Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks

Alberto Rodriguez-Mayol and Javier Gozalvez
Ubiquituous Wireless Communications Research Laboratory
Uwicore, http://www.uwicore.umh.es
University Miguel Hernandez of Elche, Spain
f.rodriguez@umh.es, j.gozalvez@umh.es

***Abstract*— MCN-MR (Multi-hop Cellular Network – Mobile Relay) has been proposed as a promising technology for future Beyond 3G and 4G systems due to its foreseen capacity to increase transmission rates and provide homogeneous quality of service levels in the service area. To this aim, mobile nodes are required to cooperate in the relaying of information of other nodes. As a result, selfish nodes refusing to relay packets can have damaging effects on the overall multi-hop connectivity of MCN-MR networks. Different reputation protocols have been already proposed to cope with selfishness in mobile ad-hoc networks, but they tend to overestimate the selfish behavior of nodes, due to the effects of radio errors or packet collisions that can be mistaken for intentional packet drops. Thus, the availability of valid multi-hop routes usable by nodes is reduced. In this context, this paper proposes and evaluates two techniques that improve the operation and ability to accurately detect selfish nodes of the watchdog detection mechanism that is generally employed in reputation based selfishness prevention protocols.**

Keywords-component– Multi-hop Cellular Networks; selfishness; reputation techniques; watchdog; MANET.

I. INTRODUCTION

One of the distinctive and most challenging features of future Beyond 3G networks will be the provision of spatial homogeneous Quality of Service (QoS) levels [1]. Conventional cellular networks have achieved universal coverage, but fail to offer homogeneous QoS levels and high bit rates out of the proximities of the Base Station (BS) due to the exponential decrease of the signal level with the distance. To overcome this limitation, operators can augment the density of BSs, which could increase the planning complexity and the deployment and maintenance costs in addition to the current social rejection towards the deployment of new antennas. Alternatively, Multi-hop Cellular Networks (MCN) [2], combining ad-hoc and cellular transmission capabilities, have been proposed to increase data rates and provide homogeneous QoS levels throughout a cell. In MCN networks, long-range single hop cellular transmissions are replaced by a combination of multiple ad-hoc hops and a cellular short-range last hop connection with the BS. These multi-hop cellular communications capabilities extend the high data rates from the centre to the border of the cell, in addition to improving capacity, coverage and energy utilization [3].

Two modalities of MCN networks have been identified. In MCN-Fixed Relay (MCN-FR), fixed relaying antennas are deployed at the border of the cell to reduce the transmission distance with users far away from the BS. To achieve the expected benefits, the fixed relay antenna should also have good propagation conditions with the cell BS, preferably Line Of Sight (LOS) conditions. MCN-FR networks have a relatively low design complexity, but require the deployment of new antennas with the consequent economic and social cost [3]. On the other hand, MCN-Mobile Relay (MCN-MR) networks are characterized by a higher flexibility as they would use other Mobile Terminals (MTs) as relay stations. However, significant challenges must yet be overcome to achieve the expected MCN-MR benefits. One of these challenges is to ensure the cooperation of MTs in the packet relay process [4]. Selfish behavior may be motivated by several reasons, e.g. battery exhaustion, traffic overload, distrust for MCN-MR technology, intrinsic selfishness, etc., and will cause network performance disruption. In this context, the goal of Selfishness Prevention Protocols (SPPs) is to incentive nodes to cooperate in network functions, and to prevent intentional attacks from malicious nodes.

Previous publications have addressed the problem of packet dropping, in which nodes refuse to retransmit data packets originated in other nodes, even when they agreed to do so previously during the multi-hop route establishment process, in the context of MANETs (Mobile Ad-hoc NETworks) [5]. Three groups are established to categorize the different SPPs strategies proposed in the literature: reputation-based, credit-based, and those based on game theory. Credit-based schemes use a virtual or real currency to pay for self originated data retransmitted by other nodes. Credit is then used to compensate for the utilization of resources in the relaying process, and it can be obtained by retransmitting other nodes packets or just by exchanging real money. The lack of scalability, centralization, or the need for a tamper-proof hardware are limitations of some of the credit based schemes [5]. Game theory models simulate a game where each mobile node can choose either to retransmit other nodes data or not. Equilibrium stability of different strategies can be studied analytically. However, game theory models usually fail to reproduce important parameters of real systems. Alternatively, this work focuses on reputation techniques, which in general use the watchdog technique proposed in [6] to observe the behavior of other nodes, which will be explained later. These observations are used to fill a reputation table where the willingness to cooperate of the neighbor nodes is quantified. The reputation

table is used in the route establishment process to select a route without selfish nodes. Reputation schemes are fully distributed and achieve good network performance [4]. However, a previous study [7] showed that the evaluation of these schemes under simplistic operating conditions can provide inaccurate indications about their operation and performance. In particular, the work reported in [7] demonstrated the important impact of the radio propagation conditions and potential channel congestion on the expected performance of reputation based SPPs. Based on these observations, this work proposes two novel strategies to improve the performance of reputation based cooperation schemes in MCN-MR, and evaluates their operation in realistic scenario simulations.

The rest of the paper is organized as follows. Reputation-based cooperation protocols are presented in section II, along with a description of the watchdog detection technique. Section III presents the reputation-based SPPs improvements proposed in this paper. Section IV introduces the simulation platform implemented, and section V discusses the performance achieved with the proposed techniques. Finally, the conclusions are presented in section VI.

II. REPUTATION-BASED SELFISHNESS PREVENTION PROTOCOLS

The SPPs employed to counteract packet dropping attacks are aimed at detecting and isolating selfish nodes in order to incentive them to cooperate. Reputation-based methods are generally made up of two modules: detection and reaction. The detection module in each node watches the behavior of neighbor nodes, i.e. whether they retransmit other node's data or not, using the watchdog detection mechanism explained in section II.A. The reaction module maintains a local reputation table where each node is assigned a trust level based on the observations made by the detection module. Furthermore, trust information is reported to the correspondent routing protocol in order to avoid already detected selfish nodes in future route establishments. In addition, countermeasures like isolation may be employed against selfish nodes.

A. Watchdog detection technique

The watchdog detection technique [6] is based on the passive acknowledgment of the relaying of packets by other nodes, by overhearing the relay node's transmissions, as illustrated in the example of Figure 1.

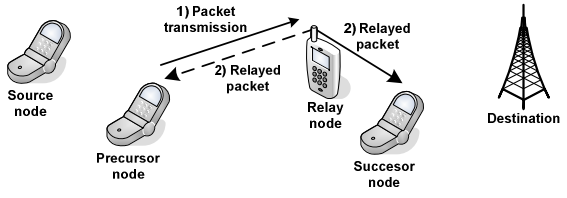

Figure 1. Operation of the watchdog detection technique

In this figure, the source node has established a multi-hop link to the destination to transmit its data packets. The route has been established following a multi-hop routing protocol. The data packets are then transmitted in a hop-by-hop fashion following the sequence source node – precursor node – relay node – successor node – destination node. In Figure 1, a packet is transmitted from the precursor node to the relay node. A packets buffer in the precursor node keeps a temporary copy of the transmitted packets that have to be forwarded by the relay node. Each buffered packet is assigned a timeout within which the packet has to be forwarded to the successor node by the relay node. If the relay node transmits the packet within the timeout, this transmission is overheard by the precursor node, and the relay node is noted to have cooperated correctly. The precursor node looks for the copy of the packet relayed that was stored in the buffer, and removes the copy. If the relayed packet is not overheard correctly by the precursor node within the timeout, then the relay node is assumed to have acted selfishly, i.e. it has dropped the packet. This is referred to as selfish behavior detection. Some countermeasures are taken, depending on the SPP considered, affecting the trust level of the relay node in the reputation table of the precursor node. An important parameter of the watchdog detection process is the packet timeout, which refers to the time within which the relay node must relay the packet; the value of this parameter was not specified in [6]. A too large value of the timeout parameter increases the time necessary to detect nodes acting selfishly, while a too low value prevents the relay nodes to forward the packet in time. To correctly adjust this parameter, a set of preliminary simulations where conducted. The obtained results showed that more than 99% of the packets were correctly forwarded by the relay node 50ms after the precursor node transmits the packet. Consequently, the packet timeout has been set to 50ms in this work. Another parameter defined in the present implementation of the watchdog technique is the buffer check interval, which represents the interval between the instants at which it is checked whether packets have been relayed correctly. This parameter was set to 25ms, according to the results obtained in preliminary simulations.

The watchdog technique is used by most of the reputation-based SPPs proposed so far. However, as the authors demonstrated in [7], radio propagation errors and packet collisions due to channel congestion significantly impact the performance of the watchdog detection technique and its capacity to accurately detect selfish nodes. In the example illustrated in Figure 1, packet collisions could prevent the precursor node to correctly observe the forwarding of the packet by the relay node. Reference [8] claims that packet collisions may not affect the watchdog's detection capability even with very high traffic load. However, the conclusion was extracted using a four laptop testbed, which might be a too limited testing environment. In case that the precursor node does not overhear the retransmission of the packet, it will incorrectly detect a selfish behavior. Repeated incorrect detections affecting one relay node may provoke that this node is incorrectly accused of acting selfishly, being avoided in future route establishments and isolated or penalized in its own data transmission. These incorrect detections will also impact the operation of other nodes since they will reduce the number of safe routes. Safe routes are multi-hop routes without any relaying node that has been previously classified as a selfish node. In this context, this work presents two enhancements of the original watchdog detection technique that aim to reduce the rate of incorrect accusations to overcome its negative effects.

B. Marti's reputation-based selfishness prevention protocol

The SPP implemented in this work was proposed by [6], and is referred to in the rest of the paper as Marti's protocol. Marti's protocol is made up of two modules: watchdog and pathrater. In the watchdog module, each precursor node uses

the watchdog detection technique to observe the behaviour of the relay nodes. The watchdog module counts the number of times that a relay node has refused to retransmit packets. When the number of faults is greater than a certain threshold, which is referred to as maximum faults threshold, the relay node is accused of acting selfishly. The exact value of the maximum faults parameter was not specified in [6]. A too large value of the maximum faults parameter increments the number of packets that nodes acting selfishly drop before being accused. A too small value increases the number of times that cooperative nodes are accused incorrectly, for example due to packet collisions or radio errors. Parameter-sweep simulations where conducted to find its optimal value, which was finally set to 5. The pathrater, run by each node in the network, uses the knowledge of the watchdog to select the route most likely to be reliable, i.e. without selfish nodes. The pathrater maintains a reputation table in which the reputation of every known node is rated based on the information collected by the watchdog module. Unless otherwise stated, all parameter values in the present implementation are chosen according to [6]. When a node in the network becomes known to the pathrater, it assigns the node a rating of 0.5. A node always rates itself with a 1.0. The pathrater increments the rating of nodes on all actively used paths by 0.01 at periodic intervals of 200ms, which is called the rate increment interval. An actively used path is one on which the node has sent a packet within the previous rate increment interval. Two different node categories are established: neutral nodes and selfish nodes. The maximum value a neutral node, i.e. a node not accused of acting selfishly, can attain is 0.8. The relay node's rating is decremented by 0.05 when the watchdog of the precursor node detects a fault. The lower bound rating of a neutral node is 0. If one node is accused of being selfish, its rating is set automatically to a highly negative value, i.e. -100. This selfish rating is maintained for a period of time, called the isolation time, which was no specified in the original implementation, because their simulations were too short [6]. In this work, the isolation time is set to 500s. After this period, the rating of the node is set again to 0.5, to let the node participate in the network, and the node becomes a neutral node again. The Marti's protocol also introduces accusation messages that let the precursor node warn the source node about the presence of a selfish node in the route. Notwithstanding, these messages are subject to forgery and may increase overhead. During route discovery, the routing protocol selects a route without selfish nodes, according to the information of the reputation table. Packet forwarding requests coming from known selfish nodes are not accepted by pathrater.

III. WATCHDOG DETECTION ENHANCEMENT MECHANISMS

To overcome the negative effects of the watchdog's detection inaccuracy, due to, for example, radio errors or packet collisions, this work proposes and evaluates two enhancements of the original watchdog technique. These proposals are intended to be run in parallel with any reputation based SPP using the watchdog mechanism to detect nodes acting selfishly. In this work, they have been implemented to be executed with the Marti's protocol previously explained.

A. Warning Mode

The Warning Mode (WM) operation is proposed to prevent false accusations caused by radio and packet collision errors. WM introduces an intermediate category, the 'suspicious' category, between a 'neutral' node and a node marked as 'selfish'. In the original watchdog technique implementation, when the relay node, which is being watched by the precursor node, exhibits bad behavior during a certain period of time (see Figure 1), it is marked as selfish directly, and all the links in which the node is involved are broken since the node is supposed not to be relaying packets. However, it is important to highlight that the selfish accusations could be incorrect due to radio transmission errors experienced at the precursor or relay node. In this context, in the warning mode, when the number of faults exceeds the maximum faults parameter, the relay node is first marked as suspicious, and its links are broken temporally. The suspicious nodes can participate in routing tasks again, but some additional restrictions are applied in order to prevent an increase in packet dropping due to a real selfish behavior. In particular, nodes will deal with suspicious nodes as if they where neutral nodes, with two exceptions. First, the timeout a suspicious relay node has to forward a packet is reduced by a factor α. In this work, the α parameter was set to 0.5, but an adaptive approach could be used to tune its value, depending on the observed congestion in the radio channel. This issue is left for future work. In addition, the maximum faults threshold is set to 1, instead of 5, for suspicious nodes. Thus, if the precursor node detects one more fault by a suspicious node, it will definitively be accused of acting selfishly. On the other hand, if a precursor node detects that a suspicious node is cooperating again, then its reputation will be incremented to give the suspicious node the chance to recover from previous bad reputation, which could have been provoked by packet collisions or radio errors.

The improvement expected with WM comes from the fact that spurious radio channel errors, fading and packet collisions can provoke a damaging increment of incorrect accusations in the original Marti's implementation. Incorrect accusations have several negative effects. Incorrectly accused cooperating nodes are isolated unfairly. Isolation of cooperating nodes will prevent them from reaching the BS through a multi-hop connection. Additionally, since false selfish nodes will be avoided in multi-hop routes, the number of potential valid multi-hop routes is wrongly reduced. This will result in that some valid multi-hop routes will be underutilized, while other cooperating nodes will be overloaded by packet forwarding requests. On the contrary, in the WM mode, suspicious nodes have an extra chance to recover from incorrectly assigned bad reputation. If such bad reputation was provoked by packet collisions or radio transmission errors, the participation of the suspicious node can be reestablished when communications conditions improve. On the contrary, if the suspicious node is truly acting selfishly, then few extra packet droppings will be allowed, as it will be quickly detected and isolated due to the strict conditions established in WM for suspicious nodes.

B. Reset Failure Mode

The Reset Failure Mode (RFM) aims to counteract false accusations provoked when the link between two nodes becomes unusable. Link failures can be caused by channel effects like fading or by the mobility of the nodes. The MAC (Medium Access Control) layer is responsible for detecting link failures and triggering a link failure event to inform the routing protocol. However, before the link failure event is triggered, some of the packets transmitted by the precursor node to the relay node may have not been relayed (see Figure 1). As a result, the copies of the packets in the packet buffer of

the precursor node will timeout, and the rating of the relay node will be degraded unreasonably.

In the RFM mode, if a link failure is detected, the rating of the relay node is reset to 0.5, i.e. the initial rating assigned to a node that becomes known for the pathrater for the first time. Besides, the number of faults is reset to 0, since these faults are assumed to have been provoked by the link failure and not by a possible selfish behavior of the node. In addition, the copies of the packets in the buffer of the precursor node that are pending to be forwarded by the relay node are removed, irrespective of their expiration time, as the node is not able to retransmit them. It has to be noticed that these exceptions established in the RFM mode are only used when the relay node is seen as a neutral node by the precursor node. If the relay node is accused of acting selfishly before the link failure event is triggered, then the selfish rating and the faults of the relay node remain unchanged.

Link failures may affect both to selfish and non selfish nodes. Thus, a potential drawback of RFM is that reputation restoration due to link failures may increase the reputation of real selfish nodes, i.e. nodes that are currently acting selfishly. This could happen if a link failure is detected and the next node in the route is a real selfish node which has not been discovered yet. In this case, the reputation of a real selfish node will be unreasonably restored. However, it is important to note that this might only happen in multi-hop transmissions with a short lifetime of multi-hop links, which in fact should be avoided by efficient multi-hop ad-hoc routing protocols. In addition, links are expected to have a mean lifetime greater than the time needed to detect the selfish behavior of a node in a low to medium mobility scenario, where cooperative multi-hop communications in MCN networks are more feasible.

C. *Complexity and cost*

The WM and RFM proposals are easy to implement, as they require only slight modifications of the original implementation of the reputation-based SPP that is executed in parallel. In addition, RFM introduces little computational cost, due to the utilization of basic functions like the restoration of the reputation level, the reset of the number of faults and the removal of the copies of the packets in the packets buffer. However, it is important to note that the operation of the WM technique increases the number of route establishments in 40% approximately compared to the original Marti's protocol, and the corresponding signaling associated to the route discovery process. A reduction of the induced overhead, which will be investigated in future work, could be achieved increasing the isolation time to punish selfish nodes.

IV. EVALUATION PLATFORM

A. *Simulation scenario*

System level simulations emulating the operation of multi-hop wireless networks have been carried out using the ns2 simulation platform and the Rice Monarch Project extension for mobile and multi-hop networks [10]. The simulation environment consists of a Manhattan layout of 1350x1350 square meters, where pedestrians move following the Random Walk Obstacle model [11] and communicate with a BS located at the centre of the scenario through multi-hop transmissions. Nodes are distributed uniformly. A density of nodes equal to one per 80 meters has been chosen to ensure the establishment of multi-hop routes. Traffic sessions consist of web browsing transmissions with a variable number of pages as specified in [12], with 5 pages per session, an average reading time between pages of 30s, an average of 25 objects (packets) per page, and inter-arrival packet time 0.0228s. To consider potential channel congestion situations, 15% of nodes on average have an active traffic session simultaneously. The ad-hoc radio interface corresponds to the 802.11a standard operating at the 5.8GHz frequency band and transmitting with a fixed power level of 17dBm.

B. *Routing protocol*

Multi-hop ad-hoc communications are established using the IEEE 802.11s standard for mesh networks. HWMP (Hybrid Wireless Mesh Protocol) is a default and mandatory routing protocol defined in 802.11s, although the standard is open for the implementation of alternative routing protocols [13]. HWMP combines the AODV (Ad-hoc On-demand Distance Vector) [14] reactive routing protocol, and a proactive tree-based routing protocol. To avoid the signalling load associated to proactive routing protocols under mobile conditions, this work is based on the AODV protocol. This protocol only searches and establishes a multi-hop route when the source node has information to transmit. In this case, Route REQuest (RREQ) messages are sent by the source node, and retransmitted by neighbour nodes. When the destination node receives the RREQ message, it replies with a unicast Route REPly (RREP) message for confirmation. In the original AODV protocol, intermediate nodes, i.e. nodes between the source and destination, only process the first RREQ coming from a source node, and discard the replicas of the RREQ coming through other multi-hop routes with a greater latency. As a result, the route selected between the source and destination nodes is that with the lower latency, which generally coincides with the route with the lowest number of hops from source to destination. The reception of RREQ and RREP messages allow intermediate nodes to know the identity of their neighbours in the route towards the source and destination nodes. However, the information of the identity of all the nodes in the route to the destination or source node is not considered in the original AODV. Since this information is needed for the operation of reputation-based SPPs, a modified AODV protocol has been implemented for this study. In the implemented protocol, routing packets include information about the identity of all the nodes it passed through in the multi-hop route. In addition, intermediate nodes are allowed to process multiple replicas of a routing packet more than once. This allows for the establishment of diverse multi-hop routes following the selected multi-hop cost functions. It is important to note that these features are included in the Dynamic MANET On-demand (DYMO) routing protocol [15], successor to the AODV protocol.

C. *Radio propagation modeling*

The pathloss is modelled following the urban micro-cell channel model in [16], which differentiates between LOS (Line Of Sight) and NLOS (Non Line Of Sight) conditions. The implemented propagation model considers also the multipath fading and the shadowing effects. The multipath fading effect, resulting from the reception of multiple replicas of the transmitted signal at the receiver, is modelled through a Ricean distribution under LOS conditions, and a Rayleigh distribution under NLOS conditions. The shadowing is also modelled

through a log-normal distribution with 3dB and 4dB standard deviation under LOS and NLOS conditions. In addition, the spatial autocorrelation characteristic of the shadowing has been modelled through the Gudmunson model [17].

V. PERFORMANCE EVALUATION

This work's proposals are aimed at enhancing the detection accuracy of the watchdog detection mechanism employed by most of the reputation based SPPs. Enhancing the detection accuracy would increase the overall network performance and connectivity by improving the ability to rapidly and precisely distinguish between cooperative and selfish nodes. This ability would in turn augment the number of multi-hop routes without selfish nodes.

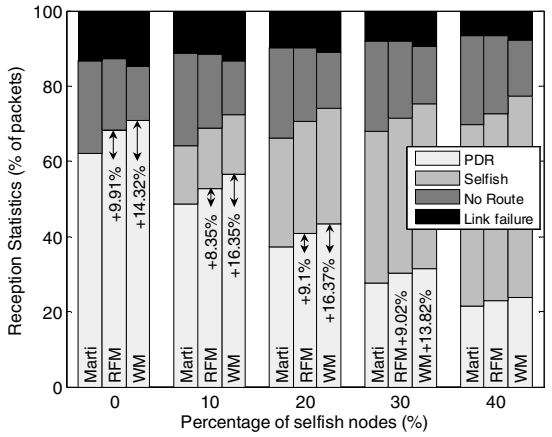

Figure 2. Packet reception statistics for Marti's system.

Figure 2 represents the packet reception statistics for the different detection techniques analyzed in this work. Packet reception statistics refer to the Packet Delivery Ratio (PDR), the percentage of packets dropped by selfish nodes, and the percentage of packets lost due to unavailability of multi-hop routes or due to link failures. PDR represents the number of packets correctly received divided by the total number of packets transmitted. Each group of bars in Figure 2 corresponds to a different percentage of selfish nodes. Each of the bars in a group corresponds to a different technique (RFM, WM and Marti). The numbers in the figure indicate the percentage of increment of the PDR achieved with our proposals compared to the original Marti technique. The ability to accurately detect selfish and cooperative behavior with the techniques proposed leads to a notable increase of the PDR. This is due to the increment of the number of valid routes available, especially for the WM proposal. The increase of the number of valid routes available with the techniques proposed can be appreciated in the decrease of the percentage of packets dropped due to the unavailability of routes ('no route' in the legend). The cost of this improvement is a small increase of approximately 5% in the percentage of packets dropped by selfish nodes in the WM mode. The reason for this increase is implicit in the operation of the WM technique. When the selfish behavior of a relay node is detected, it is first categorized as a suspicious node before it is marked as selfish node and isolated if it continues dropping packets during the suspicious period. However, as shown in Figure 2, the increase in the packets dropped during the suspicious period has a low impact on the overall PDR.

The increase of the PDR achieved with the proposed techniques is due to the decrease of the number of incorrect accusations and the ability to select the multi-hop routes without selfish nodes. The number of incorrect accusations, which is represented in Figure 3(a), refers to the number of times that a non selfish relay node was accused of acting selfishly due to the accumulation of incorrect detections provoked by radio propagation errors and packet collisions (see section II.A). The most remarkable result is the important reduction in the number of wrong accusations achieved with the WM proposal (over 95%), compared to the original Marti's technique. This reduction is caused by the operation of the suspicious category introduced by the WM technique, as explained in section III.A. Relay nodes that are marked as suspicious have another chance to recover a good reputation level. In addition, a suspicious node may not interact again with the precursor node that marked it as suspicious. In these two cases, no accusation is computed. The reason for the decrease of the number of incorrect accusations achieved by the RFM technique is that in case that a link failure is detected before the relay node is accused of acting selfishly, its reputation is restored. Thus, the negative effects of link failures on the reputation levels are mitigated.

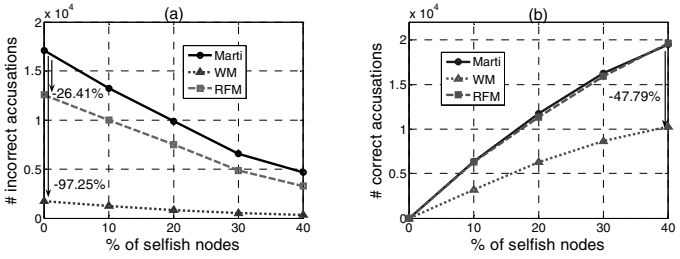

Figure 3. Number of (a) incorrect and (b) correct accusations

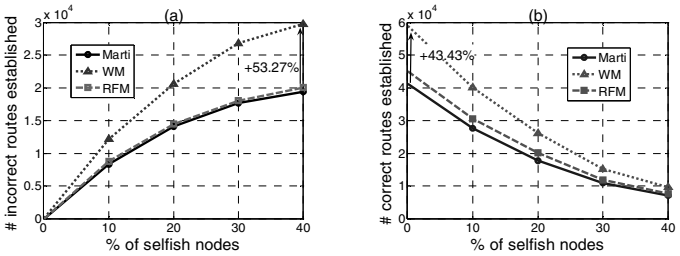

Figure 4. Number of (a) incorrect and (b) correct routes established.

Correct accusations increase the number of established multi-hop routes without selfish nodes. Figure 3(b) shows that this parameter remains almost unchanged for the RFM technique compared to the Marti's protocol, which confirms that the reputation restoration process in the RFM technique does not benefit selfish nodes, since they are rapidly accused before a possible link failure event is triggered. On the other hand, WM technique results in a decrease of the number of correct accusations (approximately 45%), although the results depicted in Figure 2 showed that this decrease does not have a noticeable impact on the PDR. This is the case, because when using the WM technique, nodes that are marked as suspicious may not interact again with the precursor node that marked it as suspicious, and as a result, they will not be able to drop its packets.

Figure 4(a) shows the number of times that a multi-hop route with selfish nodes was established, referred as incorrect

route establishments. On the other hand, correct route establishments , in Figure 4(b), refers to the number of times that a multi-hop route without selfish nodes was established. There is a notable increment of the number of correct and incorrect routes established with the WM technique. This is due to the operation of the WM technique. In case that a relay node is observed acting selfishly, it is categorized as suspicious and the link with the node is broken. Nodes marked as suspicious may participate again in route establishments. This process implies an increment in the number of route establishments, both correct and incorrect. Nevertheless, incorrect route establishments do not affect PDR notably, as was shown in Figure 2, because suspicious nodes are observed very tightly in the WM technique. The RFM technique maintains the same level of incorrect route establishments than Marti's protocol, and increases by approximately 14% the number of correct route establishments. This improvement is due to the fact that the RFM technique reduces the number of incorrect accusations while maintaining the number of correct accusations, as was shown in the previous figures.

In the reputation-based SPPs, route forwarding requests are dropped if the node that receives the routing message detects that any of the nodes participating in the multi-hop route is a selfish node. This is referred to as route denials. Incorrect route denials, represented in Figure 5(a), refer to the case when no real selfish node participated in the denied multi-hop route. Both WM and RFM techniques achieve a notable decrease of the number of incorrect route denials, especially WM, reducing the number of packets dropped due to the unavailability of routes, and increasing the PDR (see Figure 2). The reduction in the number of incorrect route denials is due to the reduction of the number of incorrect accusations (Figure 3). WM and RFM maintain a similar level of number of correct route denials compared to the Marti's protocol, as shown in Figure 5(b). This means that decreasing the number of incorrect route denials, which increases the availability of routes without selfish nodes, does not come at the price of decreasing also the number of correct route denials, which would in turn augment the percentage of packets dropped by selfish nodes.

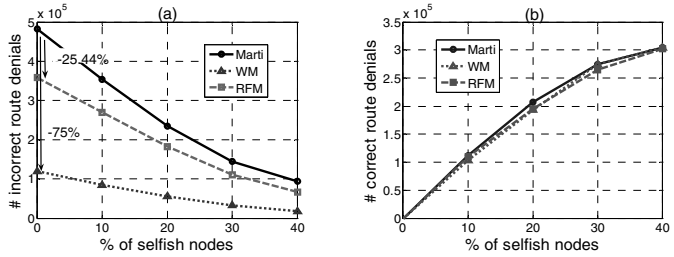

Figure 5. Number of (a) incorrect and (b) correct route denials

VI. CONCLUSIONS

This work has presented two novel improvements of the basic watchdog detection mechanism generally employed by reputation-based selfishness prevention protocols. Reputation based SPPs are aimed at detecting and isolating selfish nodes that do not participate in the relaying of other nodes data, but benefit of their relaying capacity to retransmit their own data. It has been shown that radio errors and packet collisions can result in an inefficient operation of the watchdog module that overestimates the selfish behavior of the nodes. To overcome these inefficiencies, this paper has proposed two techniques that enhance the ability of the SPP to detect the real selfish nodes and reduce the number of incorrect accusations. As it has been shown, the proposed techniques increase the availability of multi-hop routes without selfish nodes, and consequently the final packet delivery ratio in cooperative multi-hop ad-hoc networks.

ACKNOWLEDGMENT

This work has been supported by the Spanish Ministry of Science and Innovation, the Spanish Ministry of Industry, Tourism and Commerce, FEDER funds under the projects TEC2008-06728 and TSI-02400-2008-113 and the Local Government of Valencia with reference BFPI/2007/269.

REFERENCES

[1] Rec. ITU-R M.1645 – "Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000".

[2] Y. Lin and Y. Hsu, "Multi-hop Cellular: a new architecture for wireless communications," *Proceedings of the IEEE Computer Communications (INFOCOM)*, pp. 1273-1282, Mar. 2000, Israel.

[3] X. J. Li, B.-C. Seet and P. H. J. Chong, "Multihop cellular networks: Technology and economics," *Computer Networks*, Elsevier, vol. 52, No. 9, pp. 1825-1837, Jun. 2008.

[4] S. Buchegger, J. Mundinger and J.-Y. Le Boudec, "Reputation systems for self-organized networks," *IEEE Technology and Society Magazine*, vol. 27, issue 1, pp. 41 – 47, Apr. 2008.

[5] Y. Yoo and D. P. Agrawal, "Why does it pay to be selfish in a MANET?," *IEEE Wireless Communications Magazine*, vol. 13, issue 6, pp. 87-97, Dec. 2006.

[6] S. Marti, T. J. Giuli and K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks," *Proceedings of the International Conference on Mobile Computing And Networking ACM (MobiCOM 2000)*, pp 255-265, Aug. 2000.

[7] A. Rodriguez-Mayol and J. Gozalvez, "On the Implementation Feasibility of Reputation Techniques for Cooperative Mobile Ad-hoc Networks," *Proceedings of the European Wireless Conference EW2010*, Apr. 2010.

[8] S. Buchegger, C. Tissieres and J.Y.Le Boudec, "A test-bed for misbehavior detection in mobile ad-hoc networks," *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications WMCSA,* pp.102 – 111, Dec. 2004.

[9] Y. Liu and Y.R. Yang, "Reputation Propagation and Agreement in Mobile Ad-Hoc Networks," *Proceedings of IEEE Wireless Communications and Networking Conference WCNC*, vol. 3, pp. 1510 – 1515, Mar. 2003.

[10] Rice Monarch Project "Wireless and mobility extensions to ns-2," http://www.monarch.cs.rice.edu/cmu-ns.html

[11] K. Maeda, A. Uchiyama, T. Umedu, H. Yamaguchi and T. Higashino, "Urban pedestrian mobility for mobile wireless network simulation," *Ad Hoc Networks, Elsevier*, vol. 7, no. 1, pp. 153–170, 2009.

[12] UMTS 30.03 v3.2.0 TR 101 112 "Selection procedures for the choice of radio transmission technologies of the UMTS," ETSI, Apr. 1998.

[13] IEEE P802.11s/D2.0, draft amendment to standard IEEE 802.11: Mesh Networking, *IEEE Standard*, 2007.

[14] C. Perkins and E. Royer, "Ad hoc On-Demand Distance Vector Routing," *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA), pp. 90-100, 1999.

[15] Ian D. Chakeres and Charles E. Perkins, "Dynamic MANET on-demand (DYMO) Routing," draft-ietf-manet-dymo-05, Internet Draft, Jun. 2006.

[16] WINNER, "DI. 1.1. WINNER II interim channel models," *Public Deliverable*, http://www.ist-winner.org/

[17] M. Sepulcre and J. Gozalvez, "On the importance of radio channel modeling for the dimensioning of wireless vehicular communication systems," *Proceedings of the International Conference on ITS Telecommunications 2007*, ITST '07, pp 1–5, Jun. 2007.