TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES
Trans. Emerging Tel. Tech. 2013; **24**:582–588
Published online 20 June 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/ett.2545

RESEARCH ARTICLE

Detection mechanism for reputation-based selfishness prevention in MANETs

Alberto Rodriguez-Mayol* and Javier Gozalvez*

Uwicore Laboratory, University Miguel Hernandez of Elche, Avda. de la Universidad s/n, 03202 Elche, Spain

ABSTRACT

Mobile ad-hoc networks require users to cooperate in the relaying of data. Reputation-based selfishness prevention mechanisms are aimed at observing the behavior of nodes, and detecting and isolating selfish nodes that might drop packets. Mechanisms are therefore necessary to adequately and rapidly detect cooperative and selfish nodes. This work proposes a novel detection mechanism that outperforms the Bayesian techniques reported to date, and that can better cope with the unknown selfish behavior of nodes. Copyright © 2012 John Wiley & Sons, Ltd.

KEY WORDS

mobile ad-hoc networks; MANET; selfishness prevention; reputation; watchdog

***Correspondence**

Alberto Rodriguez-Mayol and Javier Gozalvez, Uwicore Laboratory, University Miguel Hernandez of Elche, Avda. de la Universidad s/n, 03202 Elche, Spain.

E-mail: f.rodriguez@umh.es; j.gozalvez@umh.es

Received 28 October 2011; Revised 14 March 2012; Accepted 13 April 2012

1. INTRODUCTION

To ensure adequate connectivity levels, mobile ad-hoc networks (MANET) require the cooperation of nodes to relay packets from source to destination [1]. Because nodes may refuse to cooperate (e.g., to save their battery, communications, and computing resources), the research community has been working over the past years in developing selfishness prevention schemes, such as those based on statistical methods [2], credit, reputation, or game theory [3]. Although other attacks like backoff misbehavior are possible [4], this work focuses on packet dropping attacks in which selfish nodes refuse to relay packets for other nodes. In this context, reputation-based strategies are in charge of detecting the cooperative or selfish behavior of nodes by overhearing their retransmissions, and registering their cooperation level in tables to build a trust system [5]. Such tables are used by routing protocols to select the most reliable routes by isolating identified selfish nodes.

Different techniques have been proposed to date to observe neighboring nodes and detect their cooperative or selfish behavior. One of the most relevant techniques because of its acceptance, simplicity, and efficiency (it does not introduce additional overhead in the observation process) is the watchdog technique [6]. With watchdog, a node (precursor node) that transmits a packet to a relay node will use the promiscuous mode of the media access control to observe the correct relaying of the packet within an established timeout. If such relaying is observed, a cooperative action is registered by the precursor node in the reputation table; otherwise, a selfish action is recorded. However, spurious radio transmission errors or packet collisions may prevent the correct observation of the retransmission, which would result in an incorrect selfish action being registered [7]. These incorrect registrations negatively impact the operation of the detection process, which has to decide whether or not a node must be accused of acting selfishly based on the evidence registered. Related studies base their detection process on a Bayesian approach [8, 9], which usually requires a large number of observations to reduce the probability of incorrectly accusing a cooperative node or failing to detect a selfish node. In this context, this work presents a novel exponential detection approach that outperforms the Bayesian techniques in terms of accuracy and speed of decision. To demonstrate its benefits, the proposed approach is applied over the watchdog mechanism.

2. BAYESIAN SELFISHNESS DETECTION

Let us consider a MANET network in which some of the nodes refuse, with probability p_s, to relay packets coming

from other nodes. p_s is a random variable with unknown probability density function $f_{ps}(x)$. Let p_e be the probability of error, that is, the probability that the observation technique mistakes a cooperative action as a selfish one. In watchdog, p_e is equivalent to the packet error probability because of radio transmission errors and packet collisions. Let D be the random experiment of the observation of the relaying action with two possible outcomes: $D = 0$ if a correct relaying is observed, $D = 1$ otherwise. Two reasons can prevent the precursor node to correctly observe the relaying of a packet: the relay node has discarded it with probability p_s, or the relaying has gone unnoticed with probability $(1–p_s)p_e$. This process is repeated with every transmitted packet conforming a Binomial process D_n with probability p_d:

$$Pr(D = 1) = p_s + (1 - p_s)p_e = p_d \tag{1}$$

After each new observation it must be determined if a node is acting selfishly ($p_s > 0$). This decision must be accurate to minimize the rate of Incorrect Accusations (*IA*) and of Incorrect No Accusations (*INA*),* and quick so that the number δ of selfish actions before a node is correctly accused of acting selfishly is also minimized.

The most extended detection mechanisms reported in the literature are variants of the Bayesian approach proposed in [8]. It assumes that p_s follows a Beta distribution Beta(α, β). α and β, initially equal to one, are incremented whenever a selfish or cooperative behavior is observed respectively. With a large number of observations, the real value of p_s is approximated by the expected value of Beta(α, β), which is used as a metric to decide whether a node is acting selfishly. Different Bayesian variants have been proposed based on this procedure. The first one, here referred to as BIW (Bayesian with Infinite Window) [8], defines the metric as $M_{BIW}(n, \alpha, l) = \frac{\alpha_n}{n}\big|_{n \geq l}$, where α_n is the number of selfish actions registered in the past n observations. n varies between l and N, with l representing the minimum number of observations required before the decision is taken and N the maximum observations before the connection ends. The second metric, referred to as BFW (Bayesian with Finite Window) and reported in [9], takes into account only the last l observations, and is defined as $M_{BFW}(n, \alpha, l) = \frac{\alpha_{n-l,n}}{l}\Big|_{n \geq l}$. Reference [8] proposes an additional metric, referred to as BDF (Bayesian with Discount Factor), which introduces a discount factor $u = 1 - (1/l)$. If s is the outcome of the last observation, α and β are updated as

$$\begin{aligned} \alpha_i &:= u\alpha_{i-1} + s \\ \beta_i &:= u\beta_{i-1} + (1 - s) \end{aligned} \tag{2}$$

The BDF selfishness metric is then computed as $M_{BDF}(n, \alpha, \beta, l) = \frac{\alpha_n}{\alpha_n + \beta_n}\Big|_{n \geq l}$. In addition, a BDF metric with finite window (BFWDF) can be defined as $M_{BFWDF}(n, \alpha, \beta, l) = \frac{\alpha_{n-l,n}}{\alpha_{n-l,n} + \beta_{n-l,n}}\Big|_{n \geq l}$.

An adequate operation of the Bayesian detection techniques require the proper selection of its configuration parameters (l and τ, with τ representing the threshold of the metric over which a node is accused of acting selfishly) to maximize the accuracy and speed of the detection process. The optimization of these parameters must take into account the parameters $f_{ps}(x)$ and p_e. While the value of p_e can be estimated in real time (see, e.g., [10]), the estimation of the $f_{ps}(x)$ function in a MANET is a difficult task. Additionally, a large number of observations might be needed to obtain an acceptable detection error rate, thereby increasing the number of selfish actions δ. To better understand the importance of the (τ, l) couple, their influence on the *IA* and *INA* parameters is next analytically derived for the BFW technique. If a large number of experiments are considered, the average *IA* and *INA* rates can be approximated by the probability of a cooperative node being accused of acting selfishly and the probability of a selfish node going undetected. Let the BFW detection method be modeled as a Markov chain process with two states: accusation (A) and no accusation (NA) (see Figure 1). It is possible to derive the following expressions for the probability of the initial states A_l and NA_l after the minimum mandatory l observations

$$\begin{aligned} Pr(NA_l) &= \sum_{i=0}^{\lfloor l\tau \rfloor} \binom{l}{i} p_d^i (1 - p_d)^{l-i} \\ Pr(A_l) &= \sum_{i=\lfloor l\tau \rfloor + 1}^{l} \binom{l}{i} p_d^i (1 - p_d)^{l-i} \\ &= 1 - Pr(NA_l) \end{aligned} \tag{3}$$

where τ represents the accusation threshold. These expressions represent the cumulative distribution function (CDF)

$$\begin{aligned} \Pr(NA \to A) &= (1 - p_d)^{l - \lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor + 1} \binom{l-1}{\lfloor l\tau \rfloor} \\ \Pr(NA \to NA) &= 1 - (1 - p_d)^{l - \lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor + 1} \binom{l-1}{\lfloor l\tau \rfloor} \\ \Pr(A \to A) &= 1 \\ \Pr(A \to NA) &= 0 \end{aligned}$$

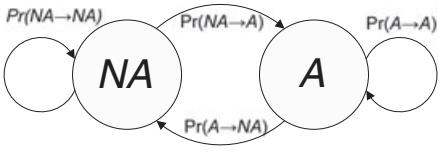

Figure 1. Markov chain states for the BFW detection process.

*IA is defined as the ratio of cooperative nodes incorrectly accused of being selfish and total number of cooperative nodes. *INA* is the ratio of non accused selfish nodes and total number of selfish nodes.

of the binomial distribution after l observations. The transitions between the two states are described by

$$\begin{aligned} Pr(NA \rightarrow A) &= (1-p_d)^{l-\lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor+1} \begin{pmatrix} l-1 \\ \lfloor l\tau \rfloor \end{pmatrix} \\ Pr(NA \rightarrow NA) &= 1-(1-p_d)^{l-\lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor+1} \begin{pmatrix} l-1 \\ \lfloor l\tau \rfloor \end{pmatrix} \end{aligned} \tag{4}$$

$$\begin{aligned} Pr(A \rightarrow A) &= 1 \\ Pr(A \rightarrow NA) &= 0 \end{aligned} \tag{5}$$

A is an absorbing state because once a node is accused of acting selfishly it will not leave the state. The probability of transition to the accusation state $\Pr(NA \rightarrow A)$ has been calculated using the binomial probability mass function. It can be proved using properties related to Markov chains that after n observations ($n > l$) the probabilities of NA and A can be expressed as follows:

$$\begin{aligned} \Pr(A_n) &= 1-\Pr(NA_l)\Pr(NA \rightarrow NA)^{n-l} \\ \Pr(NA_n) &= \Pr(NA_l)\Pr(NA \rightarrow NA)^{n-l} \end{aligned} \tag{6}$$

Following (4), (5), and (6), the *IA* and *INA* probabilities are presented next:

$$\begin{aligned} Pr(IA) &= 1-F(\lfloor l\tau \rfloor; l, p_e) \\ &\quad \times [(1-f(\lfloor l\tau \rfloor; l-1, p_e))\, p_e(1-p_e)]^{n-l} \\ Pr(INA) &= F(\lfloor l\tau \rfloor; l, p_d) \\ &\quad \times [(1-f(\lfloor l\tau \rfloor; l-1, p_d))\, p_d(1-p_d)]^{n-l} \end{aligned} \tag{7}$$

where F and f represent the Binomial cumulative and mass distribution functions, p_d and p_e are defined in (1).

Figure 2 highlights the dependence of the *IA* and *INA* probabilities with regards to the accusation threshold τ for various probabilities of nodes acting selfishly (p_s), and a fixed $l = 12$ and $p_e = 0.1$. A design objective would be to minimize *IA* and *INA*, although the plotted results show that both parameters follow opposite trends when varying τ. Moreover, the existing trade-off is narrower for nodes with low p_s. In fact, if p_s is larger or equal to 0.2, *IA* and *INA* can be simultaneously minimized at $\tau = 0.45$. However, τ should be fixed around 0.35 for p_s equal to 0.1, and still *IA* and *INA* cannot be reduced below 0.1. *IA* can be reduced by increasing the number of observations l, although this would also result in an increase of the number of packets dropped by selfish nodes (δ) before their selfish behavior is detected and the nodes are isolated. In this context, it is important to highlight that different distributions of p_s, unknown *a priori*, and different values of the estimated p_e, would require different optimal values of τ and l, which limits the performance and implementation perspectives of the Bayesian approach.

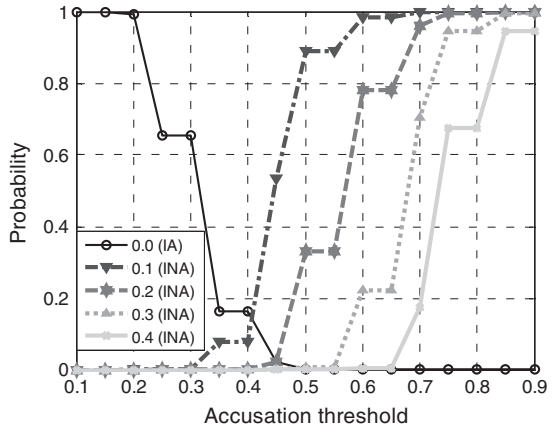

Figure 2. *IA* and *INA* as a function of the accusation threshold τ. The legend corresponds to different values of p_s.

3. EXPONENTIAL SELFISHNESS DETECTION

To overcome the limitations of the Bayesian selfishness detection techniques, this paper proposes a novel exponential mechanism. The proposal defines a new metric designed to test after every observation D_n if the number of selfish actions observed α_n is likely to have been provoked by a certain error probability of the watchdog technique p_e (because of radio transmission errors or packet collisions), or by the selfish behavior of the node. In this context, a function is needed to measure the probability that the (null) hypothesis "the observed selfish actions are due to the observation method's inaccuracy" is true. Following the Binomial modeling of the observation process, this paper proposes an exponential function F_e (8) based on an approximation of the binomial distribution function derived from the Hoeffding inequality [11]

$$F_e(\alpha; n, p_e) \approx \exp\left(-2\frac{(\Delta_-(np_e-\alpha_n))^2}{n}\right) \tag{8}$$

where Δ_- is defined as

$$\Delta_-(x) = \frac{x-|x|}{2} = \begin{cases} 0 & x \geqslant 0 \\ x & x < 0 \end{cases} \tag{9}$$

After each observation, the exponential function (8) is computed and its output stored. The proposed Exponential Infinite Window (EIW) metric is then defined as the average of all the stored outputs. On the other hand, the Exponential Finite Window (EFW) metric is computed as

Trans. Emerging Tel. Tech. **24**:582–588 (2013)
DOI: 10.1002/ett

the average of the last l outputs:

$$M_{\mathrm{EIW}}(n,\alpha,l) = \frac{1}{n}\sum_{i=1}^{n} \times\exp\left(-2\frac{(\Delta_-(i\,p_{\mathrm{e}}-\alpha_i))^2}{i}\right)\Bigg|_{n\geq l}$$
$$M_{\mathrm{EFW}}(n,\alpha,l) = \frac{1}{l}\sum_{i=n-l+1}^{n} \times\exp\left(-2\frac{(\Delta_-(i\,p_{\mathrm{e}}-\alpha_i))^2}{i}\right)\Bigg|_{n\geq l} \quad (10)$$

Differently from the Bayesian approach, the exponential detection proposal accuses a node of acting selfishly when the computed value of the exponential metric falls below the accusation threshold τ. In this case, it is important to note that τ is not directly related to the distribution of p_{s} among the set of nodes and the estimated p_{e}. This feature facilitates the selection of an adequate value of τ, and improves the implementation perspectives of the exponential proposal. This characteristic is further exhibited through Figures 3(a) and (b), where the solid line curves represent the CDF of the number of observed non-relayed packets α for different values of p_{s}. Non-relayed packets are packets that the precursor node observes as "non-relayed" by the relay node as a result of the watchdog's inaccuracy (p_{e}) or the relay node's selfishness (p_{s}). The CDF plots the probability that α stays below a certain level for $p_{\mathrm{s}} = \{0, 0.1, 0.3\}$ and p_{e}=0.1 in Figure 3(a) and p_{e}=0.2 in Figure 3(b). These CDFs are obtained by using the cumulative distribution function of the binomial distribution for $p = p_{\mathrm{d}}$ in (1). The dotted line curves represent the Bayesian metric (α/n) and the expression (8) used in the exponential proposal (10).

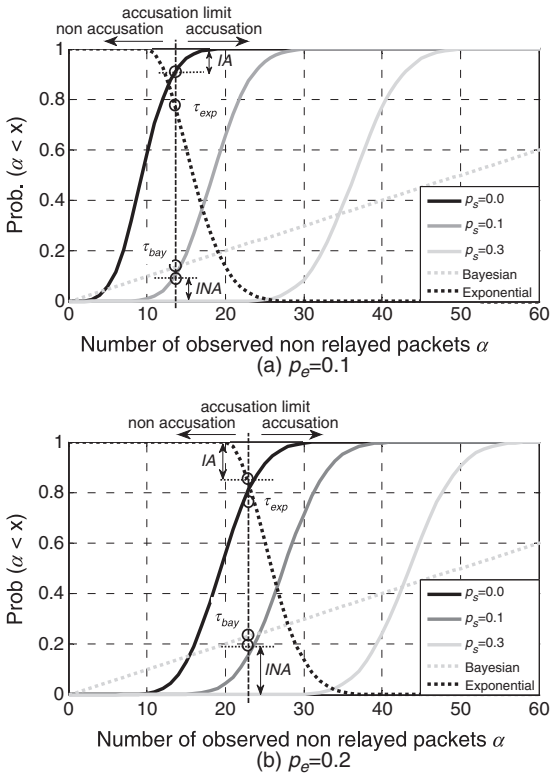

Figure 3. Comparison of the Bayesian and exponential functions for a) $p_{\mathrm{e}} = 0.1$ and b) $p_{\mathrm{e}} = 0.2$.

Let us suppose that the accusation limit is set to 13 in Figure 3(a) and 23 in Figure 3(b); the accusation limit represents the maximum number of non-relayed packets observed before an accusation is triggered after a certain number of packets is sent. In Figure 3(b), a higher p_{e} demands a higher accusation limit because more packets are observed incorrectly as non-relayed and the CDFs are shifted to the right. These accusation limits provide a balance between the *IA* of non-selfish nodes and the *INA* of selfish nodes with $p_{\mathrm{s}} = 0.1$ and they imply different accusation thresholds τ for each of the metrics (τ_{bay} and τ_{exp} in the figures). τ_{bay} and τ_{exp} can be derived as the intersection of the accusation limit and the corresponding function curve. *IA* and *INA* are determined by the intersection of the accusation limit with the CDF for non-selfish nodes and for nodes with $p_{\mathrm{s}} = 0.1$, respectively.

It is important to note that in the case of the exponential function, τ_{exp} remains the same for $p_{\mathrm{e}} = 0.1$ and $p_{\mathrm{e}} = 0.2$. This is the case because p_{e} is explicitly considered in the exponential function, and thus the function's curve is shifted when p_{e} changes. On the other hand, τ_{bay} has to be readjusted with p_{e} in Figure 3(b), which highlights the need to determine the optimal τ_{bay} for each p_{e}. Another important difference between the Bayesian and exponential approaches is that in the exponential method the metric consists of the average of the last l values of the exponential function in (8), and not just the last one. This is aimed at mitigating the effect in *IA* that may be caused by temporary incorrect observations of packets discarded.

4. PERFORMANCE EVALUATION

Simulations have been conducted to select the optimal values of the configuration parameters (τ, l) for the Bayesian and exponential detection techniques in scenarios with different input parameters p_{s}, p_{e}, and N. Iterative simulations based on the binomial detection process were carried out. The total number of experiments guarantees that the obtained results are characterized by a relative error below 0.51%. For each iteration, a sample sequence $\{\alpha_n\}$ of N observations is computed and evaluated by each of the detection techniques. Each detection mechanism m indicates that the node is acting selfishly if its metric tests positive in any of the observations α_n of that sample. An accusation is incorrect if $p_{\mathrm{s}} = 0$ for that sample, and a non-accusation is incorrect if $p_{\mathrm{s}} > 0$. The average of the *IA*,

INA, and δ parameters is then obtained over all iterations. Let $x_i \in \{0.0, 0.1, \ldots, 1.0\}$ with $i = 1, \ldots, N_{\text{ps}}$ be the set of possible discrete values of the parameter p_{s} with mass[†] distribution function $f_{\text{ps}}(x)$ in a set of nodes. N_{ps} represents the number of discrete p_{s} levels. The average values of *IA*, *INA*, and δ can then be computed using the proportionality principle

$$\begin{aligned} IA(m, f_{\text{ps}}, \tau, l, N, p_{\text{e}}) &= f_{\text{ps}}(0.0) \\ &\quad \times IA(m, \tau, l, N, p_{\text{e}}) \\ INA(m, f_{\text{ps}}, \tau, l, N, p_{\text{e}}) &= \sum_{i=2}^{N_{\text{ps}}} f_{\text{ps}}(x_i) \\ &\quad \times INA(m, x_i, \tau, l, N, p_{\text{e}}) \\ \delta(m, f_{\text{ps}}, \tau, l, N, p_{\text{e}}) &= \sum_{i=2}^{N_{\text{ps}}} f_{\text{ps}}(x_i) \\ &\quad \times \delta(m, x_i, \tau, l, N, p_{\text{e}}) \end{aligned} \tag{11}$$

Next, we define a set of distributions $f_{\text{ps}}^{i}(x)$ that include two factors that have a major impact in the selection of the techniques' configuration parameters: the proportion of non-selfish nodes $f_{\text{ps}}(0)$, and the proportion of selfish nodes with a relatively low but non-null p_{s} probability. Taking into account the trade-off between *IA* and *INA,* reducing *IA* should be a priority in a network with a large proportion of non-selfish nodes. On the other hand, detecting selfish nodes with low p_{s} is more challenging, because the range of τ where *IA* and *INA* can be simultaneously minimized is narrower (see Figure 3). In this case, l must be increased to compensate the low p_{s} nodes' effect. Simulations have then been conducted for 24 different combinations of the proportion of non-selfish nodes ($f_{\text{ps}}(0) \in \{0.1, 0.2, \ldots, 0.8\}$), and uniform, linear decreasing and linear increasing functions $f_{\text{ps}}(x)$ for selfish nodes. A decreasing function represents a network with a larger rate of nodes with low p_{s}. *IA*, *INA*, and δ are averaged over the set of distributions $\left\{f_{\text{ps}}^{i}(x)\right\}_{i=1}^{24}$ and the maximum number of observations N. The criterion to select the optimum (τ, l) for each metric m and p_{e} is to minimize the sum of the *IA*, *INA*, and δ parameters to improve both the accuracy and speed. The set of (τ, l) values evaluated were all the possible combinations of $\tau \in \{0.1, 0.15, \ldots, 0.9\}$ and $l \in \{3, 6, 12, 24, 48\}$. The finally selected (τ, l) values are shown in Tables I and II. All the Bayesian techniques must adjust the value of τ because it must always be higher than the estimated p_{e}, but not too high to be able to detect selfish nodes with low p_{s}. On the other hand, the exponential mechanisms, and in particular EFW, do not need to adjust τ because it is already considered in the exponential function (8). However, it has to be noted that Bayesian techniques must estimate the value of p_{e} to adjust the τ parameter, whereas the exponential techniques must estimate the value of p_{e} to correctly compute the metric function (8). As a result, the need to estimate p_{e} cannot be considered as a drawback of the exponential proposal.

[†]For simplicity, p_{s} is considered a discrete random variable in this discussion.

Table I. τ optimum value.

p_e	BIW	BFW	BDF	BFWDF	EIW	EFW
0.1	0.30	0.45	0.40	0.45	0.40	0.10
0.2	0.40	0.45	0.50	0.40	0.35	0.10
0.3	0.45	0.55	0.50	0.65	0.35	0.10
0.4	0.55	0.60	0.50	0.65	0.35	0.10

Table II. l optimum value.

p_e	BIW	BFW	BDF	BFWDF	EIW	EFW
0.1	12	12	48	12	3	3
0.2	12	24	6	48	6	3
0.3	24	24	12	12	6	3
0.4	24	48	48	24	6	3

Figure 4 shows the influence of N on the *IA*, *INA*, and δ parameters. EFW obtains the best performance in terms of accuracy, especially with regards to *INA*, at a low cost of dropped packets. Figure 4(a) shows that BFW and BFWDF result in a lower *IA* for low values of N, but also in a high *INA* inaccuracy. As expected, increasing the maximum number of observations N allows the precursor node to better detect selfish nodes in Figure 4(b). This is the case because nodes with a low p_{s} are harder to distinguish from cooperative nodes. For this reason, when N increases, all the techniques are more capable to detect selfish nodes with low p_{s}, but also the number of dropped packets δ increases in Figure 4(c): more selfish nodes are detected, but they will also have discarded more packets.

The value of p_{e} has a strong influence on the selection of the (τ, l) parameters for the Bayesian techniques (Tables I and II), and on the accuracy and speed of the detection mechanisms (Figure 5). Figures 5(a) and (b) illustrate the effect of p_{e} on *IA* and *INA*, whereas Figure 5(c) shows its influence in the speed of detection δ. The adjustment of the configuration parameters for the Bayesian techniques explains the non-uniform variation of their performance parameters as a function of p_{e}. In the case of EFW and EIW, the unique selected (τ, l) configuration results in a more uniform behavior of its performance parameters as a function of p_{e}. However, an increase of p_{e} degrades the accuracy and speed off all the detection mechanisms. It is important to highlight that the depicted results clearly show that EFW achieves the best performance in terms of accuracy, in particular for *INA*, at a lower cost of dropped packets.

The observed differences between the Bayesian and exponential approaches are due to the τ parameter and the averaging process in the exponential metric (10). In the

Trans. Emerging Tel. Tech. **24**:582–588 (2013) © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

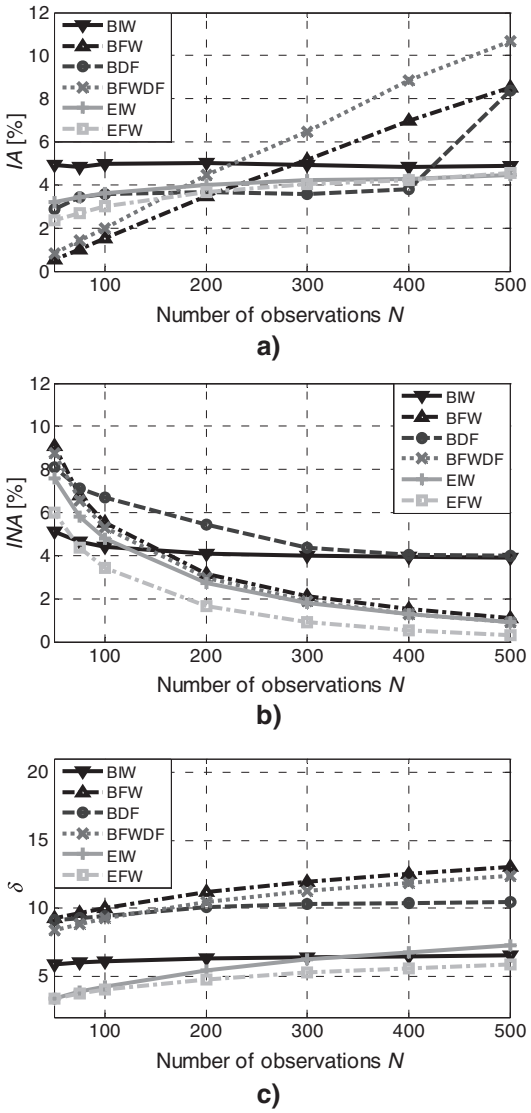

Figure 4. (a) *IA*, (b) *INA*, and (c) δ as a function of the maximum number of observations *N*.

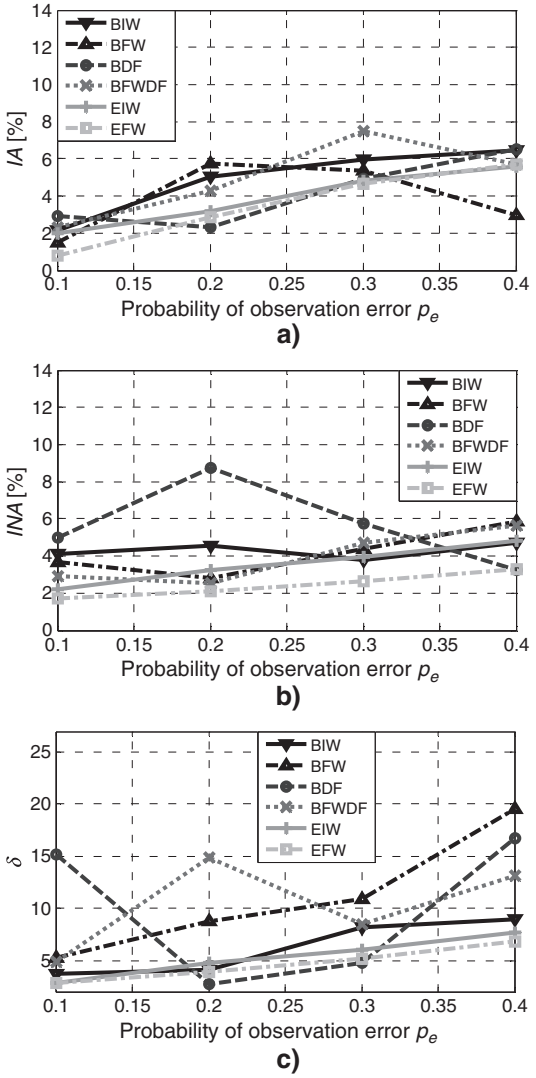

Figure 5. (a) *IA*, (b) *INA*, and (c) δ as a function of p_e.

Bayesian approach, τ is defined as the maximum acceptable threshold of selfishness. Consequently, increasing its value to reduce *IA* results in that selfish nodes characterized by $p_s < \tau - p_e$ are hardly detected and *INA* increases. On the other hand, τ represents the probability that the node is not acting selfishly in the case of EFW. In this case, reducing τ (i.e. requiring a lower likelihood) decreases *IA*, but does not result in that selfish nodes with low p_s are not detected because τ does not refer directly to their selfishness. The higher performance of EFW compared with EIW is due to the fact that EIW averages the outputs of the exponential function (8) for all the observations, including the first observations that may be inaccurate. On the other hand, EFW only considers the last l outputs and discards the previous ones.

5. CONCLUSIONS

Reputation-based selfishness prevention schemes have been proposed to detect and isolate selfish nodes in MANETs. The Bayesian detection techniques reported in the literature are characterized by a trade-off between the accuracy and speed of the detection process. In this context, this work has proposed a novel exponential detection mechanism that explicitly takes into account the probability of incorrect observations before categorizing the behavior of nodes. The conducted study has shown that the exponential proposal outperforms, both in terms of detection accuracy and speed, the Bayesian approach. It has also been shown that the exponential proposal can achieve an optimum performance with the same configuration

under different error probabilities of the observation technique and different distributions of the selfishness probability. This characteristic significantly improves the implementation perspective of the exponential approach in real networks characterized by a dynamic and varying performance and behavior of nodes.

LIST OF ABBREVIATIONS AND SYMBOLS

αn: sample sequence of N observations.
A: accusation state of the Markov chain accusation process.
BFW: Bayesian with finite window.
BFWDF: Bayesian with finite window and discount factor.
BIW: Bayesian with discount factor.
BIW: Bayesian with infinite window.
CDF: cumulative distribution function.
D: random experiment of the observation of the relaying action.
Dn: repeated random experiment D.
EFW: exponential with finite window.
EIW: exponential with infinite window.
F: binomial cumulative distribution function.
f: binomial mass distribution function.
F_{e}: exponential function used in the exponential metric.
$f_{\mathrm{ps}}(x)$: probability density function of p_{s}.
IA: incorrect accusations ratio.
INA: incorrect no accusations ratio.
l: minimum number of observations required.
m: selfishness detection method.
MANET: mobile ad hoc network
M_{m}: selfishness metric function.
N: maximum observations before the connection ends.
n: total number of observed actions.
NA: no accusation state of the Markov chain accusation process.
p_{d}: probability that a selfish action is detected.
p_{e}: probability that the observation technique mistakes a cooperative action as a selfish one.
p_{s}: probability that a selfish node refuses to relay a packet.
u: selfishness metric discount factor.
α: number of observed selfish actions.
α_n: number of observed selfish actions in the past n observations.
β: number of observed cooperative actions.
$\Delta\_(x)$: auxiliary function.
δ: number of discarded packets before a selfish node is accused.
τ: accusation threshold.
τ_{bay}: Bayesian metric's accusation threshold.
τ_{exp}: exponential metric's accusation threshold.

ACKNOWLEDGEMENTS

This work was supported by the Ministry of Science and Innovation (Spain) and FEDER funds under the project TEC2008-06728, by the 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. Buchegger S, Mundinger J, Le Boudec J. Reputation systems for self-organized networks. *IEEE Technology and Society Magazine* 2008; **27**(1): 41–47.
2. Callegari C, Vaton S, Pagano M. A new statistical method for detecting network anomalies in TCP traffic. *European Transactions on Telecommunications* 2010; **21**(7): 575–588.
3. Yoo Y, Agrawal DP. Why does it pay to be selfish in a MANET? *IEEE Wireless Communications Magazine* 2006; **13**(6): 87–97.
4. Szott S, Natkaniec M, Canonico R. Detecting backoff misbehaviour in IEEE 802.11 EDCA. *European Transactions on Telecommunications* 2011; **22**(1): 31–34.
5. Zahariadis T, Leligou HC, Trakadas P, Voliotis S. Trust management in wireless sensor networks. *European Transactions on Telecommunications* 2010; **21**(4): 386–395.
6. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad-hoc networks, In *Proceedings of the ACM International Conference on Mobile Computing and Networking*, Boston (Massachusetts), August 2000; 255–265.
7. Rodriguez–Mayol A, Gozalvez J. On the implementation feasibility of reputation techniques for cooperative mobile ad-hoc networks, In *Proceedings of the 16th European Wireless*, Lucca (Italy), June 2010; 615–623.
8. Buchegger S, Le Boudec J. A robust reputation system for P2P and mobile ad-hoc networks, In *Proceedings of the 2nd Workshop on the Economics of Peer-to-Peer Systems*, Harvard University, Cambridge (Massachusetts), June 2004.
9. Yang L, Kizza JM, Alma-Cemerlic, Liu F. Fine-grained reputation-based routing in wireless ad hoc networks, In *Proceedings of the IEEE Intelligence and Security Informatics*, New Brunswick (New Jersey), June 2007; 75–78.
10. Jiang H, Yang Y, Xu J, Wang L. Estimation of packet error rate at wireless link of Vanet. *Advances in Wireless Sensors and Sensor Networks, Lecture Notes in Electrical Engineering* 2010; **64**: 329–359.
11. Alon N, Spencer JH. *The Probabilistic Method*. John Wiley and Sons: New York, 2000.

DOI: 10.1002/ett