Formal Analysis of MAC Protocols for WSNs: a Review

Maissa Elleuch[1,2], Osman Hasan[2], Sofiène Tahar[2], and Mohamed Abid[1]

[1] CES Laboratory, National School of Engineers of Sfax, Sfax University
Soukra Street, 3052 Sfax, Tunisia
maissa.elleuch@ceslab.org
mohamed.abid@enis.rnu.tn
[2] Dept. of Electrical & Computer Engineering, Concordia University
1455 de Maisonneuve W., Montreal, Quebec, H3G 1M8, Canada
{melleuch,o_hasan,tahar}@ece.concordia.ca

1 Introduction

In the first section of this report, I give a general presentation of MAC protocols designed for wireless sensor networks (WSNs). After that, I review the most interesting works found in the literature for the formal verification of these protocols.

2 MAC protocols for WSNs

In WSNs, the main goal of a MAC protocol is to manage the access to the shared wireless medium while reducing the energy consumption. The energy constraint was not really taken into account in previous MAC protocols for wireless networks so that existing protocols have been completely inadequate for WSNs. Other criterions such as throughput and delay, which were critical for wireless networks, are no longer in the WSNs context. In this section, I present the two major categories of MAC protocols, then I review some simulation works done for their validation.

2.1 Categories of MAC protocols

Minimizing the energy consumption of a given MAC protocol is mainly based on a good collision scheme. A collision occurs if two or more nodes use simultaneously the medium for sending. According to the number of nodes looking to transmit at a given time, MAC protocols can be classified into two categories:

Contention-based protocols: The sensor nodes compete to access the medium. A node can send data at any time but collision can occur if another node is sending data at the same time. In this case, the whole sent data is corrupted and the only solution is to send it again from each side by trying to avoid another

collision. Since collisions are source of energy waste, the designed MAC protocol should include many mechanisms in order to avoid or to reduce the probability of collisions occurrence. The most used mechanism for the contention resolution is the random exponential back off procedure. This procedure is inspired from the BEB procedure for the local network. The back off procedure can be summarized as follows. Each node looking to send a data has to:

1. wait for a random duration chosen uniformly in the interval [0 - (2^{BE} - 1)] where BE is the exponential back off
2. find out the channel state by a CCA (Clear Channel Assessment) procedure
3. if the channel is free then, the node begins sending
4. else, if the channel is busy then the retransmissions number is increased and the number BE is also updated. The transmission fails if the retransmissions number is over a given threshold, otherwise, the node goes back to the first step.

Examples of contention-based MAC protocols include S-MAC [22], X-MAC [5] and LEACH [11].

Scheduling-based protocols: The nodes collaborate to access the medium according to a given scheme. This scheme can be based on frequency (FDMA, frequency division multiple access), code (CDMA) or time (TDMA). For the TDMA scheme, each node is assigned a time period during which it can communicate. Beyond this period, the node enters in the idle state and is not allowed to send data over the wireless medium. Collisions when transmitting data can never occur. The most advantage of this scheme is reducing the energy consumption. Nevertheless, initial network configuration needs a lot of data and can lead hence to a waste of energy. Examples of protocols belonging to this category are SMACS [20] and TRAMA [19].

There are also hybrid MAC protocols which combine the features of the two categories of MAC protocols cited above.

2.2 Validation by simulation

The main validation technique of MAC protocols designed for WSNs is simulation. In general, the approach is based on developing a theoretical paper-and-pencil based model of the protocol, doing some analysis, and finally illustrating theoretical results through a performance evaluation provided by simulation. For example, the behavior of the MAC protocol of the IEEE 802.15.4 standard [4] has been widely studied through simulation for single-hop networks in [18], [16] and [17]. These works have evaluated different network models with various assumptions related to traffic (saturated and unsaturated), acknowledgments (with and without) and retransmissions (with and without).

The theoretical models proposed for the IEEE 802.15.4 MAC have been usually based on the corresponding Markov chain, which is inspired from the Markov chain of Bianchi for the IEEE 802.11 MAC [3]. Due to the probabilistic behavior

of the protocol, the proposed models are commonly probabilistic. Nevertheless, they have been frequently very simplified. Some recent attempts to reflect more the reality can be noticed in the work of [13]. The authors have given a realistic theoretical analysis by taking into account many constraints like heterogenous traffic within multi-hop networks and with hidden terminals. The mathematical analysis has given some performance indicators like reliability as the success probability, the delay of received packets and the expected energy consumption. This analysis is done for the single hop networks, and then generalized to multi-hop ones. On the other hand, the Monte Carlo simulation done has shown the impact of the routing decision on the MAC performance in terms of reliability, delay and balance. The work of [9] has also presented a very good analytical model of the unslotted IEEE 802.15.4 MAC giving probabilities related to delay, packets reception and energy consumption. The proposed model has been evaluated within the NS-2 simulator.

The performance evaluation of the CSMA/CA mechanism of the IEEE 802.15.4 MAC has also drawn a great attention. It has been hence evaluated using Markov chain in [14] and [15]. The proposed analytical results have illustrated the throughput and access delay within the network. Other aspects of the slotted CSMA/CA like impacts of the beacon order, the superframe order and the exponential back off, have been taken into account in [12] in order to evaluate the mechanism in terms of throughput, average detection delay and success probability.

3 Formal analysis of MAC protocols

In this section, I review the most important works of formal verification of MAC protocols for WSNs. For each work, I give a small description of the verified MAC protocol, then I present an analysis of the formal verification done.

3.1 Model checking of the S-MAC protocol within PRISM

The S-MAC protocol: The S-MAC protocol is based on the observation that, besides collision, keeping the radio switched on in idle listening, is also a source of energy waste. The idea of the S-MAC [22] protocol is to turn off the radio by period of time. Hence, periodically, nodes are put into a sleep state. Each node can be in one of the two following modes: LISTEN where the radio is switched on and by opposition, SLEEP where the radio is turned off. The major difficulty here is to synchronize the sleeping schedules of the different nodes to be able to communicate. This is done by a coordinate sleeping where each node maintains a schedule table including the LISTEN/SLEEP period of each of its neighbors. Despite the existence of the schedule concept, The S-MAC belongs to the first category of MAC protocol. In fact, the schedule concept is done for the same node by switching between LISTEN and SLEEP states but not between nodes. Hence, collisions can occur when two nodes in the LISTEN mode tries to access the medium at the same time.

Formal analysis: In [2], the authors have verified the reachability of packets to the sink node for a simple network model of 3-hops. In particular, they check the following property saying "How long does it take for packets sent by the source node to reach the destination (sink node)?". After that, by labeling the model with cost values, it has been possible to evaluate the expected communication latency and energy consumption.

Although the probabilistic model checking of S-MAC within PRISM has been done successfully, this work suffers of the common problem of state explosion. Indeed, the authors pointed out that the network hops have been restricted to 3 so that the number of scheduled subsets is 2, and the built model can be tractable within PRISM. Added to that, the expected values given for the communication latency and energy consumption were obtained by running several experiments on the specified model. Given the capabilities of PRISM to compute expectation, these values are specific to the simulated model and can not be viewed as general.

3.2 Model checking of the ECO-MAC protocol within PRISM

The ECO-MAC protocol: The ECO-MAC [23] saves energy by taking advantage from the very low traffic in the majority of WSNs. This protocol is an hybrid media access control protocol for wireless sensor networks. It combines three access techniques which are CSMA, TDMA (Time Division Medium Access) and multi-channel protocols. By doing a multi-band communication and time division in time slots for channel access scheduling, the ECO-MAC allows easier synchronization within the network. Performance evaluation under the OPNET simulator has shown that ECO-MAC is better than S-MAC in terms of energy consumption and latency.

Formal analysis: The probabilistic model checking of ECO-MAC within PRISM [24] has focused on the randomized back-off procedure. The network modeled has included one receiver and a number of senders. The proposed probabilistic model has been composed of three modules which are: the receiver, the sender and the channel. Properties related to the number of packet retransmissions such as "if sender1 rejects its packet then the unsuccessful transmissions number has been reached the bounded value of transmissions", have been successfully verified. Another property related to hidden senders saying that "if the two hidden senders have started their transmission simultaneously, a collision will be occurred and detected by the receiver", has been also verified. During the verification process, an unpredictable problem related to state explosion has appeared after more than 4 hours of model building. Thus, the authors have been obliged to adjust some parameters by a reduction factor.

3.3 Model checking of the IEEE 802.15.4 protocol within PRISM

The IEEE 802.15.4 MAC protocol: The IEEE 802.15.4 standard [4] is designed for LR-WPAN (Low-Rate Wireless Private Area Networks) networks

which include WSNs. This kind of network is characterized by a low cost, small coverage, low transmission power, bit rate and energy consumption. The IEEE standard specifies both MAC and PHY layers. The contention resolution mechanism to avoid collision is the CSMA-CA. The MAC layer of the IEEE802.15.4 provides two modes which are beacon and non-beacon. This mode is selected by a central coordinator node called PAN. One of the most attractive features of the standard IEEE 802.15.4 is that it adopted by the Zigbee standard [1], published in 2004, and which defines the higher layer of the communication stack, i.e., routing and application. A complete protocol stack can be then adopted, with the IEEE standard for the lower layers and Zigbee for the higher ones.

Formal analysis: In [10], the PRISM model checker has been used to verify the CSMA-CA contention resolution protocol of the IEEE 802.15.4 standard. The properties of interest were "the minimum probability that both stations successfully complete their transmissions", and "the maximum probability of at least k collisions". Thanks to the aspect of reachability rewards available within PRSIM, the authors have also evaluated the maximum expected number of collisions and the average transmission delay.

Compared to previous works, this work has the advantage to make realistic assumptions with an accurate time modeling. The authors have also advocated that the IEEE 802.15.4 standard is very suitable for model checking since it uses smaller numerical values so that the state explosion problem can be eventually avoided. Nevertheless, once the model checker launched, a state explosion problem occurred. Therefore, other temporal abstractions and some parameters reduction have been needed. Added to that, the expected values have been given by simulation.

3.4 Model checking of the LMAC protocol within UPPAL

The LMAC protocol: The LMAC protocol [21] is a scheduling-based protocol. If a node wants to transmit some data, it has to wait until its own time slot comes up. This way collision is not really possible except in the discovery phase. Indeed, the schedule configuration is set by the node itself and not by a central node, where the steps are the following: a given node collects information about the busy time slots of its neighbors, then it has to choose at random a free time slot among the set of free time slots available in order to evolve to the active phase. This random choice can easily lead to collision if two nodes claim the same time slot.

Formal analysis: The model checking of the LMAC protocol [8] under UPPAAL, has given good results for the detection and resolution of collision for all connected topologies with 4 and 5 nodes. The verification has been exhaustive for all the considered configurations.

In particular, it has been possible to easily verify a reachability probability property, and safety properties such as freedom from deadlocks. However,

some problems of state explosion have been encountered while verifying the liveness properties for most topologies. Thereby, the model has been simplified; the number of clocks and non-essential interleaving reduced, so that the same behavior is performed. The authors have also indicated that once the number of nodes increased, a state explosion problem appeared instantly. At the end of the paper, they discussed the major limitations of their work which include the capacities of UPPAAL to verify probabilistic properties. Therefore, probabilistic model checking through PRISM has been proposed as a furture work, and the corresponding approach has been briefly presented.

3.5 Model checking of a contention-free MAC protocol within APMC

The contention-free MAC protocol of [6]: The MAC protocol of [6] is distributed, contention-free and self-stabilizing. This last feature reflects the scalability of the protocol that can be easily adapted dynamically to nodes joining or leaving the network. This protocol uses the TDMA schedule in which time is divided into frames which in turn are divided into slots. The protocol is composed of two phases called respectively LooseMAC and TightMAC. First, the LooseMAC phase is performed in order to build the TDMA schedule, then, the TightMAC is run so that the remaining free slots are used. The LooseMAC is randomized and ensures that a node find quickly the slot. Besides that, the TightMAC phase enhances the efficiency of the MAC protocol.

Formal analysis: The work of [7] has formally verified the theoretical model, given in [6], for the MAC protocol. The formal verification has been achieved through the Approximate Probabilistic Model Checker (APMC). Such model checker is based on approximation to get the satisfaction probability of a temporal specification. Verified properties have been especially related to contention-freeness and the network self-stabilizing. The authors have also computed the probability of a node to successfully choose a free time slot without conflict with another node. The model checking within APMC overcomes the problem of state explosion and reduces the memory consumption, however, obtained results are not completely valid; they depend on the approximation parameter chosen.

4 Synthesis

Since the results obtained by simulation can never be totally accurate, simulation cannot be considered as an effective solution for the probabilistic analysis of WSNs, especially when applied to validate WSNs for mission-critical applications. Formal analysis techniques have been proposed as an efficient solution to validate MAC protocols for WSNs. In particular, the use of probabilistic model checking is widely accepted in this context where the most used probabilistic model checker is PRISM. As in wireless networks, the formal analysis has somhow focused on the verification of the contention resolution mechanism.

Thus, properties of interest have included the number of retransmissions, the delay and the energy consumption. The verified models are different by the abstraction levels, assumptions, network configurations and temporal modeling. Nevertheless, the major limitation consists on the state explosion problem especially when trying to extend the verified model. Besides that, while statistical quantities like expectation and variance are very important in the probabilistic analysis of the model, probabilistic model checking gives an unreliable approach to measure such quantities.

The cited works for the model checking of MAC protocols for WSNs are conscious of the limitations imposed by this technique. Each paper has almost reported a problem of state explosion that the authors have tried to overcome by reducing some parameters or by making additional abstractions. However, these "local" solutions seem to reduce the effectiveness of the probabilistic model checking applied to WSNs. The mentioned difficulties can be considered as very motivating for the use of the probabilistic framework developed in HOL for the formal analysis of MAC protocols for WSNs.

Questions: Related to WSNs

1. Why the WSNs community continue to propose ad hoc MAC protocols which are not conform to any standard, in particular to IEEE?

2. How can I fix a MAC protocol, including probability in his behavior and properties of interest, to formally analyze? Should I fix in advance some criterions such as the application domain and deployment so that the scope of MAC protocols will be automatically reduced?

Questions: Related to formal verification

1. Why the cited works have proposed to overcome encountered problems of model checking by various solutions like probabilistic or parameterized model checking, but they have never proposed theorem proving?
   Is it because MAC protocols are typically modeled by Markov chains so that the natural verification technique is model checking?

2. Some of the cited works by simulation deduce a theoretical model from the Markov chain. How this deduction is done?

3. Once the MAC protocol is fixed, should I formally verify the specification or the implementation?

4. Is probabilistic theorem proving can efficiently model time and properties related to energy evaluation?

References

1. ZigBee Alliance. Zigbee specification. Available for download at: http://www.zigbee.org, December 2004.
2. P. Ballarini and A. Miller. Model checking medium access control for sensor networks. In *Proceedings of the Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation*, pages 255–262, Washington, DC, USA, 2006. IEEE Computer Society.
3. G. Bianchi. Performance analysis of the ieee 802.11 distributed cordination function. *IEEE on Selected Areas in Communications*, 18(3):535–547, March 2000.
4. IEEESA Standards Board. Part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans). online, December 2003.
5. M. Buettner, G.V. Yee, E. Anderson, and R. Han. X-mac: a short preamble mac protocol for duty-cycled wireless sensor networks. In *Proceedings of the 4th international conference on Embedded networked sensor systems*, SenSys '06, pages 307–320, New York, NY, USA, 2006. ACM.
6. C. Busch, M. Magdon-Ismail, F. Sivrikaya, and B. Yener. Contention-free mac protocols for wireless sensor networks. In *Proceedings of 18th International Conference of Distributed Computing (DISC)*, LNCS, pages 245–259, Berlin, Heidelberg, 2004. Springer-Verlag.
7. M. Cadilhac, T. Hérault, R. Lassaigne, S. Peyronnet, and S. Tixeuil. Evaluating complex mac protocols for sensor networks with apmc. *Electron. Notes Theor. Comput. Sci.*, 185:33–46, July 2007.
8. A. Fehnker, L. Van Hoesel, and A. Mader. Modelling and verification of the lmac protocol for wireless sensor networks. In *Proceedings of the 6th international conference on Integrated formal methods*, IFM'07, pages 253–272, Berlin, Heidelberg, 2007. Springer-Verlag.
9. C. Fischione, S. C. Ergen, P. Park, K. H. Johansson, and A. Sangiovanni-Vincentelli. Medium access control analytical modeling and optimization in unslotted ieee 802.15.4 wireless sensor networks. In *Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks*, SECON'09, pages 440–448, Piscataway, NJ, USA, 2009. IEEE Press.
10. M. Fruth. Probabilistic model checking of contention resolution in the ieee 802.15.4 low-rate wireless personal area network protocol. In *Proceedings of the Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation*, pages 290–297, Washington, DC, USA, 2006. IEEE Computer Society.
11. W.B. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8 - Volume 8*, HICSS '00, page 8020, Washington, DC, USA, 2000. IEEE Computer Society.
12. A. Koubaa, M. Alves, and E. Tovar. A comprehensive simulation study of slotted csma/ca for ieee 802.15.4 wireless sensor networks. In *Proceedings of the IEEE WFCS*, pages 183–192, 2006.
13. P. Di Marco, P. Park, C. Fischione, and K.H. Johansson. Analytical modelling of ieee 802.15.4 for multi-hop networks with heterogeneous traffic and hidden terminals. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, SenSys '03, 2010.

14. J. Mišić and V.B. Mišić. Access delay for nodes with finite buffers in ieee 802.15.4 beacon enabled pan with uplink transmissions. *Comput. Commun.*, 28(10):1152–1166, June 2005.
15. J. Mišić, S. Shafi, and V.B. Mišić. The impact of mac parameters on the performance of 802.15.4 pan. *Ad Hoc Netw.*, 3(5):509–528, September 2005.
16. J. Mišić, S. Shafi, and V.B. Mišić. Performance of a beacon enabled ieee 802.15.4 cluster with downlink and uplink traffic. *IEEE Trans. Parallel Distrib. Syst.*, 17(4):361–376, April 2006.
17. P. Park, P. Di Marco, P. Soldati, C. Fischione, and K. H. Johansson. A generalized markov chain model for effective analysis of slotted ieee 802.15.4. In *Proceedings of the 6th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, MASS '09, pages 130–139. IEEE Press, 2009.
18. S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L.V. Perre, I. Moerman, A. Bahai, P. Varaiya, and F. Catthoor. Performance of a beacon enabled ieee 802.15.4 cluster with downlink and uplink traffic. *IEEE Transactions on Wireless Communication*, 7(9):3359–3371, 2008.
19. V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves. Energy-efficient collision-free medium access control for wireless sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, SenSys '03, pages 181–192, New York, NY, USA, 2003. ACM.
20. K. Sohrabi, J. Gao, V. Ailawadhi, and G.J. Pottie. Protocols for self-organization of a wireless sensor network. *IEEE Personal Communications*, 7(5):16–27, June 2000.
21. L. van Hoesel and P. Havinga. A lightweight medium access protocol (lmac) for wireless sensor networks: reducing preamble transmissions and transceiver state switches. In *Proceedings of the International Conference on Networked Sensing Systems (INSS)*, 2004.
22. W. Ye, J. Heidemann, and D. Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 12(3):493–506, June 2004.
23. H. Zayani, R.Ben Ayed, K. Djouani, and K. Barkaoui. Eco-mac: an energy-efficient and low-latencyhybrid mac protocol for wireless sensor networks. In *Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, PM2HW2N '07, pages 68–71, New York, NY, USA, 2007. ACM.
24. H. Zayani, K. Barkaoui, and R.Ben Ayed. Probabilistic verification and evaluation of backoff procedure of the wsn eco-mac protocol. *Wireless & Mobile Networks*, 2(2):156–170, 2010.