Telecommun Syst (2014) 57:181–195
DOI 10.1007/s11235-013-9786-y

Reputation based selfishness prevention techniques for mobile ad-hoc networks

Alberto Rodriguez-Mayol · Javier Gozalvez

Published online: 17 August 2013

Abstract Mobile ad-hoc networks require nodes to cooperate in the relaying of data from source to destination. However, due to their limited resources, selfish nodes may be unwilling to forward packets, which can deteriorate the multi-hop connectivity. Different reputation-based protocols have been proposed to cope with selfishness in mobile ad-hoc networks. These protocols utilize the watchdog detection mechanism to observe the correct relaying of packets, and to compile information about potential selfish nodes. This information is used to prevent the participation of selfish nodes in the establishment of multi-hop routes. Despite its wide use, watchdog tends to overestimate the selfish behavior of nodes due to the effects of radio transmission errors or packet collisions that can be mistaken for intentional packet drops. As a result, the availability of valid multi-hop routes is reduced, and the overall performance deteriorates. This paper proposes and evaluates three detection techniques that improve the ability of selfishness prevention protocols to detect selfish nodes and to increase the number of valid routes.

Keywords MANET · Mobile ad-hoc networks · Selfishness · Reputation techniques · Watchdog

1 Introduction

The Internet Engineering Task Force (IETF) MANET (Mobile Ad hoc NETwork) working group describes MANETs as autonomous networks comprised of free roaming nodes (wireless communication devices) [3]. These nodes can communicate with each other either directly (single-hop) or indirectly (multi-hop) to perform the required tasks. In addition, nodes may be powered by an exhaustible energy source, and the link between them may be bandwidth-constrained. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. When data transfer is required between any pair of non-adjacent nodes, the network relies on the nodes between them to forward data packets. However, because mobile nodes are typically constrained by power and computing resources, a selfish node may not be willing to use its resources to always forward packets that are not of its interest, even though it would expect others to forward its packets [9]. In this context, encouraging the nodes' cooperation in the packet relaying process is of primary importance [17].

The problem of selfish nodes has been widely studied in the MANET community [21], where Selfishness Prevention Protocols (SPP) have been proposed to encourage nodes to cooperate in network functions, and prevent intentional attacks from malicious nodes [14]. Different categories of SPP have been proposed to cope with the packet dropping caused by selfish nodes refusing to relay other nodes' packets: reputation-based [1], credit-based and those based on game theory [21]. Credit-based schemes use a virtual or real currency to pay for self originated data retransmitted by other nodes. Credit is also used to compensate for the utilization of resources in the relaying process. Nodes can also gain credit by retransmitting other nodes' packets or by exchanging real money. The lack of scalability, centralization, and the need for a tamper-proof hardware are some of the potential limitations of the credit based schemes [21]. Game theory models simulate a game where each mobile

A. Rodriguez-Mayol (✉) · J. Gozalvez
Uwicore, Ubiquitous Wireless Communications Research Laboratory, University Miguel Hernandez of Elche, Avda. de la Universidad, s/n, 03202 Elche, Spain
e-mail: f.rodriguez@umh.es

J. Gozalvez
e-mail: j.gozalvez@umh.es

node can choose either to retransmit other nodes' data or not. Equilibrium stability of different strategies can be studied analytically [18]. However, game theory models usually fail to reproduce important parameters of real systems. Game theoretic studies usually assume unrealistic scenario conditions, and underestimate the importance of the wireless channel unreliability in the detection accuracy of misbehaving nodes, with few exceptions [22]. In addition, [22] highlights that the repeated game model, which is widely used in the literature to model the nodes' cooperation strategies, is not directly applicable to mobile ad-hoc networks.

This study focuses on reputation-based SPP techniques in which nodes register the observed behavior of other nodes (i.e. whether they relay packets or not) generally using the watchdog detection technique proposed in [12]. Other techniques have been proposed to replace the watchdog and monitor the correct relaying of packets by neighboring nodes. The TWOACK scheme proposed in [10] is an alternative detection technique that makes use of extra acknowledgement packets to avoid the potential watchdog's detection inaccuracy. However, it results in additional system overhead. Other detection methods like [8] consider statistical data of the reception of frames at the data link layer to derive the identity of potential misbehaving nodes. Nevertheless, the accuracy of probability-based detection methods depends on the compilation of a large set of observations, which may not be rapidly available. Watchdog is the most referenced detection method, and was first introduced in [12], and utilized in [13] and [2]. When implementing watchdog, each node launches a "watchdog" to monitor its neighbors' packet forwarding activities. Following [12], Core was proposed to enforce cooperation among selfish nodes [13], using watchdog to identify and isolate misbehaving nodes. More recently, TEAM introduced the concept of indirect observation, which is a generalization of the watchdog detection method [2], and also proposed the use of recommendations to complement the information provided by the watchdog detection technique. All these concepts will be fully discussed in Sect. 3, where the TEAM protocol is also explained.

Reputation-based SPP protocols using the watchdog detection technique are fully distributed, and generally exhibit good performance and an efficient use of the wireless communications channel [4]. However, previous studies showed that the evaluation of these protocols under simplistic operating conditions can provide inaccurate indications about their operation and performance [16]. In particular, the authors demonstrated the important impact of the radio propagation conditions and packet collisions on the expected performance of reputation based SPP techniques. Based on these observations, this work proposes three novel strategies to improve the operation and performance of reputation-based cooperation schemes in MANETs, and evaluates their operation under realistic conditions.

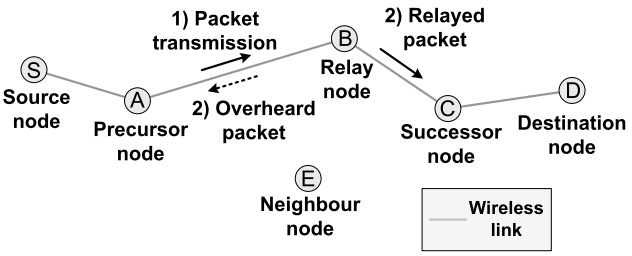


Fig. 1 Operation of the watchdog detection technique

2 Watchdog detection technique

SPP protocols are aimed at detecting and isolating selfish nodes in order to encourage them to cooperate in multi-hop communications. Reputation-based protocols are usually made up of two modules: detection and reaction. Each node uses its detection module to observe whether neighbor nodes retransmit or not packets from other nodes. The reaction module is in charge of updating a reputation table in which each neighbor node is assigned a rating level following the observations made by the detection module. This information can then be used by routing protocols to select a multi-hop route free from selfish nodes. In addition, selfish nodes could be isolated from the participation and establishment of multi-hop communications. The majority of reputation-based SPP protocols employ the watchdog detection technique [12]. This technique 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 Fig. 1. From here onwards, the scenario depicted in Fig. 1 will be used to explain the operation of the SPP protocols.

In the example shown in Fig. 1, the source node (S) establishes a multi-hop route to transmit its data packets to the destination node (D). In particular, the packets from the source node are transmitted following the multi-hop sequence S, A, B, C and D. In Fig. 1, a packet originated in the source node is being transmitted from node A, which has the role of a precursor node in the current transmission, to node B, which has the role of a relay node (step 1). A packet buffer in the precursor node keeps a temporary copy of the transmitted packets that have to be forwarded by the relay node. Each packet buffered is assigned a timeout within which the packet has to be forwarded to the successor node, in this case node C, by the relay node. If the relay node transmits the packet within the timeout (step 2), this transmission is overheard by the precursor node, and the relay node is noted to have cooperated correctly. This will be referred to as 'packet forwarding detection'. The precursor node looks for the copy of the packet relayed that was stored in its buffer, and removes it from the buffer. If the relayed packet is not overheard correctly by the precursor node within the timeout, then the relay node is assumed

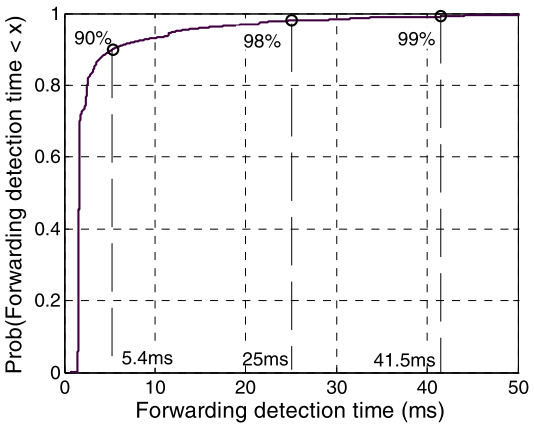


Fig. 2 Cumulative distribution function of the forwarding detection time

to have acted selfishly, i.e. it has dropped the packet. Similarly, this is referred to as a 'packet dropping detection'. Such dropping is reported to the reaction module, which can then downgrade the reputation rating of the relay node in the reputation table of the precursor node. Depending on the implemented SPP technique, two types of reputation can be distinguished: direct and indirect. Direct reputation corresponds to the case that has been previously explained, where it is the precursor node which observes the behavior of the relay node. Alternatively, in Fig. 1, a neighbor node *E* could indirectly observe the relaying of the packet from the precursor node to the relay node, and then from the relay node to the successor node.

The *Packet Timeout* is the time within which the relay node must forward a packet it has received from another node. In this context, the forwarding detection time refers to the interval between the instant at which the copy of the packet that has to be forwarded is stored at the buffer of the precursor node, and the instant when it is correctly overheard and removed from the buffer. The forwarding detection time includes the sum of all delays introduced during the transmission of the packet from the precursor to the relay node. Packets are correctly overheard only when the *Packet Timeout* is larger than the forwarding detection time. A too large value of the *Packet Timeout* increases the time necessary to detect nodes acting selfishly, while a too short one may prevent the relay nodes to retransmit the packets in time, increasing the inaccuracy of the selfishness detection process. Simulations were conducted to find an adequate balance for the *Packet Timeout* parameter. The conducted simulations used the platform described in Sect. 5 and considered that all nodes cooperated in the relaying of the packets. Figure 2 represents the obtained CDF (Cumulative Distribution Function) of the forwarding detection time. In order to ensure that all relayed packets can be correctly overheard, the *Packet Timeout* has been selected to be larger than the 99th percentile of the forwarding detection time (i.e. 41.5 ms). In particular, the *Packet Timeout* has been set to 50 ms in this work.

The watchdog technique is used by the majority of reputation-based SPP protocols reported in the literature. However, radio propagation errors and packet collisions due to channel congestion can notably deteriorate the performance and the selfishness detection capability of the watchdog technique [16]. In the example illustrated in Fig. 1, packet collisions could prevent the precursor node to correctly observe the forwarding of the packet by the relay node. Reference [5] claims that packet collisions do not affect the watchdog's detection capability, even with high traffic load. However, the conclusion was extracted using a four laptop test-bed, which might be a too limited testing environment. Repeated incorrect dropping detections affecting one relay node lead to its incorrect accusation as selfish node, which would then prevent its participation in further multi-hop communications. As a result, the availability of routes without known selfish nodes, referred to as safe routes, can be severely reduced. This paper presents three techniques aimed at improving the capacity to detect and isolate selfish nodes of SPP protocols using the watchdog mechanism. The proposed techniques have also been designed to mitigate the negative effects resulting from the detection inaccuracy of the original watchdog detection mechanism in the presence of packet collisions and radio transmission errors. The proposed techniques can be adapted to be executed in parallel to any existing reputation-based SPP protocol. To demonstrate their flexibility, the performance of the proposed techniques will be analyzed considering two different SPP protocols: Marti's protocol proposed in [12], and the TEAM protocol presented in [2].

3 Reputation-based selfishness prevention protocols

3.1 Marti's selfishness prevention protocol

The first SPP implemented in this work was proposed in [12], and it is referred to in the rest of the paper as Marti's protocol. In Marti's protocol, each precursor node uses the watchdog detection technique to observe the behavior of the relay nodes. A reputation table is maintained in each precursor node to register the reputation and the number of faults of every other known node, following the information collected by the watchdog technique. A heuristic algorithm, which is explained below,[1] is then executed to select the route most likely to be reliable, i.e. without selfish nodes.

Each node counts the number of times that a relay node has refused to retransmit its packets. When the number of

[1] Unless otherwise stated, the numerical values of the implementation parameters are chosen following the indications in the original implementation of Marti's protocol [12] (see Table 1).

Table 1 Marti's protocol main configuration parameters

Parameter	Value
Default Rating	0.5
Isolation Time (s)	500
Maximum Faults Threshold	5
Non-Accused Node Rating	0.0–1.0

faults is greater than a certain threshold, which is referred to as *Maximum Faults Threshold*, the relay node is accused of acting selfishly. The accusation lasts for a period referred to as *Isolation Time*, after which the node's reputation is restored. The *Isolation Time* parameter was not specified in the original Marti's implementation [12]. In this work, the *Isolation Time* has been set to 500 s, a value larger than the average duration of a user traffic session (151 s for the traffic model implemented in this work). The defined *Isolation Time* ensures that the technique is tested sufficiently during the simulation time. In addition, each node is assigned a reputation rating, which starts at the *Default Rating* and is updated following the observations made by the detection module (additional details can be found in [12]). The rating of a non-accused node is in the range [0.0–1.0]. If one node is accused of acting selfishly, its rating is set automatically to a highly negative value (*Selfish Node Rating*).

The exact value of the *Maximum Faults Threshold* was not specified in Marti's original paper [12]. A trade-off between the speed and accuracy of the detection of selfish nodes must be considered to set its optimal value. A too large value will increment the number of packets that nodes acting selfishly drop before being accused. A too small value will increase the number of times that cooperative nodes are accused incorrectly, for example due to packet collisions or radio transmission errors. In this context, preliminary simulations for different values of the *Maximum Faults Threshold* parameter have been conducted to select its optimal value using the platform and simulation conditions reported in Sect. 5. The maximum PDR (Packet Delivery Ratio) achieved for non-selfish nodes is reached for a threshold equal to 5, which also guarantees the lowest PDR for selfish nodes. This is a desirable effect in order to encourage selfish nodes to participate in the relaying of packets from other users. PDR refers to the ratio of packets correctly received divided by the number of transmitted packets.

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. To establish a multi-hop link, the routing protocol tries to select a route without selfish nodes. To this aim, Marti's protocol calculates the *Trust Level Path* metric for each multi-hop route by averaging the rating of all the nodes participating in the multi-hop route under evaluation. Selfish nodes have a very negative reputation value, and therefore, the *Trust Level Path* metric for a route request with selfish nodes is negative and the request is automatically rejected. The selection of the route with the higher average reduces the probability of the participation of selfish nodes. Packet forwarding requests coming from identified selfish nodes are not accepted by Marti's protocol.

3.2 TEAM selfishness prevention protocol

The second SPP technique implemented in this work is the TEAM (Trust Enhanced security Architecture for Mobile ad-hoc networks) protocol [2]. TEAM is composed of a detection module and a reaction module. The detection module uses three types of entry information to make a decision on whether a node is acting selfishly: direct reputation, indirect reputation (using the watchdog detection technique), and recommended reputation. The trust of a node is the weighted sum of the three reputation levels, as shown in (1):

$$T_N^i(t_{a+1}) = \sum U^{type} \cdot \varpi_{N-i}^{type}(t_a), \tag{1}$$

where $\sum U^{type} = 1$, $type \in \{direct, indirect, recommended\}$, $T_N^i(t_{a+1})$ is the new trust level of the node i in the opinion of the node N, $\varpi_{N-i}^{type}(t_a)$ is the previous reputation level of type $type$ of the node i in the opinion of the node N, and U^{type} is the weight of each reputation type. Non-uniform weights are assigned to each type of reputation since the estimation of direct reputation is more reliable. The direct, observed, and recommended reputations for all other nodes are initialized to a default value, the *threshold-limit* Δ. The direct and indirect reputations levels are incremented or decremented when forwarded or dropped packets are detected. Also, when a node receives a packet that has to be forwarded, the recommended reputation of the nodes that have previously forwarded the packet are updated following the assumption that if a node forwards a packet from another node it implicitly recommends it (details can be found in [2]). If the trust level of a relay node is smaller than the threshold-limit Δ, the relay node is accused of acting selfishly for a period of time called the *Isolation Time*.

The reaction module of the TEAM protocol is required to perform the following trust computations: trust for a node, trust for a packet and trust for a route. The calculation of the trust for a node has been explained before. When an intermediate node receives a packet that has to be forwarded, it agrees to relay the packet only if the trust for the packet is at least equal to the threshold-limit Δ. In addition, when a node receives a *Route Request* (RREQ) or a *Route Reply* (RREP) message sent to discover and establish a new multi-hop route, the reaction module accepts the petition only if the trust for the route is greater than the threshold-limit Δ. The trust for a route corresponds to the average of the trust values assigned to every node in the route. Unless otherwise stated, the TEAM implementation parameters have been configured following the original TEAM proposal; these parameters are summarized in Table 2.

Table 2 TEAM configuration parameters

Parameter	Value
Direct Reputation Weight	0.75
Indirect Reputation Weight	0.15
Recommended Reputation Weight	0.15
Threshold-limit Δ	0.5
Reputation Range	−1.0–1.0
Isolation Time (s)	500

RAM technique
Packet forwarding detection event
  Is relay node categorized as cooperative? →
    YES: Is relay node's reputation smaller than default? →
      YES: Restore relay node's reputation
    Reset number of faults of relay node
    Packets pending to be relayed are not considered

Fig. 3 Pseudocode of the RAM technique

4 Reputation-based SPP detection proposals

As it has been previously mentioned, radio transmission errors and packet collisions can reduce the capability of the watchdog technique to accurately detect selfish nodes, and increase the number of occasions in which safe nodes are accused of acting selfishly. The detection accuracy of the observation technique is a crucial aspect for the correct operation of reputation-based SPP protocols. Incorrect accusations have several negative effects. Cooperating nodes that are incorrectly accused of acting selfishly are isolated unreasonably. Isolation of cooperating nodes will prevent them from reaching a destination node through multi-hop communications. Additionally, since incorrectly accused nodes will be avoided in multi-hop routes, the number of potential safe multi-hop routes is wrongly reduced. This will result in that some safe multi-hop routes will be underutilized, while other cooperating nodes will be overloaded by packet forwarding requests. In this context, this section presents three techniques proposed to enhance under realistic conditions the performance of SPP protocols using the watchdog technique as observation method. The proposed techniques are designed to prevent the undesirable effects of radio transmission errors and packet collisions in the accusation decisions.

4.1 RAM—reset activity mode

The first proposal, named Reset Activity Mode (RAM), aims to reduce the number of incorrect selfish accusations due to the highly variant radio channel or packet collisions. It is intended to be executed as an add-on in conjunction with any reputation-based SPP protocol, like the implemented Marti's and TEAM protocols. In the original implementation of these protocols, nodes accumulate good or bad reputation depending on their behavior observed by other nodes. If a node is repeatedly detected dropping packets, it will be accused of acting selfishly and will be isolated. However, this operation can result in inaccurate selfish accusations if a node is not capable to overhear the correct relaying of a packet by another node. This can be due to packet collisions caused by channel congestion, and to radio transmission errors that are mistaken for intentional packet droppings. To avoid these inaccurate accusations, RAM is proposed to increase the contribution of forwarding detection in the reputation of a node. The RAM technique reduces the number of incorrect selfish accusations by defining some actions to be taken by the precursor node after a packet forwarding detection. More specifically, when the watchdog module detects the forwarding of a packet by a relaying node, the reputation of the relay node in the precursor node's reputation table is reset to the default value assigned to an 'unknown' node if it was previously downgraded. The term 'unknown' node refers to a node that becomes visible to another one for the first time. Additionally, if the considered SPP protocol establishes that the precursor node has to count the number of faults that the relay node accumulates, this count is reset to 0. Finally, the packets that remain in the buffer are removed, and no dropping fault is computed. It is important to note that the RAM mode is not applied to nodes that have been accused of behaving selfishly, but only to nodes still categorized as cooperative. Selfish nodes will not be able to recover their reputation until the expiration of the *Isolation Time*. The pseudocode of the RAM proposal is presented in Fig. 3.

4.2 WM—warning mode

The Warning Mode (WM) proposal is also designed to prevent incorrect selfish accusations caused by radio transmission errors and packet collisions, but with a different methodology compared to RAM. In the original implementation of the reputation-based SPP protocols considered in this work, when the relay node exhibits bad behavior during a certain period of time, it is directly marked as selfish, and all the links in which the node is involved are broken. On the other hand, WM introduces an intermediate category, the 'suspicious' category, between a 'neutral' node and a node marked as 'selfish'. The 'suspicious' category operates as a warning for the nodes that are suspected of behaving selfishly. Before they are definitively marked as selfish, they have another chance to recover from bad reputation. When the conditions to make a selfish accusation are matched, the relay node is first marked as 'suspicious', and its links are broken temporally. These conditions can vary

depending on the considered SPP protocol. In Marti's protocol, a relay node is accused of acting selfishly when the number of faults exceeds the *Maximum Faults Threshold*. On the other hand, in the TEAM protocol, a relay node is accused of acting selfishly when its reputation becomes smaller than the *Threshold Limit*. 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 were neutral nodes, but the mechanisms that control the observation and the accusation of the nodes are readjusted to reduce the number of additional data packets dropped by potential selfish nodes. First, the timeout a relay node has to forward a packet is reduced by a factor α. This work sets the *Packet Timeout* for suspicious nodes to 25 ms ($\alpha = 0.5$) following the existing trade-off between the reduction in the time needed to eventually accuse a suspicious node, and the increment in the number of undetected forwarded packets. Preliminary simulations showed that a *Packet timeout* of 25 ms for suspicious nodes only resulted in 2 % of undetected forwarded packets. The WM reduction of the *Packet Timeout* targets to reduce the time needed to confirm that a suspicious node is really a selfish one. In this context, a single additional dropping detection is enough to accuse a suspicious node of acting selfishly. To this end, the accusation mechanism of the specific SPP protocol must be modified. When a packet dropping detection is reported, if the relay node has been previously marked as 'suspicious', it will be then accused of acting selfishly following the specific procedure established in the considered SPP protocol. If the relay node is not a 'suspicious' node, then no special modification of the original implementation of the SPP protocol is needed. On the other hand, if a precursor node detects that a 'suspicious' node is cooperating again, then its reputation will be reset to the level assigned by default to 'unknown' nodes in order to give the 'suspicious' node the chance to recover from previous bad reputation, which could have been provoked by packet collisions or radio transmission errors. The specific actions that must be taken to reset the reputation of a 'suspicious' node depend on the considered SPP protocol. For Marti's protocol, the faults count and the reputation level are reset. In the case of the TEAM protocol, direct and indirect reputations are considered separately, and restored to the *Threshold Limit* value established for 'unknown' nodes.

The improvement expected with WM comes from the fact that spurious radio transmission errors, fading and packet collisions provoke a damaging increment of incorrect selfishness accusations in the original implementation of the watchdog detection technique. On the contrary, using 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 re-established when communications conditions improve. Alternatively, if the 'suspicious' node is truly acting selfishly, then only few extra packet droppings will be allowed since its selfish behavior will be quickly detected and the node isolated due to the strict conditions established in WM for 'suspicious' nodes. It is also possible that a node and the precursor node that marked it as 'suspicious' never interact again due to the mobility of the nodes. In this case, no selfish accusation is made, but this is not harmful to the precursor node since it will not use the 'suspicious' node to relay its packets. The pseudocode of the WM proposal is presented in Fig. 4.

WM technique

Packet dropping detection event
- Is it a suspicious node? →
  - YES: Initiate node's definitive accusation
  - NO: Conditions for accusation are matched? →
    - YES: Mark node as suspicious
    - Break link and search another route
    - Adjust *Packet timeout*
    - NO: Follow protocol's indications

Packet forwarding detection event
- Is it a suspicious node? →
  - YES: Restore node's reputation
  - Reset number of faults
  - NO: Follow protocol's indications

Fig. 4 Pseudocode of the WM technique

4.3 RFM—reset failure mode

The Reset Failure Mode (RFM) aims to counteract false accusations provoked by link failures in the link between the precursor and the relay node, or the relay and the successor nodes, which can be caused by channel effects like fading or by the mobility of nodes. The MAC layer is responsible for detecting link failures and triggering a link failure event to inform the routing protocol. The routing protocol transmits a "Route Error" message to inform the nodes using the route that the link has failed. However, before the link failure event is triggered, some of the packets transmitted by the precursor node to the relay node may not have been relayed. As a result, the copies of the packets in the packet buffer of the precursor node will time out, and the rating of the relay node in the route will be deteriorated unreasonably.

To avoid this watchdog malfunction in the presence of link failures, the reputation of the relay node in the precursor node's reputation table is restored by RFM to the default value assigned to an unknown node. In addition, RFM removes the packets in the buffer of the precursor node that are pending to be forwarded by the relay node, irrespective

```
RFM technique
Link failure detection event
  Is relay node's reputation smaller than default? →
    YES: Reset relay node's number of faults
    Packets pending to be relayed are removed
    Restore relay node's reputation
```

Fig. 5 Pseudocode of the RFM technique

of their expiration time, since the node is not able to retransmit them. The implementation of RFM depends on the technique considered. When applied to Marti's protocol, if a link failure is detected, the rating of the relay node is evaluated. If it has been downgraded, it is reset to 0.5 and 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. If applied to the TEAM protocol, the RFM mode only modifies the reputation of the nodes since the number of faults parameter is not considered. In this case, the RFM mode increments the direct and indirect reputation levels proportionally to the number of packets np that were pending to be forwarded in the buffer of the precursor node at the moment of the link failure. In particular the reputation levels are adjusted as follows:

$$R_1 = R_0 + k \cdot np \tag{2}$$

where R_1 and R_0 represent the reputation levels (direct or indirect) after and before the adjustment performed by the RFM mode when a link failure is detected. The k parameter has been set to 0.1, which is the penalization applied to the direct or the indirect reputation of a node for dropping packets in the original implementation of the TEAM protocol. It has to be noted that the RFM mode exceptions 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.

A potential drawback of RFM is that reputation restoration due to link failures might, in few cases, increase the reputation of real selfish nodes. 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 yet discovered. 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 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 are more feasible. The pseudocode of the RFM proposal is presented in Fig. 5.

5 Evaluation environment

5.1 Ad-hoc routing protocol

To evaluate the capability of the techniques proposed in this paper to enhance the operation and performance of reputation-based SPP protocols, multi-hop communications need to be simulated, and an ad-hoc routing protocol needs to be implemented to select an optimum multi-hop route following the information provided by the SPP techniques. In this work, multi-hop communications are established using the Dynamic MANET On-demand (DYMO) routing protocol [6], successor to the AODV protocol. In the DYMO protocol, source nodes use Route REQuest (RREQ) messages to discover a new route to a destination. RREQ replicas are relayed by neighbor nodes until one of them reaches the destination. A RREP message is then generated and passed back to the origin to allow for the multi-hop route to be established. Routing packets include information about the identity of all the nodes it passed through in the multi-hop route so that every node receiving a RREQ or RREP message can immediately record a route back to the origin or destination. 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 a selected multi-hop cost function.

5.2 Simulation platform

System level simulations emulating the operation of multi-hop wireless networks have been carried out using the ns-2 simulation platform and the Rice Monarch Project extension for mobile and multi-hop networks [15]. The simulation environment corresponds to a Manhattan layout of 6×6 square-shaped buildings totaling a scenario of 1350×1350 m^2, where pedestrians move following the Random Walk Obstacle model [11]. The density of nodes has been set on average as equal to one node every 80 m along a street. This density allows for the establishment of multi-hop transmissions between random nodes, and therefore to test the performance of the proposed techniques in mobile ad-hoc networks. The initial distribution of the nodes is chosen randomly. Traffic sessions emulate web browsing transmissions based on the model reported in [19], with a fixed number of 5 pages per session and a fixed reading time between pages of 29.5 s. Each page is composed of 25 objects (packets) with an inter-arrival packet time of 0.0228 s. To consider potential channel congestion situations, 15 % of nodes on average have an active traffic session simultaneously. The simulated ad-hoc radio interface corresponds to the 802.11a standard operating at the 5.8 GHz frequency band, and transmitting with a fixed power level of 17 dBm.

The radio propagation effects are considered through the path loss, shadowing and multipath fading. The path loss

represents the local average received signal power relative to the transmit power as a function of the distance between the transmitter and the receiver. The shadow fading models the effect of surrounding obstacles on the mean signal attenuation at a given distance. The path loss is modeled following the urban micro-cell channel model proposed in the WINNER project [20], which differentiates between LOS (Line Of Sight) and NLOS (Non Line Of Sight) conditions. The work reported in [20] also indicates that the shadowing standard deviation should be set equal to 3 dB and 4 dB for LOS and NLOS conditions respectively. To account for the shadowing correlation properties, the Gudmunson model has also been implemented for this work. The multipath fading effect, resulting from the reception of multiple replicas of the transmitted signal at the receiver, is modeled through a Ricean distribution under LOS conditions, and a Rayleigh distribution under NLOS conditions.

The ns-2 simulation platform models the 802.11a MAC layer based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) and its DCF (Distributed Coordination Function) operation mode. The modeled MAC layer also includes the optional RTS/CTS (Request to Send/Clear to Send) mechanism. To reduce the complexity of system level simulations, the effects at the physical layer resulting from the probabilistic nature of the radio environment are modeled by means of Look-Up Tables (LUTs) following the results from [7]. These LUTs, extracted from link level simulations, map the Packet Error Rate (PER) to the experienced channel quality conditions.

6 Performance evaluation

The proposed techniques have been designed to enhance the detection accuracy of reputation-based SPP protocols that use the watchdog detection mechanism. Such enhancement would increase the overall network performance and connectivity thanks to improving the ability to rapidly and precisely identify cooperative and selfish nodes; this ability would in turn augment the number of safe multi-hop routes. In this context, Marti and TEAM protocols have been selected as benchmark techniques, and their original performance is compared against that achieved when they also implement the three proposed mechanisms.

Tables 3 and 4 show the improvement that can be obtained when combining the techniques proposed compared to the original Marti and TEAM implementations. WRAM refers to the combined use of WM and RAM. Correct route establishments refers to the number of times that a multi-hop route without selfish nodes was established, while incorrect route establishments refers to the case when the route includes selfish nodes. Reputation-based SPP protocols discard route forwarding requests if the node that receives the routing message detects that any of the nodes participating in the route is a known selfish node. This is referred to as route denials. Incorrect route denials refer to the case when no real selfish node actually participated in the denied route, while correct route denials indicate that a real selfish node was included in the route. Incorrect route denials are motivated by previous incorrect accusations due to repeated incorrect dropping detections provoked by radio transmission errors and packet collisions. The results reported in Tables 3 and 4 correspond to 20 % of selfish nodes. The results obtained for other percentages of selfish nodes follow similar trends, and are thus omitted for brevity reasons.

Table 3 Improvement obtained with the proposed techniques compared to the original Marti's protocol (%)

	RFM	WM	RAM	WRAM
Incorrect accusations	−24.45	−91.39	−59.58	−97.01
Correct accusations	−3.35	−46.59	−6.57	−51.5
Incorrect route establishments	2.47	45.92	−1.26	38.47
Correct route establishments	14.19	47.49	26.38	39.46
Incorrect route denials	−22.35	−76.51	−56.66	−94.27
Correct route denials	−5.78	−6.81	−10.36	−17.67

Table 4 Improvement obtained with the proposed techniques compared to the original TEAM protocol (%)

	RFM	WM	RAM	WRAM
Incorrect accusations	−37.16	−62.96	−76.01	−92.47
Correct accusations	−7.82	−10.7	−7.54	−15.51
Incorrect route establishments	5.3	24.8	−2.13	17.92
Correct route establishments	9.48	24.18	20.43	24.5
Incorrect route denials	−37.39	−73.48	−79.44	−95.22
Correct route denials	−11.62	−24.32	−20.48	−34.67

All the proposed techniques are capable to significantly reduce the number of incorrect route denials. Moreover, there is a high correlation between the decrease in the number of incorrect accusations, the decrease in the number of incorrect route denials, and the decrease in the percentage of lost packets due to the unavailability of safe routes (which will be discussed next). Incorrect route denials reduce the availability of safe routes, and therefore they reduce the multi-hop connectivity and the PDR (Packet Delivery Ratio, defined as the ratio of packets correctly received to the total number of transmitted packets). This negative effect of the original Marti's and TEAM implementations is mitigated with the techniques proposed in this work by reducing the number of incorrect accusations. Although all the proposed techniques significantly reduce the number of incorrect accusations, it is important to highlight the strong reduction achieved with WRAM; in both cases, the reduction in the number of incorrect accusations is higher than 90 %. This is

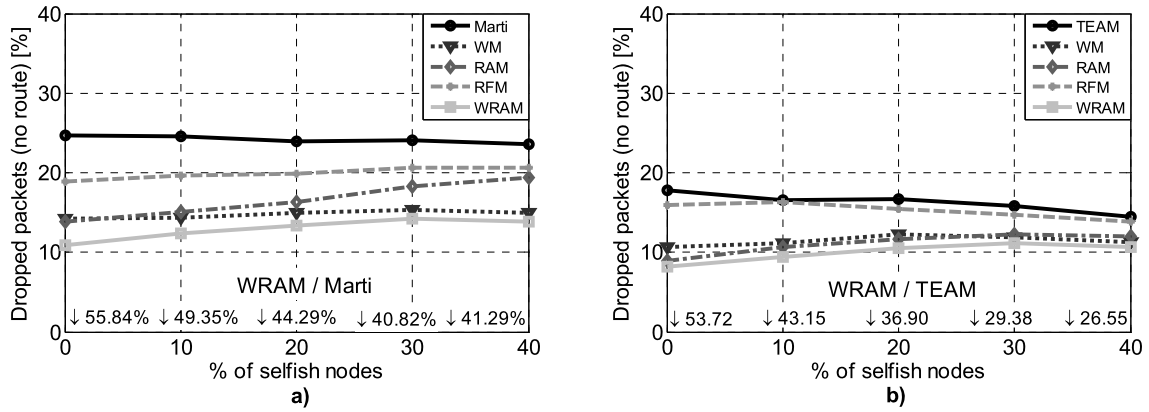


Fig. 6 Percentage of dropped packets without route for (**a**) Marti's and (**b**) TEAM protocols

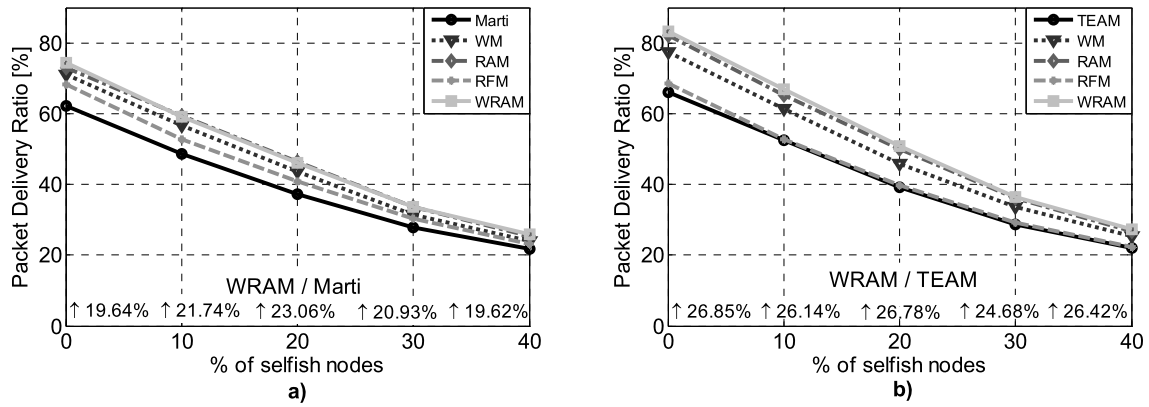


Fig. 7 Packet Delivery Ratio (PDR) as a function of the percentage of selfish nodes for (**a**) Marti's and (**b**) TEAM protocols

due to the individual contributions of each of the techniques proposed. In the case of RAM, whenever a forwarding detection occurs, the reputation of the relay node is restored if it was previously deteriorated unreasonably due to the accumulation of incorrect detections provoked by radio transmission errors and packet collisions. With WM, the introduction of the 'suspicious' category also contributes towards reducing the number of incorrect accusations. RFM achieves a reduction in the number of incorrect accusations in Tables 3 and 4 by restoring the reputation of a relay node if a link failure is detected before the node is accused of acting selfishly. Thus, the negative effects of link failures on the reputation levels are alleviated with the RFM proposal.

Figure 6 represents the percentage of lost packets due to the unavailability of safe routes as function of the percentage of selfish nodes. The results obtained when applying the proposed techniques are compared to Marti's (Fig. 6(a)) and TEAM (Fig. 6(b)) protocols. The terms TEAM and Marti in the figures (legend) correspond to the results obtained with their original implementation. For clarity, only WM, RAM, RFM and WRAM are included. The numbers included in the figures indicate the difference in performance between our best proposal and the original Marti's and TEAM protocols. It is important to note that increasing the number of available safe multi-hop routes results in a notable reduction of the percentage of dropped packets due to the unavailability of safe multi-hop routes.

The results reported in Tables 3 and 4 showed that the proposed techniques reduce the number of correct route denials, with the reductions being more significant for the techniques using the warning mode, i.e. WM and WRAM. This is due to the operation of the 'suspicious' category in the warning mode that also reduced the number of correct accusations. Although this is not a desirable effect, Fig. 7 shows that overall it does not have a negative impact on the PDR. Figure 7 represents the PDR obtained by the different techniques proposed in this work when applied to Marti and TEAM. The ability to accurately detect selfish and cooperative relaying nodes with the techniques proposed in this work leads to a notable increase of the PDR with respect to the original SPP protocols. It can be appreciated in Fig. 7 that this increase is maintained with slight variations when the percentage of active selfish nodes changes. RAM achieves the greatest increment in PDR when applied

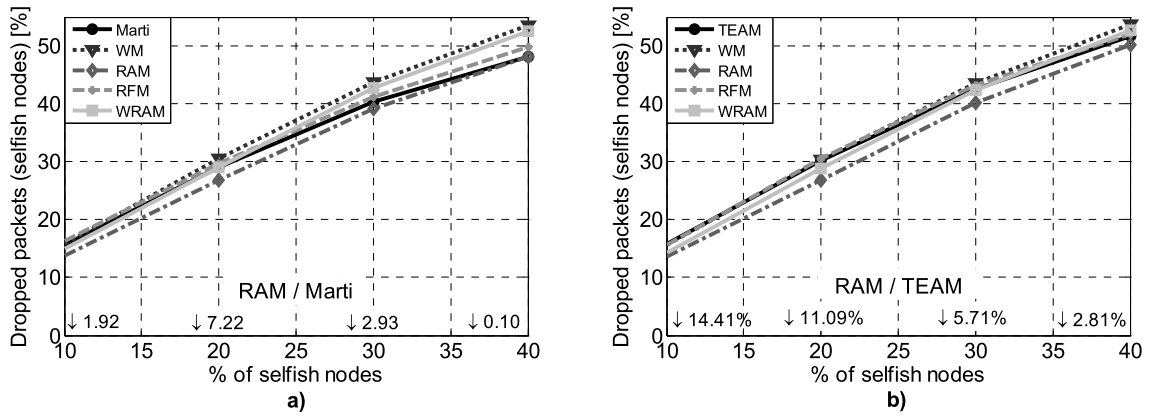


Fig. 8 Percentage of packets dropped by selfish nodes for (**a**) Marti's and (**b**) TEAM protocols

over Marti's protocol. However, when applied over TEAM, WRAM achieves a higher increment. The results depicted in Fig. 7 show than the increase in PDR obtained with the proposed techniques is in general higher when applied over TEAM than over Marti's protocol. However, the reduction in the percentage of lost packets due to the unavailability of safe routes (Fig. 6) is more important with Marti's protocol than with TEAM. This apparent contradiction is due to the fact that when combining the proposed techniques with the Marti's protocol there is a slight increase of lost packets due to link failures (this effect is discussed later). On the other hand, when the proposed techniques are combined with TEAM, a small reduction of lost packets due to link failures is observed.

The PDR performance is not only influenced by the percentage of lost packets due the unavailability of routes, but also by the percentage of packets dropped by selfish nodes (see Fig. 8). This factor is influenced by a combination of the reputation parameters shown in Tables 3 and 4. Reducing the number of incorrect route establishments, or increasing the number of correct route establishments, will decrease the percentage of packets dropped by selfish nodes. In addition, incrementing the number of correct accusations and the number of correct route denials will also reduce the number of packets dropped by selfish nodes. RAM is the only technique that reduces packets dropping in Fig. 8. As a result, only the combinations including RAM (WRAM) achieve a reduction or at least a minimum increase of the percentage of packets dropped by selfish nodes. This is because RAM is the only technique that reduces the number of incorrect route establishments in Tables 3 and 4. The rest of techniques, and in particular WM, increase the number of incorrect route establishments. When a node is accused of acting selfishly, WM breaks the link and marks the node as 'suspicious'. Route requests coming from 'suspicious' nodes are not rejected in order to rule out the possibility that the accusation was motivated by incorrect dropping detections. Thus, the WM proposal increases the number of incorrect route establishments, but also only slightly increases the percentage of packets dropped by selfish nodes (Fig. 8). This is due to the fact that the duration of routes with selfish nodes is short since 'suspicious' nodes are observed more tightly than neutral nodes. Therefore, if a 'suspicious' node is acting selfishly, one more dropping detection will be enough to accuse it definitively of acting selfishly, which consequently reduces the impact of increasing the number of incorrect routes establishments in the percentage of packets dropped by selfish nodes. The RFM proposal also increases slightly the packets dropped by selfish nodes in Fig. 8 due to the small increase in the number of incorrect routes established, and the reduction in the number of correct route denials (see Tables 3 and 4). This is motivated by the restoration of reputation performed by RFM in case of link failure. On occasion, the reputation of a selfish node may be restored because of a link failure if the node has not been accused yet of acting selfishly. However, the increase in the percentage of packets dropped by selfish nodes in the case of RFM is below 3 % in Fig. 8. As a result, the majority of selfish nodes are detected before a link failure is triggered. To decrease the packets dropped by selfish nodes in RFM and WM, it would be necessary to make the reputation protocols less tolerant to packet dropping, e.g. reducing the timeout or reducing the number of maximum faults, but this should be made carefully as it could in turn increase the number of incorrect accusations.

Another factor influencing the PDR performance in Fig. 7 is the percentage of lost packets due to link failures, which is illustrated in Fig. 9. The 802.11 MAC layer coordinates the access to the shared radio channel among the different mobile nodes through the Distributed Coordination Function (DCF) protocol. With radio-based networks, a transmitting node cannot listen for collisions while sending data, as it cannot sense the channel while transmitting a frame. As a result, the receiving node needs to send an ACK

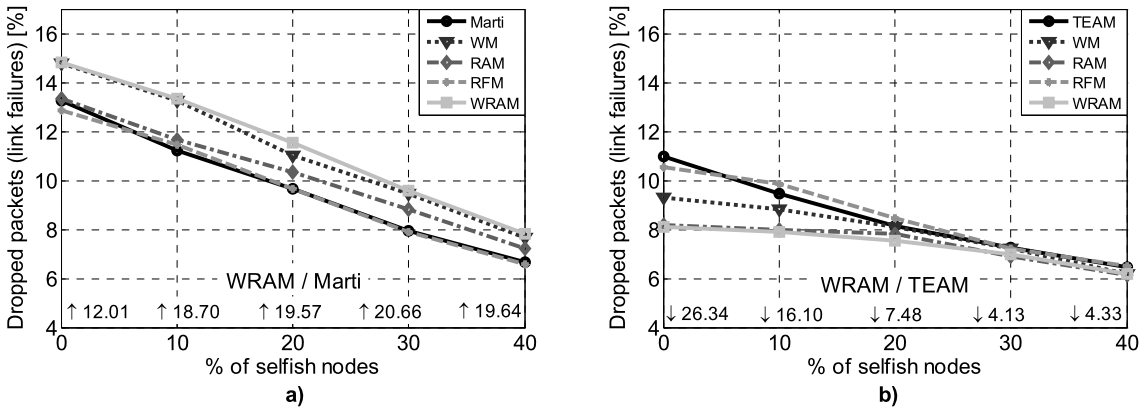


Fig. 9 Percentage of packets dropped due to link failures for (**a**) Marti's and (**b**) TEAM protocols

if no errors are detected in the received frame. If an ACK is not received by the transmitting node after a specified period of time, it will assume that collisions or radio propagation errors may have prevented the correct transmission of the packet, and will retransmit the frame. When the maximum number of retransmissions established is reached, the MAC of the transmitting node drops the packet, and reports a link failure to the upper layers. The routing protocol breaks the route and initiates a route discovery process if needed. Figure 9 shows that the percentage of lost packets due to link failures is higher for Marti than for TEAM. Moreover, the results in Fig. 9 show that when the proposed techniques are applied to TEAM, the percentage of lost packets due to link failures decreases compared to the original TEAM implementation; on the other hand, the opposite applies to Marti's protocol. The conditions that route discovery packets received by a relaying node have to match in order to be accepted and relayed are stricter for TEAM than for Marti's protocol (see Sect. 3). Marti's protocol only rejects route discovery packets when a selfish node is detected in the route. On the other hand, when a node receives a route discovery message to establish a new multi-hop route, TEAM evaluates whether the average rating of the nodes participating in the route is higher than the threshold-limit established. As a result, a greater number of route requests are forwarded with Marti's protocol, which increases the number of RREQ messages generated compared to TEAM. The routing overhead generated by Marti's protocol leads to an increased utilization of the communications channel, and the loss of MAC data frames as a result of packet collisions.

TEAM evaluates the ratio of every data packet that must be forwarded by a relay node. If the packet rating is smaller than the established rating threshold, the packet is discarded due to its unsafe origin (see Sect. 3). As expected, the important reduction in the number of incorrect accusations, and also in the number of correct accusations (see Table 4), leads to an important reduction of the number of unsafe packets

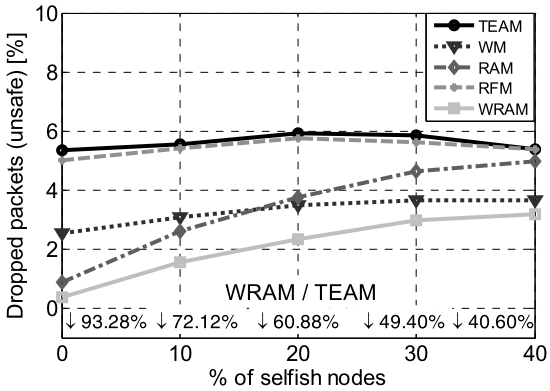


Fig. 10 Percentage of packets dropped by the TEAM protocol due to its unsafe origin

dropped by TEAM when the proposed techniques are also applied (Fig. 10). This in turn explains the increase of the PDR achieved with the proposed techniques when applied to TEAM (Fig. 7).

Figures 11 and 12 show the effect of varying the percentage of radio transmission errors on the main performance parameters. The figures compare the performance achieved with the WM, RAM, RFM, and WRAM proposals when applied to the original Marti and TEAM protocols.[2] The percentage of radio transmission errors has been modified by changing the transmission power level (14 dBm, 17 dBm and 20 dBm). Increasing the transmission power reduces the percentage of radio transmission errors, and augments the nodes' communication range. As a result, the mean number of hops per route decreases, and fewer packets are dropped because no route could be established. This results in a significant improvement of the PDR with the transmission power for all the techniques. Like in the default case

[2]The figures indicate the maximum improvement that can be obtained by any of the proposed techniques, as well as the mean percentage of radio transmission errors for each power level.

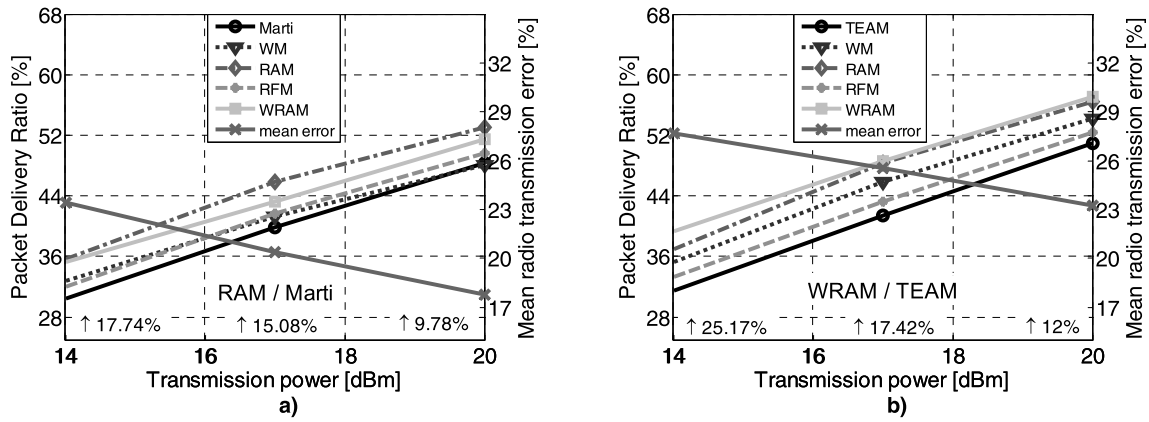


Fig. 11 PDR as a function of transmission power: (**a**) Marti and (**b**) TEAM

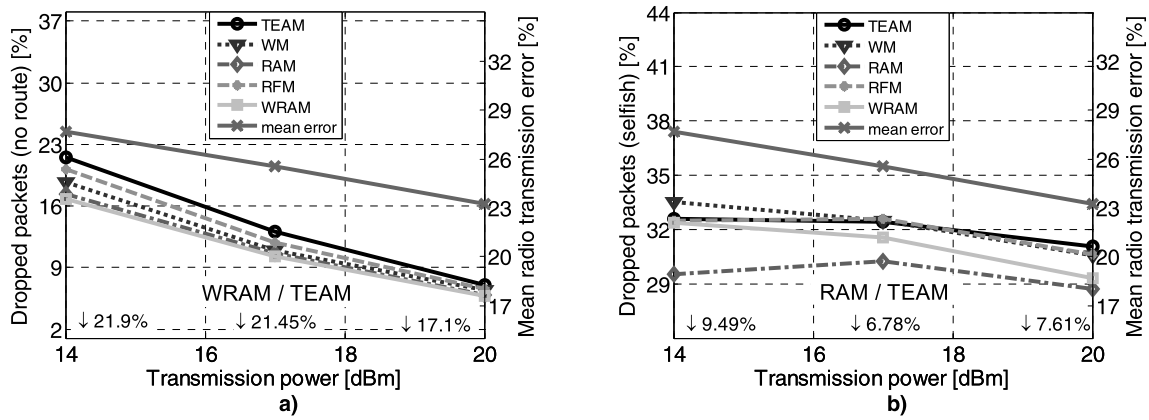


Fig. 12 Percentage of dropped packets as a function of transmission power: (**a**) without route and (**b**) due to selfish nodes

(17 dBm transmission power), only the RAM technique is able to reduce the number of packets dropped by selfish nodes. However, all the techniques proposed improved the PDR with respect to the original SPP protocol, with the improvement being larger as the transmission power is reduced.

The effect of varying the percentage of packet collisions has also been analyzed. To modify this percentage, the percentage of simultaneous active user sessions has been varied from 15 % (default case) to 65 %. This was obtained by reducing the mean interval between the start of sessions as the total number of users remained unchanged. The obtained results show that increasing the percentage of active sessions (and as a result the rate of packet collisions) increases the number of packets dropped without route (only TEAM results are shown in Fig. 14(a) for brevity) and decreases the PDR (Fig. 13), especially when only the original Marti or TEAM protocols are used. However, all the techniques proposed (in particular WRAM and RAM) considerably reduce the percentage of dropped packets with no route compared to the original Marti and TEAM protocols; the reduction increases with the packet collision rate. Increasing the percentage of active user sessions reduces the number of packets dropped by selfish nodes (Fig. 14(b)). This is because when nodes use more frequently the communications channel, they are more capable to learn the identity of selfish nodes, and as a result the number of incorrect route establishments decreases (and the number of correct route denials increases). Figure 15(a) shows the number of route establishments with selfish nodes (normalized by the percentage of active user sessions to make a fair comparison) using the TEAM protocol and the proposed techniques. Figure 15(b) shows the number of correct route denials. The obtained results show that the improvements obtained with WRAM with respect to Marti and TEAM increase with the percentage of active user sessions (Fig. 13). This is due to the fact that as the percentage of active user sessions increases, the number of packets dropped by selfish nodes decreases (Fig. 14(b)), and there is only a slight increase in the number of packets dropped without route (Fig. 14(a)).

The results presented in this section have shown that the proposed techniques manage to increase the availability of

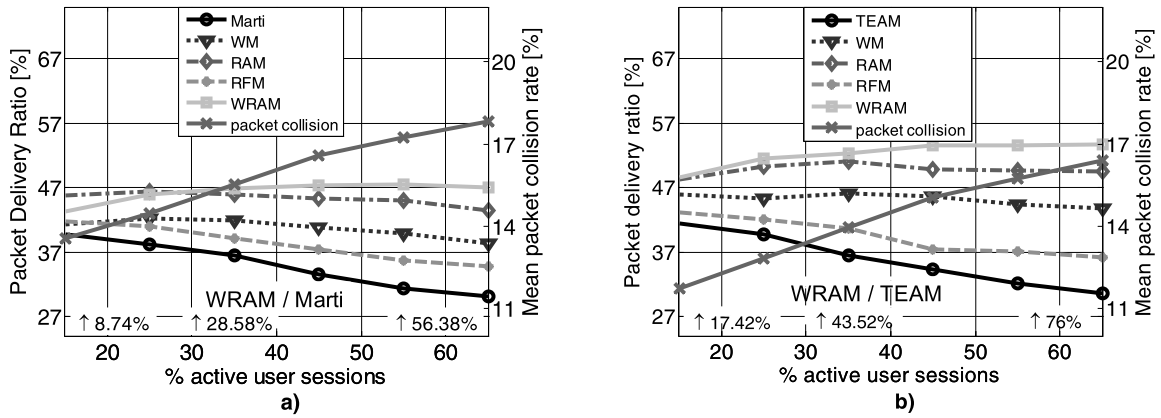


Fig. 13 PDR as a function of the percentage of active user sessions: (**a**) Marti and (**b**) TEAM

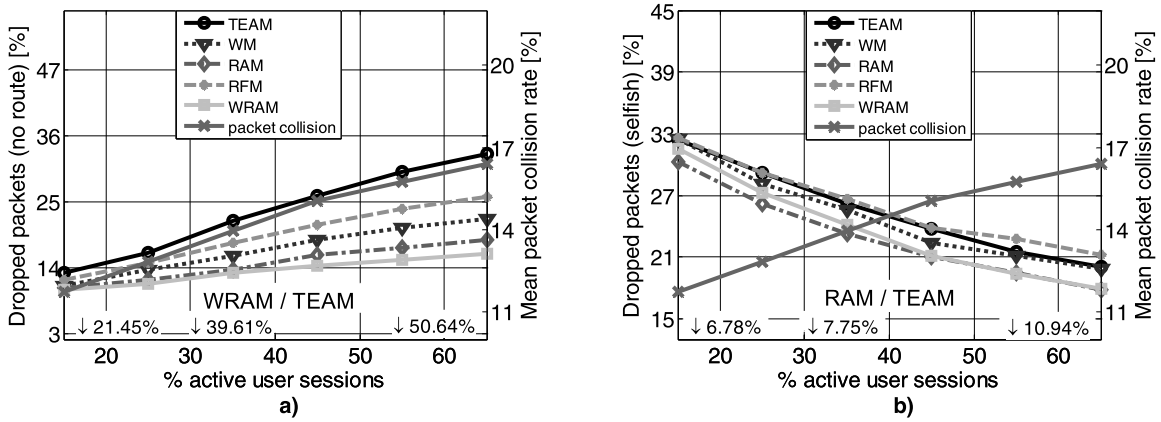


Fig. 14 Percentage of dropped packets as a function of the percentage of active user sessions: (**a**) without routes and (**b**) due to selfish nodes

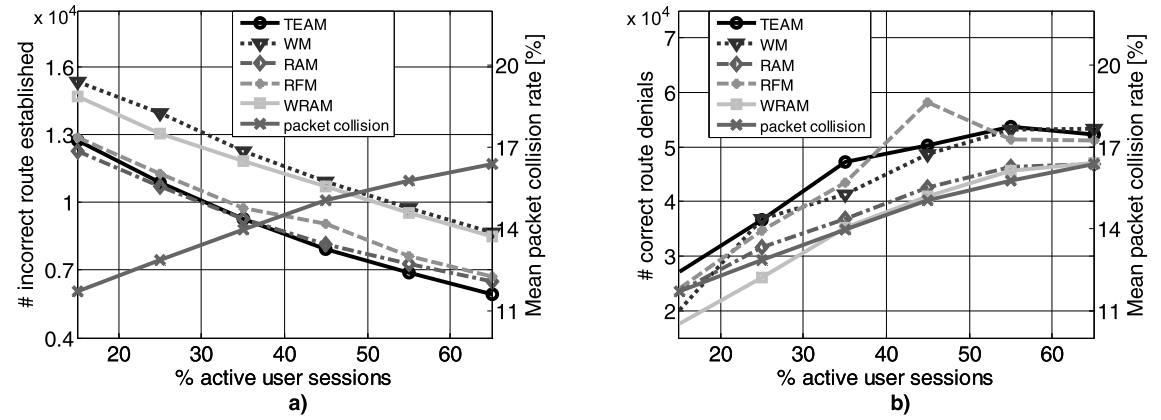


Fig. 15 Number of (**a**) incorrect routes established and (**b**) correct route denials as a function of the percentage of active user sessions

safe multi-hop routes that may be used by the nodes to establish links with distant peers. This in turn results in a noticeable decrease of the network latency, as shown in Table 5. Table 5 shows the latency reduction achieved by the proposed techniques with respect to original Marti's and TEAM protocols. The latency is measured as the time elapsed between the generation of a packet at the application layer in the source node and the correct reception of the packet in the destination node. The important increase of the availability of routes achieved with WM and its combinations explains their higher latency reduction compared to RFM and RAM.

Table 5 Latency reduction compared to the original Marti's and TEAM protocols (%)

	RFM	WM	RAM	WRAFM	WRAM
Marti	24.85	54.82	36.74	55.33	58.84
TEAM	23.62	43.86	24.46	52.95	43.84

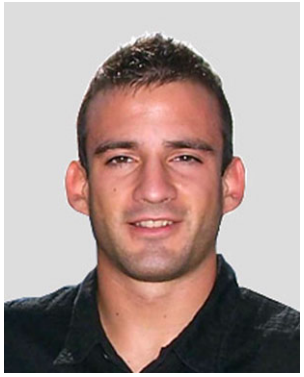
7 Conclusions

Mobile ad-hoc nodes are expected to forward packets to extend the communications range through multi-hop transmissions. However, selfish nodes may decide not to cooperate to save their resources while still using the network to relay their traffic. In this context, selfishness prevention protocols are designed to encourage nodes to cooperate in network functions, and prevent intentional attacks from malicious nodes. Reputation-based SPP techniques are fully distributed and can achieve good network performance, but are very dependent on reliable mechanisms to detect selfish nodes. Previous studies showed that traditional reputation-based SPP protocols tend to overestimate the selfish behavior of mobile nodes due to packet collisions and radio transmission errors that can be mistaken with intentional packet drops. To overcome these inefficiencies, this paper has presented and evaluated three techniques that improve the capability of SPP protocols to accurately detect real selfish nodes, and increase the performance of cooperative mobile ad-hoc networks. To evaluate their performance and applicability to any reputation-based SPP, this study has implemented the proposed techniques together with TEAM and Marti's protocols. The obtained results have demonstrated the capacity of the proposed techniques to reduce the number of incorrect selfish accusations, and increase the availability of safe multi-hop routes, thereby improving the final packet delivery ratio of mobile ad-hoc networks in presence of selfish nodes.

Acknowledgements This work has been supported by the Ministry of Science and Innovation (Spain) and FEDER funds under the project TEC2008-06728, by the Local Government of Valencia under the projects ACOMP/2010/111 and BFPI/2007/269, and by the Ministry of Industry, Tourism and Trade (Spain) under the project TSI-020400-2008-113 (CELTIC proposal CP5-013).

References

1. Aivaloglou, E., Gritzalis, S., & Skianis, Ch. (2007). Towards a flexible trust establishment framework for sensor networks. *Telecommunications Systems*, *35*(3–4), 207–213.
2. Balakrishnan, V., Varadharajan, V., & Tupakula, U. (2010). Trust management in mobile ad hoc networks. In S. Misra (Ed.), *Guide to wireless ad hoc and sensor networks* (pp. 473–502). London: Springer.
3. Balfe, S., Yau, P., & Peterson, K. G. (2010). A guide to trust in mobile ad hoc networks. *Security and Communication Networks*, *3*(6), 503–516.
4. Buchegger, S., Mundinger, J., & Le Boudee, J. Y. (2008). Reputation systems for self-organized networks. *IEEE Technology & Society Magazine*, *27*(1), 41–47.
5. Buchegger, S., Tissieres, C., & Le Boudee, J. Y. (2004). A test-bed for misbehavior detection in mobile ad-hoc networks. In *Proceedings of the IEEE workshop on mobile computing systems and applications WMCSA* (pp. 102–111).
6. Chakeres, I. D., & Perkins, C. E. (2006). Dynamic MANET On-demand (DYMO) routing. http://tools.ietf.org/html/draft-ietf-manet-aodvv2-02 (July 2013)
7. Choudhury, S., & Gibson, J. D. (2006). Joint PHY/MAC based link adaptation for wireless LANs with multipath fading. In *Proceedings of IEEE wireless communications and networking conference* (Vol. 2, pp. 757–762).
8. Dehnie, S., & Tomasin, S. (2010). Detection of selfish nodes in networks using CoopMAC protocol with ARQ. *IEEE Transactions on Wireless Communications*, *9*(7), 2328–2337.
9. He, Q., Wu, D., & Khosla, P. (2006). A secure incentive architecture for ad hoc networks. *Wireless Communications and Mobile Computing*, *6*(3), 333–346.
10. Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE Transactions on Mobile Computing*, *6*, 536–550.
11. Maeda, K., Uchiyama, A., Umedu, T., Yamaguchi, H., & Higashino, T. (2009). Urban pedestrian mobility for mobile wireless network simulation. *Ad Hoc Networks*, *7*(1), 153–170.
12. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad-hoc networks. In *Proceedings of the ACM international conference on mobile computing and networking MobiCOM* (pp. 255–265).
13. Michiardi, P., & Molva, R. (2005). Analysis of coalition formation and cooperation strategies in mobile ad hoc networks. *Ad Hoc Networks*, *3*(2), 193–219.
14. Nadeem, A., & Howarth, M. (2011). Protection of MANETs from a range of attacks using an intrusion detection and prevention system. *Telecommunication Systems*, 1–12.
15. Rice Monarch Project (2010). Wireless and mobility extensions to ns-2. http://www.monarch.cs.rice.edu/cmu-ns.html.
16. Rodriguez-Mayol, A., & Gozalvez, J. (2010). On the implementation feasibility of reputation techniques for cooperative mobile ad-hoc networks. In *Proceedings of the European wireless conference* (pp. 616–623).
17. Sundararajan, T. V. P., & Shanmugam, A. (2010). Modeling the behavior of selfish forwarding nodes to stimulate cooperation in MANET. *International Journal of Network Security & Its Applications (IJNSA)*, *2*(2), 147–160.
18. Thong, T., & Buttyán, L. (2011). On automating the verification of secure ad-hoc network routing protocols. *Telecommunication Systems*, 1–25.
19. UMTS 30.03 v3.2.0 TR 101 112. Selection procedures for the choice of radio transmission technologies of the UMTS. ETSI, 1998.
20. WINNER (2010). DI. 1.1. WINNER II Interim channel models. Public deliverable, http://www.ist-winner.org/.
21. Yoo, Y., & Agrawal, D. P. (2006). Why does it pay to be selfish in a MANET? *IEEE Wireless Communications Magazine*, *13*(6), 87–97.
22. Yu, W., & Liu, K. J. R. (2007). Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, *6*(5), 507–521.



Alberto Rodriguez-Mayol received a Telecommunications Engineering degree in 2005 and a Ph.D. in Telecommunications from the University Miguel Hernandez of Elche (Spain) in 2013. On April 2006, he joined the Uwicore research laboratory of the University Miguel Hernandez as a researcher working on the development of GIS-based WiMAX network planning platforms for rural areas. On April 2007, he obtained a Ph.D. fellowship from the Valencian Regional government. His Ph.D. research was focused in mobile and wireless communication systems, and in particular in studying the cooperation among nodes in multi-hop cellular networks.

Javier Gozalvez received an electronics engineering degree from the Engineering School ENSEIRB (Bordeaux, France), and a Ph.D. in mobile communications from the University of Strathclyde, Glasgow, UK. Since October 2002, he is with the University Miguel Hernandez of Elche, Spain, where he is currently an Associate Professor and Director of the Uwicore Laboratory. At Uwicore, he is leading research activities in the areas of wireless vehicular communications, radio resource management, heterogeneous wireless systems, and wireless system design and optimization. He currently serves as Mobile Radio Senior Editor of IEEE Vehicular Technology Magazine, and previously served as AE of IEEE Communication Letters. He was TPC Co-Chair of the 2011 IEEE Vehicular Technology Conference-Fall, TPC Co-Chair of the 2009 IEEE Vehicular Technology Conference-Spring, and General Co-Chair of the 3rd ISWCS 2006. He is also the founder and General Co-Chair of the IEEE International Symposium on Wireless Vehicular communications (WiVeC) in its 2007, 2008, and 2010 editions. He has been elected to the Board of Governors of the IEEE Vehicular Technology Society (2011–2013), and to the IEEE Distinguished Lecturers program of the IEEE Vehicular Technology Society.