Toward a cross-layer monitoring process for mobile ad hoc networks

Abderrezak Rachedi and Abderrahim Benslimane*

LIA/CERI, University of Avignon, Agroparc BP 1228, 84911 Avignon, France

Summary

The intrusion detection system (IDS) for mobile ad hoc networks (MANET) consists in monitoring the nodes’ behavior, in order to detect the malicious activity of nodes. Many existing solutions deal with the problem at each layer separately. But new kinds of misbehavior attacks are cross-layer attacks. And such smart misbehaviors 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. A new analytical model is proposed to illustrate the parameters’ effect on these different layers. The impact of the signal to noise ratio (SNR) and the distance between monitor and monitored nodes are clearly introduced. Moreover, the difference between the carrier sense, the interference range, and the transmission range is taken into account in our model. The proposed model improves the evaluation of the nodes’ cooperation and reduces the risk of having any false positive rate. The analytical study and simulation results illustrate our purpose. In addition, with the simulations’ results, we illustrate the impact of the distance between monitor and monitored nodes on the monitoring mechanism. Finally, we show that our cross-layer mechanism has a lower false positive rate than the classical Watchdog mechanism in different network’s parameters such as the nodes’ density, the speed mobility, and the different traffic loads. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: MANET; security; monitoring process; cross-layer; false positive

1. Introduction

A mobile ad hoc network (MANET) is a special type of wireless network in which a collection of mobile nodes may form a temporary network without the aid of any established infrastructure or centralized administration. A MANET has applications in emergency search-and-rescue operations, in decision making in the battlefield, in data acquisition operations in hostile terrain, etc.

The detection of a certain type of misbehavior nodes in MANETs is one of the hardest problems, because MANETs are characterized by their self-configuration, an open peer-to-peer network architecture, a shared wireless medium, stringent resource constraints, and a highly dynamic network topology. These characteristics make them vulnerable to security attacks. The absence of any intrusion detection system (IDS) of misbehavior nodes would dramatically reduce the performance of the network [1]. Already existing IDS solutions for wired or wireless networks with infrastructure (WLANs) cannot be directly applied to MANETs. Furthermore, the solutions already proposed for MANETs [2–4] did not take into account

*Correspondence to: Abderrahim Benslimane, LIA/CERI, University of Avignon, Agroparc BP 1228, 84911 Avignon, France.
†E-mail: abderrahim.benslimane@univ-avignon.fr

Copyright © 2008 John Wiley & Sons, Ltd.
all MANETs constraints. Indeed, in the network-based IDS, all data can be captured and analyzed by audit mechanisms, which are run on fixed gateways of the network. Thus, the network’s traffic is monitored on wired networks. However, in MANETs, the nodes can only monitor the network’s traffic within their radio transmission range. Except in certain situations, the mobile nodes have not the same observation as their neighbors. For example, when a collision occurs at the monitor node and prevents the observation of the monitored node during a certain period of time. The monitored node could have acted honestly or not. This situation can be brought about by the hidden nodes’ problem. Therefore, the IDS for MANETs cannot efficiently monitor the activity in its neighborhood. In addition, the IDS for MANETs has to deal with another problem related to the lack of interaction between MAC and routing layers [5]. This vulnerability is exploited by the malicious nodes, in order to launch a new class of attacks called “cross-layer attacks.” Generally, these attacks originate from the MAC layer but their target is the denial of service (DoS) at the routing and the upper layers. For this reason, a new approach is necessary to improve the monitoring process in MANET. As far as we know, there is no work dealing with the MAC layer’s parameters, in order to improve the monitoring process.

In this paper, we study the monitoring mechanism used by the IDS in order to observe the nodes’ activities and to estimate their cooperation in the network. We focus on the packet forwarding ratio or the nodes’ participation’s percentage in the routing operation. The monitoring mechanism plays a major role in the evaluation of the nodes’ reputation and in the updating of the nodes’ trust level. We deal with a few issues that have a negative impact, particularly on the monitoring mechanism, when a collision occurs at the monitor node (node with an IDS) during the monitoring process. This situation significantly increases the false positive rate. In order to reduce the false positive rate and to improve the monitoring mechanism, the cross-layer solution is tested. Moreover, we propose a new analytical model that takes into account the physical layer’s, the MAC layer’s, and the routing layer’s parameters. As routing layer’s parameter, we consider the forwarding process. The proposed model improves the evaluation of the nodes’ cooperation and reduces the risk of having any false positive rate. The simulation results illustrate the impact of these problems on MANET IDS.

The rest of the paper is organized as follows. In Section 2, we present the existing security mechanisms, their advantages, and drawbacks. In Section 3, we introduce our motivation and the problems in MANET’s monitoring process. The vulnerable hidden regions are studied in the monitoring mechanism. In Section 4, we describe and detail our analytical model. In Section 5, we present the analytical results and their analysis. Section 6 is devoted to the simulation results and to the model validation. Finally, in Section 7 we give the conclusion of this paper and present our future works.

2. Related Work

The monitoring process is part of the IDS which is necessary to evaluate the nodes’ behavior. The monitoring mechanism is defined as the set of actions that are useful to observe the nodes’ behavior. These actions depend on the services that we want to monitor (routing, authentication, etc). Most of the current works on IDS for MANETs use a distributed and cooperative architecture. The cooperation aspect in MANETS is fundamental for efficient network’s operations and for global intrusion detection actions. Indeed, the presence of non-cooperative nodes can affect the network in a negative way. Huang and Lee [6] proposed the cooperative IDS in order to investigate on how to improve the anomaly detection approach and provide more details on the different attack types. They have presented a set of rules that can identify the type of several well-known attacks. Other works were dealing with a cluster-based IDS model in order to preserve the battery power and to reduce the bandwidth consumption [7,8,21]. In this model, a cluster of neighboring nodes can randomly elect a monitor node. The cluster head then performs IDS functions for all nodes within the cluster.

All IDS solutions proposed for MANETs need a dynamic trust model in order to evaluate the nodes’ behavior. The dynamic trust model must be frequently updated. For this reason, the reputation system is required to develop an efficient trust model. Research works were dealing with the reputation system based on the observation of the monitored nodes’ reaction [9]. In order to establish the reputation system, a Watchdog was proposed. It is based on packets’ forwarding to detect the non-forwarding nodes [2]. Watchdog is based on the routing layer; it does not take into account the physical or the MAC level’s parameters. The idea is that the monitor node can listen to the traffic between its neighbors, and detect if the monitored nodes forward the packets in routing operations. The major problem of
current models proposed to monitor the network, such as Watchdog, is the high ratio of false positives (false alarms). IDS’ developers must consider the forwarding ratio in order to determine the rate of false positives generated during a monitoring process. Furthermore, the characteristics of MANETs must be properly taken into account.

Unfortunately, the existing solutions suffer from the false positives (false alarms). That is why, in this work, we study the monitoring process in the different cases, monitor/monitored collision and false misbehavior, in order to improve the observation of the monitor node and to reduce the false positive of the monitoring process. These enhancements have a positive impact on the trust models. Indeed, these models are generally based on the reputation parameters to evaluate the nodes’ behavior.

3. Hidden Problems in Monitoring Process

3.1. Preliminary

In this subsection, we give some basic definitions such as the transmission, the sensing, and the interference ranges. In addition, we present the relation between them.

The transmission range \( R_t \) is centered on the sender, it is defined as the area in which the power of the received signal is sufficient to decode the packet correctly. The carrier sensing range \( R_s \) is the range inside which nodes are able to sense the signal, even though a correct packet’s reception may not be possible (the receiver node may not be able to decode the packet it received correctly). Furthermore, the third important aspect requires a definition that is ignored by many researchers. This aspect is the interference range \( R_i \). The interference range \( (R_i) \) is the range of the area where each node that transmits creates a collision at the receiver node. This range is variable and its variation depends on the distance between the transmitter and receiver nodes. On the other hand, when the receiver node is receiving the packet from the sender node, any new transmission in the interference range of the receiver node creates a collision at this node.

The \( R_i \) depends on the distance between a transmitter and a receiver node \( (d) \) and on the signal to noise ratio (SNR) that must be above a certain threshold \( T_{SNR} \) so as to consider if the signal is valid when it reaches the receiver node. The \( R_i \) is defined by: \( R_i = \sqrt{T_{SNR}} \times d \) [10]. The relation between the carrier sensing range, the interference range and the transmission range is \( R_i < R_s < R_t \) where \( R_s = \beta R_t \) in some network simulator, like ns2, \( \beta = 2.2 \) [11]. Table I summarizes our notations.

The distance \( d \) between two nodes can be estimated by using the received signal strength indicator (RSSI). According to the power of the receiving signal at the receiver node, it can estimate the distance from the signal source (transmitter node) with a certain accuracy [12].

We introduce the cross-layer concept in our model to consider the physical parameters like the power of the receiving signal (SNR), and the MAC layer parameter on the routing layer. That is why, it is necessary that the protocol stack layers, particularly physical, MAC, and routing layers communicate. In order to implement the cross-layer design, we need to use the architecture which enables each layer of the protocol stack to exchange the cross-layer information. Several architectures are proposed in the literature, we can quote the ConEx [13] as example. ConEx is based on the vertical communication module which is the cross-layer communication exchange process. The vertical communication module is composed of the local event notification agents (LENA) at each layer of the protocol stack which manages the information exchange at each layer and facilitates the cross-layer information exchange. Each LENA is connected to the global event notification agent (GENA).

3.2. Different Hidden Regions

In this subsection, we describe the different hidden regions which have significant impacts on the monitoring process. In Figures 1(a) and 1(b), we illustrate the hidden sensing region and the hidden transmission region of two neighbor nodes A and B. We have \( CS_B(d_{AB}) \): the sensing region of node A and does not include the sensing region of node B. \( IR_{AB}(d_{AB}) \)
represents the interference region of node A and does not include the interference region of node B. If a node in $CS_{AB}(d_{AB})$ transmits, the signal can be sensed by node A but not by node B. The difference between $CS_{AB}(d_{AB})$ and $IR_{AB}(d_{AB})$ can be seen when a node in region $IR_{AB}(d_{AB})$ transmits: it can create a collision at a receiver node A but it is not the case for the nodes in region $CS_{AB}(d_{AB})$.

The difference between $IR_{AB}(d_{AB})$ and $TR_{AB}(d_{AB})$ is the problem of the hidden nodes which can be resolved by the request-to-send/clear-to-send (RTS/CTS) mechanism (four-way handshaking method) in IEEE 802.11. This mechanism is designed and only takes into account the transmission range but not the interference range. However, in the interference region nodes cannot decode the packets correctly when node A transmits. The basic idea of the RTS/CTS mechanism is that when a node wants to transmit a data packet it sends the RTS packet to the receiver. Once the receiver node receives the RTS packet it replies by the CTS packet. All nodes receive the control packet (RTS or CTS) from the transmitter nodes and it is not the destination. They defer their transmission during network allocation vector (NAV) which belongs to the control packet. The NAV value is calculated by the sender and the receiver in both RTS and CTS packets. The problem is when a node senses a signal but cannot decode it, that means that it cannot calculate an NAV, that is why it uses the extended inter-frame spaces (EIFS)‡ [14]. IEEE 802.11 does not completely prevent collisions due to a hidden node in the sensing region.

3.3. Problem With Hidden Regions

In the context of monitoring process, we distinguish two important hidden regions as described in the following sections.

3.3.1. Monitored vulnerable hidden region

A monitor node A wants to monitor a node B which is its neighbor, but it has no complete knowledge about the environment of the monitored node. If the interference region of the monitored node ($IR_{B}$) is not covered by the carrier sense region of the monitor node ($CS_{A}$), we call this region monitored vulnerable hidden region, as shown in Figure 2(a) and it is noted by $A_{S1S2}(d_{AB})$. If any node M is located in this vulnerable region, it can reduce the forwarding rate of monitored node B by generating an important traffic to another node. The attacker’s goal is to prevent monitored node B from communicating and to reduce its capacity to forward the packets. However, the forwarding rate is used as a metric to determine the nodes’ cooperation in the network and is also named reputation rate. We detail it in Section 4.

3.3.2. Monitor vulnerable hidden region

Another vulnerable region can also affect the monitoring mechanism; this region exists only if the interference region of node A is not covered by the carrier sense region of a monitored node B; we called it “the monitor vulnerable hidden region.” It is illustrated in Figure 2(b) and noted $A_{S3S4}(d_{AB})$. If any node in this region starts to transmit, it disturbs the monitor node’s observation. That means that if any node in region $A_{S3S4}(d_{AB})$ transmits when node A monitors node B, the observation of monitor node A is not accurate.

‡The EIFS is estimated at 364 µs when using a 1 Mbps channel bit rate.
3.4. Impact of the Distance on the Hidden Areas

The distance between the monitor node and the monitored node seems to have an important impact on the monitoring mechanism. In order to show this impact, we take the example of two neighbor nodes A and B: node B transmits to node A. Let $d_{AB}$ be the distance between A and B. Figures 3(a) and 3(b) show this example: in case (a) the distance between node A and node B is longer than in case (b). This means that the interference region of node A and the region $TR_{BA}(d_{AB})$ are greater in case (a) than in case (b). When node A comes closer to node B, the region $TR_{BA}(d_{AB})$ becomes smaller and the interference region can be covered by the transmission area when $d_{AB} \leq \frac{R_t}{\sqrt{SNR}}$. The average number of nodes in region $TR_{BA}(d_{AB})$ depends on the nodes’ distribution and on the mobility model. The greater a region $TR_{BA}(d_{AB})$ is, the bigger the probability to get a great number ($k$) of nodes in this region is.

Fig. 2. The vulnerable regions in the monitoring mechanism: (a) Monitored vulnerable region and (b) Monitor vulnerable region.

(a) Fig. 3. The impact of the distance on the interference and on the hidden areas: (a) $d_{AB}$ is long and (b) $d_{AB}$ is small.

4. System Model

4.1. Network Model

In our model, we assume that nodes are distributed within a topology which is a two-dimensional Poisson process’s with parameter \( \lambda \) (memoryless property of Poisson distribution). We use the two-ray ground propagation model with a threshold of the SNR (\( T_{\text{SNR}} \)) set to 10 db. Then, the interference range is \( R_I = \sqrt{10} \times d = 1.78 \times d \), where \( k = 4 \) [10]. Moreover, all nodes have the same transmission range \( (R_t) \) and the same carrier sensing range \( (R_s) \). This means that the nodes within a circle of radius \( R_t \) centered at the transmitter may be able to receive packets correctly. Furthermore, the average number of nodes within a sensing range, an interference range, and a transmission range with a radius \( R_s, R_t \) and \( R_t \) respectively is \( N_j \approx \lambda \pi R_j^2 \) where \( j = \{s, i, t\} \) [15].

With Poisson’s parameter, the probability to get \( k \) nodes in the area \( \text{TR}_BA(d_{AB}) \) is noted by \( p(k, \text{TR}_BA(d_{AB})) \) and obtained by:

\[
p(k, \text{TR}_BA(d_{AB})) = e^{-\lambda \text{TR}_BA(d_{AB})} \frac{(\lambda \text{TR}_BA(d_{AB}))^k}{k!}
\]

The computation is the same for \( \text{CS}_BA(d_{AB}) \) and \( \text{IR}_BA(d_{AB}) \) because it is proportional to the distance \( d_{AB} \).

4.2. Monitoring Model

A 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 neighbors, if both following conditions are met:

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

The monitor node needs to estimate the probability that both conditions 1 and 2 are met, in order to calculate the probability that it correctly observes the monitored node when it transmits. This probability is noted \( p_w \).

\[
p_w = p(\text{condition 1}) \cdot p(\text{condition 2})
\]

4.3. Probability of Condition 1

The probability that condition 1 is met is defined as a successful packets’ transmission of the monitored node which is noted \( p_{\text{succ}} \) in our model. It shows the probability that a monitored node has access to the channel in order to transmit a packet coming from the monitor node. This probability may give us information about the ability of the monitored nodes to transmit packets. In order to calculate \( p_{\text{succ}} \), we need to calculate the probability \( \tau \) that a node transmits in a random time slot. \( \tau \) must take into account two traffics’ scenarios: the saturated and unsaturated cases. For the saturated case, the traffic is intensive, which means that nodes always have a packet to transmit. Many researches have been carried out in order to calculate \( \tau \) with the assumption that \( R_I = R_s = R_t \) [15,16], but as far as we know, no work took into account the difference between the transmission, the interference, and the carrier sense ranges. For the unsaturated case, the node transmission depends on the probability that a node has a packet to transmit \( q \). In order to calculate \( \tau \) according to probability \( q \) and a collision probability \( p \), we use the same result as the one obtained in Reference [17,18]. These researches are based on the bianchi’s model [16] extended and improved to the non-saturated case. In our case, \( p_{\text{succ}} \) is calculated as follows:

\[
p_{\text{succ}} = \frac{N_s \tau (1 - \tau)^{N_s - 1}}{p_{\text{tr}}}
\]

where \( N_s \) is the number of nodes which are able to sense the signal of the sender node. On the other hand, \( N_s \) is the number of nodes in the sensing region of the sender node. \( p_{\text{tr}} \) is the probability that at least one transmission in the considered time slot occurs. In the case of \( N_s \) nodes contending for the channel, \( p_{\text{tr}} \) is calculated as follows:

\[
p_{\text{tr}} = 1 - (1 - \tau)^{N_s}
\]

The probability \( \tau \) is calculated according to the backoff parameters, collision probability \( p \) and probability \( q \). The saturated case is actually a special case of the non-saturated case, when \( q = 1 \). Probability \( \tau \)
is defined by the following equation:

\[
\tau = \frac{2(1-2p)q}{q([W_0+1](1-2p)+W_0p(1-(2p)^n)]+\psi)
\]

(5)

where \(\psi = 2(1-q)(1-p)(1-2p)\). The minimum contention window of the backoff is: \(W_0 = CW_{\text{min}} + 1\) and the maximum contention window of the backoff is named \(CW_{\text{max}}\). Thus, \(m = \log_2 \frac{CW_{\text{max}}}{CW_0}\). For more details, the reader can refer to the work in Reference [17–19].

The collision probability \(p\), necessary to compute \(\tau\), is the probability that at least one node in the interference region \((R_s)\) transmits in the same time slot as the transmitter node. Thus, \(p\) can be expressed as follows:

\[
p = 1 - (1 - \tau)^{N_i-1}
\]

(6)

where \(N_i\) is the number of nodes in the interference range and, according to assumption \(N_i\) can be calculated as follows: \(N_i \sim \lambda \pi R_s^2 = \lambda \pi \sqrt{SNR}(d_{AB})^2\).

The modeling of probability \(q\) is based on the traffic load which is characterized by parameter \(\lambda^*\) which represents the rate of packets that arrive at the node’s buffer and it is measured in packets per second (pkt/s). Like in References [18,19], we assume that the packet’s arrival process is Poisson. So, probability \(q\) can be well estimated with a small buffer size as follows:

\[
q = 1 - \exp(\lambda^* T_{av})
\]

(7)

where \(T_{av}\) is the expected time per slot and is calculated according to \(p_{\text{tr}}, p_{\text{suc}}\), the successful transmission slot \((T_c)\) and collision slot time \((T_s)\) as follows:

\[
T_{av} = (1-p_{\text{tr}})\sigma + p_{\text{tr}}(1-p_{\text{suc}})T_c + p_{\text{tr}}p_{\text{suc}}T_s
\]

(8)

where \(T_c\) and \(T_s\) are the average times a channel is sensed busy due to collisions and successful data frame transmissions. \(T_c\) and \(T_s\) can be computed as follows:

\[
\begin{align*}
T_c &= H + \text{PL} + \text{ACK}_{\text{timeout}} \\
T_s &= H + T_{\text{PL}} + \text{SIFS} + 2\delta + T_{\text{ACK}} + \text{DIFS}
\end{align*}
\]

where the time duration for the physical and the MAC headers is \(H\), \(T_{\text{ACK}}\) for the ACK, \(T_{\text{PL}}\) for the data frame transmission, and the maximum propagation delay is \(\delta\). In addition, \(\text{ACK}_{\text{timeout}} = \text{SIFS} + T_{\text{ACK}} + \text{DIFS}\) [17], where SIFS and DIFS are the acronyms of short inter-frame space and distributed inter-frame space

### 4.4. Probability of Condition 2

The probability that condition 2 is met gives us a piece of information about the observation’s disruption of a monitor node. This probability equals to one when no node in region \(A_{S3S4}(d_{AB})\) transmits \((p[\text{cond.2}])\) in a vulnerable time. This period depends on the transmission time \(T_{av}\) of a packet: when node B starts to transmit at \(t_s\), the vulnerable time interval is \([t_s - T_{av} - 1, t_s + T_{av} - 1]\). The nodes in region \(A_{S3S4}(d_{AB})\) must remain silent during \(\mu\) slots time where \(\mu = (T_{av}/\sigma)\), because a node in the sensing and interference ranges waits for an EIFS when it cannot calculate an NAV vector. If the EIFS is greater than a \(T_{av}\), the packet can be received correctly by receiver node C. Otherwise, a packet cannot be received correctly. Region \(A_{S3S4}(d_{AB})\) can be equal to zero when it is covered by the carrier sense of a node B. Otherwise, \(p[\text{cond.2}](d_{AB})\) (if \(d_{AB} > \frac{R_s}{1+\frac{1}{\sqrt{SNR}}}\)) is given by:

\[
p[\text{cond.2}](d_{AB}) = \left\{\begin{array}{ll}
\sum_{k=0}^{\infty} (1-\tau)^k \frac{(N_h)^k}{k!} e^{-N_h\mu} & \text{if } d_{AB} \leq \varphi \\
e^{-\tau N_h\mu} & \text{Otherwise}
\end{array}\right.
\]

where \(N_h = \lambda A_{S3S4}(d_{AB})\).

The final equation of \(p[\text{cond.2}](d_{AB})\) is obtained by:

\[
p[\text{cond.2}](d_{AB}) = \left\{\begin{array}{ll}
1 & \text{if } d_{AB} \leq \varphi \\
e^{-\tau N_h\mu} & \text{Otherwise}
\end{array}\right.
\]

where \(\varphi = \frac{R_s}{1+\frac{1}{\sqrt{SNR}}}\).

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

\[
\text{Ar}_{[X \cap Y]}(d) = R_s \left( \arccos(\alpha) - \alpha \sqrt{1-\alpha^2} \right) + R_s \left( \arccos(\beta) - \beta \sqrt{1-\beta^2} \right)
\]

where

\[
\alpha = \frac{R_s^2 - R_i^2 + d^2}{2d R_s} \quad \text{and} \quad \beta = \frac{R_s^2 - R_i^2 + d^2}{2d R_i}
\]

\(^1\)In MAC IEEE 802.11, DIFS = 50 \(\mu\)s and SIFS = 10 \(\mu\)s.
Therefore, \( A_{S3S4}(d_{AB}) \) is expressed by:

\[
A_{S3S4}(d_{AB}) = \begin{cases} 
0 & \text{if } d_{AB} \leq \varphi \\
\pi R_s^2 - A_{\Gamma[A \cap B]}(d_{AB}) & \text{Otherwise}
\end{cases}
\]

Now, from Equations (2) and (9), we can calculate \( p_w(d_{AB}) \) as follows:

\[
p_w(d_{AB}) = \begin{cases} 
p_{\text{succ}} & \text{if } d_{AB} \leq \varphi \\
p_{\text{succ}} \cdot e^{-t\eta \varphi} & \text{Otherwise}
\end{cases}
\]

The reputation report of monitored node B generated by monitor node A is given by:

\[ R_{A,B}(d_{AB}) = \eta p_w(d_{AB}) \tag{11} \]

where \( \eta \) is the forwarding ratio assessed by a monitor node. Unlike the Watchdog mechanism, the forwarding ratio in our model is the number of packets observed by the monitor node divided by the total number of packets sent by a monitor node and well-received by a monitored node (see Equation (12)). However in Watchdog, the denominator is the total number of packets sent to the monitored node. This difference has an important impact on the monitoring process, because the total number of packets sent to the monitored node are not automatically well-received when the monitor node only focuses on the routing layer. In order to avoid the vulnerability of Equation (12), and to correctly evaluate the total number of packets (subject of the monitoring) well received by the monitored node, we consider the cross-layer approach. This approach allows to correctly evaluate the forwarding ratio \( \eta \) at the routing layer by considering the ACK packet at the MAC layer. The monitor node needs this cross-layer information to make sure that the monitored node has correctly received the packet at the routing layer. Even if there is a variation of rate, the probability that a monitored node correctly receives the packet from a monitor node enables the monitor node to evaluate the traffic in the interference range of the monitored node.

\[
\eta = \frac{\# \text{forwarded packets observed}}{\# \text{total of packets well received by a monitored}}
\tag{12}
\]

Once monitor node A has calculated the reputation report \( R_{AB} \) of node B, it can predict the number of packets likely to be forwarded next time by node B. If the difference between the predictable number and the observed number is great, the monitor node can deduce that the monitored node has changed its behavior or that it does not have the same environment as in the first evaluation. In this situation, the monitor node needs to update the evaluation of the monitored node. The predictable number of packets forwarded by any monitored node takes the three following monitoring conditions into account: nodes density, nodes mobility, and traffic load. It can be computed by the following equation:

\[
# \text{Forwarded packets} = \frac{(# \text{total sent packets}) R^w_{(AB)}}{p_w}
\tag{13}
\]

where \( R^w_{(AB)} \) is the previous evaluation report.

The goal of Equation (13) is to analyze the nodes behavior in the same condition as in the previous \( p_w \) evaluation. \( p_w \) depends on \( p\{\text{condition 1}\} \) and \( p\{\text{condition 2}\} \). \( p\{\text{condition 1}\} \) takes into account the traffic variation through the probability that a node has a packet to transmit (\( q \)) defined in Equation (7). However, \( p\{\text{condition 2}\} \) takes into account the nodes density in the monitor vulnerable region called \( A_{S3S4}(d) \) (illustrated in Figure 2(b)). So, this probability depends on the distance between the monitor and the monitored nodes (\( d \)). Therefore, the same condition for \( p_w \) calculation means that the estimation is done with the same probability \( q \) (traffic load) and the same distance between the monitor and the monitored nodes (\( d \)). In addition, in our proposed model, \( p_w \) is dynamically estimated for each packet sent to the monitored node (subject of monitoring). Hence, Equation (13) allows to discuss about the node’s behavior in the same condition as in the previous \( p_w \) calculation.

With our model, we can give the answer to the initial question: Does the monitored node intentionally refuse to cooperate or is it unable to cooperate even if it wants to do so? This means that the monitoring process is improved and that the false positive is reduced. This enhancement has a positive impact on the trust model because most of the trust models used to evaluate the behavior of nodes are based on the reputation parameter.

5. Numerical Results and Discussion

In this section, we present the numerical results of the proposed model in different situations: when the distance between monitor and monitored nodes varies and
Table II. Network parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission rate</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>Packet payload</td>
<td>1024 Bytes</td>
</tr>
<tr>
<td>MAC header</td>
<td>24 Bytes</td>
</tr>
<tr>
<td>Physical header</td>
<td>16 Bytes</td>
</tr>
<tr>
<td>ACK</td>
<td>14 Bytes</td>
</tr>
<tr>
<td>CTS</td>
<td>14 Bytes</td>
</tr>
<tr>
<td>RTS</td>
<td>20 Bytes</td>
</tr>
<tr>
<td>$\delta$</td>
<td>$1 \mu$s</td>
</tr>
<tr>
<td>Slot time $\sigma$</td>
<td>$20 \mu$s</td>
</tr>
</tbody>
</table>

When the impact of the transmission probability $\tau$ is taken into account. The typical network parameters in the case of IEEE 802.11 are presented in Table II.

In order to illustrate the impact of the distance between monitor and monitored nodes on the vulnerable region $A_{S3S4}$, we plot in Figure 4(a) the hidden area $A_{S3S4}$, according to the distance between nodes A and B with a 550 m sensing range and a $R_i = \sqrt{10} \cdot d_{AB}$ interference. When the distance between both nodes is less than 200 m $A_{S3S4} = 0$, that means that region $A_{S3S4}$ is covered by the sensing region of node B. In Figure 4(b) we plot the monitor vulnerable hidden region versus the threshold SNR, in order to study the impact of the sensitivity of a signal on the monitoring process, particularly on the vulnerable region $A_{S3S4}$. We note that when $d_{AB} = 200 m$ and $T_{SNR} = 10$, the vulnerable region $A_{S3S4} = 0$. However, $A_{S3S4} \neq 0$ when $T_{SNR} > 10$. Therefore, when the power of a signal increases, the interference range becomes greater and region $A_{S3S4}$ is less covered by the sensing region of node B ($A_{S3S4} \neq 0$). We can deduce that the power of a signal has an important impact on the monitoring process. The trade-off between $T_{SNR}$ and the distance between monitor and monitored nodes can significantly improve the monitoring process.

$p(\text{cond.2})$ is an important parameter in the proposed model. So, we study in Figure 5 $p(\text{cond.2})$ different distances between monitor and monitored nodes. Furthermore, we introduce the transmission probability and the transmission duration, in order to show their impact on the monitoring process. Figure 5(a) illustrates the probability that no node in region $A_{S3S4}(d)$ transmits during slot time $\mu = \sigma$. We notice that probability $p(\text{cond.2})$ equals to one when the distance between A and B is less than 200 m, due to region $A_{S3S4}(d)$ which is overlapped by the sensing region of node B. However, when the distance between nodes A and B becomes greater, $p(\text{cond.2})(d)$ decreases and it decreases rapidly when the probability of transmission $\tau$ is higher. For example, when $d_{AB} = 250 m$ and $\tau = 0.2$ then $p(\text{cond.2}) = 0.75$, but when $\tau = 0.8$ with the same distance, then $p(\text{cond.2})$ significantly decreases to 0.35. Figure 5(b) shows $p(\text{cond.2})(d)$; when the transmission duration $\mu$ is great ($\mu = 5\sigma$), we note that $p(\text{cond.2})(d)$ is smaller in the case of a time duration $\mu = \sigma$. When the transmission duration is high, it means that the monitoring period is also high, and that the risk of having a collision at the monitor node is important. The smaller the transmission duration is, the better the monitoring is. We can conclude that the threshold $T_{SNR}$, the distance between monitor and monitored nodes and the transmission time $\mu$ have an important impact on the monitoring process.

![Fig. 4. The hidden area $A_{S3S4}$ versus $T_{SNR}$ and distance $d_{AB}$: (a) $A_{S3S4}$ versus distance and (b) $A_{S3S4}$ versus $T_{SNR}$.](image-url)
5.1. Saturated and Non-saturated Case

We now discuss the probability $p_w$, in the general case, that the monitor node correctly observes the behavior of the monitored node. The general case includes the saturated and non-saturated cases. However, the saturated case is a specific case of the non-saturated case when the probability that any node has a packet to transmit is equal to one ($q = 1$). We study the general case by varying the following parameters: the arrival rate of packets in the buffer ($\lambda^*$) to study the probability $q$, the distance between monitor and monitored nodes ($d_{AB}$) and the nodes’ density in the carrier sensing region $N_s$.

Figures 6(a) and 6(b) illustrate the probability that a monitor node $A$ correctly monitors the monitored node $B$ ($p_w$) versus the load of arrival packets in the nodes’ buffer ($\lambda^*$), in both flowing cases: a density of nodes $N_s = 10$ and $N_s = 30$. In Figure 6(a), we remark that the maximum value of $p_w$ equals to 0.95 when the number of arrival packets in the buffer is around 5 pkt/s and when the distance between nodes $A$ and $B$ equals to 100 m. However, $p_w$ slightly decreases when $\lambda^*$ increases, but even if $\lambda^* = 50$ pkt/s the $p_w$ does not go lower than 0.85. This is a good monitoring of node $A$. $p_w$ decreases more significantly when the distance between nodes $A$ and $B$ is more than 200 m. We note that when $d_{AB} = 220$ m and $\lambda^* \geq 10$ pkt/s, $p_w$ decreases

![Fig. 5. $p(\text{cond.2})$ versus distance between nodes A and B: (a) case of $\mu = \sigma$ and (b) case of $\mu = 5\sigma$.](image)

![Fig. 6. $P_w$ versus traffic load $\lambda^*$: (a) case of $N_s = 10$ and (b) case of $N_s = 30$.](image)
to around 75%. When we increase the nodes’ density in sensing region $N_s = 30$ (Figure 6(b)), we notice that $p_w$ decreases to around 20% in comparison with a lower density of nodes. In addition, $p_w$ is null when the distance $d_{AB}$ is more than 200 m. We can say that although the traffic load and the density of nodes have an impact on the monitoring, the distance between monitor and monitored nodes has a more negative impact on the monitoring process, and on the monitor node’s observation.

In Figures 7(a) and 7(b), we plot two cases: $d_{AB} = 100$ m and $d_{AB} = 220$ m of the probability $P_w$ according to the nodes’ density in the carrier sensing region ($N_s$) and the rate of packets arriving at the nodes buffer ($\lambda^\star$). We notice that when $d_{AB} = 100$ m (Figure 7(b)), $p_w$ decreases quickly when the nodes density increases and it decreases less when $\lambda^\star$ increases. However, both increases of $N_s$ and $\lambda^\star$ decreases more significantly which means that the monitor’s observation is not correct in this situation. In Figure 7(b), we remark that $P_w$ is very low and if $N_s = 20$ nodes and $\lambda^\star = 20$ pkt/s, then $P_w$ becomes null. The monitor node’s worst case is obtained when distance $d_{AB}$ is greater than 200 m.

In wireless networks, the nodes density do not only have an important impact on the network’s performance, but also on the monitoring process. In order to study this impact on the monitoring process, we plot in Figures 8(a) and 8(b), $p_w$ according to the nodes density with both load traffics: $\lambda^\star = 5$ pkt/s and $\lambda^\star = 15$ pkt/s. We notice that $p_w$ is similar in both cases, but slightly decreases when the nodes’ density increases ($d_{AB} \leq 200$ m). We point out that $p_w$
reaches the best value (0.98) with a lower density value \( N_s = 5 \) and with a small distance between monitor and monitored nodes \( d_{AB} = 100 \) m. However, \( p_w \) decreases when the nodes density increases and it reaches 0.7 with \( N_s = 50 \) nodes. In addition, we notice that \( p_w \) significantly decreases when the distance between nodes A and B is greater than 200 m. It decreases by 30 and 60% in the case of a distance \( d_{AB} = 240 \) m and \( d_{AB} = 250 \) m, respectively with a low node density \( (N_s = 5) \). \( p_w \) equals to zero when the distance \( d_{AB} \) is greater than 200 m and when the traffic load is greater than \( \lambda^* \geq 20 \) pkt/s. This situation represents the worst monitoring condition. When we increase the traffic load \( \lambda^* \) (in Figure 8(b)), we notice that \( p_w \) decreases by around 15% in the case of \( d_{AB} > 200 \) m.

In order to show both impacts of the load traffic in the nodes buffer and of the distance between monitor and monitored nodes on \( p_w \), we plot in Figure 9, \( p_w \) according to \( \lambda^* \) and \( d_{AB} \) with a nodes density in the carrier sensing region \( N_s = 10 \). We clearly notice that, even if the load traffic has an impact on \( p_w \), the distance has a more negative impact when \( d_{AB} \geq 200 \) m. However, when the distance is less than 200 m, we remark that the distance does not have an impact on the monitoring process in comparison with the traffic load \( \lambda^* \).

In Figure 10, we illustrate the impact of both parameters: nodes density \( N_s \) and the distance \( d_{AB} \) on monitor’s observation \( p_w \) in the case of a traffic load \( \lambda^* = 15 \) pkt/s. We notice that the nodes density has a significant impact on the monitor’s observation when distance \( d_{AB} \) is inferior to a critical threshold (200 m). However, when the distance is greater than a critical threshold, \( p_w \) decreases more significantly in comparison with an increasing nodes’ density.

To conclude, we can say that the following parameters: distance between monitor and monitored nodes \( (d_{AB}) \), nodes density in the carrier sensing region \( (N_s) \), and load of packets that arrive in the nodes buffer \( (\lambda^*) \) have an impact on the monitoring process, but the most important parameter is distance \( d_{AB} \) because it can significantly reduce \( p_w \) (by more than 70%). Hence, distance \( d_{AB} \) is a key factor of the monitor’s vulnerable region \( A_{S3S4} \), because this region becomes uncovered when the distance is high. Furthermore, reducing \( p_w \) consists in increasing the probability of the false positive.

6. Simulation Results and Discussion

This section is divided into two main parts. First, we investigate on how the interference range affects the monitoring process with different distances between a monitor and a monitored node and different traffic rates. Second, we compare the Watchdog process [2] and our proposed cross-layer monitoring process. Furthermore, we study the general case of nodes density and nodes mobility with different velocities. In addition, the different traffic rates are investigated. In order to simulate these cases, we implement both mechanisms Watchdog and the cross-layer process on an NS2 simulator [11]. The NS2 simulation’s parameters are illustrated in Table III.

The metrics used to evaluate the monitoring process is the false positive metrics (FP). The FP metrics enables to know when the monitored node forwards the packet but the monitor node does not see it forwarded by the monitored node. The FP is calculated as follows:

\[
FP = 1 - \eta
\]
TOWARD A CROSS-LAYER MONITORING PROCESS

Table III. Simulation parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value in our simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes (N)</td>
<td>([5–50])</td>
</tr>
<tr>
<td>MAC Technology</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>DSR</td>
</tr>
<tr>
<td>Network size ((mxn))</td>
<td>(670 \times 670 \text{m}^2)</td>
</tr>
<tr>
<td>Mobility</td>
<td>([5–40\text{m/s}])</td>
</tr>
<tr>
<td>Transmission Range ((R_t))</td>
<td>(250\text{m})</td>
</tr>
<tr>
<td>Sensing range ((R_s))</td>
<td>(550\text{m})</td>
</tr>
<tr>
<td>Packet size</td>
<td>(512, 1000\text{ bytes})</td>
</tr>
<tr>
<td>Traffic rates</td>
<td>([20–60\text{ kbps}])</td>
</tr>
<tr>
<td>Simulation time</td>
<td>(150\text{s})</td>
</tr>
</tbody>
</table>

Fig. 11. The network topology of the simulation model.

where \(\eta\) represent the average forwarding ratio which is defined by Equation (12).

6.1. Simple Case: Distance and Traffic Rate Study

The network topology illustrated in Figure 11 is simulated with different distances between monitor node 2 and monitored node 3. Node 1 generates a constant bit rate (CBR) traffic (traffic2) to node 0, the distance between them is small \(d_{1,0} = 10\text{m}\), but the distance between node 1 and a monitor node 2 is variable during the simulation. Another CBR’s traffic (traffic1) is generated between monitor node 2 and node 4, the distance between them is larger than \(250\text{m}\); monitored node 3 must forward the packets to node 4. The packet size is set to \(1000\text{ bytes}\). We simulate the network with different traffic rates, variable between \(20\) and \(60\text{ kbps}\).

6.1.1. Case of Watchdog mechanism

In this case, we study the monitoring mechanism without taking into account the ACK packet at the MAC layer from the monitored node (Watchdog mechanism), which means that the monitor node does not check at the routing layer if the monitored node has correctly received the packet.

In Figures 12(a) and 12(b), we show the relation between the false positive, the distance, and the network’s traffic rate parameters. Figure 12(a) illustrates the case with \(d_{1,2} = 300\text{m}\). We notice that the impact of the distance between the monitor and a monitored node does not clearly appear when the traffic rate is low. However, when the network’s traffic rate is high, the FP increases, although the vulnerable region is covered. That is mainly due to the packets’ drop, because the monitor node generates the packets at the routing layer and does not check if the packets did not drop at lower layers and are well arrived to the monitored node. For a \(350\)-m distance between monitor nodes 2 and 1, the results obtained are plotted in Figure 12(b). We notice some difference compared to the first case. When the distance between monitor and monitored nodes is greater than \(200\text{m}\), FP increases rapidly. That means that the monitor’s observation is permanently disturbed. The explanation for this deterioration of the monitor’s monitoring is the collision at the monitor node because the interference range of the monitor node is not covered by the sensing range of the monitored node. That means that when the monitored node transmits, the monitor node gets the collision and cannot monitor the monitored node’s transmission. As a conclusion for these results, not only the distance between the monitor and monitored nodes has a negative impact on the monitoring process with the Watchdog mechanism but also the traffic rate.

6.1.2. Case of cross-layer mechanism

In this subsection, we illustrate and analyze the simulation’s results, when the ACK packets of the MAC layer are taken into account by the monitor node at the routing layer. If the RTS/CTS mechanism is taken into account, we plot the false positive parameter, FP, according to the different distances between a monitor node and a monitored node with different positions of nodes 0 and 1. The results are illustrated in Figure 13(a). When the distance between monitor node and monitored node is less than \(100\text{m}\), the false positive is null; if the distance between node 1 and a monitor node 2 is \(450\text{m}\), it means that the interference region of monitor node 2 is covered by the carrier sense of a monitored node 3 (\(d_{2,3} + d_{1,2} \leq 550\text{m}\)). We notice that when \(d_{2,3}\) becomes larger than \(100\text{m}\), FP becomes higher, to around \(84\%\), because of the interference region of node 2 which is not covered by the sensing range of a monitored node 3. We remark that when the interference region of the monitor node is covered by the sensing range of the monitored node, the observation is correct and the FP is null, otherwise FP increases and the monitoring is wrong.

When the RTS/CTS mechanism is disabled, the results obtained are shown in Figure 13(b). We notice some difference in comparison with the previous case.
The monitor’s monitoring is disturbed, even if the monitor’s interference region is covered. That is due to the packets’ collision at the monitor node. Furthermore, we note that FP is low when the interference region of a monitor node is covered, but not null like in the first case (Figure 13(a)). We can say that the RTS/CTS mechanism has a positive impact on the monitoring process if the interference region of the monitor node is covered. However, when the distance between the monitor and the monitored node is greater than 200 m, the false positive is great in the both cases with and without RTS/CTS mechanism. On the other hand, it is preferable in terms of monitoring mechanism to use the RTS/CTS mechanism if the distance is small otherwise it is not important to use the RTS/CTS mechanism.

The traffic rate has no significant impact; in the case of a cross-layer approach, the results are close to those presented in Figures 13(a) and 13(b).

As a conclusion for these results, the RTS/CTS mechanism has a positive impact on the monitoring process. The results illustrated in Figures 13(a) and 13(b) prove that conclusion. Moreover, the monitor node must take into account the distance with the monitored node, in order to estimate if its vulnerable region is covered by the sensing region of the monitored node or not. As

Fig. 12. The false positive rate according to $d_{2,3}$ without ACK consideration: (a) $d_{1,2} = 300$ m and (b) $d_{1,2} = 350$ m.

Fig. 13. The false positive according to the $d_{2,3}$ with ACK consideration: (a) case with RTS-CTS and (b) Case without RTS-CTS.
shown in both results with and without the RTS/CTS mechanism, the distance between monitor and monitored nodes affects both monitor’s and monitored’s vulnerable regions. Furthermore, the cross-layer approach which takes into account the ACK packet at the routing layer increases the accuracy of the monitor’s observation and reduces the false positive alarm. We can summarize as follows: the cross-layer approach with the RTS/CTS mechanism significantly reduces the false positive alarm and increases the monitor node’s correct observation.

6.2. Simulation of the General Scenario Case

In this subsection, we study the general scenarios with different traffic rates, different nodes densities in the network and different nodes mobilities. In addition, the number of hops from a source to a destination and the transmission, i.e., path length (PL), range are also taken into account.

6.2.1. Traffic load impact

Figure 14 illustrates the average FP according to different traffic rates. We distribute 50 nodes randomly. We use a CBR traffic connection generated by the NS2 tool, called “cbrgen,” with different traffic rates. We notice that the FP increases when the traffic rate increases. In addition, we remark that our cross-layer approach gets a better result than Watchdog. The cross-layer mechanism reduces the FP by more than 20% in comparison to the Watchdog mechanism. This improvement is mainly due to the cross-layer approach, because the monitor node correctly estimates the forwarding $\eta$ ratio at the routing layer by only taking into account the well received packet at the monitored node. We remark that the bad values of FP are obtained when the traffic is intense. In terms of worst cases, FP cannot exceed 0.45 in our scheme. However, FP reaches 0.72 with the Watchdog mechanism. In this case, the FP decrease is due to the traffic load.

The explanation of these results is as follows: in the proposed model, we significantly reduce the FP in the case of an intense traffic load because only the well received packet by the monitored node is taken into account to calculate the forwarding ratio. We know that the forwarding ratio is calculated at the routing layer and that the intense traffic load generates more collisions and packet losses. That is why we consider the ACK packet at the MAC layer to be sure that the packet destined to the monitored node is well received. However, in the case of a low traffic, the difference of FP in our proposed model and Watchdog is very small because when the traffic is low, the probability that the packet is well received by the monitor node is high.

6.2.2. Nodes density impact

We plot in Figure 15 the FP according to the nodes’ density in the network with a rate of 10 pkt/s. We remark that the FP increases when the nodes’ density in the network increases in both mechanisms. However, FP in the case of Watchdog is close to FP in the case of the cross-layer mechanism when the node’s density is small (less than 10 nodes). In the worst case, we obtain 45% of FP in our case, but 68% with Watchdog. We
notice that with a cross-layer mechanism, we reduce by around 20% the FP compared to the Watchdog mechanism. The nodes density in the network has a direct impact on the collision probability which has a negative impact on the monitoring process. When the nodes density increases, the collision probability increases, too [16]. In addition, when the nodes density increases, the probability to have a node in the monitor vulnerable region ($A_{S3S4}$) increases, too. In this region, any node that transmits during the monitoring process will create a collision at the monitor node and disturb the monitor node’s observation. That is why the nodes density has a negative impact on the monitoring process and it increases the FP.

### 6.2.3. Mobility impact

In this subsection, we study the mobility impact on the monitoring process. The problem in the monitoring process with nodes mobility occurs when the monitor node sends a packet to the monitored node in order to forward it, but the monitored node moved out of the transmission region of the monitor node. In this case, two situations appear:

- First, the monitored node moves out of the monitor node’s range after having sent the ACK packet to the monitor node. In this case, both mechanisms Watchdog and cross-layer monitoring produce the FP if the monitored node forwards the packet.
- Second, the monitored node moves out of the monitor node’s range before having sent the ACK packet to the monitor node. In this case, our proposed approach permits to avoid the FP, unlike the Watchdog mechanism which does not take into account the ACK thanks to the MAC layer and cannot evaluate the probability of good observation $p_w$.

In order to study the impact of mobility on both Watchdog and our proposed cross-layer monitoring mechanism, we select the perfect mobility model proposed by Le Boudec and Vojnovic [20] called random trip model particularly the random way point model (RWP). Figures 16(a) and 16(b) illustrate the FP according to the average nodes speed and constant nodes speed respectively with 30 nodes and 15 CBR traffic connections (30 pkt/s). We notice that in both cases, the FP increases when the nodes speed relatively increases. However, even the proposed cross-layer model is affected by the nodes mobility but it reduces the FP by more than 30% compared to Watchdog in the case of an average nodes speed. In the case of a constant nodes speed, the FP increases slightly more than in the previous case but with the proposed model, the FP decreases by around 20% compared to the case of Watchdog. As conclusion for the mobility impact on the monitoring process, we can say that the mobility has a negative impact on both the Watchdog and the cross-layer monitoring models. However, the impact is not significant in the proposed model compared to the watchdog mechanism.

The advantage of the proposed model in the case of the mobility scenario is when the monitored node moves out of the range of the monitor node before transmitting the ACK packet. In this case, the monitor node does not take into account this packet to calculate the forwarding ratio. However, the Watchdog mechanism generates the FP in this situation.
6.2.4. The average path length and the transmission range impact

In this subsection, we study the impact of the number of hops (i.e., the PL) and of the transmission range on the monitoring process. Figure 17(a) shows the FP according to the PL in the case of 50 static nodes with 20 CBR flows connections (30 pkt/s). Different area sizes and transmission ranges are taken into account in order to get the different numbers of hops. We remark that the average number of hops does not give us a clear conclusion about its impacts on the monitoring process. The FP increases when the PL increases in certain cases like $PL = 2$ and $PL = 2.5$ but it decreases when $PL = 3$ and $PL = 3.5$. The explanation of these results is as follows: the PL does not have a direct impact on the monitoring process. However, when the PL increases, the number of monitor nodes increases. Hence, the probability that the monitor node has an important neighboring number is great. So, the probability that a node in the monitor vulnerable region ($A_{S3S4}$ see Figure 2(a)) transmits in the monitoring period is great. Whatever the average PL is, the proposed cross-layer model gives a better result than Watchdog and it can reduce the FP by more than 20%.

As conclusion, we can say that the average PL does not have a direct impact on the monitoring process but it has a relation with the nodes density at the monitor node and the distance between the monitor and the monitored nodes. That is why we study the impact of the transmission range on the monitoring process. Figure 17(b) illustrates the FP versus the transmission range in the case of 50 static nodes with 20 CBR traffic connections (30 pkt/s). We notice that the FP increases when the transmission range increases. When the transmission range increases, the number of monitor’s neighbors increases, the nodes density increases and the number of contenders nodes in the monitor vulnerable region increases, too. When the transmission range equals to 100 m, the FP in the Watchdog case is around 0.66, but in our proposed model it does not exceed 0.28. In the classical case of transmission range (250 m), the FP in Watchdog reaches 0.8 but in the cross-layer approach, it is limited to 0.47. These simulation results show that the monitoring cross-layer approach is more efficient than the Watchdog mechanism in different cases of nodes density, different degrees of the monitor nodes neighboring and the average PL.

According to the results presented above, we can say that with a cross-layer consideration in the monitoring process, we obtain better results: the false positive is significantly reduced in different cases such as: rate variation, nodes density, and nodes speed. Finally, these results prove our analytical model.

7. Conclusions

In this paper, we have shown the benefit of the cross-layer approach on the monitoring mechanism. A new analytical model for a monitor node is proposed, in order to evaluate the reputation and cooperation of a monitored node correctly. The impact of the SNR and the distance between monitor and monitored nodes are clearly introduced. In our model, the monitor’s best observation is when the monitor node is close to the
monitored node. The difference between transmission, interference, and sensing ranges is taken into account, unlike many modelings, that assume that sensing and transmission ranges are the same. Furthermore, with a cross-layer approach (Physical, MAC, and routing layers), adopted for our model by taken into account SNR and ACK packets from lower layers (physical and MAC layers) backup to the routing layer. The objective of the cross-layer approach for the monitoring process is to get an accurate evaluation of a monitored node, the monitor node can estimate the accuracy of its observations. The simulation’ results confirm the impact of the distance between monitor and monitored nodes on the monitoring mechanism. Moreover, these results illustrate that our cross-layer approach mechanism has a lower false positive than the classical Watchdog mechanism with different network’s parameters such as: the nodes’ density, the nodes’ mobility, and different traffic loads.

One possible direction for a future work is to extend the simulation’s results to experiment results by implementation of some DoS attacks and study the monitor mechanism with a false negative parameter.

Acknowledgement

This work is supported by the ANR “Agence Nationale de la Recherche, France” within the project framework ARA/CLADIS.

References