A Survey on Evaluation Schemes for Routing Misbehaviors in Manet

Rose Ann Cyril
Department of IT
Rajagiri School of Engineering & Technology, Kerala, India

Saritha S
Department of IT
Rajagiri School of Engineering & Technology, Kerala, India

ABSTRACT
Mobile ad hoc network has emerged as a trending topic of research in recent years owing to the highlighted pervasive computing culture. MANETs are decentralized, and therefore all network activities are carried out by nodes themselves. Transmissions are not controlled by any central authority as like base stations in the case of cellular networks. Each node is both an end-system as well as a relay node (router) to forward packets for other nodes. This requires that every node in the network contribute full cooperation as to cater to the routing needs of adhoc network. The route creation and maintenance tasks in Manet are autonomous operation. The flexibility of wireless transmission is however affected by its limitations as well like limited range, bandwidth, energy constraints etc. To cope up with these limitations, many a time's mobile nodes may decide either not to cooperate or partially cooperate for the benefit of their own. This strategic dimension of mobile nodes to conserve energy may be detrimental to the health of efficient Manet systems. Selfishness substantially reduces the performance of network at the routing layer. The selfishness may also cause data loss making the scenario more badly. It is hence the need of the hour to discover the selfish nodes and device new schemes wherein data accessibility is never affected on varying environments.

General Terms
Selfishness, credit based schemes, Reputation based schemes

Keywords
Manet, PPM, PTM, Secure Incentive Protocol, Sprite, Watchdog, Pathrater, CONFIDANT, CORE

1. INTRODUCTION
A MANET is a collection of autonomous wireless nodes that can dynamically form a network on the run to communicate with the peers without using any pre-existing fixed network infrastructure. Nodes in the network operate without any base station infrastructure as in the case of cellular networks. Nodes are assumed to fully cooperate among each other to provide seamless connectivity centralized administration. Although Manets are defined to be infrastructure-less, the constituent nodes in the network forms an "equivalent" topology as with the case of wired or infrastructure based scenario. The nodes exhibit dynamic multi hop routing when the two nodes designated as sender and receiver do not fall in the limited range capabilities of Manet. Each node in the network acts as routers to bypass information among the member nodes. Route failures can happen due to mobility attribute of Manets. However Manets are capable of dynamic route repairs to tackle the same.

Manets often face numerous challenges in view of its limited capabilities. The nodes are mostly batter operated and hence by its way energy constrained. The network features distributed state in unreliable environments. Mobility aspects highly influence the dynamism in topology and the network usually has limited capacity. Manet also faces issues of security, cooperation and other wireless issues. Routing protocols are designed with a notion that in an ideal scenario, codes fully cooperate among the peers to establish a concrete routing pattern in an infrastructure less framework. However node misbehaviors are a common occurrence in mobile environment mainly because of its energy constraints of low residual battery power. Most commonly, nodes exhibit a selfish behavior as to conserve energy and leverage the same only for the benefit of themselves. Mitigating the issues with node misbehaviors is a hot topic in Manets due to an increased need for efficient performance. Selfishness in nodes can cause a diminished output in course of Manet operation. Selfish nodes create havoc on the route discovery and route maintenance phases in routing. A selfish node does not participate in routing process. A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value. In addition, Selfish nodes do not reply or send hello messages. A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it. Selfish nodes also may intentionally delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths. They may also drop data packets in between to conserve their energy. Selfish nodes may participate in routing messages but may not relay data packets. A selfish node is never a malicious node which performs content alteration, spoofing etc. that may be detrimental. Several motivation or incentive scheme approaches are usually implemented in mobile networks to render nodes with an interest in packet forwarding even if the process doesn't bring them any gain in return.

1.1 Related Work
In recent years remarkable studies were carried out in the domain of routing misbehaviors as to identify the detrimental nodes to prevent data loss and diminishing performance characteristics. One of such a scheme is the use of virtual currency named as a nugget [1] [3]. The virtual currency is readily supplied in the system on behalf of source or destination to make them forwardable nodes. The cost of a packet may depend on several parameters such as required total transmission power and the battery status of the intermediate nodes. Packets sent by or destined to nodes that do not have a sufficient amount of nugget are discarded. The major drawback of this approach is the demand for trusted hardware to secure and maintain the record of the currency at central level. Ad hoc VCG [2] protocol is one such protocol that deploys monetary transfers to discover an energy-efficient path between the source and the destination.

2. ISOLATING SELFISH NODES

Broadly there are two methods to detect selfishness, categorized as credit based schemes and reputation based schemes. Credit based scheme work by issuing credits to nodes for faithful their actions. The credit based scheme may be implemented using models like, the Packet Purse Model (PPM), Packet Trade Model (PTM), Secure Incentive Protocol (SIP) Sprite and auction based aodv protocol for mobile ad hoc networks with selfish nodes. Reputation based scheme operates by collectively detecting and declaring the misbehavior of a suspicious node. Such a declaration from the network nodes are then propagated throughout the network so that the misbehaving node will be removed from the rest of the network. Two models deployed under reputation based scheme are Path rater, Watchdog [6] mechanism, CONFIDANT, CORE, token based approach, end to end acknowledgement schemes and reputation based algorithms.

2.1 Credit based schemes

2.1.1 Packet purse model

A Packet purse model (PPM) depicts a model wherein the originator or sender pays for the packet forwarding service. Originator is initialized with adequate number of beans or nuggets to guarantee its receipt of packet at the destination. The packet on its journey from its sender node to the destination distributes one or more beans as an incentive to the forwarding service of the intermediate nodes. When a bean less packet arrives at an intermediate node, it gets the fate of dismissal. The approximation of beans for initialization is therefore important. Nuggets are stored in the packet purse header (PPH) which is an additional header between the MAC layer header and the Network layer header. Packet purse headers are recomputed at every forwarding node. It is comprised of three parts viz part intended for security module of next hop, part acknowledging the previous hop and a common part intended for both the previous and next hop nodes. The method relies on a packet forwarding protocol for packet creation and final delivery.

2.1.2 Packet trade model

Packet Trade Model (PTM) overcomes the disadvantage of PPM of having the originator aware of the number of beans per packet required for transmission. Packet Trade Model works by trading the packet for beans. Each intermediary buys it from previous one for some beans and sells it to the next one for more beans. The total cost of forwarding the packet is covered by destination of the packet. Here it is assumed that there exists a public key infrastructure that the terminodes can use to authenticate each other and to establish secure communication links [15].The system also relies on a Packet Trade Header as like PPM. Here, instead of nuggets, it stores the price of the packet in transit. PTM also uses a packet forwarding protocol for packet creation and delivery. Security module of each forwarding terminodes decreases the nugget counter by the price in the PTH header for buying the packet. Also it increases the price by one when recomputing the PTH header and increases nugget counter by new price.

2.1.3 Secure incentive protocol

Secure Incentive protocol charges or rewards nodes for the service they receive or provide. SIP assumes that each mobile node (MN) has a tamper-proof security module such as SIM cards in GSM networks, which deals with security related functions and each intermediate node (IN) puts non forged stamps on the forwarded packets as a proof of forwarding[6].[4] Secure Incentive Protocol, (SIP) uses "credits" as the incentives to stimulate packet forwarding. SIP is implemented in the smartcard of each MN. SIP is session-based and mainly consists of three phases. [14]During the first Session initialization phase, a session initiator(SI) negotiates session keys and other information with a session responder (SR) and INs between them. And each IN puts a non-forged stamp on each data packet forwarded and SI/SR collect those stamps for later rewarding use in the next Data forwarding phase. The final phase is Rewarding phase, in which each IN is awarded a certain number of credits based on the number of forwarded packets.

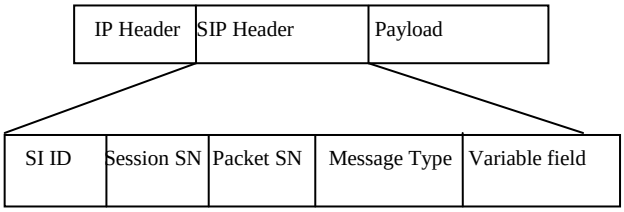

Fig 2.1 SIP Protocol Header

2.1.4 Sprite

Sprite system comprises consists of the Credit Clearance Service (CCS) [8] and a collection of mobile nodes. CCS determines the charge and credit to each node involved in transmission of message. The nodes are equipped with network interfaces that allow them to send and receive messages through a wireless overlay network. To identify each node, sprite assumes that each node has a certificate issued by a scalable certificate authority and the sender knows the full path from the sender to the destination, using a secure ad hoc routing protocol based on DSR. When a node sends its own messages, the node will lose credit to the network because other nodes incur a cost to forward the messages. On the other hand, when a node forwards others messages, it should gain credit and therefore be able to send its messages later. The receiving node also keeps a receipt of message and later forwards them to CCS at fast connection. Thus the sender is charged for the message. Any node engaged in forwarding process is compensated by charges whether or not the transmission is successful. A transfer is considered successful if the next hop neighbor reports a valid receipt to the CCS. There are two ways for a node to get more credit. First, a node can pay its debit or buy more credit using real money, at a variable rate to the virtual money, based on the current performance of the system. However, the preferred and dominant way to get more credit is by forwarding others messages. Sprite suffers from two main issues. Formerly, since different nodes in the path submit their receipts at different times, it may become difficult for the CCS to determine the actual payment to each node. Also, if routing is based on DSR, some nodes not belonging to DSR path may collude with nodes in the path to forge the receipt and thereby spoof CCS.

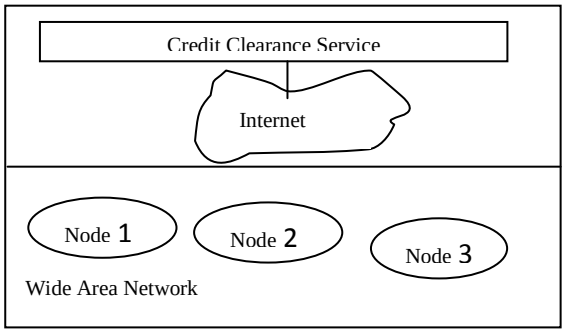

Fig 2.2 Architecture of SPRITE

2.1.5 *An auction based aodv protocol for mobile ad hoc networks with selfish nodes*

This strategy is based on digital economy created in the network. In this virtual economy, a source node has to pay some amount of a digital currency to intermediate nodes to have its packet forwarded, whereas the intermediate nodes bid and declare the amount of currency that they would request from the source if they forward the packet. The sender node chooses the route with the lowest bid. Payment is packed in the message packet in its transit. Intermediate nodes are paid an amount greater than the amount that it bid. Bids are made based upon their energy level and the amount of currency that they have. Generally, bids are high if nodes have low energy and low if the currency levels at a node are low. The strategy uses an auction based routing mechanism to increase fairness in distributing the energy compensation on a network. Vickrey auction is a mechanism wherein the highest bidder wins the auction but pays with the second highest bid. This kind of second price auctioning is deployed in the network with the route selection based on minimum cost. The bidding formula is calculated as, b=a*(log(C)/Er) where b denotes the bid value of node, C denotes the node's current currency amount and Er denotes node's energy ratio; computed as (current energy/initial energy).The parameter a is multiplied to influence the bidding parameter. Modifications are made to AODV to incorporate some additional fields like lowest route bid for destination, second lowest bid for destination and a node's own bid. When a node's energy goes down and currency level remains the same, bids are made high. When currency level goes up and energy goes down, bids are lowered. When both the parameters are down, bids increases.

2.2 Reputation based schemes

2.2.1 Watchdog

The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium. Nodes operate in a promiscuous mode wherein, the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. Watchdog is implemented by maintaining a buffer of recently sent packets. Each overheard packet is then compared with the packet in the buffer. On occurrence of packet match, the packets are removed from the buffer. If some packets remain in the buffer for long, the system increments a failure tally. If the failure tally of any nodes goes above a threshold value, the node is accused to be misbehaving. The source of packet is also notified about the misbehavior. Suppose there exist a path from S to D through A, B and C.A needs to transmit packet through B to C.A can overhear the packet transmission from B, thereby detecting misbehaviors on B's traffic.

Watchdog however suffers from the following weaknesses:

1. Ambiguous collision – Ambiguous collision prevents a node A sending packet to C through B to overhear forwarding packets from B due to collisions that may occur at node A with data reception from other neighboring nodes.

2. Receiver collisions- Receiver collisions results from the simultaneous transmission of forwarding packets from B and packet transmissions from other neighboring node to C causing collision at C.

3. Limited transmission power

4. False misbehavior

5. Collision

6. Partial dropping

2.2.2 Path rater

The Path rater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. Path rater calculates a path metric by averaging the node ratings in the path. If there are multiple paths to the same destination, the path with the highest metric is chosen. The Path rater, run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Negative path values indicate the existence of one or more suspected misbehaving nodes in the path.

2.2.3 CONFIDANT protocol

CONFIDANT stands for Cooperation of Nodes Fairness in Dynamic Ad-hoc Network [10]. It aims at detecting and isolating misbehaving nodes. Nodes monitor their neighbors and update the reputation accordingly based on experiences and recommendations. Reputation is used to evaluate routing and forwarding behavior according to the network protocol. Trust is used to evaluate participation in the CONFIDANT meta-protocol. The system consists of the Monitor, the Trust Manager, the Reputation System and the Path Manager. The monitor does "neighbor watch", where nodes notifies any malicious act in its neighborhood. The trust manager deals with incoming and outgoing ALARM messages. ALARM messages are sent by the trust manager of a node to warn others of malicious nodes. Outgoing ALARM messages are generated by the node itself after having experienced, observed, or received a report of malicious behavior [10].The incoming ALARM messages are intended by a node to the friends in the friend list. The source of ALARM messages is to be evaluated to verify the trustworthiness of the message. Reputation system manages a table which populates itself with rating corresponding to each node. Ratings can be changed when malicious activity seemingly exceeds a predefined threshold. Path Manager is responsible for re ranking of path according to reputation of constituent nodes.

2.2.4 CORE

Collaborative Reputation (CORE), proposed by Michiardi and Molva [9] uses a collaborative monitoring and a reputation mechanism. Core system is a generic mechanism that can be integrated with any packet functions. A Reputation value is used to make decisions about cooperation or isolation of a node. The CORE scheme involves two types of protocol entities, a requester and one or more providers, that are within the wireless transmission range of the requester. Reputation values are obtained by regarding nodes as requesters and providers by comparing expected result to actually obtained

result of a request. Value ranges from positive through null to negative. It allows a good reputation to be rewarded and bad behavior to be punished. This allows good reputation makes use of resources and bad reputed nodes to be excluded from community. It consists of network entity (mobile node), reputation table (RT) and a watchdog mechanism (WD). Watchdog mechanism detects the misbehaving nodes. Reputation table is a data structure consisting of tuple <unique identifier, collection of subjective observations, list of indirect reputation, value of reputation evaluated for a predefined function>.If provider refuses to cooperate, it decreases reputation of provider. Route tables are updated for subjective reputation value and indirect reputation value in request and reply phases respectively.

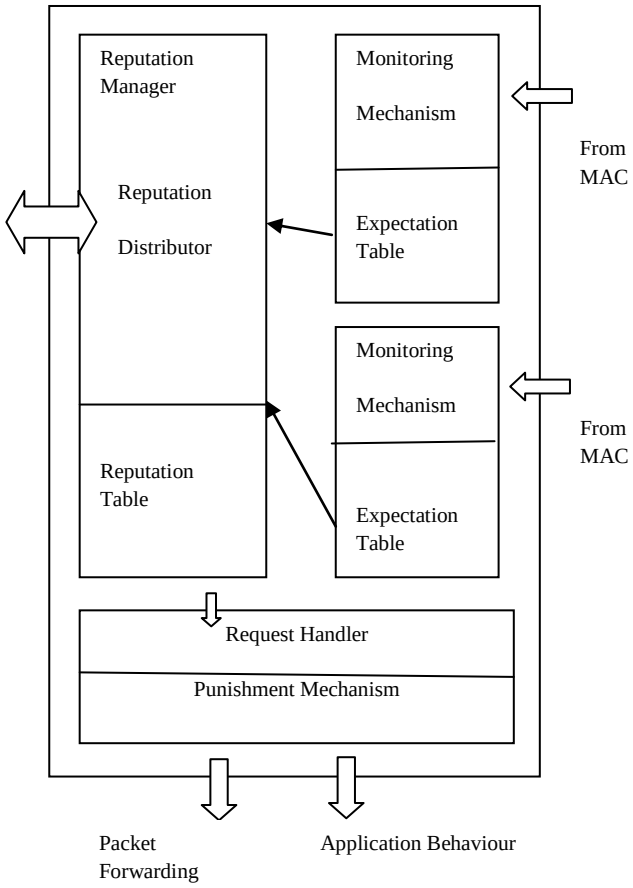

Fig 2.3 CORE Architecture

2.2.5 Token based approach

In this proposal, each node has to have a token in order to participate in the network operations. For each node, its neighbors detect any misbehavior in routing or packet forwarding services [11]. The token is renewed by multiple neighbors after it is expired. The period of validity of a node's token is dependent on how long it has stayed and behaved well in the network. A well behaving node accumulates its credit and renews its token less and less frequently as time evolves [12]. The solution is composed of four components:

(i)Neighbor verification: verify whether each node is legitimate or malicious.

(ii)Neighbor monitoring: monitor behaviors of each Node and detect attacks from malicious ones.

(iii)Intrusion reaction: alert the network and isolate the attackers.

(iv)Security enhanced routing protocol: incorporates the security information into the mobile ad hoc network routing protocol.

2.2.6 End-to-end acknowledgment scheme

The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol in the following manner: the 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive.TCP, on the other hand, uses ACK and SACK to measure the usefulness of the current route and to take appropriate action.2 ACK scheme overcomes the main issue with watchdog mechanism that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link as the watchdog technique only monitors the transmission from the sender of the next-hop link. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, the ACK based technique focuses on the problem of detecting misbehaving links instead of misbehaving nodes.

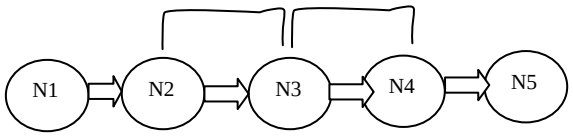

Fig 2.4 Two ACK Scheme

The 2ACK scheme detects misbehavior through the use of a new type of acknowledgement packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops with 3 nodes in the opposite direction of the data traffic route. The 2ACK scheme requires an explicit acknowledgement to be sent by N3 to notify N1 of its successful reception of a data packet: When node N3 receives the data packet successfully, it sends out a 2ACK packet over two hops to N1, with the ID of the corresponding data packet. The triplet [N1-> N2- > N3] is derived from the route of the original data traffic. Such a triplet is used by N1 to monitor the link N2 -> N3. 2ACK transmission takes place for every set of triplets along the route.

2.2.7 A reputation-based mechanisms to enforce cooperation in Manet

This method detects selfish nodes as well as enforces the selfish nodes to cooperate in MANET. In addition to this, system also encourages cooperating nodes by providing them faster service. This approach to detect selfish nodes has three main modules. Checking System, Reputation System and Priority processing System. [13] .The reputation system uses the proportion of the number of Packets which are sent by a node to the number of Packets which are received by a node as the cooperation coefficient of a node. The priority module determines the priority of each packet depends on the cooperation coefficient field of it.When the node receives multiple packets and the simultaneous forwarding of packets is not possible, the packet of the node whose cooperation coefficient is higher will be forwarded first. Therefore, the co-operator nodes will be encouraged by receiving the services earlier and the selfish nodes will be punished by receiving the

services later. This coefficient is the same as Reputation and considered as follow:

Cooperation coefficient A is computed as,

A = No. of sent packets/No. of received packets.

'A' is a number between zero and one. The values which are near to zero show that the cooperation of node is low and it is a selfish node but the values which are near to one show the cooperation and as a result the reputation of node is high.

3. CONCLUSION

Different strategies to detect and isolate selfish nodes were keenly studied. The two prominent methods in this regard, i.e. using credit based scheme and using reputation based techniques were analyzed to determine the most efficient means for isolation. Some of the schemes like reputation based mechanism for cooperation segregates as well as well as rerouting. Credit based schemes are sometimes found to have failures as it may be impossible for the source nodes to initialize themselves with adequate credit beforehand. Reputation based schemes like the use of two hop acknowledgements in reverse routing directions involves additional overhead of additional packets of ACK. However this demerit may be reduced to an extent by allowing only a fraction of packets to be acknowledged. This method also allows choosing an alternate path for transmission. Auction based protocol also helps encouragement of cooperation among nodes. The detection of selfish nodes helps segregation of network thereby removing selfish nodes as to generate routes devoid of misbehaving nodes. The routes may be further computed dynamically on the run with residual network constituents each time selfishness is detected. The future work revolves around breaking down the network into small clusters further which selfish node detection may be carried out as to reduce the overhead on the same.

4. REFERENCES

[1] Shailender Gupta, C. K. Nagpal And Charu Singla,"Impact Of Selfish Node Concentration In Manet",International Journal Of Wireless & Mobile Networks (ijwmn) Vol. 3, No. 2, April 2011

[2] L. Anderegg, S. Eidenbenz, "Ad hoc-VCG: A Truthful and Cost- Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents", Proc. ACM Mobicom, pp. 245–259, 2003.

[3] L.Buttyan and J-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in Proc. of First IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, MA, USA, August 2000.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), August 2000.

[5] V.Srinivasan, P. Nuggehalli, C.F. Chiasserini and R.Rao,"Cooperation in wireless Ad Hoc Network", in IEEE INFOCOM,California,USA,2003.

[6] Yanchao Zhang , Wenjing Lou , Wei Liu, Yuguang Fang, " A secure incentive protocol for mobile ad hoc networks" in Journal of Wireless Networks ,Volume 13 Issue 5, pp. 663-678 , October 2007

[7] S.Marti, T.Giuli, K.Lai and M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks," in Proc. ACM MOBICOM, pp. 255-265, 2000.

[8] S.Zhong, J.Chen, and Y.R.Yang, "Sprite: A Simple, Cheat Proof, Credit based System for Mobile Ad Hoc Networks", in Proceedings of INFOCOM, Apr. 2003

[9] Pietro Michiardi and Refik Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, 2002.

[10] Hongxun Liu, José G. Delgado-Frias, and Sirisha Medidi, "Using a cache scheme to detect selfish nodes in mobile adhoc networks "in proceedings of IEEE international Conference on Networks, pp- 7– 12, Nov.2007

[11] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing, T.Imielinski and H. Korth, Eds. Norwell, MA: Kluwer,vol. 353, pp. 153–181, 1996.

[12]Jerzy Konorski and Rafał Orlikowski "AFramework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks in "Journal of telecommunications and Information technology pp34-40,2009

[13] Zahara Safaei, Mohammad Hossein Anisi a Fatemeh Torgheh, "A Reputation based mechanism to enforce Cooperation in MANET's",Software Telecommunications and Computer Networks",2008(SoftCOM2008)16th International Conference on 25-27 Sept 2008.

[14] Yanchao Zhang, Wenjing Lou, Yuguang Fang," SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc Networks"

[15] Levente Buttyan, Jean-Pierre Hubaux "Enforcing Service Availability in Mobile Ad-Hoc WANs", IEEE 2000.