Cross-layer approach to improve the monitoring process for mobile ad hoc networks based on IEEE 802.11

Abderrezak Rachedi, Abderrahim Benslimane

Cross-Layer approach to improve the monitoring process for Mobile Ad Hoc Networks based on IEEE 802.11*

Abderrezak Rachedi and Abderrahim Benslimane
LIA/CERI, University of Avignon, Agroparc
BP 1228, 84911 Avignon, France
Email: {abderrezak.rachedi, abderrahim.benslimane}@univ-avignon.fr

***Abstract*— The monitoring process consists in evaluating the behaviour of nodes in networks in order to detect if the monitored nodes well-behave or misbehave. Many existing solutions deal the problem at each layer separately. Actually new kinds of misbehaviour attacks are cross-layer. So, such smart misbehaviours cannot be detected at the level of one layer. In this paper, we propose a new cross-layer approach based on physical, MAC and routing layers for a monitoring mechanism. An analytical model is proposed to illustrate the parameters' effect on these different layers. The impact of the Signal to Noise Rate (SNR), the distance between monitor and monitored nodes are clearly introduced. Moreover, the difference between the carrier sense, the interference and the transmission ranges is taken into account in our model. The simulations' results show the effectiveness of the proposed analytical model, we reach until 90% of observation's correction in some cases.**

I. Introduction

The detection of a certain type of misbehaviour nodes in Mobile Ad hoc Networks (MANETs) is one of the hardest issues. Misbehaviour means deviation from the regular activity of nodes, for example routing and forwarding. It arises because of several reasons, non-intentionally when a node is faulty or doesn't have any plan to attack any node in a network. Intentional misbehaviour can aim at taking advantage (like intercepting the network traffic, saving its power, increasing its bandwidth ...etc) or just at constituting some damage in a network. Without any detection system of misbehaviour nodes, the result effects of misbehaviour have shown that they dramatically decreased the performance of the network [1] and produced the denial of service (DoS). In order to solve the problem, many recent works proposed the solution based on the preventive aspect, for example secure a routing using cryptography such as Ariadne or SRP [2] and ARAN protocols [3]. Although these solutions are limited in an open network, for example the unknown nodes can arrive in the network, the problem is how to protect the confident nodes against prospective attacks from unknown nodes. That's why we need to monitor the behaviour of nodes in a network. A recent research work was dealing with the reputation system based on the observation of the reaction of monitored nodes [2]. For example a watchdog solution based on packets forwarding to detect the non-forwarding nodes [4]. The definition of the monitoring process is the set of actions that are useful to supervise the nodes' behaviour. These actions depend on the services which we want to monitor (routing, authentication, integrity, ...). The major problem of a current proposal of monitoring process like watchdog for example is that it doesn't take into account some characteristics of MANETs.

In this paper, we study the monitoring process to maintain the security in Mobile Ad hoc Networks (MANETs). The impact of physical and MAC's parameters protocols on the monitoring mechanisms on MANETs are investigated. The distributed coordination function (DCF) mode in IEEE 802.11 is taken as an example. We analyze different situations of monitor and monitored nodes (a distance between them, a transmission time duration, a transmission probability, ...). Furthermore, we propose a new analytical model which takes into account the physical layer's parameters, the MAC layer's parameters and routing layer's parameters like a forwarding process. The model proposed improves the evaluation of the nodes' cooperation and clearly distinguishes nodes which can not and those which don't want to cooperate correctly.

The rest of the paper is organized as follows. In section 2, we introduce our motivation and the problematic in monitoring process. In section 3, we describe the network assumption and a model. In section 4, we present the analytic and simulation results of a proposed model. The last section is the conclusion and we also present our future works.

II. Motivation

In MANETs, all the mobile nodes don't have the same information of their neighbours, because the characteristics of MANETs like dynamic topology and the hidden nodes complicate the problem of monitoring. If we only based on the monitoring process at the network level, for example the rate of packets forwarded, we would take the risk of get a false estimation of the monitored nodes' reputation. That's why we adopt a cross-layer approach to design the monitoring process. When a monitor node wants to supervise the behaviour of its neighbours, it needs to know some important piece of information like the number of nodes in the interference range, the throughput and delay in the neighbourhood of the monitored nodes.

* This work is supported by the ANR "Agence Nationale de la Recherche - France" within the project framework ARA/CLADIS.

When the monitor node A wants to monitor a node B which is its neighbour, the node A doesn't have any piece of information about the environment of the monitored node B, if a node C is located in the interference range of the node B and cannot be heard by the monitor node A. The node C can reduce the reputation of the node B by generating an important traffic to an other node out of a sensing region of the node A and prevent the monitored node B from communicating and forwarding packets. In this event, the monitor node A gives a low estimation of the node B's reputation and classes the node B as non-cooperative.

In order to avoid this problem, the monitor node needs to know the MAC layer's parameters of its monitored neighbours. We conclude that the presence of an important traffic of nodes in the interference range of the monitored nodes and out of the carrier senses of the monitor nodes can punish the well-behaving nodes and disturb the monitoring process.

The monitoring process proposed by Marti et al. [4], called Watchdog, is based on the network level; it didn't take into account the physical or the MAC level's parameters. The idea is that the monitor node can listen to the traffic of its neighbours, and detect if the monitored nodes forward the packets in the event of a routing procedure. The Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) monitor/monitored collisions, 2) limited transmission power, 3) false misbehaviour.

The monitor nodes can generate a false evaluation of the monitored nodes' cooperation in these following events:

- *The case of a monitor collision*: the monitor node can get a collision because some nodes transmit in its interference region but not in the sensing region of the monitored nodes; in this situation, the monitored node can forward the packets (subject of monitoring) but the monitor node cannot hear them. Therefore, the monitor node doesn't take into account these forwarding operations, that means the reputation reported is underestimated by the monitor node.
- *The case of a monitored collision*: the monitored node can have more collisions than a monitor node because it has many competing nodes that want to have access to the channel in its sensing range. In this case, the monitored node cannot transmit the packets, although it doesn't refuse to forward them. That's why, the monitor node needs to know what is going on in the hidden region (sensing region of the monitored node but not of the monitor node).
- *The case concerning the presence of malicious nodes*: the presence of any malicious node in the common interference region of monitor and monitored nodes doesn't affect the monitoring process because both nodes (monitor and monitored ones) have the same observation in this region. The problem occurs when the malicious nodes are present in the interference region of the monitored nodes and cannot be heard by the monitor one.

The goal of this work is to study the monitoring process in the different cases, monitor/monitored collision and false misbehaviour.

III. Monitoring model

A. Network model and assumption

This subsection deals with the assumptions and the network model used in the analysis described below.

- Spacial distribution of nodes: we assume that nodes are distributed within topology which is a two-dimensional Poisson process's with parameter λ (memoryless property of Poisson distribution).
- The transmission range (R_t): all nodes have the same transmission range (R_t). This means that nodes within a circle of radius R_t centred at the transmitter may be able to receive correct packets.
- The Carrier sensing range (R_s): the range inside which nodes are able to sense the signal, even though a correct packet reception may not be possible (it may not be able to decode the received packet correctly).
- The interference range (R_i): the range inside which any new transmission may interfere with the packet reception. The R_i depends on the distance between a transmitter and a receiver (d) and the Signal to Noise Ratio (SNR) which must be above a certain threshold T_{SNR} to consider if the signal is valid at the receiver or not. The R_i is defined by,

  $$R_i = \sqrt[k]{T_{SNR}} * d$$

  In practice, under the TWO-RAY GROUND model (open space environnement), k is equal to 4. The T_{SNR} is usully set to 10. Then, the interference range is $R_i = \sqrt[4]{10} * d = 1.78 * d$ [5].
- The average number of nodes within a sensing range, an interference range and a transmission range with a radius R_s, R_i and R_t respectively is $N_j \approx \lambda \pi R_j^2$ where $j = \{s, i, t\}$ [6].
- The probability that a node transmits in a randomly time slot is noted by τ which is independent on any time slot. The slot time size, σ, is set equal to the time needed by any node to detect the transmission of a packet from any other node. The transmission time T_p of a packet is assumed to be the same for all nodes. The number of slot times γ necessary to transmit a packet is ($\gamma = T_p/\sigma$). Like [7] we assume that the duration of the successful packet transmission (RTS/CTS mode) is

  $$T_{all} = T_{rts} + T_{cts} + T_{data} + T_{ack} + 4\sigma$$

According to the assumptions quoted above, the relation between the carrier sensing range, the interference range and the transmission range is $R_t < R_i < R_s$ where $R_s = \delta R_t$, in some network simulator, like ns2 $\delta = 2.2$ [11].

B. The different hidden areas

The figure 1 illustrates the hidden sensing region and the hidden transmission region of two neighbour nodes A and B. The $CS_{AB}(r)$ ($IR_{AB}(r)$) is the sensing region of the node A but not the sensing region of the node B (the interference

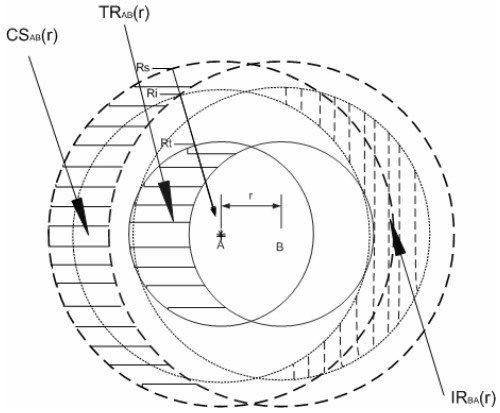

Fig. 1. The different hidden regions, CS_{AB}, IR_{AB} and TR_{AB}

region of the node A but not the interference region of the node B). If any node in $CS_{AB}(r)$ transmits, the signal can be sensed by the node A but not by the node B. The difference between $CS_{AB}(r)$ and $IR_{AB}(r)$ is seen when a node in the region $IR_{AB}(r)$ transmits, it can create a collision in a receiver node A but it is not the case for the nodes in region $CS_{AB}(r)$. $TR_{AB}(r)$ is the transmission region of the node A but not the transmission region of the node B, that means the nodes in $TR_{AB}(r)$ can receive the packets correctly from the node A but it can not from the node B.

The difference between $IR_{AB}(r)$ and $TR_{AB}(r)$ is the problem of the hidden nodes, in $TR_{AB}(r)$ this problem is resolved by the RTS/CTS mechanism in IEEE 802.11 but in $IR_{AB}(r)$ the RTS/CTS mechanism cannot resolve this problem because the nodes in this region cannot decode the packets correctly when the node A transmits RTS/CTS/DATA/ACT. When a node senses a signal but cannot decode it, that means it cannot calculate a NAV (Network Allocation Vector), that's why it uses the EIFS (Extended Inter-Frame Spaces)[1] [10]. The IEEE 802.11 does not completely prevent from collisions due to a hidden node in the sensing region.

In the context of monitoring process, we assume that the node A monitors the node B. In order to get some piece of information about a cooperation with the node B, the node A transmits a few packets to it, so that it forwards them. After the monitor A has observed the behaviour of the node B, it generates the report about the forwarding rate. In this work, we focus on the region $CS_{AB}(r)$, $IR_{AB}(r)$ and the region $TR_{AB}(r)$ because these regions have important effects on the monitoring process. In the figure 1, when a node A monitors a node B, the node A cannot see what is happening in the region $TR_{BA}(r)$ (transmission region of the node B and not of the node A), the problem is that the monitor node A is unable to know if the node B doesn't want or if it can not transmit because the number of competition nodes in $TR_{BA}(r)$ is great. Another problem occurs in the monitoring process, in the interference region of the monitor node A and out of the carrier sense of the monitored node $[IR_A - CS_B]$. When a monitor A has a collision because a few nodes in $IR_{AB}(r)$ transmit, when a node B forwards a packet that it received from a node A, in this situation the node A is unable to know if the node B has successfully forwarded a packet or not. Thus, the monitor node A underestimated the forwarding ratio of the node B.

The regions $TR_{AB}(r)$ and $CS_{AB}(r)$ depend on the transmission range (R_t) and the sensing range (R_s) respectively and (d) is a distance between nodes A and B. We can formulate these regions by the equation 1:

$$\begin{aligned} CS_{AB}(r) &= \pi R_s^2 - 2R_s^2 q(r/2R_s) \text{ where, } r < R_s \\ TR_{AB}(r) &= \pi R_t^2 - 2R_t^2 q(r/2R_t) \text{ where, } r < R_t \end{aligned} \quad (1)$$

where $q(t) = arcos(t) - t\sqrt{(1-t^2)}$ and $R_s = \alpha R_t$

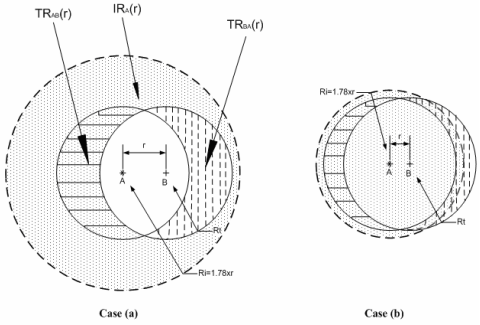

Fig. 2. The impact of a distance on the interference and the hidden areas

Figure 2 shows an example of two neighbour nodes A and B with a different distance between them. Let r be the distance between two neighbour nodes A and B. In the case (a), the distance between node A and node B is greater than in the case (b), which means that the interference region and the region $TR_{BA}(r)$ in the case (a) is greater than in the case (b). When a node A comes closer to a node B, the region $TR_{BA}(r)$ becomes smaller and the interference region can be covered by the transmission area when the $r \leq \frac{R_t}{\sqrt[4]{T_{SNR}}}$. The average number of nodes in the region $TR_{BA}(r)$ depends on the distribution of the nodes and the mobility model. The greater a region $TR_{BA}(r)$ is, the bigger the probability to get a certain number (k) of nodes in this region is. The probability to get k nodes in the area $TR_{BA}(r)$ is noted $p(k, TR_{BA}(r))$ and obtained by:

$$p(k, TR_{BA}(r)) = e^{-\lambda TR_{BA}(r)} \frac{(\lambda TR_{BA}(r))^k}{k!} \quad (2)$$

This analysis is valid for the $CS_{BA}(r)$ and $IR_{BA}(r)$ because it's proportional to the distance r.

Remark: The monitoring process is more accurate when the monitor node A is close to the monitored node B, because the hidden region of the monitor $TR_{BA}(r)$ becomes small. As $TR_{BA}(r)$, $IR_{BA}(r)$ and $CS_{BA}(r)$ are proportional to r, when r is small, these areas are small and the probability to get a node in these regions is small, the carrier sense of a monitor node can also cover the interference region of a monitored node. Furthermore, the interference area can be covered by the

[1]The EIFS is estimated at $364\mu s$ when using a 1 Mbps channel bit rate

transmission region when $r \leq 0.56 * R_t$. Thus, the probability to have a disturbance in the observation is small when the monitor node is close to the monitored node.

Therefore, before the monitor node generates the reputation report of the monitored node which is in its transmitting range, it needs to know that the event which disturbs the observation occurs and also to estimate the throughput of the monitored node. The accuracy of this information depends on the distance between monitor node A and monitored node B.

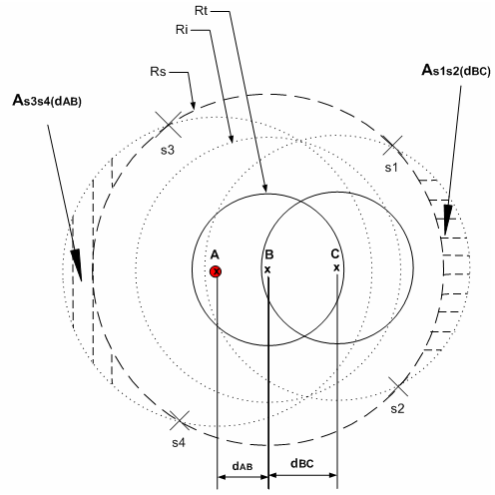

Fig. 3. An illustration of different vulnerable regions in the monitoring process

Figure 3 illustrates the interference region of a node C that is out of the sensing region of a monitored node B ($A_{S1S2}(d_{BC})$) where the distance between both nodes is d_{BC}. The $A_{S1S2}(d_{BC})$ is a vulnerable region when a monitored node B transmits a packet to a node C. Furthermore, the vulnerable region of a monitor node A is the interference region of a monitor node A that is out of the sensing region of a monitored node B ($A_{S3S4}(d_{AB})$), where the d_{AB} is the distance between monitor node A and monitored node B. The $A_{S3S4}(d_{AB})$ can have a negative impact on the monitor node's observation.

Any disturbing event in the monitoring process occurs "when a monitored node transmits successfully, and at least one node in the interference region of the monitor node and out of the sensing region of the monitored node transmits at the same time". In other words, the monitor node can correctly monitor its neighbour, if the following two conditions are met,

- *Condition 1*: The monitored node transmits successfully a packet to another node of its neighbourhood.
- *Condition 2*: The monitor node can correctly hear the transmission of a monitored node. No node in the interference region of a monitor node and out of the sensing region of a monitored node ($A_{S3S4}(d_{AB})$) transmits.

The monitor node needs to estimate the probability that the condition 1 and 2 are met, in order to calculate the probability that the monitor node correctly observes the monitored node when it transmits. This probability is noted P_w.

$$P_w = P\{\text{condition 1}\}.P\{\text{condition 2}\} \quad (3)$$

The probability of condition 1 is defined as a successful packets' transmission of the monitored nodes noted P_{succ}. P_{succ} may give us information about the ability of the monitored nodes to transmit packets. However, the probability that a monitor node gets P_{succ} of the monitored node is small, because it cannot see what happens in the whole sensing region of the monitored node, particularly in region $CS_{BA}(d_{AB})$. According to the assumptions quoted above, the monitor node A can estimate the average number of nodes in the region $CS_{BA}(d_{AB})$, but another problem has to be solved is the traffic load in this region. Two main cases appear. The first one: the traffic is intensive, that means that all nodes have a packet to transmit (saturated case). In this case, many researches have been carried out in order to calculate P_{succ} with the assumption that $R_t = R_i = R_s$ [8] [6], but as far as we know no work took into account the difference between the transmission, the interference and the carrier sense ranges. The second case (non-saturated case): the nodes have or not packets to transmit, that depends on the probability that nodes have a packet to transmit q. In order to calculate the P_{succ} in this case a few researches have been carried out like Malone et al. [9] but they didn't take into account the difference between R_t, R_i and R_s. In the second case, the monitor node A can not correctly estimate the P_{succ}, it needs a cooperation with a monitored node's neighbors which overlaps the region $CS_{BA}(d_{BA})$.

In order to calculate P_w, we distinguish two different situations, the saturated case and the non-saturated case. In this work, we focus on the saturated case.

C. Saturate case

In this case, the estimated nodes in each region are the competiting nodes which want to have access to the channel.

The probability of condition 2 gives us information about the observation disruption of a monitor node. This probability is obtained by the assessment of the probability that any node in region $A_{S3S4}(d_{AB})$ transmits ($P\{cond.2\}$) in a vulnerable period. This period depends on the transmission time of a packet T_{all}, when a node B starts to transmit at t_s the vulnerable time interval is $[t_s - T_{all} - 1, t_s + T_{all} - 1]$. The nodes in region $A_{S3S4}(d_{AB})$ must remain silent during the μ slots time where $\mu = (T_{all}/\sigma)$, because a node in sensing and interference range waits for a EIFS when it can not calculate a NAV vector. If EIFS is greater than a T_{all}, the packet can be received correctly by the receiver node C. Otherwise, a packet can not be correctly received. The region $A_{S3S4}(d_{AB})$ can be equal to zero when it is covered by the carrier sense of a node B. Thus, the $P\{cond.2\}(d_{AB})$ in the case of $d_{AB} > \frac{R_s}{1+\sqrt[k]{T_{SNR}}}$ is given by,

$$P\{cond.2\}(d_{AB}) = \Big(\sum_{k=0}^{\infty}(1-\tau)^k \frac{(N_h)^k}{k!} e^{-N_h}\Big) = e^{-\tau N_h . \mu}$$

where, $N_h = \lambda A_{S3S4}(d_{AB})$.
The final equation of $P\{cond.2\}(d_{AB})$ is obtained by,

$$P\{cond.2\}(d_{AB}) = \begin{cases} 1 & \text{if } d_{AB} \leq \frac{R_s}{1+\sqrt[k]{T_{SNR}}} \\ e^{-\tau N_h.\mu} & \text{Otherwise} \end{cases} \quad (4)$$

In order to calculate $A_{S3S4}(d_{AB})$, we calculate the area of intersection of sensing region and interference region of two nodes X and Y; the distance between them both is d.

$$Ar_{\{X \bigcap Y\}}(d) = R_s(arccos(\alpha) - \alpha\sqrt{1-\alpha^2}) + R_i(arccos(\beta) - \beta\sqrt{1-\beta^2})$$

where $\alpha = \dfrac{R_s^2 - R_i^2 + d^2}{2dR_s}$ and $\beta = \dfrac{R_i^2 - R_s^2 + d^2}{2dR_i}$

Therefore, the $A_{S3S4}(d_{AB})$ is expressed by,

$$A_{S3S4}(d_{AB}) = \begin{cases} 0 & \text{if } d_{AB} \leq \frac{R_s}{1+\sqrt[k]{T_{SNR}}} \\ \pi R_s^2 - Ar_{\{A \bigcap B\}}(d_{AB}) & \text{Otherwise} \end{cases}$$

If $A_{S1S2}(d_{BC}) = 0$, that means that the carrier sensing region of a node B overlaps the interference region of a node C and no node transmits.

Now, from equations 3 and 4, we can calculate $P_w(d_{AB})$ as follows:

$$P_w(d_{AB}) = \begin{cases} P_{succ} & \text{if } d_{AB} \leq \frac{R_s}{1+\sqrt[k]{T_{SNR}}} \\ P_{succ}.e^{-\tau N_h.\mu} & \text{Otherwise} \end{cases} \quad (5)$$

The reputation report of the monitored node (B) generated by the monitor node (A) is given by,

$$R_{A,B}(d_{AB}) = \eta.P_w(d_{AB}) \quad (6)$$

where η is the forwarding ratio observed by a monitor node,

$$\eta = \left(\frac{\text{\#forwarded packets}}{\text{\#total sent packets}}\right)$$

The predictable forwarding packets of any monitored node depends on its reputation calculated by monitor nodes and the total number of packets it forwards.

$$\text{\#Forwarded packets} = R^*_{(A,B)}.(\text{\#total sent packets}).P_w \quad (7)$$

IV. Numerical results and discussion

In this section, we present the results of our model in different situations ; when the distance between monitor and monitored nodes is different and also the impact of the transmission probability τ.

The figure 4 shows the hidden area A_{S3S4} according to the distance between nodes A and B with $550m$ of sensing range and interference $R_i = \sqrt[4]{10}.d_{AB}$. When the distance between nodes is less than $200m$ the $A_{S3S4} = 0$, that means the region A_{S3S4} is covered by the sensing region of a node B in the case of $R_i = 1.78.d_{AB}$. When the sensibility of a signal is great the interference range becomes greater and the region A_{S3S4} becomes less covered by the sensing region of a node B as shows in the figure 4 when $R_i = 1.90.d_{AB}$.

The figure 5 illustrates the probability that any node in the region $A_{s3s4}(d)$ transmits during the slot time $\mu = 1.\sigma$. We remark that the probability $P\{cond.2\}$ equals to one when

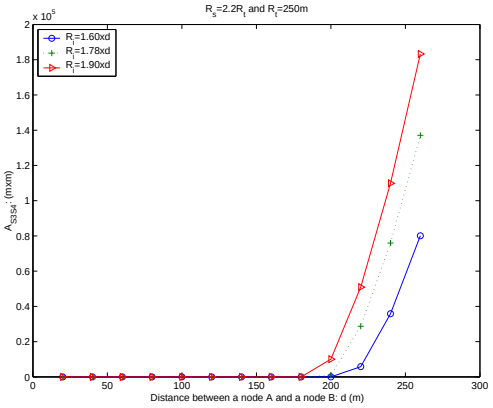

Fig. 4. The hidden area A_{S3S4} versus distance between nodes A and B

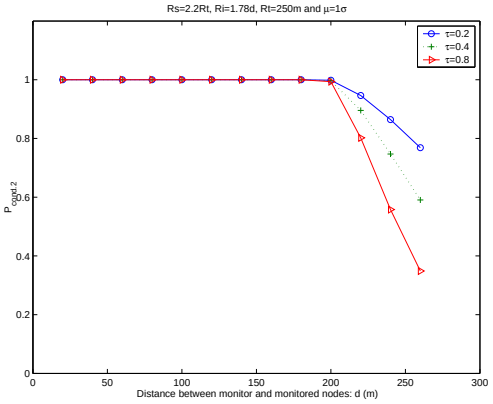

Fig. 5. $P\{cond.2\}$ versus distance between nodes A and B (case of $\mu = \sigma$)

the distance between A and B is less than 200 meter, due to the region $A_{s3s4}(d)$ which is overlapped by the sensing region of a node B. However, when the distance between a node A and a node B becomes greater the $P\{cond.2\}(d)$ decreases and it decreases rapidly when the probability of transmission τ is great. The figure 6 shows the $P\{cond.2\}(d)$ when a transmission duration μ is great ($\mu = 5\sigma$), we note that the $P\{cond.2\}(d)$ is smaller than in the case of time duration $\mu = \sigma$. We can conclude that the threshold T_{SNR}, the distance between monitor and monitored nodes and the transmission time μ have an important impact on the monitoring process.

Figure 7 shows the probability that a monitor node A correctly receives the transmission from a monitored node B, that means a node A doesn't have a collision because no node in region $A_{s3s4}(d_{AB})$ transmits. We note the degradation of the monitor's observation when the distance between monitor and monitored nodes is great. In this case, the degradation of the monitor's observation can reach until 40%. Furthermore, the figure 8 and 9 illustrate the impact of the transmission probability τ and the number of slots time μ on the monitor's observation. The worst case occurs when the distance between monitor and monitored nodes is great and the probabilities of transmission τ and μ are great, and the degradation of the monitor's observation can reach until 95%.

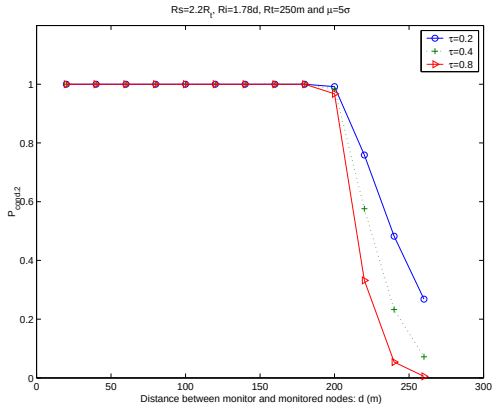

Fig. 6. $P\{cond.2\}$ versus distance between nodes A and B (case of $\mu = 5\sigma$)

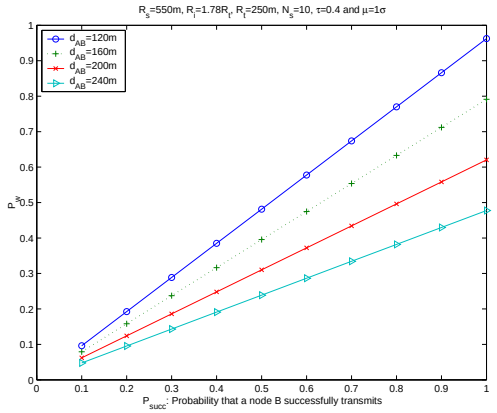

Fig. 7. P_w versus distance between two nodes ($\tau = 0.4$ and $\mu = 1.\sigma$)

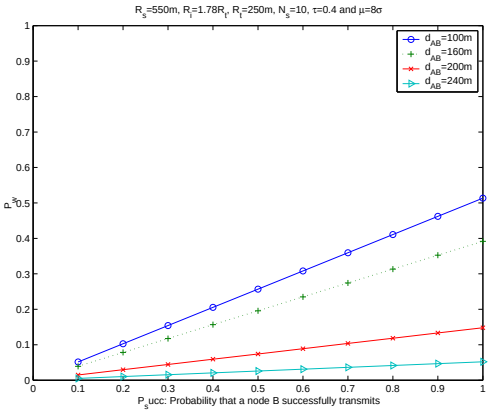

Fig. 8. P_w versus distance between two nodes ($\tau = 0.4$ and $\mu = 8.\sigma$)

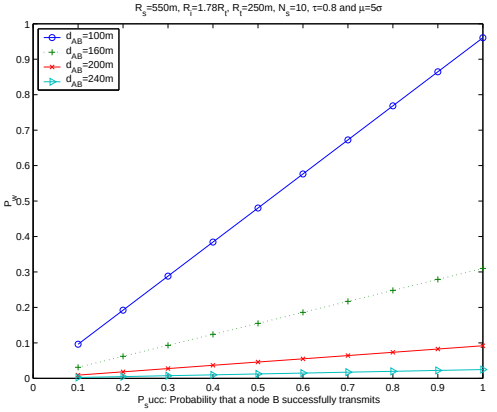

Fig. 9. P_w versus distance between two nodes ($\tau = 0.8$ and $\mu = 5.\sigma$)

V. Conclusion

In this paper, we have developed an analytical model for a monitor node in order to correctly evaluate the reputation and cooperation of a monitored node. The impact of the Signal to Noise Rate (SNR) and the distance between monitor and monitored nodes is clearly introduced, the monitor's best observation is when the monitor is close to the monitored node. In our model, the difference between transmission, interference and sensing ranges is taken into account, unlike many modellings which assume that sensing and transmission ranges are the same. Furthermore, with a cross-layer approach (Physical, MAC and routing layers) adopted for our model to get an accurate evaluation of a monitored node, we can correct until 90% of a monitor's observations.

One possible direction for a future work is to extend our model to the non-saturated case [9] and improve the watchdog process [4] by integrating our model.

References

[1] S. Buchegger and J.-Y. Le Boudec. *Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks*, In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, June 2002.

[2] L. Buttyan and J.-P. Hubaux. *Report on a working session on security in wireless ad hoc networks*, ACM Mobile Computing and Communications Review (MC2R), October 2002.

[3] K. Sanzgiri and B. Dahill and D. LaFlamme and B. N. Levine and C. Shields and E.M. Belding-Royer: An Authenticated Routing Protocol for Secure Ad Hoc Networks. Selected Areas in Communication (JSAC), 598–610, 2005.

[4] S. Marti, T.J. Giuli, K. Lai and M. Baker, *Mitigating Routing Misebehavior in Mobile Ad Hoc Networks*, In Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, pages 255–265, 2000.

[5] K. Xu, M. Gerla and S. Bae, *Effectiveness of RTS/CTS Handshake in IEEE 802.11 based Ad Hoc Networks*, in Ad Hoc Network Journal, Vol. 1 No. 1, Elsevier Science, 2003.

[6] H. Takagi and L. Kleinrock, *Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals*, IEEE Transactions on Communications, Vol.Com-32, No.3, 1984.

[7] Y. Wang and J.J. Garcia-Luna-Aceves, *Performance of Collision Avoidence Protocols in Single-Channel Ad Hoc Networks*, In Proceedings of IEEE ICNP 2002.

[8] G. Bianchi, *Performance Analysis of the IEEE 802.11 Distributed Coordination Function*, IEEE Journal of Selected Area in Telecommunication, Wireless series, vol. 18, no. 3, PP. 535-547, 2000.

[9] D. Malone, K. Duffy, D. Leith *Modeling the 802.11 Distributed Coordination Function in Non-saturated Heterogeneous Conditions*, IEEE/ACM Transactions on Natworking, 2006.

[10] The editors of IEEE 802.11, *Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specification*, 1997.

[11] UC Berkeley and USC ISI, *The network simulator ns-2*, Part of the VINT project. Available from http://www.isi.edu/nsnam/ns, 1998.