On the Implementation Feasibility of Reputation Techniques 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, Elche, Spain
f.rodriguez@umh.es, j.gozalvez@umh.es

Abstract— **MCN-MR (Multi-hop Cellular Network – Mobile Relay) is envisioned as a new technology to face up the need for transmission rate homogeneity in future high speed Beyond 3G networks. To achieve its objectives, MCN-MR networks need to overcome the damaging effects that selfish nodes refusing to relay packets can have on the overall multi-hop connectivity. In this context, this paper evaluates the use of reputation based protocols to counteract packet dropping attacks through the watchdog detection technique. In particular, this paper analyzes the performance and operation of reputation techniques, including their capacity to detect selfish nodes, under realistic operation conditions. This study will provide valuable input to the optimization of reputation techniques to be used in future MCN-MR networks.**

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

I. Introduction

It is envisioned that users of future Beyond 3G networks will enjoy a flexible access to a variety of radio access networks that will provide them with high data rates to correspond to the ever growing demand for ubiquitous broadband wireless access. Current cellular networks have achieved universal coverage, but fail to offer homogeneous Quality of Service (QoS) levels and high bit rates out of the proximities of the Base Station (BS). On the other hand, users connected to WLAN networks enjoy higher data rates in infrastructure or ad-hoc mode, but are restricted to reduced hot spot areas. In this context, Multi-hop Cellular Networks (MCN) [1], combining ad-hoc and cellular networks, have been proposed to overcome the limitations of both technologies. 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, pushing the high data rates from the centre to the boundaries of the cell. Two different varieties of MCN networks have been identified: MCN-Fixed Relay (MCN-FR) and MCN-Mobile Relay (MCN-MR), depending on the mobility of the relays. On the one hand, MCN-FR networks have a lower design complexity, but may incur in costly deployments of new relay stations, in addition to the current social rejection towards the deployment of new antennas. On the other hand, MCN-MR networks are flexible and easy to deploy as they use the User Equipment (UEs) as relay stations, but some conditions must be matched to make them feasible: UEs must be able to establish both MANET and cellular communications, efficient routing protocols must be used to save up battery resources and reduce overhead [2], and a consistent density of cooperative nodes must exist to ensure connectivity. In fact, the cooperation of mobile nodes is a critical aspect to ensure the operation of MCN-MR, and achieve the QoS benefits expected from multi-hop cooperative communications. In this regard, MCN-MR networks inherit some of the security issues that threaten the correct operation of MANETs, and although the centralized component of MCN-MR may help in future Beyond3G networks [3], mobile nodes will still play a major role in the distributed functions that aim to preserve connectivity and security in the MANET part of the network. While there exist other concerns about security in general MANETs [4], this work focuses in packet dropping attack, in which nodes fail to retransmit data packets originated in other nodes, even when they agreed to do so previously during the multi-hop route establishment process. This behavior may be motivated by several reasons, e.g. battery exhaustion, traffic overload, distrust for new technologies, intrinsic selfishness, etc., and will cause network performance disruption. To achieve the expected multi-hop QoS benefits, countermeasures should be adopted to promote cooperation among users. In this context, Selfishness Prevention Protocols (SPP) aim to incentive nodes to cooperate in network functions like routing and data packets relaying and to prevent the attacks from malicious nodes.

This work analyzes different SPP protocols proposed in the literature, and evaluates the influence of important modeling aspects on the performance and operation of SPP techniques in mobile multi-hop ad-hoc networks. In particular, this work investigates the impact of accurate radio propagation models, channel congestion and operating conditions, on the performance of SPP techniques, and their capability to detect selfish nodes. An adequate understanding of the impact of these factors on the operation of SPP techniques is crucial for the design of valuable novel techniques for future MCN-MR networks. The rest of the paper is organized as follows. Selfishness prevention techniques are presented in section II. Section III introduces the simulation platform implemented to conduct this study. Section IV discusses the influence of radio channel modeling accuracy and other MCN-MR networks simulation parameters on the performance of SPP protocols. Finally, the conclusions are presented in section V.

II. SELFISHNESS PREVENTION PROTOCOLS

The techniques used to face packet dropping attacks are aimed at detecting and isolating selfish nodes in order to incentive them to cooperate. Reference [5] establishes three groups to categorize the different SPP strategies proposed in the literature: reputation-based, credit-based and those based on game theory. Reputation-based methods are generally made up of two modules: detection and reaction. The detection module in each node watches neighbor nodes behavior, whether they retransmit other node's data or not, while the reaction module maintains a local reputation table where each node is assigned a reputation based on the observations made by the detection module. Furthermore, reputation information is reported to the correspondent routing protocol in order to avoid detected selfish nodes in future route establishments. Besides, countermeasures like isolation may be employed against selfish nodes. In opposition to reputation-based methods, credit-based schemes use a virtual or real currency to trade data retransmissions. This virtual currency is used to pay for self originated data retransmitted by other nodes, to compensate them for the usage of their resources. Credit can be obtained by retransmitting other nodes packets or exchanging real money. These schemes depend in general on a trusted central authority and a tamper-proof hardware for the user equipment that compromise scalability. Moreover, all nodes in the network must use the same credit-based technique, as nodes not using it will not be able to retransmit their own data. Finally, game theory models multi-hop ad-hoc networks as 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. Due to the disadvantages of credit-based and game theory schemes, this work focuses on reputation techniques, which in general use the watchdog technique proposed in [6] to observe the behavior of other nodes.

A. Watchdog detection mechanism

The watchdog detection technique is based on the passive acknowledgment of the retransmission of self originated packets by other nodes, by overhearing the next node's forwarding transmissions, as indicated in the example of Figure 1. In the example, source node establishes a multi-hop link to the destination using one relay node. Initial transmission of data in the Figure 1(a) is followed by the retransmission in the Figure 1(b), in case that relay node is not acting selfishly. Retransmission is observed by source node and maybe by other neighbor nodes, contributing to direct reputation and indirect reputation respectively. In figure 1(b), the source node adjusts the direct reputation of the relay node after observing the correct retransmission of the packet. Similarly, the neighbor node modifies the indirect reputation of the relay node after overhearing the retransmission. In opposition to the case presented in Figure 1(a), if one node does not overhear the correspondent retransmission of the next node within a timeout, the relay node is supposed to have acted selfishly, since it did not forward the source node's data, and retaliation will be taken against him, depending on the used SPP technique. The watchdog technique is used by most of the reputation-based SPP proposed so far.

Channel propagation errors and collisions due to channel congestion can affect the performance of the watchdog detection mechanism. For example, ambiguous collision could prevent the source node to correctly observe the retransmission of packet in Figure 1(b) if it coincides with the reception of another packet. In case that the source node does not overhear the retransmission of the packet correctly, and no link failure or collision has been detected, it may falsely accuse the relay node of acting selfishly. This error can be seen as a false positive. On the contrary, if the source node detects that a link failure or collision has prevented the correct transmission of the packet, it will not accuse the relay node, independently of its selfishness. In case that the relay node is a selfish node, this is referred to as a false negative. An enhanced version of the watchdog technique has been proposed in [4], to broaden the type of attacks that can be detected with the passive acknowledgment technique presented above. Reference [4] claims that ambiguous collisions may not affect 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. It should be noted that indirect reputation has a higher error rate compared to direct reputation. This is due to the fact that the neighbor node that indirectly overhears the first hop transmission in Figure 1(a) may be located out of the range of the relay node. For this reason, it will be unable to detect the second hop transmission in Figure 1(b) and will accuse him falsely.

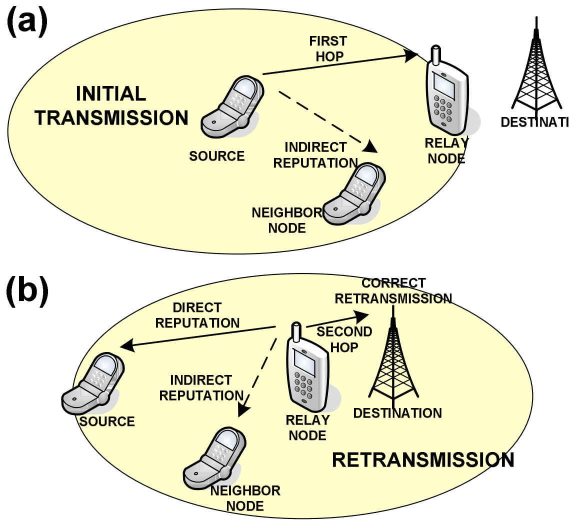

Figure 1. Operation of the watchdog detection technique

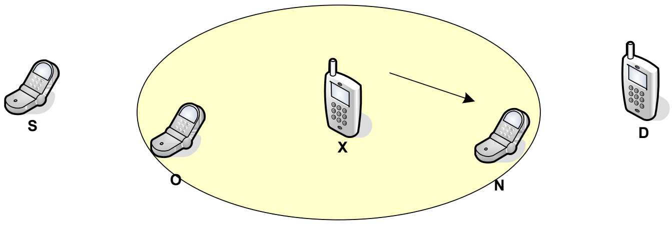

Figure 2. Operation of the recommended reputation technique

B. Reputation-based selfishness prevention protocols

The first SPP protocol considered in this work is the Watchdog protocol [6], referred to in the rest of the paper as WD. WD is made up of two modules: watchdog and pathrater. In the watchdog module, each node uses watchdog detection mechanism introduced in section II.A to watch the behaviour of relay nodes considering only direct reputation. Mobile nodes count the number of times that one node has refused to retransmit one packet, until the tally of faults is greater than the threshold considered. When the threshold is reached, the relay node is accused of being selfish. Besides, [6] introduced the pathrater module to calculate each neighbour's reputation using the information provided by the watchdog module. The pathrater assumes that past observations may be suitable to predict future selfishness of the nodes. If one node is accused of being selfish, it will be avoided in forthcoming route establishments. The WD protocol also introduces accusation messages to 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.

The second technique implemented in this work is the TEAM protocol [10]. This protocol uses three types of entry information to make a decision whether a node is acting selfishly: direct reputation, indirect reputation (as explained in section II.A), and recommended reputation, which is based on the list of nodes that have retransmitted the packet before. An example of recommended reputation is presented in Figure 2. In this figure, a multi-hop transmission is established from node *S* to node *D* through nodes *O*, *X* and *N*. When node *N* receives the retransmission of the packet from node *X*, it can estimate a new recommended reputation for node *O*, assuming that *O* has a good reputation in the opinion of *X*, as it has retransmitted its packet. In this way, when node *X* retransmits the packet, it implicitly 'recommends' node *O*. This can also be used to deduce an approximation of the reputation of node *S* in the opinion of node *O*, in a recursive manner. Each of these three reputation values (i.e. direct, indirect and recommended) is weighted to compute the global trust level for each node. Besides, TEAM also defines a trust formula for a route and for a packet, and establishes some rules to decide whether routing requests and data packets coming from other nodes should be accepted and/or retransmitted. These rules state that one route must not be accepted if its trust value does not exceed the trust threshold for a route. Similarly, one packet should not be relayed if its trust value does not exceed the minimum trust threshold for a packet.

III. Evaluation Platform

The aim of this work is to analyze the performance of potential reputation SPP techniques to be employed in future MCN-MR networks to foster relaying cooperation among nodes. It is also the aim of this paper to investigate the effect of realistic conditions, in particular with regards to the radio channel conditions and the channel congestion, on the operation of these techniques, and their capacity to accurately detect selfish nodes. In this context, this work focuses on a urban scenario with different congestion levels, and different radio conditions modeling accuracy. It is also important to adequately model the multi-hop ad-hoc communications protocols over which cooperation techniques will rely on. In this context, this work adopts the 802.11s mesh standard for the multi-hop ad-hoc communications and its reactive Ad-hoc On-demand Distance Vector (AODV) routing protocol.

A. Simulation scenario

Extensive system level simulations emulating the operation of multi-hop cellular networks have been carried out using the ns2 simulation platform and the Rice Monarch Project extension for mobile and multi-hop networks [12]. The simulation environment corresponds to a Manhattan layout of different dimensions, e.g. 900, 1350 and 1800 meters of side, where pedestrians move following the Random Walk Obstacle model [11] and communicate with a BS located at the centre of the scenario using multi-hop transmissions. The number of nodes in each scenario has been adjusted to maintain a nodes' density of at least one node per 80 meters along a street; this value has been chosen to ensure the establishment of multi-hop routes. Two traffic patterns have been simulated to analyze the impact of channel congestion on the SPP performance. In the first one, there is only one simultaneous active user, and no simultaneous sessions are allowed. In the second one, 15% of nodes on average have an active traffic session simultaneously. In both cases, traffic sessions consist of web browsing transmissions with a variable number of pages as specified in [13]. The ad-hoc radio interface corresponds to the 802.11a standard operating at the 5.8GHz frequency band and transmitting with two different power levels, 17dBm and 20dBm, in order to analyze the impact of this parameter on SPP protocols performance.

B. Routing protocol

To allow for multi-hop ad-hoc communications, this work is based on the IEEE 802.11s standard for mesh networks. HWMP (Hybrid Wireless Mesh Protocol) is the default mandatory routing protocol defined in 802.11s, although it is open for the implementation of alternative routing protocols [14]. HWMP is a combination of AODV as a reactive routing protocol, and a proactive tree-based routing protocol. Given that the use of proactive routing protocols in mobile and wireless environments would result in a significant signalling load, this work is based on the AODV protocol implemented in the Monarch Project extension for ns-2, and it is used in parallel with TEAM and WD techniques.

AODV [17][15] is a reactive routing protocol that only searches and establishes a route when the source has information to transmit and does not know the route to reach the destination node; therefore overall network information is not required unlike proactive protocols. In this case, the source node sends a broadcast Route REQuest (RREQ) message that is retransmitted by neighboring nodes. When the destination node receives the RREQ message, it replies with a unicast Route REPly (RREP) message to confirm the route establishment. The reception of RREQ and RREP messages allow intermediate nodes to know their neighboring nodes in the route towards the source and destination nodes. In the original AODV protocol, 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.

Generally, reputation based systems need to be implemented on top of source routing protocols like Dynamic Source Routing protocol (DSR), letting every node in the route know the identity of the other nodes. Thus, every node receiving a route request is able to evaluate the reputation of all the nodes participating in the route, and is not restricted to consider only the source, destination and consecutive neighbour nodes, as it is the case in the original AODV protocol. Additionally, nodes can process multiple replicas of RREQs coming from different routes. To emulate this scenario, routing packets in our implementation include information about the identity of all the nodes it passed through in the route. In this context, it is important to note that Dynamic MANET On-demand (DYMO) routing protocol, successor to AODV protocol, include this characteristic in its definition [15]. Additionally, the AODV modification in 802.11s allows intermediate nodes to process multiple replicas of a routing packet more than once, so they can evaluate and optimize the cost function of multi-hop route. In this work, the metric function considered to measure the multi-hop link cost depends on the SPP protocol. WD evaluates first if the route is free of selfish nodes. In that case, the route with less number of hops will be chosen. If the two routes have an equal number of hops, then it chooses the route with greater reputation average. In TEAM, incoming route establishment packets must pass some consecutive tests in order to be accepted. First, previous node's trust must be greater than the minimum threshold established for trust checking. Then the trust levels of the source and destination nodes are checked separately, before checking the mean trust level of all the nodes participating in the multi-hop route.

C. Channel propagation models

Three different types of channel propagation models [7] have been considered. First, the ns2 default model, the 2Ray model, has been used as a reference due to its widespread usage in the literature. The 2Ray model considers a log-distance pahtloss model with log-normal shadowing. The numeric values for the pahtloss exponent and the shadowing standard deviation have been chosen as indicated in [16] for urban scenarios, 3.5dB and 4dB respectively. Next, a more realistic pathloss model, referred to as LOS-NLOS [7], developed in the European WINNER project [8] and that takes into account the presence of obstructions between transmitter and receiver, has also been implemented. Different expressions are used for the computation of pahtloss under LOS (*Line Of Sight*) and NLOS (*Non Line Of Sight*) conditions. Under LOS conditions, the pathloss is expressed as follows

$$PL_{LOS}(d[m]) = \begin{cases} 22.7\log_{10}(d[m]) + 41 + 20\log_{10}(f[GHz]/5) \\ \quad if\ d < R_{bp} \\ 40\log_{10}(d[m]) + 41 - 17.3\log_{10}(R_{bp}) + 20\log_{10}(f[GHz]/5) \\ \quad if\ d > R_{bp} \end{cases} \tag{1}$$

where

$$R_{bp} = 4\frac{(h_A - 1)(h_B - 1)}{\lambda} \tag{2}$$

d[m] is the distance between transmitter and receiver, h_A and h_B are their respective antenna heights, f is the carrier frequency, and λ is the wavelength in meters. For NLOS conditions, the pathloss can be expressed as

$$PL_{NLOS}(d_A[m], d_B[m]) = PL_{NLOS}(d_A[m]) + 20 - 12.5n_j + \\ + 10n_j \log_{10}(d_B[m]) \tag{3}$$

where

$$n_j = \max(2.8 - 0.0024 d_A[m], 1.84) \tag{4}$$

and d_A and d_B represent the transmitter and receiver distances to the closest intersection. The third implemented propagation model, referred to as Realistic model, adds to the previous LOS-NLOS pathloss model, the fast fading and shadowing effects. The fast 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 through 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 respectively. In addition, the spatial autocorrelation characteristic of the shadowing has been modelled through the Gudmunson model [7].

In the 2Ray model the received power is only affected by the distance, while in the Realistic model the instantaneous received power may vary sharply in short distances or time intervals. Additionally, the presence of buildings in the Manhattan layout will strongly influence the performance of SPP protocols in both LOS-NLOS and Realistic models. In particular, the lack of direct visibility between nodes can force them to circumvent buildings in the route establishment process, which in fact increases the total distance covered by packets.

IV. Simulation Results

This work is aimed at investigating the performance of SPP techniques under realistic modelling conditions, in order to evaluate their capacity to detect selfish nodes that might prevent an adequate multi-hop connectivity in future MCN-MR networks. Such connectivity might be influenced by a large number of factors such as the number of selfish nodes, the radio propagation conditions or even the nodes transmission power. In this context, Figure 3 summarizes the connectivity studies that have been conducted in this work, that are discussed in detail in this section. Different parameters affecting connectivity are shown on the left side of the figure. The influence of these parameters on some important factors, i.e. the percentage of true and false detections of the SPP, the mean hop distance, the mean distance between source and destination nodes, in this case a cellular BS, and the mean number of hops per transmission, has been analyzed, in addition to the resulting multi-hop connectivity. The conducted studies have shown that these parameters are related to each other. In Figure 3, sign '+' means that the two parameters are directly related, e.g. an increase in the power transmission will lead to an increase in the mean hop distance. Similarly, '–' means that an increase in one parameter leads to a reduction in the other one, e.g. an increase in the percentage of selfish nodes will reduce the connectivity of the network.

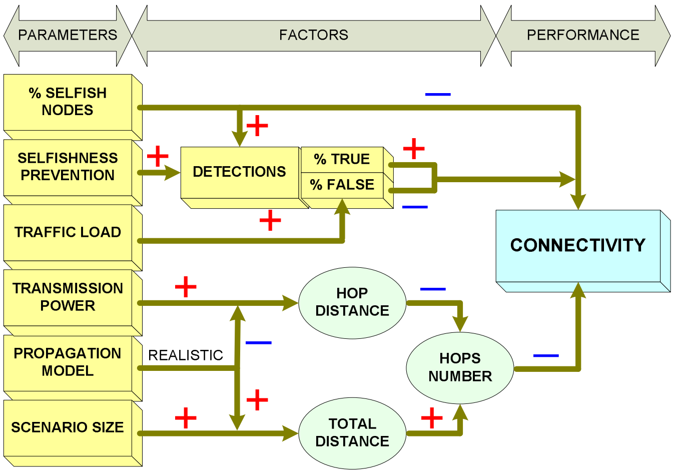

Figure 3. Factors influencing connectivity in MCN networks

One of the main factors influencing connectivity is the number of hops between source and destination, which is in turn affected by the transmission power, the channel propagation model and the number of nodes. As shown in Figure 4, the higher the number of hops between source and destination, the higher the probability of establishing a multi-hop route that includes a selfish node. If such selfish node cannot be detected with the SPP technique, the multi-hop connectivity will be severely constrained. Figure 4 represents the probability of choosing a not valid route, that is, a route with selfish nodes. It is assumed that the placement of the nodes in the route is random, so favorable cases divided by total outcomes can be applied to find this probability in equation (5); where *P* stands for probability of finding a route without selfish nodes, *nn* is the number of nodes in the scenario, *nh* is the number of hops and *rsn* is the ratio of selfish nodes. Figure 4 highlights that connectivity is severely degraded when the number of hops per transmission is increased in the presence of selfish nodes.

$$P = \prod_{i=0 \ldots nh-2} \frac{\lfloor nn(1-rsn) \rfloor - i}{nn - i} \qquad (5)$$

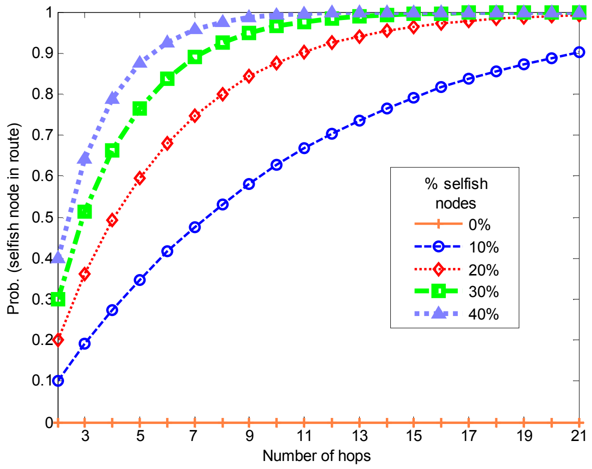

Figure 4. Probability of discovering a multi-hop route between source and destination with selfish nodes in it

A. *Multi-hop connectivity*

Table I shows the total multi-hop distance covered between source and destination for the received data packets at the destination node. The results are shown for different scenarios, varying the number of selfish nodes and the three implemented radio models. A transmission power of 17dBm and AODV routing protocol without any SPP technique are considered. The obtained results clearly highlight the impact of the radio propagation effects on the connectivity of the network. In fact, when there are no selfish nodes, the use of the Realistic and the LOS-NLOS radio models results in an increase above 25% of the total distance compared to when the 2Ray model is applied. Increasing the number of selfish nodes prevents distant nodes from finding a valid route. This reduces their multi-hop connectivity, and only routes with a short number of hops (and therefore total distance), are capable to forward the data packets to the destination node; this trend was already highlighted by Figure 4. As observed in Table I, and as it could be expected, increasing the dimensions of the simulated scenario also increases total multi-hop distance and therefore the difficulty to establish a long distance multi-hop route when selfish nodes are present (Figure 4). Table II depicts the mean and 95th percentile hop distance when varying the transmission power and the radio propagation modeling accuracy. The obtained results show that when accurately modeling the radio propagation, the hop distance is importantly reduced, irrespective of the transmission power.

TABLE I. MEAN MULTI-HOP DISTANCE FOR DATA PACKETS RECEIVED

Scenario size (m)	**Channel Model**	**% of Selfish Nodes**		
		0	***20***	***40***
1350	2Ray	555.21m	526.27m	489.95m
	LOS-NLOS	689.64m (+24.21%)[a]	559.01m (+6.22%)[a]	446.53m (-8.86%)[a]
	Realistic	705.41m (+27.05%)[a]	600.57m (+14.12%)[a]	470.94m (-3.88%)[a]
900	Realistic	482.57m (-31.59%)[b]	420.74m (-29.94%)[b]	369.85m (-21.47 %)[b]
1800	Realistic	913.63m (+29.52%)[b]	706.78m (+17.68%)[b]	512.32m (+8.79%)[b]

a. Percentage of increment compared to 2Ray model with a scenario size of 1350x1350m^2

b. Percentage of increment compared to Realistic model with a scenario size of 1350x1350m^2

TABLE II. MEAN HOP DISTANCE FOR DATA PACKETS RECEIVED

Hop Distance (m)		**Channel Model**		
	Power (dBm)	***2Ray***	***LOS-NLOS***	***Realistic***
Mean	17	301.38	166.75 (-44.67%) [a]	171.89 (-42.97)[a]
	20	400.90 (+33,02%)[b]	189.89 (+13.88%)[b]	198.12 (+15.26%)[b]
95th percentile	17	403.70	260.87 (-35.38)[a]	300.27 (-25.62)[a]
	20	546.46 (+35.36%)[b]	295.11 (+13.13%)[b]	352.09 (+17.26%)[b]

a. Percentage of increment compared to 2Ray model scenario

b. Percentage of increment compared to 17dBm transmission power scenario

TABLE III. MEAN NUMBER OF HOPS PER PACKET RECEIVED

Selfishness Prevention Protocol	**Propagation Model**	**Mean number of hops per packet**		
		0%	**20%**	**40%**
without SPP	2Ray	2.05	1.93 (-5.85%)[b]	1.80 (-12.20%) [b]
	LOS-NLOS	4.47 (+118.05%) [a]	3.43 (-23.27%) [b]	2.64 (-40.94%) [b]
	Realistic	4.61 (+124.88%)[a]	3.62 (-21.46%) [b]	2.75 (-40.35%) [b]
WD	2Ray	2.03	1.99 (-1.97%) [b]	1.99 (-1.97%) [b]
	LOS-NLOS	4.48 (+120.69%) [a]	4.06 (-9.38%) [b]	3.60 (-19.64%) [b]
	Realistic	4.61 (+127.09%) [a]	4.22 (-8.46%) [b]	3.89 (-15.62%) [b]
PD	2Ray	2.03	1.98 (-2.46%) [b]	1.94 (-4.43%) [b]
	LOS-NLOS	4.47 (+120.20%) [a]	4.38 (-2.01%) [b]	3.87 (-13.42%) [b]
	Realistic	4.61 (+127.09%) [a]	4.62 (0.21%) [b]	4.26 (-7.59%) [b]

a. Percentage of increment compared to 2Ray model scenario

b. Percentage of increment compared to 0% selfish nodes scenario

As previously explained, increasing the accuracy of the radio propagation modeling has increased the total multi-hop distance and reduced the hop distance. As observed in Table III this increases the mean number of hops needed to establish a multi-hop route from source to destination. The results marked as 'without SPP' correspond to the AODV routing protocol without any protection against selfish nodes. Perfect Detection (PD) refers to an idealistic technique that uses the AODV routing protocol and has a perfect knowledge of the identity of the selfish nodes at any time with zero signaling cost. These two techniques have been simulated to establish the SPP performance bounds. The obtained results show that similar trends are observed for the WD and TEAM SPP techniques. An interesting effect shown in Table III is that the reduction in the number of hops is more important as the number of selfish nodes increases when the radio propagation conditions are modeled more accurately. Under simplistic radio propagation conditions, the hop distance is large and there is only need for a short number of hops to reach the destination node. On the other hand, when the radio conditions are accurately modeled, the hop distance is reduced and the number of hops to reach the destination node increases. In this case, the presence of selfish nodes has a higher impact on the multi-hop route establishment. The results shown in Table III highlight that when no SPP technique is employed, the number of hops for the packets received decreases with the percentage of selfish nodes. This is the case because only routes without selfish nodes, or routes with only one hop, are able to reach the destination. On the other hand, when applying SPP techniques, selfish nodes can be detected and a higher percentage of multi-hop routes can be established. In this case, the reduction of number of hops with the percentage of selfish nodes is smaller.

B. Capacity to detect selfish nodes

The capacity of the SPP techniques to detect selfish nodes, and the probability to incorrectly accuse a non selfish node, can have a significant impact on the connectivity and probability to establish a multi-hop route from source to destination. As a result, the following parameters are defined to quantify the capacity to detect selfish nodes: positive sensibility and positive error rates. The watchdog detection technique is based on the promiscuous listening of packets that neighbor nodes have to relay. In this case, positive sensibility is the number of real forwarding denials detections (*RDD*, Real forwarding Denials Detections) divided by the number of times that selfish nodes are required to relay packets (*RSN*, Requests for Selfish Nodes). *RDD* refers to the number of occasions that a selfish node refused to relay a packet and this refusal was detected by the watching node. Similarly, positive error rate is the number of misunderstandings interpreted as forwarding denials (*FDD*, False Denial Detections) divided by the number of occasions that a non selfish node has to retransmit a packet (*RNSN*, Requests for Non-Selfish Nodes). *FDD* refers to the number of times that one node could not overhear correctly the retransmission of the packet by the next node due to channel propagation errors or collisions due to channel congestion.

$$S_+ = {}^{RDD}\!/_{RSN} \quad E_+ = {}^{FDD}\!/_{RNSN} \qquad (6)$$

Table IV shows the S_+ and E_+ rates for different scenarios. The first scenario corresponds to a medium size field with 238 nodes, 17dBm transmission power, no simultaneous sessions and the 2Ray radio channel model. To appreciate the influence of accurately modelling radio channel effects, in the second scenario the Realistic radio channel model is used instead. Simultaneous sessions are simulated in the third scenario to study the performance of the SPP protocols under channel congestion. The fourth scenario is similar to the third one but it reduces the size of the scenario and the resulting number of nodes to 114. The fifth scenario studies the influence of increasing the transmission power from 17dBm to 20dBm.

Both WD and TEAM protocols perform well in the simplest and less modelling accurate scenario, with S_+ near 100%. Moreover, positive detection in TEAM keeps performing well in all the scenarios, which means that almost all selfish misbehaviours are detected by TEAM nodes in all the scenarios. On the contrary, S_+ for WD degrades 4% when considering realistic radio channel effects in the second scenario, and around 9% with channel congestion in scenario 3. As it was mentioned in section II.A, this degradation of the detection capacity of WD corresponds to the number of occasions that link failures, radio channel errors or collisions where detected before the relay node was accused. The value of the S_+ parameter does not change when varying the dimensions of the simulation area or the transmission power, in the fourth and fifth scenarios respectively. On the other hand, accurate modelling of channel propagation effects in the second scenario leads to an increase in the number of times that one non-selfish node is falsely accused, reflected in the positive error rate E_+. This is due to the difficulty of the watchdog detection mechanism to distinguish between radio channel errors and packet dropping by selfish nodes, as described in section II.A. It was shown in previous section IV.B that the number of hops needed to establish a multi-hop transmission increases in case of accurate radio channel modelling (second and third scenario). As a consequence of the increase in the number of hops, and the difficulty of watchdog mechanism to detect selfish nodes when radio channel effects are accurately modelled, nodes are more exposed to dropping attacks and are less capable to counteract them. The rise in false detections increases the percent false accusations in the realistic propagation modelling scenarios. However, it must be noticed that these two figures are not completely equivalent: false accusation rate is defined as the percent of false accusations divided by the total amount of accusations, while E_+ refers to the rate of false detections of non selfish nodes divided by the number of packets that a non selfish node was required to relay. One node may be detected by several other nodes but it may be only accused by some of them, when the tally of detections reaches the maximum faults threshold established in WD. It is also noticeable that even a not very high error rate of around 10% in WD leads to a rate of false accusations of around 35% in scenarios with channel congestion (3rd to 5th scenarios). The increase in false accusations difficults finding of a valid multi-hop route, as more non-selfish nodes are avoided in the route establishments.

As observed in Table IV, TEAM increases the positive error rate with respect to WD. While WD only uses first hand observations, TEAM computes also indirect reputation based on the observations of neighbors relaying packets on behalf of other nodes, which are only valid when the suspicious node and the vigilant node are visible to each other, as explained in section II.A. As this is not usually the case for indirect reputation, especially when considering LOS-NLOS conditions, TEAM E_+ significantly increases when accurately modeling the radio propagation effects, as shown in Table IV. However, indirect reputation inaccuracy has a moderate impact on the false accusations, due to the fact that the weight of indirect reputation is considerably lower than the direct reputation in the calculation of node trust in the TEAM protocol.

All these results clearly demonstrate the strong impact that the radio propagation and the traffic modeling accuracy have on the operation of SPP techniques, and in particular on their capacity to detect selfish nodes.

TABLE IV. CAPABILITY TO DETECT SELFISH NODES(%)

SPP	Parameter	Scenario				
		1	2	3	4	5
WD	S_+	98.59	93.87	89.76	90.55	91.14
	E_+	4.85	10.79	10.80	9.31	10.10
	False acc.	21.93	20.63	36.57	41.36	34.81
TEAM	S_+	99.98	99.30	98.70	98.86	98.97
	E_+	41.79	65.52	65.86	59.52	64.24
	False acc.	17.50	30.23	45.18	38.41	43.33

C. Packet delivery ratio

Figures 5 and 6 plot the Packet Delivery Ratio (PDR) achieved when modeling the radio conditions through the simplistic 2Ray model or the Realistic one, considering no simultaneous traffic sessions. The figures also show the percentage of packets lost due to unavailability of routes or due to link failures, the percentage of packets dropped by selfish nodes, and the percentage of packets dropped because of its 'untrusted' origin or route. PDR refers to the number of packets correctly received divided by the number of packets transmitted. In each figure, each group of five contiguous bars corresponds to a different SPP technique, while each bar represents a different percentage of selfish nodes. 'No SPP' refers to AODV routing protocol without any SPP running in parallel, in order to set a low performance bound. PD was implemented as an idealistic SPP technique to establish a high performance bound, since it is capable to identify all selfish nodes.

As observed in Figures 5 and 6, increasing the percentage of selfish nodes decreases the PDR and increases the percentage of packets dropped by selfish nodes, or dropped without a valid route, as was expected. Considering realistic channel propagation conditions in Figure 6 reduces the PDR considerably compared to Figure 5, while the percentage of packets dropped by selfish nodes is notably increased, due to the influence of accurate modeling of radio propagation effects on the detection capacity of SPP techniques, and the increment in the number of hops of multi-hop transmissions. PDR also degrades when modeling realistic channel effects in Figure 6 compared to Figure 5, even when no selfish nodes and no SPP are considered. In the case of PD, the PDR reduction observed as the percentage of selfish nodes increases is due to the reduction of available multi-hop valid routes between the source and destination nodes, and the perfect isolation of selfish nodes. These effects are more appreciable when considering realistic channel modeling in Figure 6, where the number of hops in multi-hop transmissions between the source and destination nodes increases. For this reason, distant selfish nodes are completely isolated and non-selfish nodes are less capable to find a route without selfish nodes. On the contrary, Figure 7 shows that the WD protocol is unable to isolate selfish nodes when channel propagation is accurately modeled. PDR is represented separately for selfish nodes and for non selfish nodes. While PD manages to isolate selfish nodes, which obtain a very low successful delivery rate, PDR for selfish and for non selfish is almost equal in the rest of protocols (only WD and without SPP are shown for the sake of clarity, as the WD performance is very close to that achieved with TEAM). Only the selfish nodes that are able to establish a one hop transmission with the destination BS may bypass PD isolation, as shown in Figure 7. As observed in Figure 8, increasing the channel congestion through simultaneous traffic sessions also reduces the PDR for all SPP techniques irrespective of the percentage of selfish nodes, compared to Figure 6.

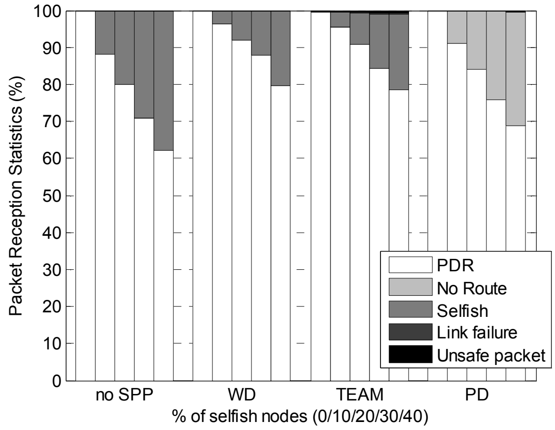

Figure 5. Statistics on packet reception when considering the 2Ray channel model and no simultaneous traffic sessions

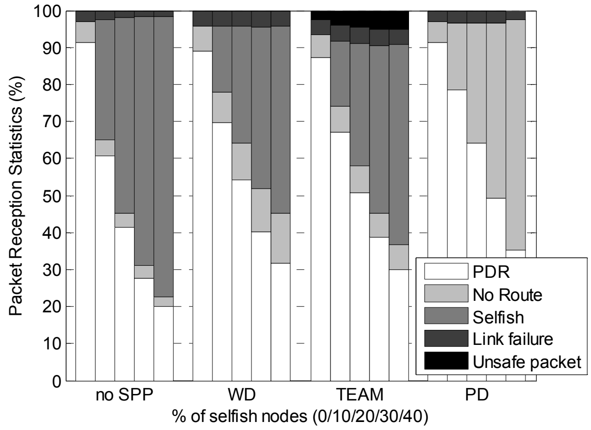

Figure 6. Statistics on packet reception when considering the Realistic channel model and no simultaneous traffic sessions.

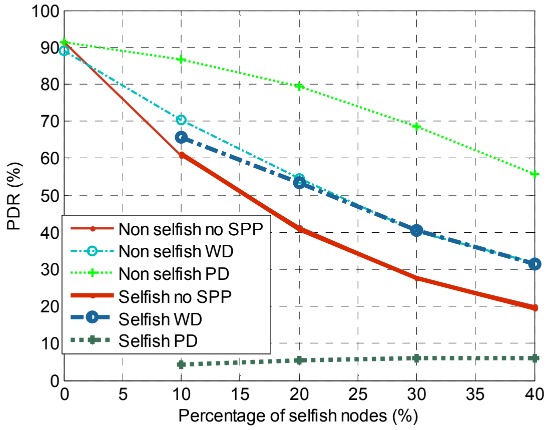

Figure 7. PDR for scenario with simultaneous traffic sessions when considering Realistic channel model and a 20% of nodes acting selfishly

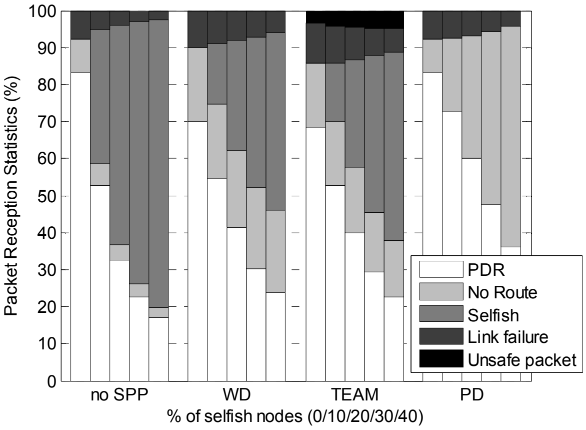

Figure 8. Statistics on packet reception when considering the Realistic model and simultaneous traffic sessions.

Numerical values of PDR and packet dropping for the scenarios mentioned in subsection IV.B are shown in Table V for comparison, and considering that 20% of nodes act selfishly. Improving the channel modeling accuracy in the 2nd scenario degrades PDR from 80.05% to 41.37% (no SPP protocol), and from 92.03% to 54.24% (WD protocol). Channel congestion due to simultaneous traffic sessions in 3rd scenario makes PDR fall to 32.70% and 41.46% respectively. Reducing the dimensions of the simulation area in the 4th scenario decreases the number of hops needed to transmit packets, as was shown in section IV.A. In this case, there is an increment in the PDR measured in the 4th scenario compared to the 3rd one. The reduced number of hops per multi-hop transmission when increasing the transmission power in the 5th scenario explains also the increment in the PDR. The obtained results shows that these traditional strategies for bit rate enhancement are also valid in the presence of selfish nodes, as they increase the PDR, but at the expense of reducing the number of hops between the source and destination nodes, instead of fighting against nodes acting selfishly.

TABLE V. PDR AND PACKET DROPPING FIGURES (%)

SPP	Parameter	Scenario				
		1	2	3	4	5
no SPP	*PDR* (%)	80.05	41.37	32.70	52.24	38.92
	No route (%)	0.01	3.94	4.00	4.94	2.11
	Selfish drop (%)	19.80	52.82	59.42	40.22	55.88
	Unsafe (%)	0.00	0.00	0.00	0.00	0.00
	Link fail (%)	0.14	1.87	3.88	2.60	3.09
WD	*PDR* (%)	92.03	54.24	41.46	59.28	52.26
	No route (%)	0.05	10.01	20.74	18.32	11.36
	Selfish drop (%)	7.76	31.43	29.87	17.63	29.69
	Unsafe (%)	0.00	0.00	0.00	0.00	0.00
	Link fail (%)	0.16	4.32	7.93	4.77	6.69

V. CONCLUSIONS

This work has investigated the impact that the radio channel modeling accuracy and operation conditions have on the performance and operation of selfishness prevention protocols. Such protocols are expected to play a main role in fostering cooperation among mobile terminals to achieve the expected benefits of MCN-MR networks. The reputation based techniques analyzed in this work are aimed at detecting and isolating selfish nodes that do not participate in the relaying of other nodes data, but benefit for their relaying capacity to retransmit their own data. The conducted studies have demonstrated the important impact of the radio channel propagation and channel congestion conditions on the performance and operation of SPP techniques, and in particular on their capacity to adequately detect selfish nodes. Based on these observations, the authors are currently working on improving the WD and TEAM protocols under realistic operating and modeling conditions.

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] Y. Lin and Y. Hsu, “Multi-hop Cellular: a new architecture for wireless communications,” *IEEE Proceedings Computer Communications (INFOCOM)*, vol. 3, pp. 1273-1282, 2000, Israel.

[2] B.Coll-Perales and J.Gozalvez, “Energy Efficient Routing Protocols for Multi-Hop Cellular Networks,” *Proceedings IEEE 20th Personal, Indoor and Mobile Radio Communications Symposium (PIMRC'09)*, September 2009, Tokyo (Japan).

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

[4] S. Buchegger, C. Tissieres, J.Y.Le Boudec, “A test-bed for misbehavior detection in mobile ad-hoc networks,” *Proc. IEEE Workshop on Mobile Computing Systems and Applications WMCSA,* Dec. 2004, pp.102 - 111.

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

[6] Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker, “Mitigating routing misbehavior in mobile ad-hoc networks,” *Proceedings of the International Conference on Mobile Computing And Networking ACM (MobiCOM 2000)*.

[7] Miguel Sepulcre, Javier Gozalvez, "On the importance of radio channel modeling for the dimensioning of wireless vehicular communication systems," *Proc. of the International Conference on ITS Telecommunications 2007*, ITST '07, June 2007, pp 1–5.

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

[9] Choong Hock Mar, W.K.G. Seah, “An analysis of connectivity in a MANET of autonomous cooperative mobile agents under the Rayleigh fading channel,” *Proc. Vehicular Technology Conference VTC 2005-Spring*., vol. 4, June 2005, pp. 2606–2610.

[10] V. Balakrishnan, V. Varadharajan, U. Tupakula, P. Lues, “TEAM: trust enhanced security architecture for mobile ad-hoc networks,” *Proc. IEEE International Conference on Networks*, *ICON 2007*, pp.182–187.

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

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

[13] UMTS 30.03 v3.2.0 TR 101 112 “Selection procedures for the choice of radio transmission technologies of the UMTS”, ETSI, April, 1998.

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

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

[16] T. Rappaport, “Wireless Communications: Principles and Practice,” 2nd edition, Prentice Hall

[17] C. Perkins and E. Royer, “Ad hoc On-Demand Distance Vector Routing”, in IEEE Proceedings Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 90-100, 1999, USA