Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 3435674, 9 pages
http://dx.doi.org/10.1155/2016/3435674

Research Article

Comparative Study of Cooperation Tools for Mobile Ad Hoc Networks

J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil

Department of Computer Engineering and Systems, University of La Laguna, Tenerife, Spain

Correspondence should be addressed to J. Molina-Gil; jmmolina@ull.es

Received 17 June 2016; Revised 13 November 2016; Accepted 16 November 2016

Academic Editor: Laurence T. Yang

Mobile ad hoc networks are formed spontaneously to use the wireless medium for communication among nodes. Each node in this type of network is its own authority and has an unpredictable behaviour. These features involve a cooperation challenge that has been addressed in previous proposals with methods based on virtual currencies. In this work, those methods have been simulated in NS-2 and the results have been analyzed, showing several weaknesses. In particular, it has been concluded that existent methods do not provide significant advances compared with networks without any mechanism for promoting cooperation. Consequently, this work presents three new proposals that try to solve those problems. The obtained results show that the new proposals offer significant improvements over previous schemes based on virtual currencies.

1. Introduction

A mobile ad hoc network (MANET) consists of a group of mobile devices that spontaneously form a wireless network. MANETs involve facing many different security challenges mainly because each node represents its own authority and has as main target the maximization of the benefits it gets from the network. This involves that nodes try to save their own battery, even though this can degrade network performance and connectivity.

MANETs do not have any fixed infrastructure or centralized management to allow communication among distant nodes. Thus, intermediate nodes have to act as forwarding nodes, offering routes to other destinations. Besides, nodes usually have energy restrictions due to battery limitations, resulting in a difficult problem if they decide to save their own battery and not to forward others' packets, because this can disrupt the normal network functioning. Therefore, no reason exists to assume that nodes will cooperate in providing services to each other. Indeed, users can modify hardware and software of their nodes so that their behaviour is modified to suit only their own purposes. Hence, the hypothesis used here is that all nodes are selfish and try to use services of other nodes without providing theirs to the others. For this reason, tools for cooperation encouragement are essential in MANETs, where communications can become infeasible without cooperation.

This work addresses the problem of the existence of noncooperative nodes in MANETs. It contains a study of previous solutions and proposes new tools for cooperation enforcement. In particular, it includes several results obtained from many simulations of MANETs where the Dynamic Source Routing (DSR) protocol and different tools for cooperation enforcement were used.

This paper is organized as follows. Section 2 introduces the cooperation issue in MANETs through a brief bibliographic review. Several previous proposals are described in Section 3 and their weaknesses are analyzed in Section 4. Then, new credit-based tools are proposed in Section 5. Section 6 includes a performance evaluation through the analysis of results obtained from many NS-2 simulations. Finally, some conclusions are mentioned in Section 7.

2. Preliminaries

The main feature of MANETs is that devices have to perform packet forwarding [1, 2]. This feature is typically associated with routers in classical networks, where packets reach distant nodes through intermediate nodes.

The idea behind MANETs makes possible that networks with no infrastructure can increase their mobility and size in a quick and effective way, but, in order to work properly, it requires cooperation among nodes. Two main approaches to enforce cooperation can be found in the bibliography.

The first approach is based on mechanisms where nodes receive payments if they help to transmit others' packets. The works [3, 4] introduce the concepts of virtual currency and service charges. Their approach includes two models: Packet Purse and Packet Trade. While in the first model the sender is charged for sending, in the second one, intermediate nodes trade each packet and the receiver pays for the entire data transmission. The same authors analyze in [5] the use of virtual currency to implement a reward for the participation of users in packet forwarding. The paper [6] proposes a way to determine the price for forwarding services to discourage selfish behaviour in MANETs. Finally, the works [7, 8] include the analysis of several pricing schemes, cheat-proof schemes and security of payment systems to enforce cooperation in packet forwarding.

The second approach combines the concept of reputation based on the Quality of Experience, with different strategies for detection and punishment. These methods use a reputation system to identify and penalize selfish nodes in order to mitigate misbehaviour in routing. One of the first reputation-based mechanisms was called Watchdog and Pathrater [9], a scheme based on rewards and not on punishments. The reputation system called CORE [10] uses the Watchdog and Pathrater mechanism. Another method called Confidant [11, 12] aims at detecting and isolating noncooperative nodes. Other mechanisms, such as the method called OCEAN proposed in [13] and the reputation broadcast described in [14], have serious limitations because they degrade network reliability and performance. On one hand, in OCEAN a second chance mechanism is not consolidated, so malfunctioning nodes cannot rebuild their reputation when they recover from temporal problems. On the other hand, the reputation broadcast involves flooding, so it can produce a high overhead and incur lengthy latency. Finally, the work [15] presents a reputation system called Account-Aided Reputation Management, which builds a hierarchical locality-aware distributed hash table infrastructure for operation of both reputation and price systems.

3. Basic and No-Credit Models

In this paper, the simulation of a Basic Model has been used to exemplify the behaviour of the nodes in a network with no cooperation mechanism. This Basic Model has been implemented to allow a complete comparative study of existing and proposed models.

The nonbasic cooperation models analyzed in this work have been divided into two groups: no-credit models, which use virtual coins and are based on fixed per hop charges and credit models, which emerged from the study of previous models in order to correct some of their drawbacks by adding the concept of credit. The first model is described in this section while the second one is defined in the next section.

In order to ensure noncounterfeiting and illegitimate modifications of coins in packets, all nonbasic models assume the existence of tamper-proof mechanisms.

3.1. Basic Model. This model is a basic approach towards the study of the behaviour of nodes in networks with no cooperation mechanism. In this model, data packets are sent each time a source node has something to transmit, and when the intermediate nodes responsible for forwarding packets receive them, they decide whether to forward them or not.

This paper assumes that each node has a valuable and limited resource, which is its battery, and, that based on it, it makes the decision to forward packets or not. Thus, a rational behaviour of nodes is assumed so that they decide to cooperate in forwarding packets when their energy levels are high. Here, the energy level is considered high when it exceeds 50%. Thus, if nodes have energy levels lower than 50%, they are assumed to have a selfish behaviour and drop all received packets. This 50% level is here called selfishness threshold. Figure 1(a) shows the behaviour of nodes in the Basic Model according to their energy levels and this selfishness threshold.

3.2. No-Credit Models. The models not based on credit are characterized by requiring coins to pay the forwarding service among nodes. In general, this model defines a business of Packet Trade with all the nodes belonging to the source-destination path, which represents an improvement of a more basic method that establishes one coin as a fixed charge per hop.

These models assume a rational behaviour of any node that has to make a decision about forwarding or dropping packets, according to the following:

(i) If its energy level is below 25%, it drops all packets. This so-called sublimit selfishness threshold is here fixed to 25% because all nodes are assumed to have a rational behaviour so that when the battery of a node reaches 25%, it is supposed to save its battery for its personal use and not for relaying others' packets.

(ii) When its energy level is above this sublimit selfishness threshold (25%), but below the selfishness threshold (50%), the node decides based on its battery level and other factors such as its number of coins and the number of own packets it wants to send. This decision is different in each one of the three variants described below.

(iii) An energy level above the selfishness threshold of 50% means that the node forwards the packets.

Figure 1(b) shows schematically the aforementioned behaviours of nodes according to their energy levels in no-credit models.

Three different variants of no-credit models are defined below.

3.2.1. Source-Pay Model (SPM). In this model, each intermediate node earns coins for forwarding information, and the charge to cover the forwarding cost is directly done from the forwarded packets. Thus, when a source node sends

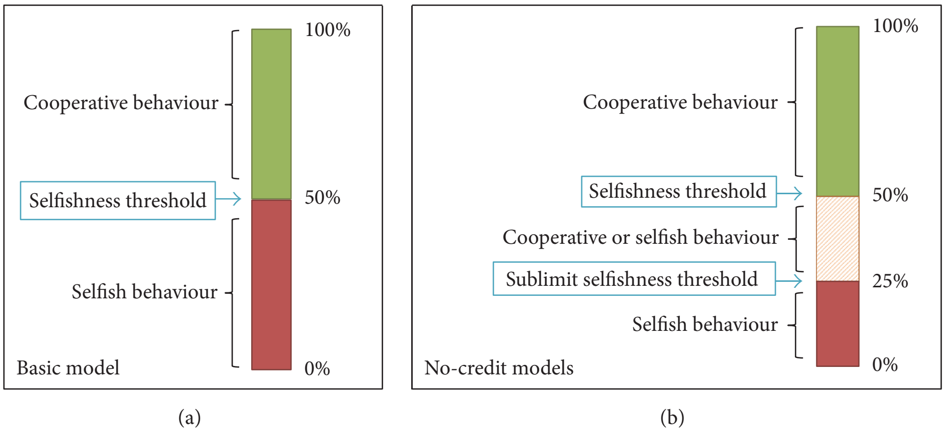


Figure 1: Thresholds and behaviours.

a packet, it should insert a sufficient number of coins to reach the destination. The number of coins acquired by each intermediate node depends on the quantity fixed by the source. In the implementation, this number was set to one, according to the proposal presented in [5] called Packet Purse Model with fixed per hop charges. A basic problem of this model is the estimation of the number of coins that the source must insert in the packet to try to reach the destination. If the source overestimates this initial number of coins, it loses coins, but if it underestimates it, it loses both the inserted coins and the packet. In order to try to solve this problem, it is possible to use the information resulting from the use of the DSR protocol. In that routing protocol each node stores a route cache with all the discovered routes during its lifetime in the network, so it can compute the number of hops required to reach many destinations and, hence, the number of coins that must be inserted to reach them. However, these data are not available for the packets used in the DSR route discovery protocol. Thus, in this case, it is necessary to overestimate the number of coins based on the number of nodes in the network so that the source always inserts a sufficient number of coins to ensure that the packet reaches the destination. In the simulations done in this paper, each node makes its decision about forwarding or dropping packets after taken into consideration not only its energy level but also its possession of coins and the estimated number of packets it wants to send in the future. In particular, when its energy level is above sublimit selfishness threshold (25%) and below selfishness threshold (50%), it decides whether to forward or to drop others packets based on its battery level and the number of own packets it wants to send. If its number of coins is lower or equal to the one required for sending that number of packets, the node has a selfish behaviour and drops others packets. Else, it forwards others packets.

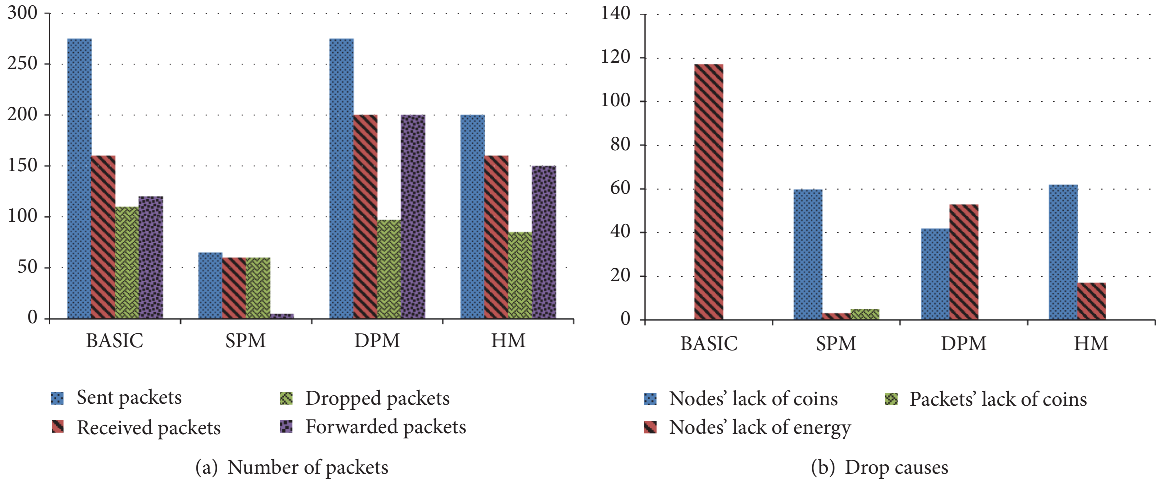
3.2.2. Destination-Pay Model (DPM). This model is based on the Packet Trade Model [3, 4] in which each intermediate node of the path receives coins for forwarding packets. In that proposal, the source nodes do not pay for sending packets, but instead the destination nodes are responsible for covering the total cost of packet retransmission. Hence, the packets travel without any coins. In the original Packet Trade Model, each packet is always sold to neighbors for nonfixed prices. However, in our proposal, each intermediate node determines whether its neighbor has sufficient coins to buy it, and if so, the packet is always sold for exactly one coin more than when bought. Otherwise, it is dropped. Thus, the aforementioned problem of the DSR route discovery disappears because nodes send the DSR packet to their neighbors so that if there is at least one neighbor who can cover the cost, the packet is sent. When the packet reaches the destination, its price equals the number of hops to reach it, and the destination covers the cost of packet forwarding. As in the SPM, the cooperative behaviour of each intermediate node depends on its number of coins and battery status. This model uses both the selfishness and the sublimit selfishness thresholds, as described in the previous section. Unlike the previous model, this model prevents losing packets by intermediate nodes in most cases, and only if no neighbor node has sufficient coins to buy a packet, it is dropped.

3.2.3. Hybrid Model (HM). This model combines the two previous schemes. If a source node wants to send a packet, it must insert some coins in it. However, unlike the SPM, it is not necessary that this number of coins is equal to the number of hops to reach the destination node. Instead, the required number of coins to be inserted in the packet by the source must be approximately equal to half the number of hops to reach the destination according to the DSR protocol. Thus, packets are forwarded according to the SPM until they run out of coins. Then, the forwarding of packets switches to be performed in accordance with the DPM. Hence, both the source and the destination share the forwarding costs. This hybrid model inherits the advantages of both models, but also partially their disadvantages.

4. Problems of No-Credit Models

Some weaknesses of the described models are analyzed below.

4.1. Peripheral Node Problem. This problem is due to the position of peripheral nodes because they have to spend their



(a) Number of packets

(b) Drop causes

Figure 2: Problems of no-credit models.

coins in sending and/or receiving packets but cannot earn any coin because they do not have any opportunity to forward packets for others. In particular, their positions do not allow them to be part of any forwarding route, so they are denied the opportunity to earn any coin. This situation would result in their isolation.

On one hand, peripheral nodes in the SPM are margined because they are not able to send their own packets. On the other hand, the peripheral node problem in the DPM results in that these nodes are isolated from the network in terms of packet reception because if they do not have sufficient coins to pay for the reception of packets, they cannot receive any. Furthermore, the HM inherits the disadvantages of both models because in that model peripheral nodes may suffer marginality both at sending and at receiving packets.

4.2. Problems Related to Coins and Energy. The behaviour of nodes in no-credit models is now analyzed according to their numbers of coins and energy levels.

For this analysis, several NS-2 simulations have been done where the number of nodes is 20, the number of coins initially assigned to each node is 20, and the maximum number of packets to be sent by each node is 100.

Figure 2(a) shows the number of sent, received, dropped, and forwarded packets for each model. According to those data, the main weakness of the SPM is that the number of sent packets is lower than in the Basic Model because nodes are required to have coins to be able to send packets. The DPM involves an improvement regarding the number of sent packets because nodes do not have to pay for sending their own packets, and in fact, compared with the Basic Model, the figures are similar. However, the number of dropped packets is higher than in the Basic Model because the cost of the packet increases in each hop, producing an increase in the total cost. Finally, the HM shows a decrease in the total number of sent packets with respect to the Basic Model due to the requirement of coins to send packets. In this case, since source and destination nodes share the forwarding cost, the number of sent packets is higher than in the SPM.

Figure 2(b) shows the identified causes why each node drops packets. The main cause to drop packets both in the Basic Model and in the DPM is the lack of energy of nodes. However, the results show that in the other two models, SPM and HM, the main problem is the lack of coins. In many cases, as with peripheral nodes, source nodes cannot forward packets, so they cannot earn any coin, what prevents them from sending own packets when they have spent all their coins. Thus, in order to solve these problems, this work proposes the idea of adding the concept of credit to the different models.

5. Credit Models

The idea of introducing the concepts of overdraft and credit in the aforementioned models is now proposed so that a node or a packet without enough coins can use forwarding services. The new models with credit allow nodes to be overdrawn as an additional way to promote cooperation because any indebted node is forced to cooperate if it wants to use the network. Besides, the proposals with credit address the peripheral node problem.

Different credit-based models can be distinguished depending on the procedure of making decisions about forwarding packets. In all of them, nodes use an intelligent system to analyze their possibility of earning coins, based on the usage of the node that neighbors have made previously. This is possible because each node maintains an array with all the neighbors that have used it for forwarding. Hence, when a node has to make a decision about whether to forward or drop a packet, it check its battery level and number of coins and the values in this array. In particular, the node queries its current one-hop neighbors and searches in the array any current neighbor that had used it as forwarding node. If this search shows a frequent use by any neighbor, the node considers it as a prediction that in the future it will be used as forwarding node and consequently will have the opportunity to earn coins. In the simulations, the specific frequencies a node considers for a positive conclusion depend on the average number of forwarding packets in the network.

Another difference with respect to no-credit models is that in Credit Models nodes are allowed to send packets even if they do not have enough coins to cover the forwarding cost. In this case, they estimate whether they could send/receive their own packets according to their previous cooperation behaviour. This information is reflected in their debt accounts. If nodes have no coin and no penalty, they receive credit to send their own packets so their number of coins becomes negative. If nodes have penalties, they are banned from sending/receiving any own packet. Nodes receive a penalty when, once indebted, they do not forward a received packet. This ban to send/receive own packets remains till their number of coins becomes positive.

When a node receives a packet to be forwarded, it analyzes the potential benefit/loss that this operation will bring to it. The benefit is calculated with the increase in its number of coins and the possibility to recover from a previous penalty. The loss is estimated with the battery level decrease and any possible penalty if the node is overdrawn and does not forward the packet. This analysis includes the computation of the number of own packets that the node would be able to send with its battery level and number of coins and of the energy consumption for forwarding the packet. Besides, the node estimates possible revenues to quantify its possibilities to recover from a penalty. After this, it makes the decision to drop the packet in any of the following cases:

(i) when its battery level is below the sublimit selfishness threshold and it has good revenue estimation,

(ii) when it has enough coins to meet its needs, a battery level below selfishness threshold, and no penalty,

(iii) when it does not get any benefit from forwarding the packet.

When the estimations of all the aforementioned parameters do not indicate any possibility to recover from a previous debt and/or penalty, the node forwards the packet in order to earn coins, even when it can run out all the battery.

In the following subsections, three variants of Credit Models are defined.

5.1. Source-Pay Model with Credit (SPMC). This model assumes that each node has a credit account. In addition to allowing nodes to be overdrawn, it introduces the idea of penalties for bad behaviour and an intelligence system in all nodes. It uses DSR information to estimate the number of coins that have to be inserted in each packet. If the number of coins a node has is below the quantity estimated by the DSR protocol, its balance becomes negative to allow that the packet can include the required number of coins. This model has several advantages. It solves the peripheral node problem. Besides, nodes are less selfish in order to try to reduce their debts. Only forwarding nodes and not sources or destinations can overload the network, due to the existence of penalties. On the negative side, the model has two disadvantages. Possible network overheads exist, and packets can be lost in route discovery due to coin underestimation.

5.2. Destination-Pay Model with Credit (DPMC). As in the previous model, each intermediate node gets a coin for each forwarded packet. Thus, after forwarding a packet, each involved node increases in one of its number of coins. Simultaneously, the forwarded packet increases its value in one. Conversely, if a node decides not to forward, its number of coins is decremented in as many coins as the value of the dropped packet. The penalty received by a node involves banning it from sending/receiving any packet. Some advantages of this model are the following. It solves the peripheral node problem. Nodes are less selfish to reduce their debts. Only forwarding nodes and not sources or destinations can overload the network, due to the existence of penalties. Intermediate nodes that drop a packet receive higher penalties when more nodes have forwarded it. On the other hand, its main disadvantage is the possibility of network overhead.

5.3. Hybrid Model with Credit (HMC). This model combines the two aforementioned schemes. When a source wants to send a packet, first it must charge it with some coins. In the original HM, the source nodes have to insert in the packet approximately half of the coins corresponding to the total number of hops indicated by the DSR protocol. In the HMC, when a node decides to send a packet, it follows the same criteria as in the SPMC, which allows sending packets even when the source node has fewer coins than required. Nodes are also banned from sending own packets if they have a penalty for a previous misbehaviour. Packet forwarding follows the SPM till the packet runs out of coins. Then, forwarding decisions follow the DPM, so the destination has to pay the debt. In order to do it, the destination node can also use credit if necessary. As a combination of the two previous models, it shares their advantages and disadvantages both for sender and for receiver.

6. Performance Analysis

A comparative study of the described methods was done, and different tests showed that the models involve distinct behaviours of nodes depending on the scenarios. Thus, by varying some important features such as numbers of coins, energy levels, and numbers of peripheral nodes, we obtained some interesting conclusions.

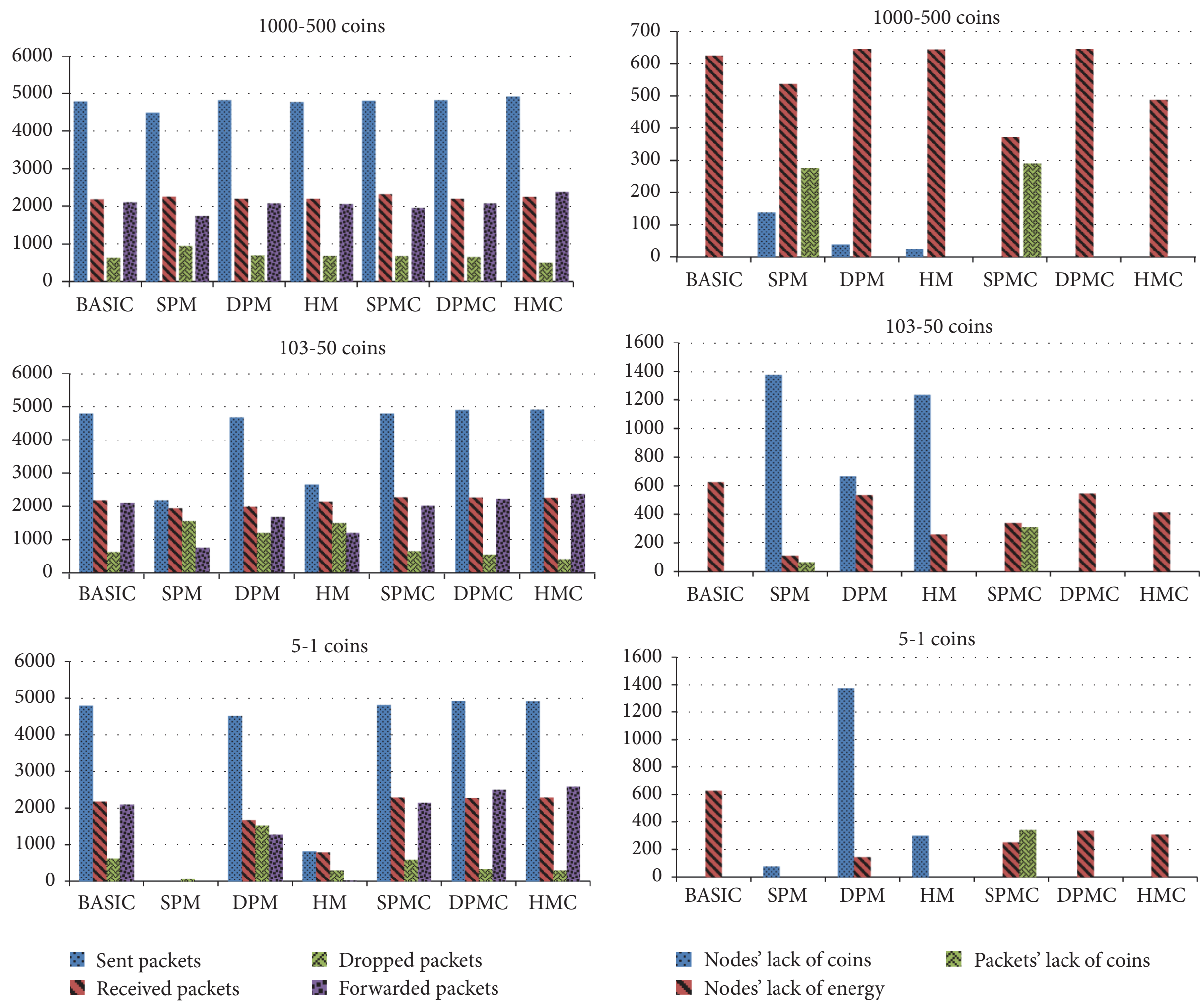
In particular, the comparisons were made for different scenarios generated at random by using setdest script to generate nodes' movements and cbrgen script to generate connections among nodes. These scripts are available with the NS distribution. Specific used simulation features are as follows:

(i) The number of sent packets per node was between 10 and 1500.

(ii) The packets were generated to be sent every 0.05 seconds.

(iii) A new connection was started every second.

(iv) The simulations lasted 20 seconds.



(a) Number of packets

(b) Drop causes

Figure 3: Number of packets and drop causes versus number of coins.

(v) The initial energy levels of nodes ranged between 50% and 75%.

(vi) The network sizes were of 15, 25, 50, 75, and 100 nodes.

(vii) For each network size and feature, 25 simulations were run.

6.1. Number of Coins. This study includes a comparison among different cooperation tools that involve the use of virtual coins.

On one hand, the initial energy level of each node for all simulations was medium (50%–70%). On the other hand, the initial number of coins assigned to each node was considered: high when the number was between 500 and 1000, medium when the number was between 103 and 50, and low when the number was between 5 and 1.

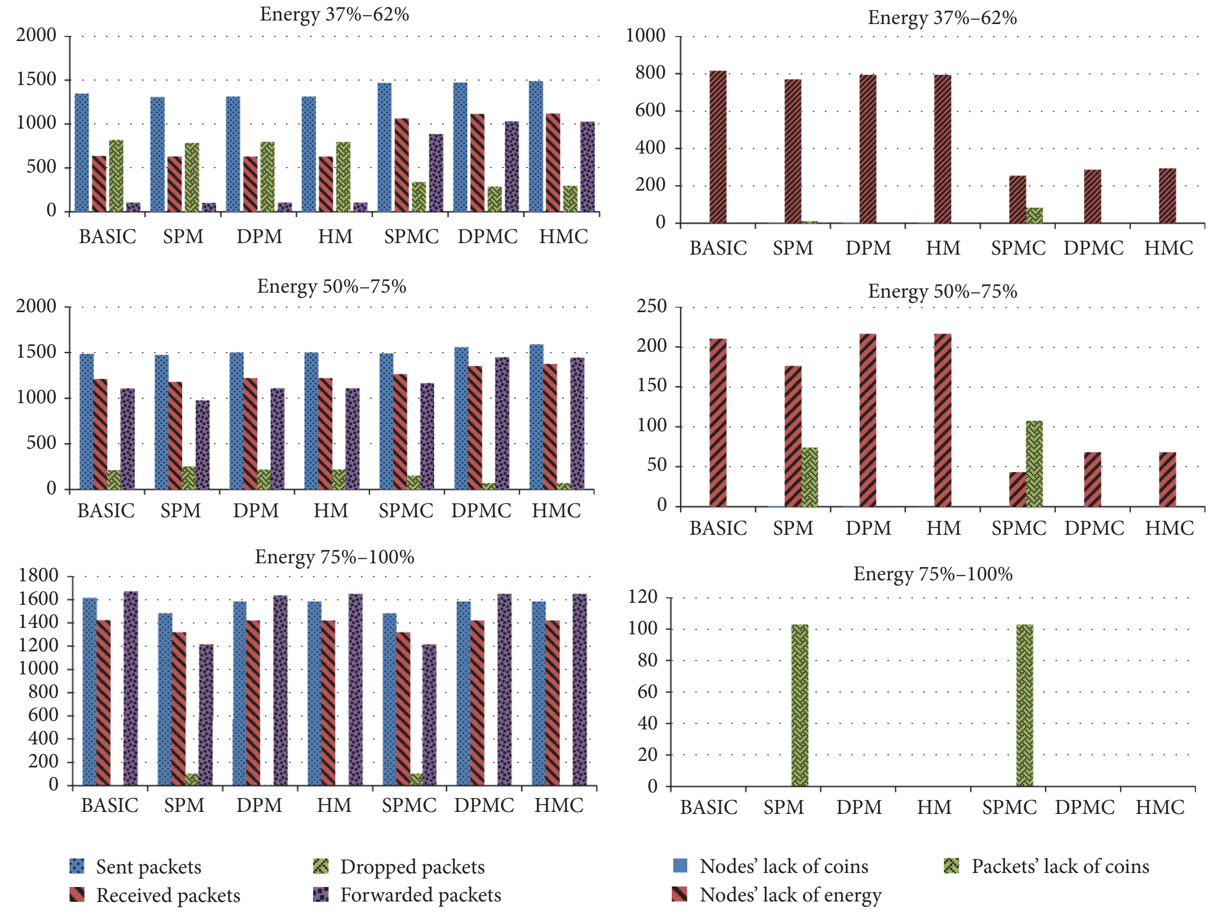
Some average results of the first 25 simulations of the different models done with 50 nodes are shown in Figure 3. In particular, Figure 3(a) displays the average numbers of packets that were sent, received, dropped, and forwarded when the number of sent packets per node was between 1000 and 1500. The main conclusions in this case are as follows:

(i) With a high number of initial coins, both the HM and the DPM are the best performing models.

(ii) With a medium number of initial coins, the numbers of sent/received and dropped/forwarded packets in no-credit and Credit Models are equal to or worse than in the Basic Model.

(iii) With a low number of initial coins, Credit Models perform better than no-credit and Basic Models.

Figure 3(b) also provides a study about the reasons why the packets are dropped. Possible causes of packet loss analyzed in this work are the lack of coins in nodes, of energy in nodes, and of coins in packets. The main conclusions of Figure 3(b) are the following. With a high number of coins, the lack of energy produces loss of packets, so too many initial coins encourage selfishness. For a medium number of coins, the main reason why packets are dropped in the Basic Model is the lack of energy and in all Credit Models is the lack of



(a) Number of packets

(b) Drop causes

Figure 4: Number of packets and drop causes versus energy level.

coins. Finally, for a low number of initial coins, the main drop cause is the lack of coins in the nodes in Credit Models and the lack of energy in Credit Models.

Thus, the concluded recommendation is to use many initial coins with no-credit models, and fewer with Credit Models.

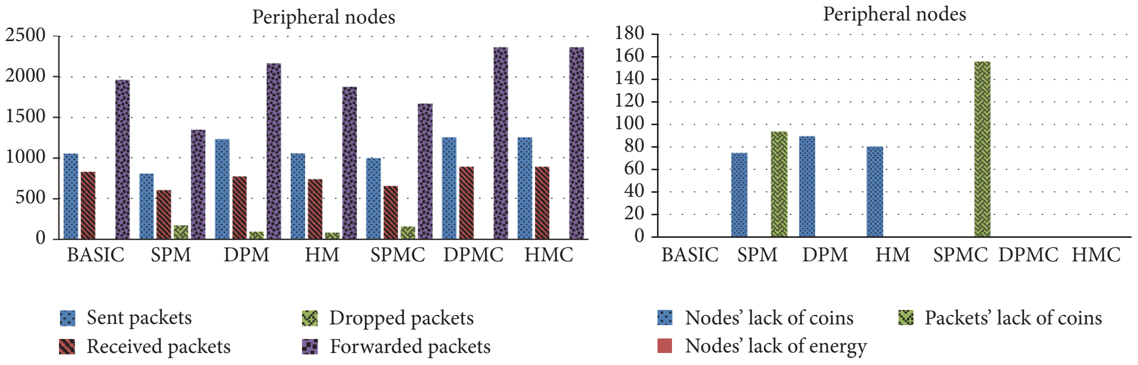
6.2. Energy Level. This work includes a study of the behaviour of nodes in all the models, considering different energy levels. Energy files have been implemented with a TCL script called energy.tcl, which is responsible for ensuring that nodes maintain the energy levels.

A specific characteristic of these simulations was that the number of initial coins in no-credit models was between 500 and 1000 and in Credit Models was 1. In these simulations, the considered energy levels are low (37%–62%), medium (50%–75%), and high (75%–100%).

As above, some average results of 25 simulations with 50 nodes are shown in Figure 4, but in this case the number of sent packets per node was between 500 and 1000. In particular, Figure 4(a) shows that the number of received packets in Credit Models is higher than in no-credit models. For low energy levels, the number of dropped packets is higher in both no-credit and Basic Models, while in no-credit models, it is much lower. For medium energy levels, the number of sent and received packets with all models is similar while the number of dropped and forwarded packets is better in the DPMC and HMC. For high energy levels, different models are similar in the numbers of sent and received packets and of dropped and forwarded packets. Therefore, it can be concluded that, with high energy levels, the proposed models have the same behaviour as the Basic Model. Figure 4(b) also shows why nodes drop packets. For both low and medium energy levels, the main reason is the lack of energy. In both SPM and SPMC, the number of dropped packets is greater due to coin underestimation. For high energy levels, packets are dropped mainly for coin underestimation.

Thus, the conclusion is that, for low energy levels, Credit Models show better performance for different network sizes.

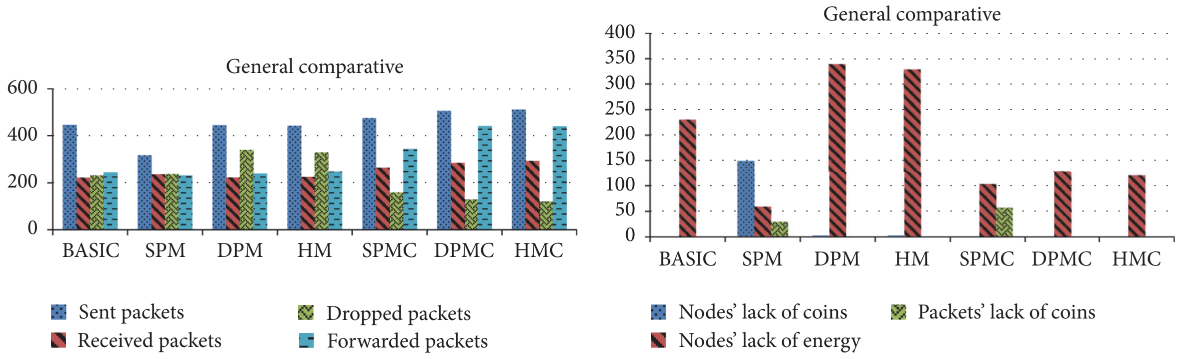
6.3. Number of Peripheral Nodes. This work includes the study of the peripheral node problem with the different models. In order to analyze the results, different scenarios were created for the simulations. Two specific characteristics of these simulations were an optimal initial number of coins for each model and a high energy level (75%–100%).



(a) Number of packets

(b) Drop causes

Figure 5: Number of packets and drop causes versus peripheral nodes.



(a) Number of packets

(b) Drop causes

Figure 6: Packets numbers and drop causes in simulations with recharge.

As in previous sections, the average results of 25 simulations are shown in Figure 5. In this case, the analysis considered only peripheral nodes among 50 nodes and a number of sent packets per node between 50 and 100. Figure 5(a) shows the numbers of sent, received, dropped, and forwarded packets in each model. The main conclusion is that Credit Models help to solve the peripheral node problem. Besides, it can be concluded that according to the number of dropped packets, both the DPMC and HMC can be considered better than the others. Figure 5(b) summarizes the reasons why nodes drop packets, and the conclusion is that the lack of coins in nodes is the main reason why peripheral nodes drop packets. Furthermore, coin underestimation arises again as a problem in both SPM and SPMC.

Therefore, the main conclusion is that both DPMC and HMC solve the peripheral node problem.

6.4. General Comparison. Finally, in order to reach general conclusions, 25 simulations were performed for each model and different network sizes (15–100 nodes), and the number of sent packets per node was between 10 and 1500.

This implementation was meant to simulate a real network where nodes can connect to the power grid to charge their battery. In particular, in the simulation all nodes initially had a high energy level and spent it with no guarantee that they could recharge, because it was considered that, every 0.5 seconds, 5 randomly selected nodes were recharged.

Figure 6(a) shows that Credit Models stand out in the numbers of sent/received packets and of dropped/forwarded packets. Thus, it can be concluded that Credit Models increase cooperation, measured with the number of forwarded packets, and decrease selfishness, measured with the number of dropped packets. Among Credit Models, the DPMC and HMC stand out.

Figure 6(b) also shows the main reason of packet drops, which is the energy lack in all models. It is also concluded that Credit Models decrease the number of dropped packets and that when the number of nodes increases, the number of dropped packets in the Basic Model is bigger than in Credit Models.

7. Conclusions and Future Works

This work provides a study of several solutions to the selfishness problem in MANETs and the identification of their main weaknesses thanks to NS-2 simulations. Besides, it includes the proposal of new schemes focused on the reduction of possible selfish behaviours, by solving the identified weaknesses. In particular, this paper begins with a study of existing cooperation stimulating mechanisms based on virtual coins, including different NS-2 simulations, whose results do not show any significant improvement over a basic network without any cooperation enforcement. Then, the main reasons why these existing methods are not successful are determined in order to propose new solutions. Simulation results of the new proposed models show that they increase node cooperation by combining a mechanism based on virtual coins and the credit concept. Thus, the conclusion is that the new proposals help to improve several weaknesses of previous schemes by maximizing the number of forwarded packets and minimizing the number of dropped packets. Related to future works, it would be interesting to propose some security mechanism to ensure that the number of coins earned by each intermediate node is only one unit and acquired after retransmission. On the other hand, it would be useful to implement the most promising methods in real networks to ensure they work correctly in real environments because this would allow determining how much overhead in space and time is required by the new proposal and which is the cost of maintaining the arrays, in order to analyze if the network performance is really reduced, considering the extra energy consumption of nodes.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

Research was supported by RTC-2014-1648-8, TEC2014-54110-R, MTM-2015-69138-REDT and DIG02-INSITU.

References

[1] J.-P. Hubaux, L. Buttyán, and S. Čapkun, "The quest for security in mobile ad hoc networks," in *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '01)*, pp. 146–155, Long Beach, Calif, USA, October 2001.

[2] N. Samian, Z. A. Zukarnain, W. K. G. Seah, A. Abdullah, and Z. M. Hanapi, "Cooperation stimulation mechanisms for wireless multihop networks: a survey," *Journal of Network and Computer Applications*, vol. 54, pp. 88–106, 2015.

[3] L. Buttyán and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *Proceedings of the 1st Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC '00)*, pp. 87–96, IEEE, Boston, Mass, USA, August 2000.

[4] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile Ad Hoc networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003.

[5] L. Buttyán and J. P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Tech. Rep. DSC/2001, Swiss Federal Institute of Technology, Lausanne, Switzerland, 2001.

[6] J. Crowcroft, R. Gibbens, F. Kelly, and S. Östring, "Modelling incentives for collaboration in mobile ad hoc networks," *Performance Evaluation*, vol. 57, no. 4, pp. 427–439, 2004.

[7] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, "A secure credit-based cooperation stimulating mechanism for MANETs using hash chains," *Future Generation Computer Systems*, vol. 25, no. 8, pp. 926–934, 2009.

[8] Z. Sheng, C. Jiang, and R. Y. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile Ad Hoc networks," in *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03)*, pp. 1987–1997, San Francisco, Calif, USA, 1987.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 255–265, ACM, Boston, Mass, USA, August 2000.

[10] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, pp. 107–121, Kluwer, September 2002.

[11] S. Buchegger and J. Le Boudec, "Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-Based Processing*, pp. 403–410, Canary Islands, Spain, 2002.

[12] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '02)*, pp. 226–236, ACM, Lausanne, Switzerland, June 2002.

[13] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," https://arxiv.org/abs/cs/0307012.

[14] S. R. Zakhary and M. Radenkovic, "Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments," in *Proceedings of the 7th International Conference on Wireless On-demand Network Systems and Services (WONS '10)*, pp. 161–167, IEEE, Kranjska Gora, Slovenia, February 2010.

[15] H. Shen and Z. Li, "A hierarchical account-aided reputation management system for manets," *IEEE/ACM Transactions on Networking*, vol. 23, no. 1, pp. 70–84, 2015.