A Novel Approach for the Fast Detection of Black Holes in MANETs

Manuel D. Serrat-Olmos, Enrique Hernández-Orallo[1], Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni

Departamento de Informática de Sistemas y Computadores

Universidad Politécnica de Valencia, Camí de Vera, s/n, Valencia, 46020 Valencia, Spain

email: mdserrat@upvnet.upv.es, {ehernandez, jucano, calafate, pmanzoni}@disca.upv.es

Abstract

MANETs (Mobile Ad Hoc Networks) are infrastructure-less wireless networks that rely on node cooperation to properly work. In this kind of networks, attack detection and reaction is a key issue to the whole network. The most common threat in MANET scenarios consists in the presence of a certain percentage of selfish nodes, which try to reduce the consumption of their own resources to prolong their battery lifetime. Those nodes do not collaborate on forwarding activities, therefore affecting the overall network performance. Watchdogs are well-known mechanisms to detect threats and attacks from misbehaved and selfish nodes in computer networks. The problem behind the use of watchdogs is that, while they can be quite effective in detecting selfishness by using their traffic overhearing behaviour, they can also cause a relatively high level of false negatives, thereby reducing their accuracy. This paper proposes a collaborative approach for detecting selfish nodes in MANETs. It is based on using a set of collaborative watchdogs, which collaborate to enhance their individual and collective performance. By using both an analytical study and simulation we demonstrate that our approach is able to improve accuracy and detection speed, while reducing the impact of false negative events.

Keywords: Wireless networks, MANETs, cooperative networks, selfishness, black-hole nodes.

[1] Contact author

1. Introduction

A Mobile Ad Hoc Network, usually known as MANET, consists in 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 in behalf of other nodes. These nodes could be classified [9] 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 network performance [8]. 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 a MANET [6].

One of the common threats in MANET scenarios consists in the presence of a certain percentage of selfish nodes, which try to reduce the consumption of their own resources to prolong their battery lifetime. Those nodes do not collaborate on forwarding activities, therefore affecting the overall network performance.

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. A *black hole attack* is a type of attack in which a node intends to disrupt the communication with its neighbourhood by attracting all traffic flows in the network, and then dropping all packets received without forwarding them to their final destination [5]. To avoid or significantly reduce this type of attack in MANETs, several of the proposed approaches are based on monitoring the traffic heard by every node to detect misbehaved and selfish nodes, and then taking appropriate actions to avoid the negative effects of that misbehaviour [10]. The main problem that arises at this point is how to detect these black holes, avoiding as much as possible wrong diagnostics, like false negatives. A false negative appears when the technique cannot 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 hole detection in MANETs.

Several solutions have been proposed for detecting, isolating or incentivating misbehaved nodes in MANETs. Marti et al. [7] proposed a Watchdog and a Pathrater over the DSR (Dynamic Source Routing) protocol to detect non-forwarding nodes, maintaining a rating for every node and selecting routes with the highest average node rating. The response module of this technique only relieves misbehaved nodes from forwarding packets, but they continue getting their traffic forwarded across the network. Buchegger and Le Boudec [1] 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. The system's response is to isolate those nodes from the network, punishing them indefinitely.

Others approaches drop reputation systems in favor of incentivation. Buttyan and Hubaux [3] presented a method using a virtual currency called *nuglet*. Every node has a credit counter, which will be increased when the node forwards packets, and decreased when sending its own packets. When a node has no nuglets, it cannot send packets anymore, so it is a motivation for nodes to forward packets for the network benefit. Zhong et al. [13] proposed SPRITE, a credit-based system to incentivate participation of selfish nodes in MANET communication. It's based on a Central Clearance System, which charges or gives credit to nodes when they send or forward a message. So, if a node wants to send a message, it must have sufficient credit to do it. That credit is earned by forwarding messages for other nodes. The response module of this method is integrated into the incentivation method, so that if a node does not forward other nodes' messages, it will not have credit to send its own messages.

Many 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 novel collaborative watchdog approach, which integrates techniques from reputation systems and bayesian filtering, and makes extensive use of the collaborative nature of MANETs. Our approach could be considered as an Intrusion Detection Systems (IDS), which collects and analyses network traffic to detect a set of attacks. In this context, intrusion detection systems aim at monitoring the activity of the nodes in the network in order to detect misbehaviour. Usually, these kinds of software products are built using two building blocks: a Detection (or sensor) module, like watchdogs, and a Response module.

The rest of this paper is organized as follows. Section 2 presents the concept of bayesian watchdog, which is a basic technique to detect black holes and selfish nodes in MANETs. Section 3 presents an enhanced proposal for a collaborative watchdog designed to perform that task. Section 4 evaluates the local performance through simulation. In section 5 we introduce an analytical model to evaluate the global effect of collaboration. Finally, we provide some concluding remarks.

2. 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 watchdogs are characterized by its inaccuracy and its low detection speed [5], basically due to mobility and signal noise. Previous works from our group [4] 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 had 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 node.

The role of the bayesian filter in the watchdog is to probabilistically estimate a system's state from noisy observations [4]. The mathematical foundation of the bayesian filter is the following: at time t, the state is estimated by a random variable θ, which is unknown, and this uncertainty is modeled by assuming that θ itself is drawn according to a distribution that is updated as new observations become available. It is commonly called *belief* or $Bel_t(\theta)$. To illustrate this, let's assume that there is a sequence of time-indexed observations $z_1,z_2,...,z_n,...,z_t$. The $Bel_i(\theta)$ is then defined by the posterior density over the random variable θ conditioned on all sensor data available at time t:

$$Bel_t(\vartheta) = p(\vartheta | z_{1,} z_{2,...}, z_n,..., z_t) = Beta(\alpha_t, \beta_t, \vartheta) \qquad (1)$$

In this approach, the random variable θ belongs to the interval [0,1]. Bayesian filtering relies on the Beta distribution, which is suitable to estimate the belief in this interval, as shown in expression 1; α and β represent the state of the system, and they are updated according to the following equations:

$$\alpha_{t+1} = \alpha_t + Z_t; \beta_{t+1} = \beta_t + Z_t \qquad (2)$$

The Beta function only requires two parameters that are continuously updated as observations are made or reported. In this approach, the observation z_t represents the information from the local watchdog obtained in time interval [t,t+Δt] about the percentage of non-forwarded packets. The bayesian watchdog uses three parameters: the first two parameters are α and β, which are handled over to the Beta function to obtain an estimation of the node's maliciousness. Thus, we can say that α and β are the numeric representation of a node's reputation. The third parameter is γ, which represents the devaluation that old observations must suffer to adapt the watchdog's behaviour to a continuously changing scenario without penalizing certain nodes forever. So it is a mechanism to reintegrate nodes into the MANET if they change their behaviour to a more cooperative one.

As a result of their work, Hortelano et al. [4] found that, compared to the standard one, the bayesian watchdog reached a 20% accuracy gain, and it presents a faster detection on 95% of times.

3. Collaborative Bayesian Watchdog

Based on the bayesian watchdog presented in Section 2, we have implemented 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 collaborative 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 that those obtained by the bayesian watchdog with the same observations; we call them “first hand information” or “direct reputations”. Periodically, the watchdog shares their information 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.

$$\underset{j\in N_i}{\forall}\ \underset{k\in N_j}{\forall}\ \alpha(i)'_j = \frac{\alpha(i)_j + \delta\cdot mean\left(\alpha(i)^k_j\right)}{2} \qquad \underset{j\in N_i}{\forall}\ \underset{k\in N_j}{\forall}\ \beta(i)'_j = \frac{\beta(i)_j + \delta\cdot mean\left(\beta(i)^k_j\right)}{2} \tag{3}$$

where

- i is the node which is performing detection
- N_i is the neighbourhood of node i
- $\alpha(i)_j$ is the value of α calculated for every neighbour j of i, obtained from direct observations at i

- $\beta(i)_j$ is the value of β calculated for every neighbour j of i, obtained from direct observations at i
- $\alpha(i)^k_j$ is the value of α calculated for every neighbour j of i, obtained from observations of every neighbour k of j
- $\beta(i)^k_j$ is the value of 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 only processes those reputations for its own neighbours, because reputations about nodes that are not in its neighbourhood are useless. Once the reputations have been obtained, and the adequate analysis has been done, the detection only needs a predefined tolerance threshold to identify if a node is misbehaved 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 using the Direct Data Collector, thereby detecting black holes as the bayesian watchdog does. In this case if the relationship between α and β exceeds a predefined tolerance level, the watchdog identifies that node as malicious (the bayesian detection module). For the collaborative approach, a node receives reputation information from its neighbours (the Indirect Data Collector module) and calculates, using Equations (3) a new set of reputations. Then if the relationship between α' and β' exceeds a predefined tolerance level, the collaborative detection module identifies the node as malicious. Finally, a misbehaving node is detected both if the local detection is positive and either if the collaborative detection is positive.

4. Evaluation through simulation

We first evaluate through simulation how our approach is able to improve previous non-collaborative watchdog proposals. After that, in Section 5 the global improvement and the effect of the collaboration will be evaluated.

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 1 shows the characteristics of the scenarios we have selected for our performance evaluation.

Some of these parameters, like the area, the number of nodes or speed, are needed by ns-2 to execute the simulation. Others, like δ, γ, or the *observation time*, are needed by our code to perform its functionality. 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.

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 approach. 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. 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[2] node A's neighbourhood, our approach allows node 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 it enters 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

[2] 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

collaborative bayesian watchdog needs to detect. This is because the interval between packets is very short. Nevertheless, in networks with low traffic load and with black holes that transmit a very small amount of packets, the performance between the two approaches could be more significant 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 node speed of 10 m/s. In fact, when node moves at 10 m/s and 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 Area Networks, or VANETs, a type of MANET formed by vehicles in movement, which share data when they cross with another car, or communicate with a fixed network infrastructure.

Figure 2 shows that the accuracy is also slightly better than with the non-collaborative bayesian watchdog, which comes from the decreased level of false negatives. The fact is that the collaborative bayesian watchdog now detects a small amount of black holes that are not detected with the bayesian watchdog. In fact, our approach is able to detect cases where a black hole quickly enters and exits from the range of a watchdog. As shown in Figure 2, 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. With respect to the standard watchdog, our approach clearly surpasses it in terms of detection accuracy.

5 Analytical modelling

On the previous section we focus the evaluation on the local performance of the collaborative bayesian watchdog. In order to evaluate the global behaviour we found that simulation was not feasible. The complexity and time consuming of the network simulation under realistic scenarios was the main reason to develop an analytical model. Thus, the goal of this section is to model and evaluate the performance of our collaborative bayesian watchdog taking into account the effect of collaboration and false negatives events.

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. For our model, we assume that the occurrence of contact between two nodes follows a Poisson distribution with rate λ. This has been shown valid for both human and vehicle mobility patterns [12, 13, 14]. Therefore, we consider that using an exponential fit is a good choice to model inter-contact times in bounded scenarios. Moreover, using exponential distributions we can formulate analytical models using Markov chains.

5.1 Modelling bayesian and collaborative detection

The watchdog is modelled using two parameters: the probability of detection p_d and the accuracy p_a. The first parameter p_d, reflects the probability that, when a node contacts another node, the bayesian watchdog has enough information to decide whether a node is acting as a selfish or black hole node 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. The second parameter p_a is the accuracy expressed as a ratio. The ratio of false negatives generated when a node contacts a black hole node can be expressed as $(1- p_a)$.

The collaboration detection is modelled using a function f_{cp}. This function reflects the probability that a node detects the selfish node 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 (3)). 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 previously detected the malicious node and nodes that have not detected them. 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:

$$f_{cp}(c_p, c_n) = \begin{cases} 0 & (c_p - c_n) \le 0 \\ \delta p_a \dfrac{\max\left[(c_p - c_n), C_t\right]}{C_t} & (c_p - c_n) > 0 \end{cases} \tag{5}$$

where c_p is the number of collaborative nodes that have a positive (i.e., have detected the selfish node), and c_n is the number of nodes that have a negative. The factor p_a reflects that only the true positives are taken into account, and δ corresponds to the level of trust.

Using the previous parameters we can model the probability of detecting a selfish node when a contact occurs: i) the node contacts with the black hole node and the local watchdog detects it, with probability $p_d \cdot p_a$; ii) the node contacts another node that has a positive about the black hole node with probability f_{cp}. Finally, a false negative can be generated with probability $p_d\,(1\text{-}p_a)$.

In the next subsection we introduce a generic analytical model for evaluating the performance of the collaborative watchdog approach. The goal is to obtain the detection time of a black hole node in a network.

5.2 A Model for the Detection of Selfish Nodes

This model takes into account the effect of the accuracy on the global detection time. 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: $c_p + c_n \le C$, so some states are not reachable. 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 (τ = C(C + 1)) and υ as the number of absorbing states (υ = (C + 1)). This model can be expressed using the following transition matrix **P** in canonical form:

$$P = \begin{pmatrix} Q & R \\ 0 & I \end{pmatrix} \qquad (6)$$

where I is a $\upsilon\times\upsilon$ identity matrix, 0 is a $\upsilon\times\tau$ zero matrix, 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 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 $\lambda(p_d\cdot p_a + f_{cp}(c_p,c_n)\max(C-c_p-c_n,0))$. The term $p_d\cdot p_a$ 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. If there are no pending nodes, this value is 0.
- (c_p, c_n) to $(c_p, c_n + 1)$: A new collaborative node has a negative (a false negative). The transition probability is $\lambda\ (p_{d(1\text{-}p_a)}+f_{cn}(c_p,c_n)\max(C-c_p- c_n,0))$.
- $(c_p + 1, c_n)$ 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: $\lambda(p_d(1\text{-}p_a)+f_{cn}(c_p,c_n)c_p)$.
- $(c_p, c_n + 1)$ 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 $\lambda(p_d\cdot p_a +f_{cp}(c_p,c_n)c_n)$.
- (c_p,c_n) to (c_p,c_n): This is the probability of no changes and is $1\text{-}\Sigma_{j\neq i}\ p_{ij}$.

Using the transition matrix 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 $N = (I - Q)^{-1}$, we can obtain a vector t of the expected time to absorption as t = Nv, where v is a column vector of ones $(v = [1, 1, \ldots\ 1]^T)$. 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:

$$T_d = E[T] = v_1 N v \qquad (7)$$

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

5.3 Model evaluation

Now, based on the previous model, we evaluate the effect of collaboration and local accuracy on the performance of the collaborative bayesian watchdog. The models allow an overall evaluation of the collaborative watchdog under a large number of scenarios. For the following experiments we used the following parameters that were obtained from the previous experimental evaluation: p_d =0.1, C_t =5, δ=0.3, p_a =0.95 and λ=0.02.

The first experiment evaluates the improvement on the global detection time using our collaborative approach. We evaluate the time that all nodes (except the misbehaving node) have a positive about this misbehaving nodes depending on the number of nodes. The results are shown in Figure 3.a. The graph starts in N = 2, that is a black hole node and a collaborative node, so both approaches have the same detection time (there is no collaboration). But, when $N \geq 2$ we can see that using our collaborative watchdog the detection time is practically the same but using only the collaborative watchdog the detection time increases exponentially.

The second experiment evaluates the impact of the local watchdog accuracy comparing the results with a non-collaborative approach (that is, depending only on the local watchdog) for a network of 40 nodes (N = 40). In this case, we expect that the diffusion of α and β can reduce the influence of false negatives. Figure 3.b shows the detection time depending on the accuracy p_a. First, we can see that detection time is greatly reduced using the collaborative watchdog. Second, the detection increases with a very little slope when p_a decreases 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. These experiments where repeated for different values of N, $p_{d,}$ λ and the results were very similar.

Two conclusions can be drawn from the performed analytical evaluation: our collaborative watchdog is able to drastically reduce the detection time of malicious nodes while also improving the overall detection accuracy.

5. Conclusions

In this paper we proposed a Bayesian watchdog based collaborative approach for a fast detection of selfishness and black holes in MANETs. We demonstrate how, by analysing second-hand information using a collaborative bayesian watchdog, we can help at boosting its performance by decreasing the amount of false negatives and speeding up the detection process. The performance simulation study exhibits a local improvement on the detection speed while slightly increasing the accuracy of the detection process. We also present a performance evaluation using an analytical model, which demonstrates that the collaborative approach is able to reduce the detection time and increase the global accuracy. These conclusions evidence that, compared to other existing solutions, the proposed technique is able to offer significant performance improvements, thereby fitting not only generic MANET environments, but also VANET environments.

As a future work, we aim at implementing the collaborative detection mechanism in a hardware testbed (Castadiva), while working on the fine-tuning of the collaborative bayesian watchdog to apply this technique on Delay Tolerant Network environments.

Acknowledgments

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

References

1. Buchegger, S., Le Boudec, J.Y. (2005). Self-policing mobile ad hoc networks by reputation systems. IEEE Communications Magazine, Vol. 43(7), pp. 101-107.
2. Buttyan, L., Hubaux, J.P. (2000). Enforcing service availability in mobile ad-hoc WANs. In: IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC'2000)
3. Buttyan, L., Hubaux, J.P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile

Networks and Applications 8(5)

4. Hortelano, J., Calafate, C.T., Cano, J.C., de Leoni, M., Manzoni, P., Mecella, M. (2010). Black-hole attacks in p2p mobile networks discovered through bayesian filters. In: Proceedings of OTM Workshops'2010, pp. 543–552

5. Hortelano, J., Cano, J.C., Calafate, C.T., Manzoni, P. (2010). Watchdog intrusion detection systems: Are they feasible in manets? In: XXI Jornadas de Paralelismo (CEDI'2010).

6. Kargl, F., Klenk, A., Schlot, S., Webber, M. (2004). 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).

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

8. Sundarajan, T., Shammugam, A. (2010). Modeling the behavior of selfish forwarding nodes to stimulate cooperation in MANET. International Journal of Network Security and its Applications (IJNSA)

9. Toh, C.K., Kim, D., Oh, S., Yoo, H. (2010). The controversy of selfish nodes in ad hoc networks. In Proceedings of the Twelveth international conference on Advanced communication technology (ICACT'10)

10. Xu, L., Lon, Z., Ye, A. (2006). 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)

11. Zhong, S., Chen, J., Yang, Y. (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: Proceedings of the Twenty-second Annual Joint Conference of the IEEE Computer And Communications Societies (INFOCOM'03).

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

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

14. Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng (2011). "The impact of node selfishness on multicasting in delay tolerant networks," Vehicular Technology, IEEE Transactions on, vol. 60, no. 5, pp. 2224 –2238, jun 2011.

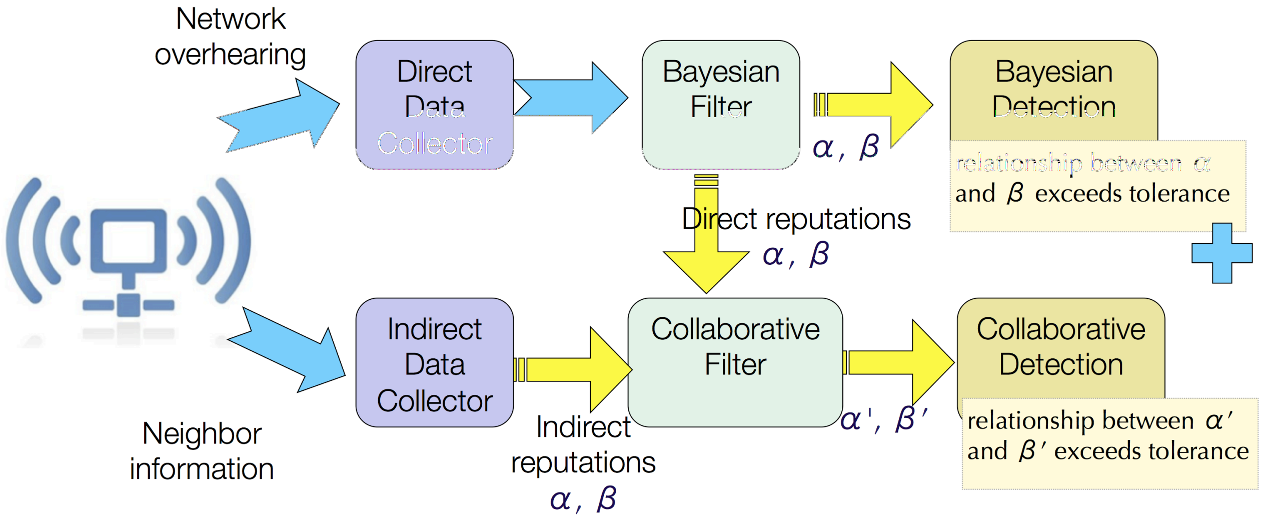


Figure 1: Architecture of the collaborative watchdog

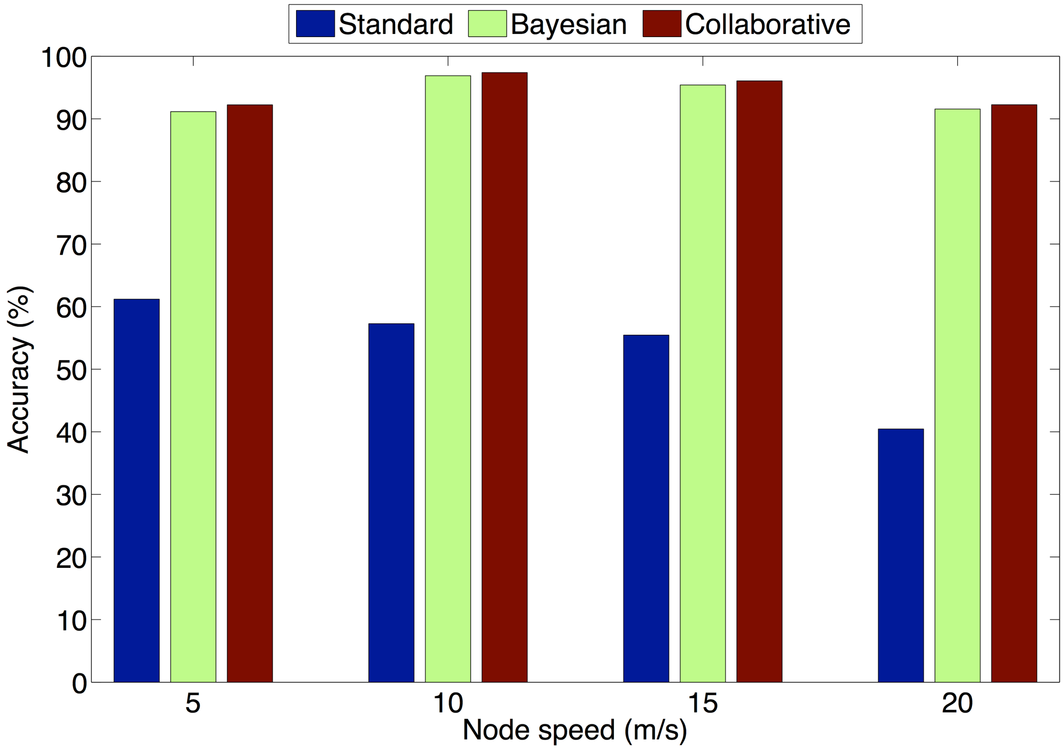
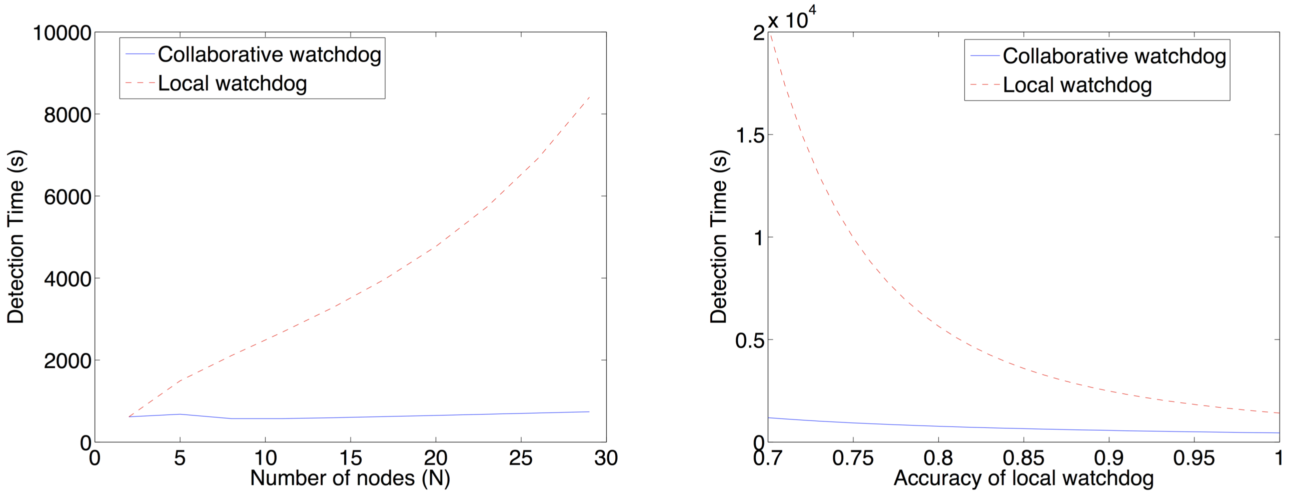


Figure 2: Accuracy comparison of the different watchdog versions



a)

b)

Figure 3:Evaluation of the collaborative watchdog using the model

Table 1. Simulation parameters

Parameter	**Value**
Nodes	50
Area	1000x1000 m.
Wireless interface and bandwidth	802.11 at 54 Mbps
Antenna	Omnidirectional
Node speed	5, 10, 15 and 20 m/s.
% of black holes	10%
δ	0.8
γ	0.85
Fading	1
Neighbour time	1 s.
Observation time	0.2 s.
UDP Unicast traffic	Three flows
UDP Broadcast traffic	Every 5 s.
Simulation time	352 s.
Scenarios	20