HAL
archives-ouvertes.fr

muDog: Smart monitoring mechanism for wireless sensor networks based on IEEE 802.15.4 MAC

Abderrezak Rachedi, Hend Baklouti

▶ **To cite this version:**

Abderrezak Rachedi, Hend Baklouti. muDog: Smart monitoring mechanism for wireless sensor networks based on IEEE 802.15.4 MAC. IEEE ICC'2011, Jun 2011, Kyoto, Japan. pp.1 - 6, 10.1109/icc.2011.5963200 . hal-00620375

HAL Id: hal-00620375

https://hal-upec-upem.archives-ouvertes.fr/hal-00620375

Submitted on 18 Jun 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

muDog: Smart Monitoring Mechanism for Wireless Sensor Networks based on IEEE 802.15.4 MAC

Abderrezak Rachedi and Hend Baklouti
Gaspard Monge Computer Science Laboratory (CNRS UMR 8049 LIGM)
University of Paris-Est Marne-la-Vallée (UPEMLV)
Champs sur Marne, France
Email: rachedi@univ-mlv.fr

***Abstract*—The resources in Wireless Sensor Networks (WSNs) are limited like energy and bandwidth which motivate nodes to reduce their energy consumption and increase their bandwidth. There are two main ways to optimize the network resources: a honest way and a malicious way. The malicious way is attractive, because it enables nodes to significantly reduce their energy consumption and increase their bandwidth with a simple and easy node reprogramming. Furthermore, detect these malicious nodes is a real challenge which is mainly due to WSNs characteristics. However, the existing monitoring mechanisms like Watchdog are not adapted to WSNs characteristics. In this paper we propose an analytical model to detect and remove malicious nodes while taking into account MAC IEEE 802.15.4 beacon-enabled technology. The proposed solution called muDog enables to monitor nodes activities with a minimal energy consumption in order to detect the suspicious behavior particularly the non-cooperative nodes in the routing process. Moreover, we analyze the cost of the monitoring mechanism in terms of energy consumption and the quality of detection by the evaluation of the monitor's observation. The impact of nodes density, packets' size, network traffic load: saturated/unsaturated cases and distance between monitor and monitored nodes are taken into account in our evaluation. The obtained results illustrate that muDog is more efficient than Watchdog whatever the parameter is.**

I. Introduction

Wireless Sensor Networks (WSNs) attract more and more researchers and industrialists because of their potential reliability, accuracy, flexibility, cheapness and easy deployment. In addition, the WSNs application is wide: natural environment monitoring (fire detection, pollution, earthquake, etc.), ecosystem tracking, healthcare, security (videosurveillance, objects tracking, etc.) and military (battlefield monitoring, objects localization, etc.).

One of the main constraints of these networks is energy limitation due to their small size and wire independance. This constraint must be taken into account in any protocol design and sensor network deployment. The energy limitation creates vulnerabilities that are exploited by attackers. There are two kinds of attacks: passive (like traffic analysis and selfish behavior) and active (like false routing information injection and impersonation). The impact of passive attacks on the network is not negligible compared to the impact of active attacks. Propose a solution to counter passive attacks is a real challenge.

In this work, we focus on passive attacks and propose a new analytical model in order to monitor and detect selfish behavior particularly non-cooperative nodes. The existing solution called Watchdog mechanism is proposed for Mobile Ad-hoc Networks (MANETs), but is not adapted to WSNs [4]. Our proposed solution called muDog is a monitoring mechanism based on MAC IEEE802.15.4 beacon-enabled technology and aims at improving the monitoring quality while minimizing the energy cost. The monitoring mechanism is a set of actions allowing specific sensor nodes to monitor the behavior of the other sensor nodes. This mechanism allows to evaluate monitored nodes and update the trust metrics. For example, muDog mechanism is able to detect the origin of packets loss at the routing nodes which do not cooperate and choose a selfish behavior. This malicious behavior consists in keeping their energy only for their own packets transmission in order to reduce the energy they consume when cooperating. The MAC IEEE802.15.4 beacon-enabled mode standard [2] is used to reduce the energy consumption in WSNs through a sleep/wakeup mechanism [6]. As far as we know, there is no monitoring mechanism adapted to this standard. Therefore, the main goal of this work is to propose a new efficient and optimal analytical model allowing to monitor the network while minimizing the energy consumption. Moreover, the cost of the monitoring mechanism is analyzed in terms of energy consumption and the quality of detection is evaluated by using as metric the probability of monitor correct observation. The impact of nodes density, packets' size, network traffic load: saturated/unsaturated cases and distance between monitor and monitored nodes are taken into account in our evaluation. The obtained results illustrate that muDog is more efficient than Watchdog whatever the parameter is.

This paper is organized as follows: in section 2, we briefly present the MAC IEEE802.15.4 beacon-enabled mode standard and the summary of the existing works related to energy aware and monitoring mechanisms. Section 3 is dedicated to the proposed analytical model and muDog mechanism. The fourth section presents the obtained results and their analysis. Finally, section 5 concludes the paper and presents our future works.

II. Related work

In this section, we briefly present MAC IEEE802.15.4 beacon-enabled mode and the existing monitoring mechanisms.

A. MAC IEEE 802.15.4

The MAC IEEE802.15.4 has two working modes: non-beacon-enabled mode and beacon-enabled mode [2]. The non-beacon-enabled mode is based on non-slotted CSMA/CA and there is no time link between backoff period and beacon. In this mode the coordinator node always stays in active Idle listening. However, the beacon-enabled mode is based on slotted CSMA/CA and when the beacon starts each node launches its backoff period. The communication between nodes is controlled by the network coordinator which transmits beacons at regular intervals (Beacon Interval) in order to synchronize the sensors. The nodes use the sleep/wakeup mechanism: they have to wake up in order to receive the coordinator's beacon. The coordinator is in charge of the data routing in the network. When they receive a beacon all nodes know the superframe duration (coordinator's activity period) and the time when they can transmit data or sleep. The advantages of this mechanism are the possibility for the coordinator to communicate with all nodes in activity periods and the reduction of energy consumption when the coordinator and nodes are inactive.

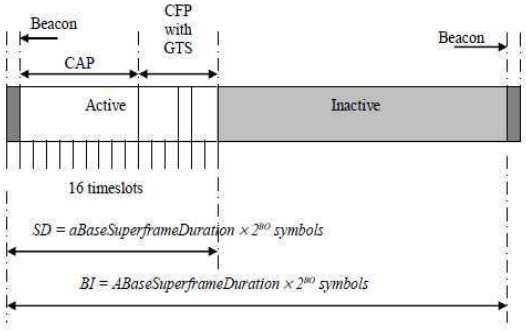


Fig. 1. Superframe structure in IEEE802.15.4

The structure of the superframe is presented in figure 1. It is composed of an active and an inactive period. The active period has 16 slots divided into 3 parts: beacon, CAP (Contention Access Period) and CFP (Contention Free Period). The beacon is transmitted at slot zero without using CSMA/CA and then the CAP period starts.

The size of both activity and inactivity periods is calculated according to the Beacon Order (BO) and the Superframe Order (SO). The following equations illustrate how to calculate the BI (Beacon Interval) and the SD (Superframe Duration).

$$\begin{cases} BI = aBaseSlotDuration \times aNumSuperframeSlots \times 2^{BO}; \\ SD = aBaseSlotDuration \times aNumSuperframeSlots \times 2^{SO} \end{cases}$$

where aBaseSlotDuration is the symboles which form the superframe when $SO = 0$.
aNumSuperframeSlots is the number of slots in the superframe.

The relation between BO and SO is: $0 \leq SO \leq BO \leq 14$. When the $BO = 15$ the network is in non-beacon-enabled mode.

The CFP uses the Scheduled TDMA mechanism like GTS (Guaranteed Timeslot) for the network traffic with QoS requirements.

There are three manners to send data in MAC IEEE802.15.4: direct transmission, indirect transmission and GTS transmission. In this work, we focus on the direct transmission.

B. Energy aware mechanisms

The MAC layer has an important role to reduce the energy consumption. It is divided into four classes [14]: the consumption related to control packets, collision, Idle listening and overhearing.

Several mechanisms are proposed to tackle the energy consumption problem in WSNs including the duty cycling [12]. This mechanism aims at saving energy by using sleep/wakeup technic which consists in activating the transmitter radio when the node has a packet to transmit and switch it off when there is no packet to transmit. The duty cycling needs cooperative nodes in order to coordinate the sleep/wakeup periods. This coordination is ensured by the sleep/wakeup scheduling distributed algorithm. The duty cycle in IEEE 802.15.4 is parametered by the cordinator which selects the SO and BO parameters. However, this mechanism reduces the bandwith and increases the delay. The study presented in [15] shows that the energy consumption decreases linearly with the size of received/transmitted packets. Unlike IEEE 802.11 in IEEE 802.15.4 the energy consumption at packet reception is more important than at the transmission packet. That's why in our proposed model, we focus on the overhearing time to evaluate the energy consumption at the monitor node.

There are three categories of sleep/wakeup protocols: the on demand protocol (the node wakes up only when another node wants to communicate with it), the scheduled Rendezvous protocol (the nodes wake up periodically at different moments in order to avoid a collision) and the asynchronous scheme protocol (each node wakes up independently without synchronisation needs).

Many MAC protocols based on CSMA and TDMA mechanims are proposed to save energy in WSNs like S-MAC, TRAMA and Z-MAC [14]. Suh et al. [1] proposed an enhancement of IEEE 802.15.4 called TEA-15.4 which consists in increasing the bandwidth and reducing the energy cost by adapting the Beacon Interval according to the kind of traffic. This solution is hybrid (beacon-enabled and beacon-non-enabled modes). However, its implementation is complex.

C. Monitoring mechanisms

The monitoring mechanism is defined as the set of actions that are useful to observe the nodes' behavior. The monitoring mechanism plays a major role in the evaluation of the nodes' reputation and in the updating of the nodes' trust level. It deals with some issues that have a negative impact, particularly on the monitoring mechanism, when a collision occurs at the monitor node during the monitoring process. This situation significantly increases the false positive rate. In fact, the

presence of non-cooperative nodes can affect the network in a negative way.

Many research works were dealing with monitoring mechanisms in IEEE 802.11. Watchdog [4] is a monitoring mechanism based on packets' forwarding to detect the non-forwarding nodes. It takes into account the routing layer but does not consider the physical and MAC level's parameters. It consists in listening to the traffic between monitor node's neighbors and detecting if the monitored nodes forward the packets in routing operations. The monitor node does not check at the routing layer if the monitored node has correctly received the packet. Thus, the ratio of false positives (false alarms) is high. To reduce the ratio of false positives, we proposed in our previous work [3] the enhancement of the monitoring mechanism while taking into account the cases of monitor's misobservation related to monitor/monitored collision. The cross-layer approach is selected in order to increase the probability to have an accurate monitor's observation. However, this solution cannot be directly applied to WSNs and particularly the IEEE 802.15.4. As far as we know there is no work focusing on the monitoring mechanism in IEEE 802.15.4. That is why in this paper, we deal with the monitoring mechanism called muDog in order to detect the non-cooperative nodes in beacon-enabled IEEE 802.15.4.

III. MUDOG: MONITORING MODEL

The monitoring mechanism muDog has as objective the improvement of the monitor's observation quality with a minimum of energy consumption. The monitoring process in beacon-enabled IEEE 802.15.4 is activated only in CAP (Contention Access Period) period. That means that the monitor node wakes up to receive the beacon frame and to track the packets transmitted by the monitroed node in the CAP duration in order to evaluate the cooperative metric of this node. The main objective of muDog is to reduce the time of overhearing and then the energy consumption by launching a targeted monitoring.

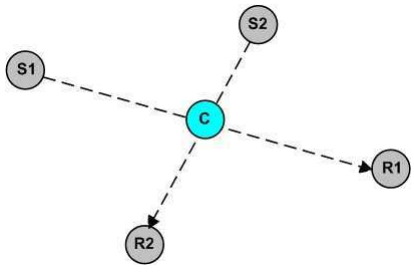


Fig. 2. Scenario of monitoring mechanism

We explain the monitoring process of muDog by an example illustrated in figure 2. In this scenario, we have two connections $\{S_1, R_1\}$ and $\{S_2, R_2\}$, coordinator node C its task is to route a packet from S_1 to R_1 and from S_2 to R_1. The node S_1 plays the role of monitor node and its goal is to monitor the coordinator node C. The node C is classified as well-behaving node if it forwads all packets to nodes R_1 and R_2 otherwise it is classified as selfish node. Only nodes S_1 and S_2 can act as monitor nodes and they target the transmission of node C by the overhearing.

The flowchart presented in figure 3 describes the muDog mechanism run by the monitor node.

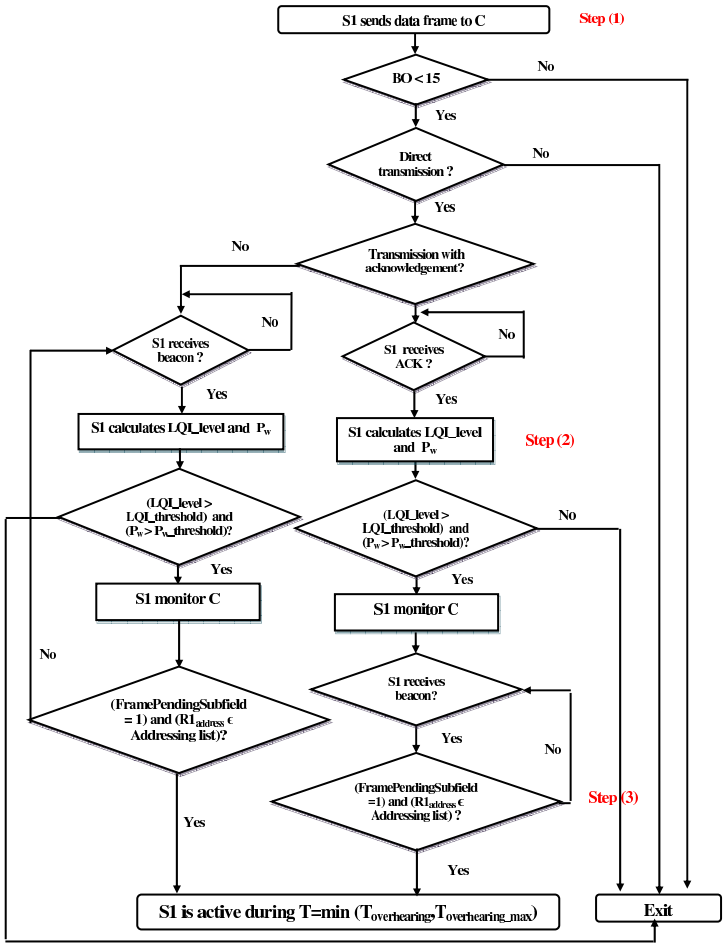


Fig. 3. The global flowchart of muDog

The node S_1 sends a packet Pkt_i to the node R_1 as illustrated in figure 2. When Pkt_i is received by the node C, then it transmits it to the receiver R_1 under the S_1 monitoring. Two kinds of transmission are possible with and without acknowledgement. Both transmissions are supported by our proposed monitoring mechanism. Let suppose the case of the transmission with acknowledgement. The node S_1 is able to check the good reception of Pkt_i by the coordinator C when it receives the ACK packet. This reception validates the first step of the monitoring process. The node S_1 acts as monitor node only if both conditions of step 2 in figure 3 are verified: $LQI > LQI_{threshold}$ and $Pw > Pw_{threshold}$ where LQI (Link Quality Indicator) and Pw is the probability to have a monitor node's accurate observation (see below for more details). This step ensures the quality of the monitoring process. We know that in beacon-enabled mode the coordinator sends periodically a beacon frame to its neighbors in order to ensure the synchronization and to give them information

related to the next transmission. The monitor node focuses on two important subfields in the beacon frame: Frame Pending (it is set to 1 if the coordinator has a packet to transmit) and Pending address Fields (address list of nodes to which the coordinator has packets to transmit). When these parameters are verified by S_1 that means that *Frame Pending Subfield =1* and $@R_1 \in \{$*Pending address Fields*$\}$, then the monitoring process is launched (see step 3). After this step, the node S_1 starts to overhear the packets sent by the node C in order to check if the coordinator correctly forwards the packets particularly Pkt_i.

The challenge is that the monitor node S_1 cannot know when the targeted packet Pkt_i will be transmitted during the overhearing period. We know that the overhearing period has an important impact on the energy consumption that's why the proposed mechanism muDog tries to optimize the overhearing period while ensuring the quality of the observation. The maximum time of overhearing does not exceed the time dedicated to CAP (Toverhearing$_{max} = T_{CAP}$)

A. Evaluation of the monitor overhearing time

In order to evalaute the overhearing time of the monitor node, we distinguish two kinds of transmission with and without acknowledgement. In the case of transmission with acknowledgement, we present two situations: the optimistic and the realistic. The optimistic situation is when the coordinator sends the first monitored packet Pkt_i to the R_1 which means the monitor node S_1 can switch off the monitoring process just after the overhearing of Pkt_i. In this situation the overhearing time is equal to the one packet transaction time ($T^{1Pkt}_{transac}$) and it is given by the following equation:

$$T_{overhearing} = T^{1Pkt}_{transac} = T_{backoff}(cw_j) + T_{DataReq} + T_{Data} + 2*\gamma + 2*\omega + 2*T_{Ack} + 2*T_{IFS} \quad (1)$$

where $T_{backoff}$ is the backoff time calculated according to CSMA/CA [2]. T_{Data} is the time needed to transmit the data frame (Mac Payload Field) and its size cannot exceed *aMaxMACPayloadSize*. $T_{DataReq}$ is the transmission duration of the data command frame. γ is the Turn around time and presents the duration between the reception of data frame and the transmission of the ACK packet. ω is *macAckWaitDuration* and consists in the maximum duration necessary to receive the ACK packet after the data frame transmission. T_{Ack} is the transmission time of the ACK packet. T_{IFS} (IFS: InterFrame Space) is the time needed to separate two consecutive data frames.

The pessimistic or realistic situation is when the monitored packet Pkt_i transmitted after a certain number of packets with different source addresses (like S_2 in the example of figure 2). NP is the number of packets transmitted before Pkt_i then the time of overhearing will be crossed by $NP + 1$. In addition, the packet retransmission for any reason must be taken into account and it is limited to only three attempts. Therefore, the overhearing time in this case is calculated as follows:

$$T_{overhearing} = (NP+1) \times (\sum_{i=0}^{2} P_i \times \sum_{j=1}^{i+1} T^{1Pkt}_{transac}(cw_j)) \quad (2)$$

where P_i is the probability to reach i^{th} attempts and it is defined as follows:

$$P_i = \begin{cases} P_{succ}(1-P_{succ})^i & if \quad i = \{0,1\} \\ (1-P_{succ})^2 & if \quad i = 2 \end{cases}$$

We based on Pollin et al. [5] Markov model to evaluate the probability P_{succ} in IEEE 802.15.4.

$$P_{succ} = N\phi(1-\phi)^{N-1}(1-\alpha)(1-\beta) \quad (3)$$

where N is the number of nodes in the network, ϕ is the stationary probability of node when it attempts CCA (Clear Channel Assessment) for the first time during one slot. α and β are the probabilities to sense the channel busy for the first and the second CCA (in IEEE 802.15.4 the transmitter must sense twice the channel by using CCA). In order to calculate the probability ϕ, we distinguish two cases: the saturated and unsaturated network.

In the case of saturated network, the node always has a packet to transmit. ϕ_{ACK} is calculated in the case of a transmission with acknowldgement as follows:

$$\phi_{ACK} = 1 - \Big(1 - \frac{\beta_{ACK}}{(1-\beta_{ACK})(2-P_{col})}\Big)^{1/N} \quad (4)$$

where P_{col} is the probability of collision during the transmission period and it is calculated as follows:

$$P_{col} = 1 - \frac{N\phi_{ACK}(1-\phi_{ACK})^{N-1}}{1-(1-\phi_{ACK})^N} \quad (5)$$

In the case of unsaturated network, the node does not always have a packet to transmit. We use the same model developped in [5] which consists in adding the delays X_1, X_2 and X_3. X_1 is the delay added after each transmission attempt when the channel is sensed busy. X_2 is the delay added before the next periodic transmission in the case of a transmission failure. X_3 is the delay added after the next transmission in the case of a successful first transmission. So, this model is valid only in the case of acknowledgement transmission, because in the other transmission mode it is not possible for the sender to be sure that the packet is correctly received.

The probability that a collision (P_c) occurs because two nodes transmit at the same time is calculated as follows:

$$P_c = 1 - (1-\phi)^{N-1} \quad (6)$$

For more details you can refer to the work [5].

The number of packets sent for each pending address is not specified in the IEEE 802.15.4 standard which makes the evaluation of NP number of packets to send before the monitored packet Pkt_i not easy. Then, we evaluate the NP_{min} and the NP_{max} in order to calculate the average number of NP (NP_{moy}). However, in the IEEE 802.15.4 standard the number of addresses pending cannot exceed 7 then the

$NP_{min} = 6$ (one packet to transmit for each address). In order to calculate the NP_{max}, we evaluate the maximum packet number possible to transmit during one CAP and we obtain:

$$NP_{max} = \frac{T_{CAP}}{T^{1Pkt}_{transac}} \quad (7)$$

where $T^{1Pkt}_{transac}$ is the time transaction for one packet with minimum backoff value.

In the case of the transmission without acknowledgement that means that the *turn around time* and the *macAckWaitDuration* are required. Therefore, the equation to calculate the overhearing time in the optimal case is:

$$T_{overhearing} = T^{1Pkt}_{transac} = T_{backoff}(cw_j) + T_{DataReq} + T_{Data} + 2 * T_{IFS} \quad (8)$$

In the realistic case, the equations 1 and 4 become as follows:

$$T^{noAck}_{overhearing} = NP_{moy}(P_0 \times T^{noAck}_{transac}(cw_j)) \quad (9)$$

B. Evaluation of the probability to have a monitor's accurate observation

The quality of the monitoring process consists in the accurate observation of the monitor node. We quote two main conditions to define the accurate observation of the monitor node: the monitored node successfully transmits the target packet (P_{cond1}) and no collision occurs at the monitor node during the monitored node transmission (P_{cond2}). Let Pw represent the probability to have a monitor's correct observation and be calculated as follows:

$$Pw = P_{cond1} \times P_{cond2} \quad (10)$$

P_{cond1} is calculated according to the equation 3 proposed in the previous subsection. However, P_{cond2} depends on many parameters particularly the distance between the monitor and monitored nodes (d). The distance between monitor and monitored nodes has an impact on the monitor's vulnerable region ($Mvr(d)$) which can affect the monitoring mechanism. This region only exists if the interference region of the monitor node is not covered by the carrier sense region of a monitored node ; we called it "the monitor vulnerable hidden region". If any node in this region starts to transmit, it disturbs the monitor node's observation. For more details about this region and how we can evaluate it, the reader can refer to our previous work [3]. Therefore, P_{cond2} equals one when no node in region $Mvr(d)$ transmits in a vulnerable time. This period depends on the transmission time T_{av} of a packet: when a 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 distribution is an important parameter, that's why we assume that the nodes are distributed within a topology which is a two-dimensional Poisson process with parameter λ (memoryless property of Poisson distribution).

The nodes in region $Mvr(d)$ must remain silent during μ slots time where $\mu = (T_{av}/\sigma)$. Region $Mrv(d)$ can be equal to zero when it is covered by the carrier sense of the monitored node. Otherwise, $P_{cond2}(d)$ (if $d > \frac{R_s}{1+\sqrt[k]{T_{SNR}}}$) is given by:

$$P_{cond2}(d) = \begin{cases} 1 & \text{if } d \leq \varphi \\ e^{-\tau N_h \cdot \mu} & \text{Otherwise} \end{cases} \quad (11)$$

where $N_h = \lambda Mvr(d)$ and $\varphi = \frac{R_s}{1+\sqrt[k]{T_{SNR}}}$ with R_s is the Carrier sensing range and T_{SNR} is the Threshold Signal to Noise Ratio.

Now, we can calculate $Pw(d)$ as follows:

$$Pw(d) = \begin{cases} P_{succ} & \text{if } d \leq \varphi \\ P_{succ}.e^{-\tau N_h \cdot \mu} & \text{Otherwise} \end{cases} \quad (12)$$

IV. Performance Evaluation

In order to evaluate muDog monitoring mechanism performances, we implement the proposed algorithm and the analytical model by using our own simulator. We evaluate the overhearing time of the monitor node with different network parameters such as: packet size and density of nodes. In addition, the probability of the monitor correct observation Pw is evaluated and analyzed according diffrent paramters: traffic load, the density of nodes in the network and the distance between monitor and monitored nodes.

A. The overhearing time evaluation

Two cases have to be distinguished: the case of a saturated network and the case of a non-saturated network. The saturated case is divided into two cases: the acknowledged and non-acknowledged cases.

1) Impact of the number of packets (NP_{moy}) and the packet size: In order to determine the variation interval of NP_{moy}, we have evaluated NP_{moy} variation according to the x packets size in both cases: with and without any acknowledgement. This evaluation enables us to deduce the average number of packets that may be sent during CAP.

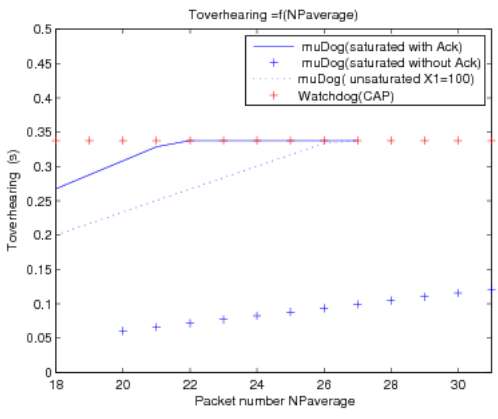


Fig. 4. $T_{overhearing}$ according to the average number of packets (NP_{moy})

The figure 4 shows that the overhearing time increases proportionally to the number of packets preceding the monitored packet and the greatest values are observed in the saturated case with acknowledgement because the packets are more often generated and the transactions are longer than in the

non-saturated case. For each acknowledged transmission, the overhearing time remains inferior to the overhearing time in Watchdog. This is true for $NP_{moy} < 22$ packets in a saturated case and $NP_{moy} < 26$ packets in a non-saturated case. For instance, for $NP_{moy} = 20$, the overhearing time is reduced by 9% in a saturated case and by 30% in a non-saturated network. For $NP_{moy} > 22$ packets and $NP_{moy} > 26$ packets respectively in a saturated and non-saturated network, the overhearing time equals the overhearing time observed with Watchdog. muDog is thus more performant than Watchdog when the queue contains less than 22 packets in a saturated network and less than 26 packets in a non-saturated network. In the case of a transmission without any acknowledgement, muDog is much more performant. Indeed, even when the queue contains the maximum number of packets (31), the overhearing time is reduced by 63%.

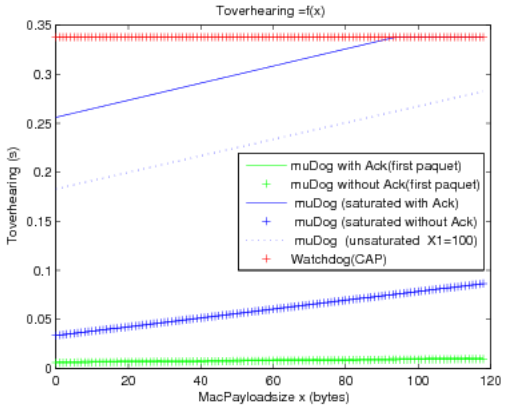


Fig. 5. $T_{overhearing}$ according to the size of MACPayload

The figure 5 shows the overhearing time according to the size of the packets in 6 different situations: in an optimal situation with and without any acknowledgement, in a realistic situation with a saturated network and an acknowledged transmission, with a non-acknowledged transmission, and with a non-saturated network. All these cases are then compared to the Watchdog (the CAP duration).

The overhearing time significantly decreases in the case of a non saturated network compared to a saturated network, although we introduced a delay $X_1 = 100$ slots. Indeed, in the case of a non saturated network, the packets are less often generated, and this reduces the probability ϕ. In the case of a non acknowledged transmission, the transaction duration is minimized, and this significantly reduces the overhearing time. muDog is quite performing in the cases of a non saturated network and of a non acknowledged transmission; it prevents the nodes from reaching Watchdog overhearing time for any packet size. With a value of $x = 118$ (maximum value), the overhearing time is reduced by 19% in a non saturated network and by 72% in the case of a non acknowledged transmission. However, in the case of saturated network, and with a great number of permanently generated packets, muDog is more efficient than Watchdog only for $x < 92$ bytes. Indeed, the small packets (for instance $x = 20$), the necessary overhearing time is of 0.265 s with muDog, whereas it is still fixed at 0.33 s with Watchdog, even for a small packet. muDog thus reduces the activity period of the monitor by 20%, which will consequently reduce the energy cost.

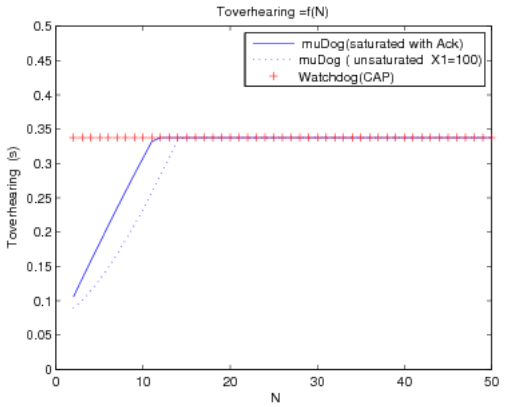
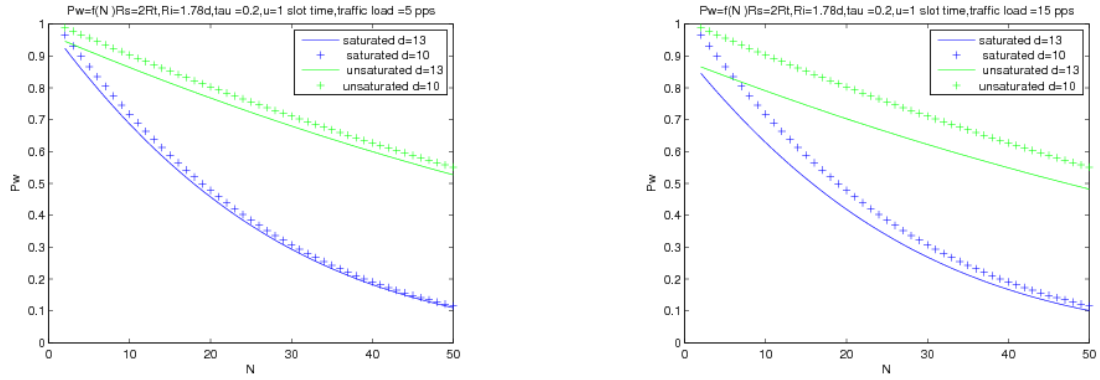


Fig. 6. $T_{overhearing}$ according to the nodes density

2) Impact of the nodes density: In order to study the impact of nodes density on the overhearing time, we varied the nodes density N from 2 to 50 nodes in the network and the obtained results are plotted in figure 6. The overhearing time obviously increases proportionally to the nodes density. However, muDog is much more performing in small saturated networks with less than 12 nodes (15 nodes in a non saturated network) than Watchdog. For a network composed of 5 nodes, the overhearing time is reduced by more than 50% (0.15 s) of the time given for Watchdog. In the case of great networks, it is important to have a great overhearing time (equal to CAP) in order to monitor a great number of nodes and thus a more intense traffic.

B. Evaluation of the probability to have an accurate observation Pw

In this subsection, we evaluate the impact of the traffic charge, nodes density and distance between the monitoring and monitored nodes on the probability to make an accurate observation Pw. In order to study the impact of the nodes density on the monitoring process, we have evaluated Pw variation according to the nodes density for two network traffic loads $5pps$ and $15pps$. The obtained results are plotted in figures 9(a) and 9(b). In both cases, the probability to have an accurate observation significantly decreases when the nodes density increases. Indeed, when the number of nodes increases, the probability to have a successful transmission decreases (because of the collisions) and thus the probability to have an accurate observation also decreases. The decrease is even more important in the case of a saturated network. The difference between both cases may reach 80%. The best values of Pw are reached when the nodes density is small (between 2 and 10 nodes) and for short distances between the monitoring and monitored nodes ($10m$). In such cases,



(a) Case of 5 pps

(b) Case of 15 pps

Fig. 7. Pw versus nodes density with 5pps and 15 pps of traffic charge

they vary between 0.2 and 0.98. When the distance and the traffic charge increase, Pw decreases more. For instance, for $N = 10$, $15pps$ and $d = 13m$, the probability decreases by 11% in a non saturated network and by 13% in a saturated network. The worst situation occurs with a saturated network, when the nodes density is high (50 nodes) and when the traffic is quite important ($15pps$). Pw is then equal to 0.1.

V. Conclusion

In this paper, we proposed an analytical model aiming at ensuring the efficient monitoring process called muDog while taking into account the energy constraints and the accuracy of the monitor's observation. In addition, the evaluation of the proposed monitoring mechanism is proposed and compared to the existing Watchdog mechanism by using different parameters and metrics. The impact of some parameters on the monitoring process like the distance between the monitor and monitored nodes, the time of overhearing (energy consumption), the network traffic load and the nodes density. The evaluations have shown that the transmission probability, the distance between the monitor and monitored nodes and the network traffic load have a negative impact on the monitoring process. However, the nodes density and the type of network (saturated or non saturated) seem to have a mostly negative impact on the observation accuracy. Moreover, the monitor node's accurate observation is thus possible in a small non saturated network with a short distance between the monitoring and the monitored nodes. The obtained results illustrate that muDog is more efficient than Watchdog whatever the parameter is.

In our future works, we plan to evaluate muDog by introducing different mobility models and by using a real test-bed.

References

[1] C. Suh, Z. Hameed Mir, Y. KO *Design and implementation of enhanced IEEE 802.15.4 for supporting multimedia service in Wireless Sensor Networks*. Computer Networks journal, Volume 52, Issue 13, 17 September 2008, Pages 2568-2581.

[2] IEEE Standard 802.15.4, *Part 15.4: Wireless Medium Access Control and Physical Layer Specification for Low Rate Wireless Personal Area Networks*. IEEE Std. 802.15.4, December 2003.

[3] A. Rachedi and A. Benslimane, *Toward a cross-layer monitoring process for mobile for mobile ad hoc networks*. Journal of Security and Communication Networks, Volume 2, Issue 4, pages 351-368, July/August 2009.

[4] S. Marti, TJ. Giuli, K. Lai, M. Baker, *Mitigating routing misbehavior in mobile ad hoc networks*. In Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Boston, USA, 2000; pp. 255-265.

[5] S. Pollin, M. Ergen, S. Coleri Ergen, B. Bougard, L. Van der Perre, I. Moerman, A. Bahai, P. Varaiya, F. Catthoor *Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer*, IEEE Transactions on wireless communications, VOL. 7, NO. 9, September 2008.

[6] A. Keshavarzian, H. Lee, L. Venkatraman, *Wakeup Scheduling in Wireless Sensor Networks*, in Proc. ACM Mobihoc 2006, Florence, Italy, May 2006, pp. 322-333.

[7] N. F. Timmons, W. G. Scanlon, *Analysis of the Performance of IEEE 802.15.4 for Medical Sensor Body Area Networking Sensor and Ad Hoc Communications and Networks*, IEEE SECON 2004, pp. 16-24, 2004.

[8] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella *Energy conservation in wireless sensor networks: A survey*. Ad Hoc Networks, Vol. 7, Issue: 3, pp. 537-568, 2009.

[9] Y. Kwon, Y. Chae *Traffic Adaptive IEEE 802.15.4 MAC for Wireless Sensor Networks*, Lecture Note in Computer Science (LNCS),Volume 4096/2006, pp. 864-873, 2006.

[10] G. Lu, B. Krishnamachari, C. S. Raghavendra, *Performance Evaluation of the IEEE802.15.4 MAC for low rate low power wireless network*, in Proceedings of the EWCN'04, Held in Conjunction with the IEEE IPCCC, April 2004.