance.In a MANET, each node identifies its neighbors by sending “hello” messages. Thus, a node can know the relative physical closeness of its neighbors by the actual communication latency. To assign IDs to managers, we first choose, a bootstrap manager and assign it ID 0.Then it chooses its physically nearest node as its successor and assigns it ID 1. The process is repeated until the bootstrap node is reached. At this time, a complete cycle is formed and all managers have been assigned numerically continuous IDs. Then, each manager builds a DHT routing .

2) Locality- Aware DHT Infrastructure Maintenance:

Proposition 3.2 states that the stability of the DHT infrastructure is determined by the moving speed and transmission extent of managers. To maintain the DHT structure in node mobility, managers need to maintain connectivity with their neighbors to guarantee that they are orderly connected from ID 0 to $N-1$.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 5, Issue 2, Februray 2016

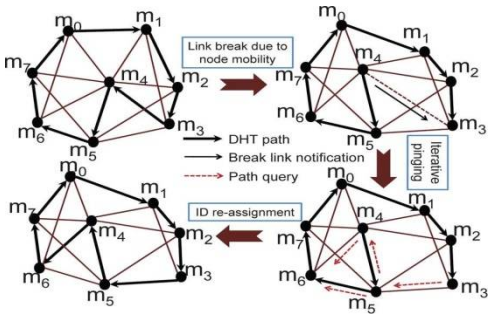


Fig. 4.Maintenance of the DHT infrastructure.

Each manager relies on the "hello" messages to check its connectivity with its successor and update the managers in its routing table.*3) DHT-Based Information Collection and Querying:* TheDHT supports efficient and ductile information collection and querying in ARM. Each ordinary mobile node n_i has a virtual id=i, which is the consistent hash of its IP address. depending on the Insert(i,B+R) , the managers marshal all the information of n_i in the system into n_i 's *owner manager*. The owner manager formulates n_i 's reputation and increases/decreases thecredits in its account.

D. Reputation Management

In ARM, the reputation managers collect reputation information, calculate global reputation, identify misbehaving nodes, and manage nodes' accounts. ARM provides more perfect node reputation for two reasons: It uses the global information rather than local partial information in reputation calculation, and the large amount of global information makes it effective in detecting falsified, conspiratorial, and misreported information through alteration.

Misreports Avoidance: When a node in a region experiencesan injurious network condition such as background interference due to traffic or thermal noise, the node's neighbors may also experience the adverse network conditions. Though the nodes are cooperative, they are unable to transmit requested data. As a result, these nodes report low R_i values for others.Since all reputations of each node in a region are reported to one manager. When a manager notices that all nodes in an area report low observed reputations, it temporarily discounts the reportsinorder to avoid punishing nodes.

False Accusation Avoidance: Some misbehaving nodes mayreport a high reputation for an perverse node, and a low reputation for a cooperative node. Since all recognised reputations of a node in a region are possessed into a manager and most nodes are benign, falsified reputations always deviate largely from most reputations. Thus, in order to reduce the effect of fal-sified reports, a manager filters the R_i 's that dramatically deviate from the average R_i .

$$R_{io}=|R_i-\sum_{nj\epsilon n} \boldsymbol{Ri}/|\boldsymbol{n}||$$

Collusion Avoidance: The nodes in a region may collude toconspiratorially report node reputations in order to fraudulently increase their reputations or decrease others' reputations. Forexample, the nodes in group A and group B are the nodes in the transmission range of m_k. The number of nodes in group A Overwhelms group B. If the nodes in group A collude with each other to report low R_i for n_i, then the justified reports from group are ignored m_k by according to (3). This problem can be resolved by another filtering process at the owner manager m that collects all from different managers N

$$R_{io}=|R_i-\sum_{nj\epsilon n} \boldsymbol{Ri}/|\boldsymbol{m}||$$

Distributed Reputation Manager Auditing

The owner reputation manager of a node calculates its final reputation value and manages its account value, if the manager modifies the reputation value, no other nodes can detect it. When a manager reports the local reputation of a node to its owner managers, it uses the consistent hash functions to generate virtual IDs .If any manager node finds a malicious manager then it will reports the suspicious malevolent manager to other c-1 managers. In this case, a high-reputed node is selected to replace the dismissed manager.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

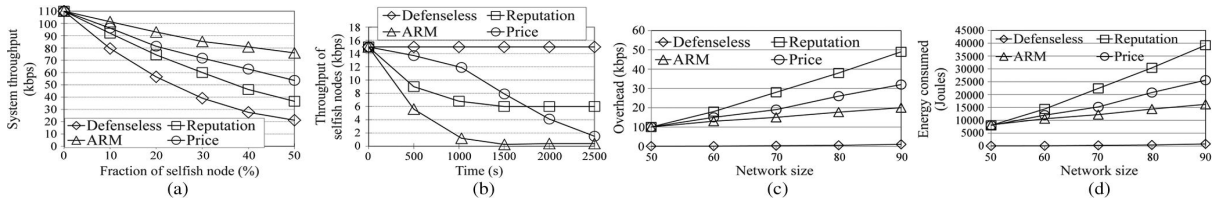
Vol. 5, Issue 2, Februray 2016

Reputation-Adaptive Account Management

ARM has an account management function to avoid balanced analysis of high-reputed nodes in different reputation levels in order to effectively provide cooperation incentives and deter selfish behaviors. ARM assigns each newly added node withan initial number of credits denoted by $A(0)$. The owner managers of nodes maintain their accounts and transparently increase and decrease the credits in the accounts of forwarding service providers and receivers, respectivelyed by another filtering process at the owner manager m.

IV. PERFORMANCE EVALUATION

We conducted simulations on NS- 2 [24] to demonstrate the performance of ARM. We employ the Distributed Coordination Function (DCF) that belong to IEEE 802.11 as the MAC-layer protocol. We selected the two-ray propagation model as the physical-layer model, and the constant bit rate as the traffic mode. We set our default settings below unless otherwise specified. The simulated network has 60 wireless nodes randomly deployed in a field of 1200 $\times$ 1200 square meters. We randomly selected 10 nodes as managers. The radio transmission ranges of low-power and high-power interfaces were set to 250 and 1000 m, respectively. The raw physical link bandwidth was set to 2 Mb/s. The heights of antennas for data transmitting and receiving were tuned to 1.5 m. We used the random way -point mobility model [25] to generate node movement.Each node initially was assigned 5000 credits and a reputation value of 1. We compared the per-formance of the DSR routing algorithm [22] in a defenseless MANET with neither reputation system nor price system (*De-fenseless*), in ARM, in a reputation system (Reputation) [3], [5],and in a price system (Price) [10], [14]. We used the basic reputation management system in [3] and [5] and the basic price management mechanism in [10] and [14] in the experiments. We chose these works for comparison because they have the repre-sentative mechanisms for reputation systems and price systems, respectively. To make the results comparable, rather than using the absolute number of forwarded packets, we use $R_{\mathrm{l}}=D_{\mathrm{r}}/D_{\mathrm{f}}$ to evaluate a node's reputation in *Reputation*. Selfish nodes keep their reputati on just above $\mathcal{T}$. In the routing, a node chooses a node not on its blacklist for data forwarding. By default, every node just has one reputation manager. Like previous reputation and prices systems, we assume that each node in the network is rational.



Performance comparison between different systems. (a) Average system throughput. (b) Throughput of selfish nodes. (c) System overhead. (d) Energy consumption.

Figure(a)plots the average system throughput of different systems versus the fraction of selfish nodes. The figure shows that ARM generates a higher throughput than *Price* and *Reputation*, which produce higher throughput than *Defenseless*.(b) plots the throughput of the selfish nodes. In *Defenseless*, selfish nodes keep a constant throughput of 15 kb/s. In *Reputation*, the throughput decreases as time elapses and then stays constant at 6 kb/s. This is because the selfish nodes keep R just above $\mathcal{T}$; thus, their transmission requests are accepted by other nodes. (c) il-lustrates the overhead in each system versus network size. We see that ARM yields much less overhead than *Price*, which pro-duces less overhead than *Reputation*(d) shows the amount of energy consumed by communication overhead during the experiment. Based on [41], we assumed that the energy con-sumption overhead is 10.50 J/packet using the high-power inter-face and is 1.76 J/packet using the low- power interface.

V. CONCLUSION

An Account-aided Reputation Management system (ARM) is proposed to adequately and effortlessly deter selfish node

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 5, Issue 2, Februray 2016

behaviors and provide collaboration incentives .ARM intelligently blends a reputation system and a price system. It constructs upon an underlying locality-aware DHT infrastructure to efficiently compile global reputation information in the entire system for node reputation evaluation, which avoids cyclic message exchanges, reduces information redundancy, and more accurately reflects a node's trust. ARM has functions for reputation management and account management, the assimilation of which fosters cooperation incentives and uncooperation deterrence. ARM can detect uncooperative nodes that obtain fraudulent benefits while still being considered trustworthy in previous reputation systems and price systems. Also, it can effectively identify falsified, conspiratorial, and misreported information so as to provide more accurate node reputations. The complementary effects between the reputation system and price system effectively prevent nodes from employing policies in individual systems for benefits. In our future work, we will study distributed methods for choosing a manager.

REFERENCES

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing mis-behavior in mobile ad hoc networks," in *Proc. MobiCom*, 2000, pp. 255–265.
[2] P. Michiardi and R. Molva, "Core: A collaborative reputation mecha-nism to enforce node cooperation in MANETs," in *Proc. CMS*, 2002, pp. 107–121.
[3] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CON-FIDANT protocol," in *Proc. MobiHoc*, 2003, pp. 226–236.
[4] T. Anantvalee and J. Wu, "Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks," in *Proc. IEEEICC*, 2007, pp. 3383–3388.
[5] M. T. Refaei, L. A. DaSilva, M. Eltoweissy, and T. Nadeem, "Adapta-tion of reputation management systems to dynamic network conditions in ad hoc networks," *IEEE Trans. Comput.*, vol. 59, no. 5, pp. 707–719, May 2010.
[6] S. Buchegger and J. Y. LeBoudec, "A robust reputation system for mobile ad-hoc networks," in *Proc. P2PEcon*, 2004, pp. 1–6.
[7] J. Mundinger and J. Le Boudec, "Analysis of a reputation system for mobile ad-hoc networks with liars," *Perform. Eval.*, vol. 65, no. 3–4, pp. 212–226, 2008.
[8] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommen-dation for mobile ad-hoc networks," *Comput. Netw.*, vol. 53, no. 14, pp. 2396–2407, 2009.
[9] X. Wang, L. Liu, and J. Su, "RLM: A general model for trust represen-tation and aggregation," *IEEE Trans. Services Comput.*, vol. 5, no. 1, pp. 131–143, Jan.–Mar. 2012.
[10] M. Jakobsson, J. Hubaux, and L. Buttyan, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," in *Proc. Fi-nancial*, 2003, pp. 15–33.
[11] S. Zhong, Y. R. Yang, and J. Chen, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks," in *Proc. IEEE IN-FOCOM*, 2003, pp. 1987–1997.
[12]J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modellingincen-tives for collaboration in mobile ad hoc networks," in *Proc. WiOpt*, 2003, pp. 78–85.
[13]L. Anderegg and S. Eidenbenz, "Ad hoc-VCG: A truthful and cost-effi-cient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. MobiCom*, 2003, pp. 245–259.
[14]H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains," *Future Generation Comput. Sys.*, vol. 25, no. 8, 926–934, 2009.
[15]Z. Li and H. Shen, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 8, pp. 1287–1303, Aug. 2013.
[16]K. Balakrishnan, Deng, and P. Varshney, "TWOACK: Preventing self-ishness in mobile ad hoc networks," in *Proc. IEEE WCNC*, 2005, pp. 2137–2142.
[17]K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowl-edgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
[18]J. J. Jaramillo and R. Srikant, "DARWIN: Distributed and adaptive rep-utation mechanism for wireless networks," in *Proc. MobiCom*, 2007, 87–98.
[19]Z. Li, H. Shen, and K. Sapra, "Leveraging social networks to combat collusion in reputation systems for peer-to-peer networks," *IEEETrans. Comput.*, vol. 62, no. 9, pp. 1745–1759, Sep. 2013.
[19] W. Wang, S. Eidenbenz, Y. Wang, and X. Y. Li, "OURS: Optimal uni-cast routing systems in non-cooperative wireless networks," in *Proc.MobiCom*, 2006, pp. 402–413.
[20] J. Choi, K. Shim, S. K. Lee, and K. L. Wu, "Handling selfishness in replica allocation over a mobile ad hoc network," *IEEE Trans. MobileComput.*, vol. 11, no. 2, pp. 276–291, Feb. 2012.
[21] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, vol. 353, no. 5, pp. 153–181, 1996.
[23]G. A. Dirac, "Some theorems on abstract graphs," *Proc. London Math.*, vol. 3, no. 2, pp. 69–81, 1952.
[24"The network simulator NS-2," [Online]. Available: http://www.isi. edu/nsnam/ns/
[25]"Delay Tolerant Networking Research Group," [Online]. Available: http://www.dtnrg.org/wiki/Home