Accurate Detection of Black Holes in MANETs using Collaborative Bayesian Watchdogs

Manuel D. Serrat-Olmos, Enrique Hernández-Orallo, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni
Departamento de Informática de Sistemas y Computadores.
Universidad Politécnica de Valencia. Valencia, Spain.
email: mdserrat@upvnet.upv.es,{ehernandez,jucano,calafate,pmanzoni}@disca.upv.es

ABSTRACT

Watchdogs are a well-known mechanism to detect threats and attacks from misbehaved and selfish nodes in computer networks. This paper proposes a collaborative approach for detecting black holes and selfish nodes in MANETs, using a set of bayesian watchdogs which collaborate to enhance their individual and collective performance. To evaluate the performance of this approach, we first introduce an analytical model. The results of this model reveal that the detection time of misbehaved nodes is reduced, and the impact of false positives and false negatives is minimised (that is, the overall accuracy is increased). These results are confirmed in the simulation results that follow. The collaborative bayesian watchdog performs better in terms of accuracy and speed detection than the standard bayesian watchdog.

I. INTRODUCTION

A Mobile Ad Hoc Network, usually known as MANET, consists of a set of wireless mobile nodes that function as a network in the absence of any kind of centralized administration and networking infrastructure. These networks rely on cooperation from their nodes to correctly work, that is, every network node generates and sends its own packets and forwards packets on behalf of other nodes. These nodes could be classified [1] as well-behaved nodes, if they cooperate with the MANET forwarding activities to achieve the community goals, or as misbehaved nodes, if they act against those global goals. In this case, nodes are further classified into three classes: faulty nodes, if they do not cooperate due to a hardware or software malfunction; selfish nodes, if they drop all the packets whose destination node are not themselves, but they use other nodes to send their own packets; and malicious nodes, when they try to disturb the normal network behaviour for their own profit.

When a MANET is deployed, we have to assume that there could be a percentage of misbehaved nodes. The types of misbehaved nodes, their number, and their positions and movement patterns are key issues which deeply impact the mobile ad hoc network performance [2]. Additionally, network performance could be drastically reduced if nothing is done to cope with these threats. To this end, an effective protection against misbehaved nodes will be mandatory to preserve the correct functionality of the MANET [3]. The final result is that packet delivery ratios in MANETs deteriorate or break significantly with the presence of these misbehaving nodes. All types of misbehaved nodes –faulty, selfish and malicious– have a common behaviour: they do not participate in forwarding activities, thus being characterized as black holes. We comprise all this misbehaviour classes using the term *black hole:* a node that disrupts, intentionally or not, the communication within its neighborhood, dropping all packets received without forwarding them to their final destination [4].

To avoid or significantly reduce the impact of black holes in MANETs, several proposed approaches are based on monitoring the traffic heard by every node to detect misbehaved nodes, and then taking the appropriate actions to avoid the negative effects of that misbehaviour [5]. The main problem that arises at this point is how to detect these black holes, while avoiding as much as possible wrong diagnostics, like false positives or false negatives. A false positive appears when the selected technique identifies a well-behaved node as a misbehaved node. A false negative appears when the technique can not detect a misbehaved node, so the network believes that it is a normal node, with its potentially disruptive effects. So, accuracy and detection speed are critical issues when designing an approach for black holes detection in MANETs.

Several solutions have been proposed for detecting and coping with misbehaved nodes in MANETs. Marti et al. [6] proposed a Watchdog and a Pathrater over DSR protocol to detect non-forwarding nodes, maintaining a rating for every node and selecting routes with the highest average node rating. Buchegger and Le Boudec [7] proposed the CONFIDANT protocol over DSR, which combines a watchdog, a reputation system, Bayesian filters and information obtained from a node and its neighbours to accurately detect misbehaved nodes.

Some of these approaches use the concept of reputation to improve the detection of black holes, just as reputation is used in human relations. If a node group says that other node is malicious, it is quite probable that this is true. So, it seems a good idea to integrate reputation systems in the mechanism to detect misbehaved nodes. Therefore, watchdog cooperation will probably increase accuracy and detection speed.

In this work we propose a collaborative watchdog which integrates techniques from reputation systems and bayesian filtering, and makes extensive use of the collaborative nature of MANETs. This watchdog must be considered as an Intrusion Detection Systems (IDS), which is a software piece that collects and analyzes network traffic to detect a set of attacks. In this context, intrusion detection systems aim at monitoring

978-1-4673-4404-3/12/$31.00 ©2012 IEEE

the activity of the nodes in the network in order to detect misbehaviour. The problem of false positives and negatives is that they can also be propagated in the network when a collaborative contact occurs, so it is important to reduce their impact.

In order to evaluate the performance of our collaborative bayesian watchdog we first introduce an analytical model. This model allows an overall evaluation of the efficiency of our approach under a large number of scenarios. The results of this model are validated through simulations. The analytical model assumes that the occurrence of contacts between two mobile nodes follows a Poisson distribution. We model the network as a Continuous Time Markov chain (CTMC) and derive expressions for obtaining the time of detection of misbehaved nodes. This model will also consider the side effects of false negatives and false positives on the global performance of the collaborative approach.

In general, we can say that the model and simulation results show a significant reduction of the detection time of black hole nodes. Regarding the impact of false negatives and false positives if we compare the results with a non collaborative approach, the collaborative bayesian watchdog drastically reduces the impact of both false negatives and false positives.

II. Bayesian Watchdog

As we stated earlier, to detect misbehaved nodes, network monitoring is needed. Every node must be aware of its neighbours' behaviour, and watchdogs are a popular component for Intrusion Detection System dedicated to this task. The main problem is that standard watchdogs are characterized by a significative amount of false positives [4], basically due to mobility and signal noise. Previous works from our group [8] have evaluated a bayesian watchdog over Ad-hoc On-demand Distance Vector (AODV) routing in MANETs. This bayesian watchdog results from the aggregation of a bayesian filter with a standard watchdog implementation.

The standard watchdog simply overhears the packets transmitted and received by its neighbours, counting the packets that should be retransmitted, and computing a trust level for every neighbour as the ratio of "packets retransmitted" to "packets that should have been retransmitted". If a node retransmits all the packets that it should have retransmitted, it has a trust level of 1. If a node has a trust level lower than the configured tolerance threshold, that node is marked as malicious.

The role of the bayesian filter in the watchdog is to probabilistically estimate a system's state from noisy observations. As a result of their work, Hortelano et al. [8] found that, compared to the standard one, the bayesian watchdog reaches a 20% accuracy gain, and it presents a faster detection on 95% of times. So, this bayesian watchdog is an excellent brick to build a MANET-wide system to detect black hole nodes even earlier and more accurately, through collaboration between nodes running this watchdog version.

III. Collaborative Bayesian Watchdog

Based on the bayesian watchdog presented in Section II, we propose a collaborative bayesian watchdog based on a message-passing mechanism in every individual watchdog that allows publishing both self and neighbour reputations. Every node running our watchdog collects the reputation information to obtain the values of α' and β' for every neighbour. The underlying idea of our approach is that if a bayesian watchdog works well for detecting black holes, a group of collaborating neighbouring bayesian watchdogs would be able to perform faster and more accurate detections.

Similarly to the bayesian watchdog, the collaborative bayesian watchdog overhears the network to collect information about the packets that its neighbours send and receive. Additionally, it obtains the α and β values for its whole neighbourhood. These values are exactly the same than those obtained by the bayesian watchdog with the same observations; we call them 'first hand information' or 'direct reputations'. Periodically, the watchdog shares these data with its neighbours, and we call them 'second hand information' or 'indirect reputation'. In our implementation, indirect reputations are modulated using a parameter δ. Whenever required, every node running the collaborative bayesian watchdog calculates, using expressions (3) and (4), the values of α' and β', which in this case are passed to the beta function to obtain an estimation of the maliciousness of a node.

$$\underset{j\in N_i}{\forall}\underset{k\in N_j}{\forall}\alpha(i)'_j = \frac{\alpha(i)_j + \delta{\cdot}mean(\alpha(i)^k_j)}{2} \tag{1}$$

$$\underset{j\in N_i}{\forall}\underset{k\in N_j}{\forall}\beta(i)'_j = \frac{\beta(i)_j + \delta{\cdot}mean(\beta(i)^k_j)}{2} \tag{2}$$

where

- *i* is the node which is performing detection
- N_i is the neighbourhood of node *i*
- $\alpha(i)_j$,$\beta(i)_j$ are the values of α, β calculated for every neighbour *j* of i, obtained from direct observations at *i*
- $\alpha(i)^k_j$, $\beta(i)^k_j$ are the values of α, β calculated for every neighbour *j* of i, obtained from observations of every neighbour *k of j*
- δ represents the level of trust or the relative importance that a neighbour's observed reputations have for node i

When indirect reputations arrive at a node from one of its neighbours, it processes those reputations for its own neighbours. Once the reputations are obtained, and the adequate analysis is done, the detection only needs a predefined tolerance threshold to identify if a node is misbehaving or not.

Figure 1 shows the main components of our collaborative bayesian watchdog. First, each individual watchdog overhears the network to make direct observations of its neighbours, thereby detecting black holes as the bayesian watchdog does. Periodically, it receives reputation information from its neighbours and evaluates their behaviour taking into account this second hand information and its direct observations.

Having introduced the mathematical model, we now set the objectives we are trying to achieve with this collaborative bayesian watchdog. In this case, we want to:

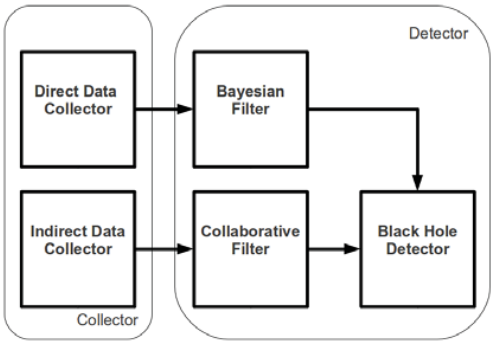


Figure 1: Components of the collaborative bayesian watchdog

- Increase the detection speed, reducing the time needed to detect a black hole. Publishing reputation information is a method that makes available to every node in scope that a certain number of nearby nodes are presenting a bad behaviour. This would have a positive impact on MANET performance because it would allow other nodes to be aware of those misbehaving nodes earlier, and to exclude them from MANET communication flows.
- Reduce the production of false positives. There are some circumstances that could lead an individual node to label another node as misbehaving when it is not. When reputation information arrives at this node from a group of neighbouring nodes that have correctly detected this node as a negative, the node has a chance to turn back its decision influenced by other nodes information, reducing the MANET-wide false positive production ratio.
- Reduce the production of false negatives. Again, there are some circumstances that could lead an individual node to label another node as well-behaving when it is not. So, when reputation information arrives from a group of neighbouring nodes, the node has a chance to turn back its decision influenced by other nodes information, reducing the MANET-wide false negative production ratio.

In section IV, we introduce an analytical performance model for this collaborative bayesian watchdog, and in, Section V, we evaluate our approach through simulation in a specific environment.

IV. System Performance Model

The goal of this section is to model and evaluate the impact of false positives and negatives on the performance of our collaborative watchdog. The network is modelled as a set of N wireless mobile nodes, with C collaborative nodes and one black hole node ($N = C + 1$). Our goal is to obtain the time required by all collaborative nodes to realize who is the black hole node in the network.

Recent works show that the occurrence of contacts between two mobile nodes follows a Poisson distribution with rate λ [9], [10], [11]. This has been shown valid for both human and vehicle mobility patterns. Therefore, we consider that using an exponential fit is a good choice to model inter-contact times.

A. Modeling bayesian and collaborative detection

The watchdog is modelled using three parameters: the probability of detection p_d, the ratio of false positives p_{fp} and the ratio of false negatives p_{fn}. The first parameter p_d, reflects the probability that, when a node contacts another node, the bayesian watchdog has enough information to decide wheter a node is a black hole or not (that is, a positive or a negative). This value depends mainly on the observation time, and the transmission and mobility pattern of the nodes.

Furthermore, the watchdog can generate false positives and false negatives. In order to measure the performance of a watchdog these values can be expressed as a ratio or probability: p_{fp} is the ratio of false positives generated when a node contacts a black hole node, and p_{fn} is the ratio of false negatives generated when a node contacts a black hole node.

The collaboration detection is modelled using a function f_{cp}. This function reflects the probability that a node changes to positive when it contacts another collaborative node. As detailed in the previous section, the α and β values are updated using the mean of the α and β obtained from the neighbour nodes (see equations 1 and 2). Thus, f_{cp} needs to reflect the probability that a new pair of α and β values obtained from the new contact node makes the detection positive. This function depends on the difference between nodes that have a positive and nodes that have negatives. When this difference is zero or negative, then the probability of change is zero, but when this difference is greater than zero the probability rises to one up to a given threshold C_t. Thus, function f_{cp} can be defined as:

$$f_{cp}(c_p, c_n) = \begin{cases} 0 & (c_p - c_n) \leq 0 \\ \delta(1 - p_{fn})\frac{\max[(c_p - c_n), C_t]}{C_t} & (c_p - c_n) > 0 \end{cases} \quad (3)$$

where c_p is the number of collaborative nodes that have a positive, and c_n is the number of nodes that have a negative. The factor $(1 - p_{fn})$ reflects that only the true positives are taken into account, and δ corresppons to the level of trust. A similar function can be derived for false negatives.

Using the previous parameters we can model the probability of generating a Positive and a Negative when a contact occurs:

- Positive: there are two possibilities: i) the node contacts with the black hole node and the local watchdog detects it, with probability $p_d(1-p_{fn})$; and ii), the node contacts another node that has a positive about the black hole node with probability f_{cp}. Note that a false positive can also be generated with probability $p_d \cdot p_{fp}$.
- Negative: two possibilities: i) a contact with a non-black hole node with probability $p_d(1 - p_{fp})$, and ii) the node contacts another node that has a negative so the probability is f_{cn}. A false negative can also be generated when it contacts with the selfish node with probability $p_d \cdot p_{fn}$.

In the next subsection we introduce a generic analytical model for evaluating the performance of the collaborative watchdog approach.

B. A Model for the Detection of Black Hole Nodes

This model takes into account the effect of false negatives. False positives do not affect the detection time of black hole

nodes, so p_{fp} is not introduced in this model. The effect of false positives will be studied later.

Using λ we can model the network using a 2D Continuous Time Markov chain (2D-CTMC) with states (c_p, c_n), where c_p represents the number of collaborative nodes that have a positive about the black hole node at time t, and c_n represents the number of *collaborative* nodes that have a negative of the black hole node (note that, in this case, is a false negative). At the beginning all nodes have no information about the black hole node. Then, when a contact occurs, c_p and c_n can be increased by one. Note, that c_p and c_n are not independent: $c_p + c_n \leq C$, so some states are not reacheable. The final (absorbing) states is when $c_p = C$. A 2D-CTMC model is used, with an initial state $s_1 = (0, 0)$, $C(C + 1)$ transient states (from $s_1 = (0, 0)$ to $s_\tau = (C - 1, C)$ states) and $C + 1$ absorbing states (from $s_{\tau+1} = (C, 0)$ to $s_{\tau+\upsilon} = (C, C)$. We define τ as the number of transient states ($\tau = C(C + 1)$) and υ as the number of absorbing states ($\upsilon = (C + 1)$). This model can be expressed using the following transition matrix P in canonical form:

$$\mathbf{P} = \begin{pmatrix} \mathbf{Q} & \mathbf{R} \\ 0 & \mathbf{I} \end{pmatrix} \tag{4}$$

where $\mathbf{I}$ is a $\upsilon \times \upsilon$ identity matrix, 0 is a $\upsilon \times \tau$ zero matrix, $\mathbf{Q}$ is a $\tau \times \tau$ matrix with elements p_{ij} denoting the transition rate from transient state s_i to transient state s_j and $\mathbf{R}$ is a $\tau \times \upsilon$ matrix with elements p_{ij} denoting the transition rate from transient state s_i to the absorbing state s_j.

Now, we derive the transition rates p_{ij}. Given the state $s_i = (c_p, c_n)$ the following transitions can occur:

- (c_p, c_n) to $(c_p + 1, c_n)$: A new collaborative node has a positive. The transition probability is $\lambda(p_d(1 - p_{fn}) + f_{cp}(c_p, c_n) \max(C - c_p - c_n, 0)$. The term $p_d(1 - p_{fn})$ represents the probability of a positive from the watchdog and $f_{cp}(c_p, c_n)$ from collaboration. Finally, the factor $(C - c_p - c_n)$ represents the number of pending collaborative nodes. Note, that $(c_p + c_n) \leq C$, so with $\max(C - c_p - c_n, 0)$ the transition probability to the *not reacheable* states is zero.
- (c_p, c_n) to $(c_p, c_n + 1)$: A new collaborative node has a negative (a *false negative*). The transition probability is $\lambda(p_d p_{fn} + f_{cn}(c_p, c_n) \max(C - c_p - c_n, 0)$.
- $(c_p + 1, c_n)$ to (c_p, c_n): A collaborative node that has a positive state changes to negative. So, the transition probability is similar to the new negative case : $\lambda(p_d p_{fn} + f_{cn}(c_p, c_n)c_p$.
- $(c_p, c_n + 1)$ to (c_p, c_n): A collaborative node that has a negative changes to positive. The transition probability is similar to the new positive case $\lambda(p_d(1 - p_{fn}) + f_{cp}(c_p, c_n)c_n$.
- (c_p, c_n) to (c_p, c_n): This is the probability of no changes and is $1 - \sum_{j \neq i} p_{ij}$.

Using the transition matrix $\mathbf{P}$ we can derive the detection time T_d. From the 2D-CTMC we can obtain how long will it take for the process to be absorbed. Using the fundamental matrix $\mathbf{N} = (\mathbf{I} - \mathbf{Q})^{-1}$, we can obtain a vector t of the expected time to absorption as $t = \mathbf{Nv}$, where $\mathbf{v}$ is a column vector of ones ($\mathbf{v} = [1, 1, \ldots, 1]^T$). Each entry t_i of t represents the expected time to absorption from state s_i. Since we only need the expected time from state $s_1 = (0, 0)$ to absorption (that is, the expected time for all nodes to have a positive), the detection time T_d, is:

$$T_d = E[T] = \mathbf{v_1 N v} \tag{5}$$

where T is a random variable denoting the detection time for all nodes and $\mathbf{v_1} = [1, 0, \ldots, 0]$.

Now, we study the effect of the false positives. When a node has a false positive, the problem is that, due to the diffusion of positives, this false positive can be quickly distributed in the network. A way to evaluate this diffusion is to obtain the time that all nodes have a false positive about a given node. Following the same process that in the model for the false negatives, we have a 2D-CMTC with the same states (c_p, c_n), but in this case c_p represents the number of nodes with false positives, and c_n the number of nodes with a negative. The transition rates (p_{ij}) of the transition matrix $\mathbf{P}$ are:

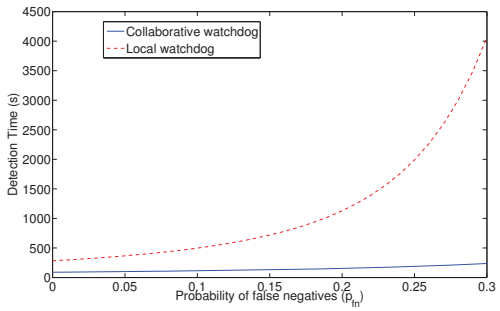
$$p_{ij} = \begin{cases} \lambda(p_d p_{fp}) + f_{cp}(c_p, c_n) \cdot \mathcal{C}() & (c_p \to c_p + 1) \\ \lambda(p_d(1 - p_{fp}) + f_{cn}(c_p, c_n) \cdot \mathcal{C}() & (c_n \to c_n + 1) \\ \lambda(p_d(1 - p_{fp}) + f_{cn}(c_p, c_n) \cdot c_p & (c_p \to c_p - 1) \\ \lambda(p_d p_{fn} + f_{cp}(c_p, c_n) \cdot c_n & (c_n \to c_n - 1) \end{cases} \tag{6}$$

where $\mathcal{C}() = \max(C - c_p - c_n, 0)$. We can see that the transition rates are the same than in the false negative model by replacing $p_{fp} = 1 - p_{fn}$. Therefore, we can use the previous model for obtaining the detection time T_d.

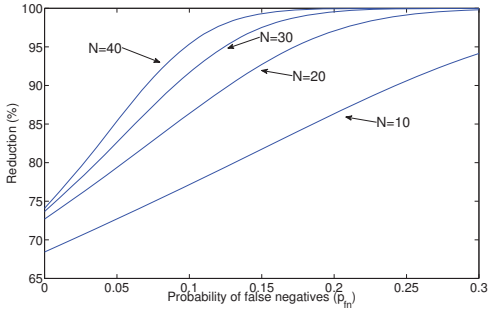
C. Model evaluation

Now, based on the previous model, we evaluate the effect of false positives and false negatives on the performance of the collaborative watchdog. The models allow an overall evaluation of the collaborative watchdog under a large number of scenarios. For the following experiments we use the following parameters that were obtained from the experimental evaluation: $p_d = 0.1$, $C_t = 5$, $\delta = 0.3$ and $\lambda = 0.02$. The first experiment evaluates the impact of the false negatives comparing the results with a non-collaborative approach (that is, depending only on the local watchdog) for a network of 10 nodes ($N = 10$). In this case, we expect that the diffusion of α and β can reduce the influence of false negatives. Figure 2a shows the detection time depending on p_{fn} for different values of N (network nodes). First, we can see that detection time is greatly reduced using the collaborative watchdog, even in the absence of false negatives. Second, the detection increases with a very little slope when p_{fn} while for the local watchdog the values increase exponentially. Note that the detection time is for all nodes in the network, so this value can be very high with no collaboration. Figure 2b shows the percentage of reduction of the detection time between the collaborative and the local watchdog for several values of N. This confirms that the reduction is very important in the absence of false negatives (from 65% to 75%) but is even greater for higher values of p_{fn} and N.

The second experiment evaluates the impact of false positives. The model introduced obtains the detection time of a false negative. Therefore, a greater value of the detection time



(a)



(b)

Figure 2: Evaluation of the impact of false negatives a) detection time for $N = 10$, b) percentage of reduction of the detection time for several values of N

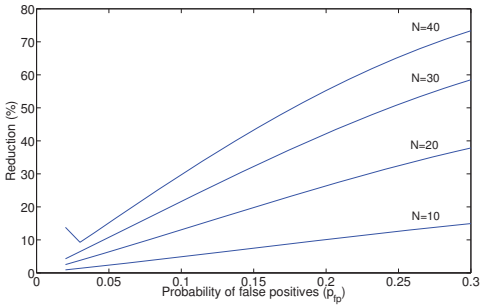


Figure 3: Reduction of the detection time depending on false positives

will imply a reduced impact of false positives. In this case, we expect that the collaborative watchdog can reduce the influence of false positives. This is shown in figure 3. In this case the reduction in not as high as in the false negatives case.

Two conclusions can be drawn from the performed analytical evaluation: our collaborative watchdog is able to reduce drastically the detection time of black hole nodes while also reducing the impact of false positives and false negatives.

V. Simulation Evaluation

The goal of this section is to validate the conclusions drawn from the analytical model through a more realistic evaluation.

We have implemented our collaborative bayesian watchdog as a Network Simulator 2 (ns-2) extension to the AODV routing protocol. We evaluate the impact that our approach has over the accuracy and the detection speed. We compare the results from the collaborative bayesian watchdog with those obtained using the non-collaborative versions, both bayesian and standard. Table I shows the characteristics of the scenarios we have selected for our performance evaluation.

Table I: Simulation parameters

Parameter	Value
Nodes	50
Area	1000 x 1000 m.
Wireless interface and bandwith	802.11 at 54 Mbps
Antenna	Onmidirectional
Transmission range	250 m.
Node speed	5, 10, 15 and 20 m/s.
% of black holes	10%
δ	0.8
γ	0.85
Fading	1
Neighbour time	1s.
Observation time	0.2s.
UDP Unicast traffic	Three flows
UDP Broadcast traffic	every 5s.
Simulation time	352 s.
Scenarios	20

Table II: Percentage of detections where the Collaborative Bayesian Watchdog detects the black holes before the Bayesian Watchdog does it

Node Speed (m/s.)	Percentage of earlier detections	Mean of detection time reduction (s.)
5	1.04%	5.000
10	11.88%	5.000
15	9.66%	5.209
20	5.72%	5.001

Some of these parameters, like area, number of nodes or speed, are needed by ns-2 to execute the simulation. Others, like δ, γ, or *Observation time*, are parameters needed by our model. For each test, we averaged the results of 20 independent simulations. To obtain normalized results, we simultaneously executed a simulation of the standard watchdog, the bayesian watchdog, and the collaborative bayesian watchdog with the same scenarios and parameters.

A. Detection speed

Accuracy is a key issue when detecting black holes, but speed is also important. A watchdog that detects 100% of black holes but requires 10 minutes is a useless watchdog. So, it is crucial for accuracy and speed to be well balanced. In that sense, watchdog enhancements will target both speed and accuracy issues.

The collaborative bayesian watchdog performed well in terms of speed. Table II shows that, on average, 7% of the times our approach detected black holes before the bayesian watchdog, with the same traffic pattern. The rest of the cases, it detects the malicious nodes at the same time. When a node B enters[1] node A's neighbourhood, our approach allows node

[1]In this context, entering a node's neighbourhood means that this node is in communication range and it announces its presence, for example, with a standard HELLO message

A to identify node B as a black hole with only a reputations sharing phase with its common neighbours. This means that, even if node B does not send or receive any data or routing packet when entering node A's neighbourhood, if it has been previously detected as black hole, node A will quickly mark it as a black hole too.

In dense networks with traffic load equally balanced between malicious and well-behaved nodes, both watchdog versions will perform nearly equally, despite of the smaller number of packets that the collaborative bayesian watchdog needs to perform detections. This is because the interval between packets is very short. Nevertheless, in networks with low traffic load and where black holes transmit a very small amount of packets, the performance differences between the two approaches could be more significative in terms of time. A single packet would make the difference between detecting or not a black hole, and the collaborative bayesian watchdog obtains better results in those cases.

Additionally, we can say that the collaborative bayesian watchdog obtains the best results at a node speed of 10 m/s. In fact, when nodes move at 10 m/s or 20 m/s, our approach behaves nearly 12% and 6% better, respectively. These results lead to the conclusion that the collaborative bayesian watchdog becomes a suitable implementation for Vehicle Ad-hoc Networks (VANETs), a type of MANET formed by vehicles in movement which share data when they cross with another car.

B. Accuracy

Figure 4 shows that the accuracy in detecting false positives and false negatives is also slightly better than with the non-collaborative bayesian watchdog, which comes from the decreased level of false negatives. The fact is that a small amount of black holes, that are not detected with the bayesian watchdog, are now detected by the collaborative bayesian watchdog. In fact, our approach is able to detect cases where a black hole enters and exits from the range of a watchdog quickly. As shown in Figure 5, although there is not a big difference between them, the collaborative bayesian watchdog performs better in terms of accuracy than the bayesian watchdog, despite of the node speed[2]. With respect to the standard watchdog, our approach clearly surpasses it in terms of detection accuracy.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we showed that a collaborative bayesian watchdog, based on the concepts of bayesian filtering and reputation sharing between collaborative nodes, boosts its performance by decreasing the amount of false negatives and false positives, while speeding up the detection process. We arrive to this conclusion through two different approaches: using an analytical model for performance evaluation, and through simulation. As a result, in the scenarios we tested our approach improves the detection speed of black holes, and slightly increases the accuracy of that detection process. These conclusions evidence

[2]The standard watchdog has a poor performance, as stated in [8] and as shown in Figure 5.

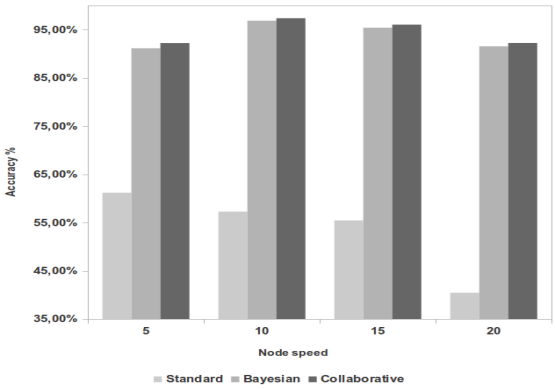


Figure 4: Accuracy comparison of the watchdog versions

that, compared to previous versions, our watchdog technique fits not only generic MANET environments, but also VANET environments.

As future work, we will implement this mechanism in a hardware testbed (Castadiva), working on the fine tuning of the collaborative bayesian watchdog to apply this technique on VANETs and Delay Tolerant Network environments.

ACKNOWLEDGMENTS

This work was partially supported by the *Ministerio de Ciencia e Innovación*, Spain. Grant TIN2011-27543-C03-01.

REFERENCES

[1] C.-K. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks," in *Proceedings of the Twelveth international conference on Advanced communication technology (ICACT'10)*, 2010.

[2] T. Sundarajan and A. Shammugam, "Modeling the behavior of selfish forwarding nodes to stimulate cooperation in manet," *International Journal of Network Security and its Applications (IJNSA)*, vol. 2, April 2010.

[3] F. Kargl, A. Klenk, S. Schlot, and M. Webber, "Advanced detection of selfish or malicious nodes in ad hoc networks," in *Proceedings of the First European Conference on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, 2004.

[4] J. Hortelano, J.-C. Cano, C.-T. Calafate, and P. Manzoni, "Watchdog intrusion detection systems: Are they feasible in manets?," in *XXI Jornadas de Paralelismo (CEDI'2010)*, 2010.

[5] L. Xu, Z. Lon, and A. Ye, "Analysis and countermeasures of selfish node problem in mobile ad hoc network," in *Proceedings of the Tenth International Conference on Computer Supported Cooperative Work in Design (CSCWD '06)*, 2006.

[6] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the Sixth International Conference on Mobile Computing and Networking (MobiCom'00)*, 2000.

[7] S. Buchegger and J.-Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communications Magazine*, July 2005.

[8] J. Hortelano, C.-T. Calafate, J.-C. Cano, M. de Leoni, P. Manzoni, and M. Mecella, "Black-hole attacks in p2p mobile networks discovered through bayesian filters," in *Proceedings of OTM Workshops'2010*, pp. 543–552, 2010.

[9] R. Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," *Performance Evaluation*, vol. 62, pp. 210–228, October 2005.

[10] H. Zhu, L. Fu, G. Xue, Y. Zhu, M. Li, and L. M. Ni, "Recognizing exponential inter-contact time in vanets," in *Proceedings of the 29th conference on Information communications*, INFOCOM'10, (Piscataway, NJ, USA), pp. 101–105, IEEE Press, 2010.

[11] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 60, pp. 2224 –2238, jun 2011.