Rethinking Incentives for Mobile Ad Hoc Networks

Elgan Huang
Laboratory for Communication Engineering,
University of Cambridge
William Gates Building, Cambridge,
United Kingdom
eh283@cam.ac.uk

Jon Crowcroft
Computer Lab,
University of Cambridge
William Gates Building, Cambridge,
United Kingdom
Jon.Crowcroft@cl.cam.ac.uk

Ian Wassell
Laboratory for Communication Engineering,
University of Cambridge
William Gates Building, Cambridge,
United Kingdom
ijw24@eng.cam.ac.uk

ABSTRACT
Without sufficient nodes cooperating to provide relaying functions, a mobile ad hoc network cannot function properly. Consequently various proposals have been made which provide incentives for individual users of an ad hoc mobile network to cooperate with each other. In this paper we examine this problem and analyse the drawbacks of currently proposed incentive systems. We then argue that there may not be a need for incentive systems at all, especially in the early stages of adoption, where excessive complexity can only hurt the deployment of ad hoc networks. We look at the needs of different customer segments at each stage of the technological adoption cycle and propose that incentive systems should not be used until ad hoc networks enter mainstream markets. Even then, incentive systems should be tailored to the needs of each individual application rather than adopting a generalised approach that may be flawed or too technically demanding to be implemented in reality.

Categories and Subject Descriptors
K.m [**Computing Milieux**]: Miscellaneous

General Terms
Performance, Design, Theory

Keywords
Mobile ad hoc networks, incentives, cooperation

SIGCOMM'04 Workshops, Aug. 30 & Sept. 3, 2004, Portland, OR, USA.

1. INTRODUCTION
Mobile ad hoc networks are fundamentally different from conventional infrastructure based networks in that they are self-organizing and formed directly by a set of mobile nodes without relying on any established infrastructure. The network thus relies on the cooperation of individual users whose devices perform the forwarding that is necessary to achieve network capability. Without sufficient nodes providing relaying functions, the network cannot function properly.

When all the nodes of an ad hoc network belong to a single authority, e.g. a military unit or a rescue team, they have a common goal and are thus naturally motivated to cooperate. However, for general applications with large numbers of unrelated users, if battery power, bandwidth, processor clock cycles and other resources are scarce, selfish users might not wish to forward packets for other users as it would impact their own ability to transmit traffic.

These concerns have resulted in a number of efforts to design incentive systems for mobile ad hoc networks that encourage users to cooperate, as well as trust management systems that identify non-cooperating nodes and punish them. However these incentive systems have a number of inherent flaws that make them difficult and undesirable to implement in practice. Ironically, if badly implemented, some of them even have the potential to backfire by offering an incentive to cheat the incentives system in order to gain further benefits.

2. TOKEN BASED INCENTIVE SYSTEMS
2.1 Quality of Service Problems
With token-based incentive systems [8,9,10,11,15,20], the basic idea is to use notional credit, monetary or otherwise to pay off users for the congestion costs (transmission and battery costs) they incur from forwarding packets from other users. These credits can then be used to forward their own packets through other users, resulting in an incentive to act as relay points, especially where there is the greatest excess demand for traffic since this is when they earn the most. Users who do not cooperate will not be able to use the network themselves, having not earned any credits.

This idea makes a lot of sense in theory, but when practically implemented is likely to run into a number of problems.

Under the general token mechanism, a user's token count is increased when it forwards, and decreased proportionally to the number of hops it needs when it sends. This inevitably means that a user needs to forward more than he sends and also limits the amount of information that any user can send at any given time, dependent on their store of tokens. In principle the node may be able to buffer packets until it earns enough to send, but this works only as long as the buffer is large enough and there are no delay constraints on the packets, which rules out many real time applications. Therefore, practically speaking, packets could often be dropped at the source, rendering it somewhat ineffective and inefficient for many types of communications.

The system also puts users on the outskirts of a network at a disadvantage unrelated to their willingness to participate. Those users will not have as much traffic routed through them due to their location and furthermore will have lower congestion prices because of that. They will thus earn significantly less than a centralised node and be penalised for it resulting in low QoS. The system might indeed stabilise overall, but not at a point that is beneficial to everyone.

To pay out credit to forwarding nodes, the transmitting node must estimate the number of hops required so that it can load sufficient credit onto its packet to pay each of the nodes. This calculation not only takes up resources but if done incorrectly will result in packets that have insufficient credit being dropped, as well as wasted credit, decreasing QoS for all concerned.

Another concern is that a significant amount of energy is thus wasted in the system transmitting dropped packets that would not have been dropped had the incentives scheme not been in place. Because of the wasted energy, a user might find that his battery drained faster than if he were to cooperate with no incentives system in place, as in both cases he would be forwarding packets for others but with the incentives system he suffers additional energy loss from dropped packets.

From a general consumer's point of view, these problems collectively result in dropped packets, excessive consumption of resources and generally poor quality of service for no apparent reason, representing a rather significant drawback to the use of ad hoc devices. Users with poor quality of service are unlikely to be sympathetic (or even aware) to arguments that the system works in such a way for the greater good. This would cause problems not only for individual users, but also for the overall network as unsatisfied users leave the system completely and bad word of mouth discourages new users to join. Ad hoc networks need a critical mass of users to function well, with the utility of the network increasing proportionally to the square of the number of nodes, as stated by Metcalfe's Law [5].

2.2 Technical Conundrums

When using tokens, there is also the question of how the balance of tokens can be maintained for users. The average token level within the system needs to be kept at a reasonable level in order for incentives to work properly. If it grows too high, everyone will be rich in tokens and no longer have an incentive to cooperate, and conversely, if there is not enough credit within the system then hardly anyone will be able to transmit. However, if an individual's token level is regularly reset (as proposed in current systems) in order to maintain a certain token level, then there is no incentive to cooperate in the long term. Nodes are free to stop cooperating once enough credit is earned to complete their transmission, since excess credit will be lost anyway.

Some systems propose using real money as credit, either directly or indirectly [20] (to buy virtual credit). In an incentives system this could prove very dangerous, because it would in itself be a strong incentive for users to game the system in order to derive monetary gains. Unless a perfect cheat proof system can be designed, which is rather unlikely, such an incentives system would ironically make it more worthwhile for users to attempt to cheat. The need to pay to communicate would also negate one of the key advantages of ad hoc networks and make it less appealing with respect to competing technologies. Also, any system that involves real money and does not incorporate tamper proof hardware requires a centralised authority. This would undermine the self-organising, decentralised nature of ad hoc networks, as well as requiring suitable infrastructure to be built, making the networks less easily deployable and less scalable. It would also be difficult in an ad hoc network to ensure that centralised authorities would always be within coverage.

Tamper proof hardware in turn is very difficult to achieve as suggested in [3]; virtually any system can be modified. A determined hacker would be able to compromise a system regardless of whether there was a 'tamper proof' module in place (even if the module was truly tamper proof the hacker might simply replace it with one of his own design). In the end this might only discourage less technically capable users who would not have tampered with the devices in the first place.

Another problem with such systems is that it is very difficult to charge users fairly, without introducing additional complexity. In most systems presented to date it is the sender that always pays, although it is technically possible to also charge either just the destination or both. This is mainly to prevent the sender from sending useless messages and flooding the network. However, in many cases it is the destination that stands to benefit from a transmission and charging only the sender may thus lead to inconvenience to the user and thereby discourage use of the system. In the same vein, charging just the destination or even both parties would not be perfect solutions either, as the beneficiary changes with each application. (An alternative method of preventing useless messages from being sent might simply be a hardwired mechanism that throttles communications exceeding a certain rate/amount). It is also unclear how this payment issue scales to two-way communications, especially when one side has enough credit and the other does not.

Complexity of solutions is another issue. The mechanisms used to enforce these incentives systems take up resources themselves. If the proportion of freeloaders is not high then the benefit derived from the incentive systems may be outweighed by the resources expended implementing them.

This is analogous to hiring security guards at a cost that is greater than the value of what they have been hired to guard.

3. TRUST MANAGEMENT SYSTEMS

The other main form of inducing cooperation is trust management systems [2,4,7,17]. Generally, these systems work by having nodes within the network exchange reputation information. When a node detects uncooperative behaviour it disseminates this observation to other nodes which take action to avoid being affected by the node in question by changing traffic routes. In addition, some systems punish misbehaving nodes by isolating them from the network for a certain period of time in order to provide an incentive for users to cooperate. Note that although some trust management systems are also used to prevent malicious attacks, in this paper we are only concerned with the incentives aspects.

As with the token-based incentives system, trust management systems are subject to some significant problems. The first problem is that they take up considerable resources due to the constant transmission of observation data, which serves no purpose other than to monitor node behaviour. This hogs valuable processor clock cycles, memory, bandwidth and battery power that could be used to send actual data.

Trust management systems also suffer from vulnerabilities due to exchanging second hand information. Nodes may falsely accuse other nodes of misbehaving or collude with each other to cheat other users on the network. Although systems which rely only on first hand information have been investigated, they suffer from sensitivity to parameter settings as well as a lessened ability to punish uncooperative nodes [4]. They also do not take collusion of nodes into account.

Making decisions on whom to believe in a self-organising ad hoc network is very hard, requiring authentication as well as trust information about the accusing node. In practice this is extremely difficult to achieve, requiring either nodes which are known to be trustworthy (impractical for ad hoc networks) or bootstrapping trust relationships which involve significant complexity and risk, and may not be possible at all for dynamic or short-lived networks [4].

These factors make it questionable whether a trust management system could be effectively implemented in reality at a reasonable cost.

In addition, there have been very few experimental tests of either type of incentives systems to date. Almost all results come from simulations, which operate under assumptions and limited conditions that do not accurately reflect reality, and most importantly do not take user behaviour into account. Real life situations are invariably more complex and humans are often irrational and unpredictable, therefore, although the systems can be shown to work reasonably in simulations, real life implementations may show completely different results.

4. TRANSPARENCY VS. CHOICE

Incentives are by definition an inducement to stimulate or spur-on activity. In this case, we seek a method to induce users to cooperate with other users by allowing their devices to forward messages. Broadly speaking, this means that if given a choice, we want users to choose to allow forwarding the majority of the time, and to keep their devices on for forwarding even when they are not being used by the user.

It thus makes sense to consider how much choice a user should be given in the first place. We can choose to either have a system which is completely transparent and operates behind the scenes without the knowledge of users, or a system that users are aware of and can adjust themselves.

The less transparent the system is, the more complex it becomes for the user. At one extreme we might imagine a sending node having the option to choose between paths every time it sends information, with faster routes being more expensive and slower paths being cheaper. At the same time, every user of every intermediate node might have the option of choosing whether or not they wished to allow the hop and how much to charge for it. Considering how many times this process would need to repeated, if user intervention was needed each time this occurred it would be extremely inconvenient in practice.

A more reasonable middle ground would be to have agents which handled forwarding decisions according to preset rules, based on criteria such as the battery level and the current token store. However, given that the incentives system makes cooperation mandatory in order to forward, there would be little difference in the way that an agent made decisions compared with a human user, since they would both inevitably have to choose to forward most of the time and only stop when battery levels were low.

This then almost completely nullifies the whole point of having an incentives system since the user is essentially unaware of what is going on, and the agent behaviour (to forward the majority of the time and only stop or minimise forwarding when resources are scarce) might as well be hardwired into the system and work transparently behind the scenes. Users therefore do not need to be given any choice in the matter as it does not provide any additional utility to them and in fact may make devices less user friendly.

5. PROPOSED SOLUTION

Given all the issues highlighted previously, it seems that ad hoc incentive systems as currently envisioned will not work successfully and ironically may cause more problems than they solve. In fact it is questionable whether incentive systems are necessary at all.

As stated in the introduction, user cooperation is only an issue when battery or other resources are scarce. Depending on the application, devices and users concerned, this may not even be an issue. As long as users are not unduly affected by forwarding for others, there should be little reason why they should not want to cooperate, especially if not cooperating requires more effort than cooperating.

In order for mobile ad hoc networks or indeed any new technology to move from concept to reality, it needs to go through successive phases of development, deployment and adoption in order to eventually achieve critical mass and enter the mainstream market. At each phase of technology adoption, there is a different target customer segment with different

needs and preferences. Solutions should therefore be designed and implemented with each segment's unique needs in mind.

For ad hoc networks in particular, there is a need to work in distinct phases with the aim of steadily building up users. There is a chicken and egg situation where the usefulness of the network increases with the number of users forming and contributing to the network, but without enough users joining in initially, it will not be useful enough to attract more users. That is why a phased deployment makes much more sense than a full-scale deployment. Trying to run before being able to walk may result in the technology never taking off at all.

Unfortunately, current research into mobile ad hoc networks has mainly been conducted under the assumption that the networks will be mainly used for large-scale general consumer applications, and that nodes will be ubiquitous and reasonably dense. Both of these assumptions are considerably far from reality and will certainly not be true for initial phases of deployment; if the networks are designed and implemented with these assumptions in mind they run a high risk of failing. It is unreasonable to make plans for a bright future without first considering how to get there in the first place; the needs of the early market must not be ignored.

Given the strengths and weaknesses of ad hoc networks, it is unlikely that they will be able to be deployed on a large scale for general applications until much further down the adoption cycle. In the early stages, it is much more reasonable to expect ad hoc networks to be used for specific applications which fully capitalise on their strengths, with solutions that are both useful and financially sustainable [13]. In the same vein, it is unrealistic to expect a sudden proliferation of devices and networks having hundreds or thousands of nodes, especially with general applications that do not belong to a single authority.

In order to bootstrap adoption of the technology, it is therefore imperative that issues such as overly complex incentive systems do not cause early adopters of the technology to shun it. Early stage networks will most likely either be formed for specific applications under a single authority, where incentives are not needed, or by small groups of pioneering, technologically savvy users.

5.1 Adoption Cycle For Mobile Ad Hoc Networks

We therefore propose a solution that evolves according to the adoption cycle of mobile ad hoc networks, loosely based on Geoffrey Moore's Crossing the Chasm model [18]. In the earliest stage, we expect users to mainly be comprised of *pioneers*, technologically savvy users who are very enthusiastic about new technology and are more interested in exploring technology than actually benefiting from it. These users are very cooperative by nature and in addition are likely to be much more forgiving of faults in developing technologies; in many cases actually contributing to its development. We can draw parallels with the case of Peer-to-Peer networks, which usually see an extremely high level of cooperation in the early days, which declines slowly as they become more mainstream and attract more general users.

At this stage, we argue that incentive systems are not needed at all; the desired behaviour for nodes can simply be hardwired into nodes at a hardware as well as a protocol level and trust that the majority of users will not tamper with the devices. This will avoid all the problems discussed previously, ease implementation, reduce complexity and allow all forwarding functions to be handled automatically within the network for it to be fully self-organising.

Pioneering users have little incentive to hack the system and early applications are likely to be both specific and limited to small groups of users with common goals. By reducing problems and limitations for users, pioneers will become champions of the technology and introduce it to the next customer segment down the adoption cycle, the *visionaries*.

Visionaries are different from pioneers in that they are not interested in technology for technology's sake but rather see the potential in new technology and are willing to make sacrifices in order to be amongst the first to see that potential realised, and thereby get a head start in reaping the benefits. Visionaries are also likely to use the technology for specific applications, although the number of users may be significantly larger.

At this stage, incentive systems are again unnecessary as users of specific applications have implicit shared goals. There is also an inherent self interest for visionaries to see the technology that they choose succeed. Once there is a strong enough build up of visionaries and the technology has proven its worth, it is then possible to make the leap from the early market to the mainstream market, where the *pragmatists* await.

Pragmatists want a product that works and unlike the customers in the early market are much less tolerant of faults. They want to be able to buy products that meet their needs out of the box and easily get support from people who've used the technology before as well as find books about it in the bookstore. In short, they want a complete solution rather than a product that is still in development.

At this point of the technology's adoption, devices are reasonably ubiquitous and the technology has advanced beyond what was available in the early days. Most importantly, there are now a lot of experimental results and experience with real life implementations of the technology; it is also better understood how people actually use and abuse the system.

It is only at this point in the adoption cycle that it may make sense to introduce some form of incentives system. Even then, it would be better to design these incentives specifically for individual applications, based on what has been learned about how people abuse the networks, rather than a general incentives system that would possess the flaws discussed previously. As discussed in [13], it is unlikely that large-scale ad hoc networks will be deployed for general consumer applications due to their limitations in comparison to competing technologies. Their strengths will best be shown in either small-scale general applications or specific larger scale applications. In both cases, incentives can stem from common interest rather than an enforced system.

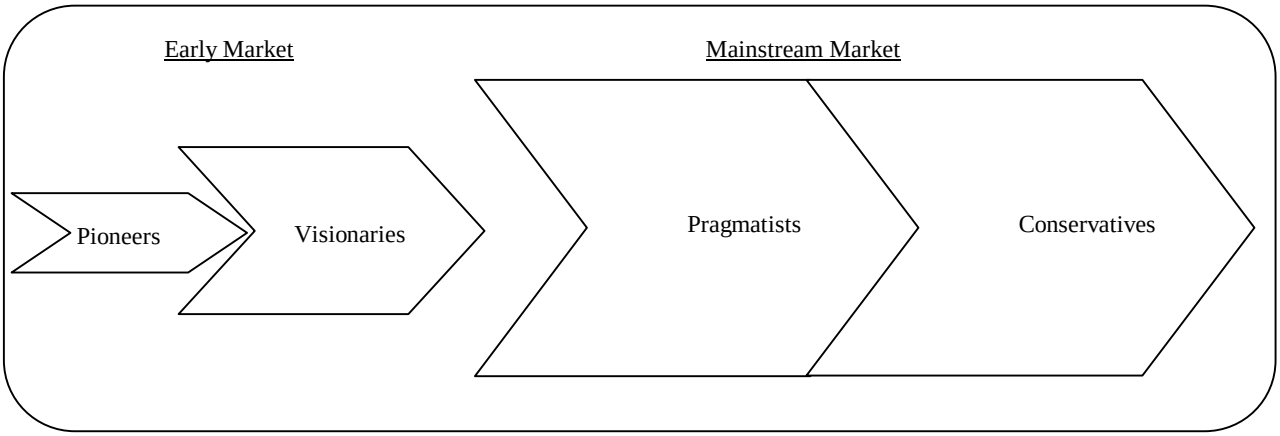

Figure 1: Adoption Cycle for Mobile Ad Hoc Networks

Finally, should mobile ad hoc networks become truly ubiquitous and used for general applications, c*onservatives* will hop onto the bandwagon, simply because they have no choice. Conservatives want products that are cheap and simple; they buy products only after everyone they know already owns one.

Figure 1 shows the adoption cycle and the relative sizes of each customer segment.

5.2 Why We Don't Need Incentive Systems Anyway

It is of course still possible that in practice users will not wish to cooperate, even in the early stages of adoption. One of the main reasons behind the research of these systems is that the hardware and software of nodes can be tampered with and their behaviour modified by users in such a way that the devices do not cooperate with others, in order to save resources. Although it is generally recognised that most users do not have the required level of knowledge and skills to modify nodes, there is concern that criminal organisations will have the resources and interest to produce and sell modified nodes on a large scale.

Our position is that the majority of users will only cheat when it is clearly beneficial to them and relatively easy to do. In the case of mobile ad hoc devices, it is unclear that there is significant benefit to be had from going to the trouble to modify devices just to save resources such as battery power, memory and processor clock cycles. Battery power is probably the most limited resource, and even that may not prove to be an issue to most users, as long as the devices do not require constant charges. Devices might also be designed with docking capabilities such that when the devices are stationary their reliance on battery power is reduced as well as improving functionality. This will also encourage users to keep devices on to forward data for others even when not in use. Also, if devices become truly ubiquitous the power needed for forwarding will decrease anyway as the distance from one hop to another becomes minimal.

While there are certainly many criminal organisations with the ability to modify devices on a large scale, there is very little incentive for them to do so, since it is doubtful that a large enough market will exist to make the exercise profitable. A prominent example of a consumer device that has fallen victim to large scale tampering is the Sony Playstation 2 which has spawned an entire side industry of illegal modifications. Mod chips are widely available to buy on the Internet for home modification, as are full service organisations that modify units on behalf of consumers for a fee.

In the case of the Playstation, there are compelling reasons for both individual consumers and criminal organisations to engage in modification. Although the cost is relatively high, consumers who modify their devices can subsequently make significant savings by buying pirated games at a fraction of the original price. The organisations thus have a large and willing market of customers for their modifications, and are able to charge a significant sum to make large profits.

Conversely, in the case of mobile ad hoc devices, practically the only benefit to consumers would be longer battery lives. It is somewhat unlikely that they would go out of their way and pay a premium to modify their devices to this end, especially when it might cost the same to simply buy an extra battery with the added benefit of not voiding the device warranty or breaking the law. With little demand and potential for profitability, criminal organisations will not go to the trouble to reverse engineer and modify devices.

In any case, it would be necessary to produce a unique ad hoc device for each different type of application (e.g., a multiplayer ad hoc gaming device would be significantly different from an in-car ad hoc communications system). The need to reverse engineer each type of device as opposed to just one standard device would further increase costs and complexity for criminals and make it even less feasible for large scale modifications to occur.

Finally, any organisation with the knowledge to tamper with these devices would know (or soon learn) that there is no long-term value proposition to be gained from large-scale modifications. Unlike peer-to-peer file sharing networks such as Kazaa or Gnutella that can function reasonably well even with a large number of freeloaders, mobile ad hoc networks

rely on cooperation for basic functionality. The more devices that do not cooperate by relaying messages, the worse the overall performance of the network will be, until finally the network is completely useless. Therefore, whilst a few isolated individuals might choose to modify their devices, a criminal organisation would gain no long-term benefit from doing so since they would rapidly destroy the network along with their own customers.

6. CONCLUSIONS

In this paper we have looked at the problem of cooperation within mobile ad hoc networks and have analysed the drawbacks of currently proposed incentive systems. We then argued that there might not be a need for incentive systems at all, especially in the early stages of adoption, where excessive complexity can only hurt the technology's deployment. We looked at the needs of different customers segments for each stage within the projected technology adoption cycle and proposed that incentive systems not be used until ad hoc networks enter mainstream markets.

Even then, incentive systems should be tailored to the needs of each individual application rather than a general solution that may be too flawed or technically demanding to be implemented in reality. Punishments/incentives other than the denial of service to misbehaving nodes might be considered as an alternative. For example, within a file sharing application, users might be punished by limiting their query returns, rather than ostracising them from the network completely.

History is littered with examples of great technologies that never saw the light of day due to deployments that attempted to achieve too much too fast, with no way of successfully monetising the technology or to build up acceptance; all of which are dangers that ad hoc networks face. It is important to remember that mobile ad hoc networks are only one of a host of competing technologies, and in order to successfully make it to the mainstream market its worth over competing technologies needs to be clear and proven to consumers.

An important caveat to note is that the problem of providing incentives to selfish nodes is a somewhat separate issue from preventing malicious attacks on the network. In this paper we have addressed the problem of nodes that wish to maximise their personal utility of the network, whereas malicious users may be less concerned with personal gain and simply wish to attack the network. Therefore, whilst we argue that incentive systems may not be necessary, it is still imperative that there are mechanisms to guard against malicious attacks in order to maintain the reliability of the network.

Future work could include experimental trials with two separate mobile ad hoc networks; one with an incentives system and the other without. Comparisons might then be made to confirm whether an incentive-less system would work as well or better than one with an incentives system in place. However, the experiment would need to be carefully designed such that users would behave in the same way as normal users along the adoption cycle, as experimental volunteers are likely to be cooperative by nature.

In conclusion, it is unlikely that there is a perfect solution to the ad hoc incentives problem. Implementations of technology are always limited in reality by cost, human behaviour, complexity and resources. Indeed, there is often only a least bad solution that provides the best cost benefit ratio rather than a best solution. It is more important at this point that mobile ad hoc networks be given the space to grow and develop rather than to choke it with complicated solutions to problems that may not even exist, causing users to shun the technology.

7. REFERENCES

[1] Adar, E. and Huberman, B. A., 2000 "Free riding on Gnutella" *First Monday*, 5(10)

[2] Anderegg, L., Eidenbenz, S., 2003, "Ad hoc VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents", *Proceedings of the 9th annual international conference on Mobile computing and networking (Mobicom)*

[3] Anderson, R. and Kuhn M., Nov 1996, "Tamper Resistance --- A Cautionary Note" *USENIX Workshop on Electronic Commerce*

[4] Bansal, S. and Baker, M., 2003, "Observation based cooperation enforcement in ad hoc networks" *Stanford University Technical Report*

[5] Boyd, C., 2004, "Metcalfe's Law" http://www.mgt.smsu.edu/mgt487/mgtissue/newstrat/metcalfe.htm

[6] Buchegger, S., Boudec, J.L., October 2002 "Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness" *Lecture Notes on Informatics, Mobile Internet Workshop, Informatik 2002*

[7] Buchegger, S., Boudec, J.L., 2002, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness in Dynamic Ad-hoc Networks" *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*

[8] Buttyan, L. and Hubaux, J.P., August 2000, "Enforcing Service Availability in Mobile Ad-Hoc WANs" *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing*

[9] Buttyan, L. and Hubaux, J.P., January 2001, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self Organized Mobile Ad Hoc Networks" *Technical Report EPFL*

[10] Buttyan, L. and Hubaux, J.P., October 2003, "Stimulating Cooperation in Self-organizing Mobile Ad Hoc Networks" *ACM/Kluwer Mobile*

[11] Crowcroft, J., Gibbens, R., Kelly, F., and Ostring, S., March 2003 " Modelling incentives for collaboration in Mobile Ad Hoc Networks", *Proceedings of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*

[12] Hsieh, H.-Y. and Sivakumar, R., June 2001 "Performance comparison of cellular and multi-hop wireless networks: A quantitative study" *Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS) 2001*

[13] Huang, E., Östring, S., Crowcroft, J. & Wassell, I., Jan 2004 "Developing Business Models for MobileMAN" T*echnical Report, Cambridge University Engineering Library*, CUED/FINFENG/TR.475

[14] Jakobsson, M., Buttyan, L. and Hubaux, J.P., January 2003 "A micro-payment scheme encouraging collaboration in multi-hop cellular networks" *Proceedings of Financial Crypto 2003*

[15] Lamparter, B., Paul, K. and Westhoff, D., 2003, "Charging Support for Ad Hoc Stub Networks," *Computer Communications*, Vol 26.

[16] Marti, S., Giuli, T.J., Lai, K., and Baker, M., 2000 "Mitigating routing misbehaviour in mobile ad hoc networks" *Proceedings of MOBICOM 2000*

[17] Michiardi, P., Molva, R., 2002, "CORE: A Collaborative Repudiation Mechanism to enforce node cooperation in Mobile Ad hoc Networks" *Sixth IFIP conference on security communications, and multimedia (CMS 2002)*

[18] Moore, G.A., 1991, "Crossing the Chasm" HarperBusiness

[19] Tschudin, C., 2003, "Embedding MANETs in the Real World" *Conference on Personal Wireless Communications (PWC)*

[20] Zhong, S., Yang, R., Chen, J., March 2003, "A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-hoc Networks" *Proceedings of INFOCOM 2003*