Impact of Application Layers over Wireless Sensor Networks

Cédric Ramassamy [†], Hacène Fouchal [*] and Philippe Hunel [†]

[*]CReSTIC Université de Reims Champagne-Ardenne, France
[†]LAMIA, Université des Antilles et de la Guyane, France

Abstract: Applications over Wireless Sensor Networks (WSNs) are various and different. Many routing protocols have been proposed for WSNs since a many years. Medium Access Control (MAC) protocols can differ from a network to another. The transmission range can also be variable from a sensor to another depending on their battery capacities. All these various protocols have an influence on the WSNs. It is worthy to choose the appropriate protocol for each specific situation in order to ensure high security of the network.

In this paper, we show that the type of applications has a real impact on WSN. Indeed, each kind of application with a specific routing protocol, MAC layer and transmission range value impact on security of network in terms of packets lost rate.

We have undertaken a set of experimentations in order to show the importance of an appropriate configuration to deploy a WSN with a high security confidence degree. For the application layer, we have handled three types of applications. For the routing layer, we have handled only with AOMDV protocol. For MAC layer we use 802.15.4 protocols. We have conducted many simulations through the NS-2 simulator in order to analyze one relevant security indicators on WSNs: lost packet rate.

1 Introduction

A WSN is mainly composed of two types of components: resource constrained independent nodes (sensors) and high resourced sink nodes (base stations). A node in a network communicates with each other through a wireless medium, where the communication energy is greater than the computational energy. In addition to that, the energy required to transmit a message is twice higher than the energy required for receiving a message. In the same time, the route of any message sent to base stations is a challenging issue about a network lifetime for many reasons. If we use the shortest routes where some nodes have small capacity batteries, we may reduce the network lifetime. If we use longer routes with many nodes, we will surely increase the network delays. For these reasons, routing objectives are, in general, conducted by higher applications: streaming video applications need longer network lifetime but fire monitoring applications need faster response time. Various routing mechanisms have been proposed for different applications. They are different according to their routing objectives and routing techniques. As said below, the network features will guide to choose adequate routing techniques. The IEEE 802.15.4 standard offers the most common communication protocols for the MAC and the physical (PHY)

layers [BPC+07]. After a deployment, it is not possible to handle nodes, in particular, for military applications, fire monitoring, underwater applications. Then it could be so complicated to replace the batteries [CoSKM04]. Thus, it is necessary to efficiently consume the energy and avoid lost packets when they communicate which will provide more security for WSNs.

We considered the following parameters in WSN: the radio range, the MAC layer, the network size, the routing protocol type, the application type

In this paper, we study the impact of applications on the WSN security.

We have conducted a large number of experimentations using the NS-2 framework. The radio range length has been tested for 25 meters. For the network size, we have used 25, 60, 100 and 300 nodes. But we show impact only for 300 nodes that represents high scalability networks. For routing, we have used AOMDV protocols. For the application type, we have used three kinds of applications having different rates: regular applications, applications with high rate communications (denoted high rate application in the rest of the paper) and applications with some burst communications (denoted burst based applications in the paper).

We observed in each case, the WSN security through the lost packets rate. We have then calculated a security metric which depends on this parameter.

This paper is organized as follows. Section 2 is dedicated to related works. Section 3 presents an overview of usual protocols used over WSNs. Section 4 describes our contribution, experimentations and analysis are also detailed. Section 5 concludes our work and gives some ideas about future work.

2 Related Work

In the literature, a comparative study of routing protocols can be found in [AY05] and [AkK04]. Authors discussed widely properties of many routing protocols. They proposed for WSNs different categories of routing protocols such as Location-based protocols, Data-centric Protocols, Hierarchical Protocols, Mobility-based Protocols, Multipath-based Protocols, Heterogeneity-based Protocols and QoS-based protocols. In [BPSM09], authors analyze the design issues of sensor networks and present a classification and a comparison of these routing protocols. They show that it is no possible to design a routing algorithm which will have the best performances under all scenarios and for all applications.

In [BMJ+98] a useful comparative study about pro-active and reactive routing protocols, where authors have evaluated four ad hoc routing protocols such as DSDV, TORA, DSR and AODV. Many studies and improvements about these routing protocols have been detailed. In [NJ10] and [DP00], authors analyze performance about AODV and DSR routing protocols. In [GS09], authors compare AODV and DSDV with an Optimized-AODV routing protocol, which provides better results than AODV and DSDV. In [MD01], authors present AOMDV, and show that AOMDV always offers better routing performances than AODV in many mobility and traffic conditions. In [Bou04], the authors study and compare

the performance of the following routing protocols AODV, PAODV (Preemptive AODV), CBRP, DSR and DSDV. They show that CBRP has a higher overhead than DSR because of its periodic hello message while AODV's end-to-end packet delay is the shortest when compared to DSR and CBRP, and PAODV has shown some improvements compared to AODV.

In [KKHH06], the authors analyze the IEEE 802.15.4 performance with large-scale WSN applications. They study the CSMA-CA mechanism and the MAC operations in a beacon-enabled cluster-tree structure. They analyze performances in terms of power consumption and goodput of the coordinator. The results are validated using WIreless SEnsor NEtwork Simulator (WISENES). In [KC12] authors deal with two categories of MAC technique: contention based and schedule based. They give a unique performance analysis and comparison of benefits and limitations of each protocol. They show that random topology contention based approach may be helpful and also schedule based approach may be more energy efficient if deployment is not random.

In [BYAH06], authors present X-MAC, a MAC protocol where the main objectives are: energy-efficiency, simple, low-overhead, distributed implementation, low latency for data, high throughput for data and applicability across all types of packeting and bit stream digital radios. They compare X-MAC and LPL. In [SRDV08] authors show that X-MAC provide a power-saving mechanism for routing nodes in Contiki simulator, with this method they show that X-MAC reduces the power consumption for ZigBee routing nodes with up to 90%. Other research studies focus on new methods to transmit data efficiently in order to reduce the energy consumption [YBO09, BOY10] or to guarantee messages arrival [AK05].

[LLW08] proposes a cross-layer handoff ordering scheme. Different quality of service (QoS) requirements of various applications would result in different frame success rate requirements. In order to indicate how critical a handoff request is, both the frame success rate requirement from the application layer and the frame success rate measurement from the MAC layer are taken into consideration in the proposed scheme. The prioritization of handoff requests follows the most-critical-first policy. Performance analysis shows that the proposed scheme effectively reduces the forced termination probabilities.

[ZHL11] investigates energy efficiency of secure communication in wireless sensor networks. It considers link layer security of WSNs which considers cryptographic mechanisms implementation schemes. They evaluate the computational energy efficiency of different symmetric key ciphers and they show that the computational energy cost of block ciphers is less than that of stream ciphers when data are encrypted and transmitted through a noisy channel. They also investigate different factors affecting the communication energy cost of link layer cryptographic schemes (size of payload, the mode of operation applied to a cipher and the quality of the communication channel). They provide a comparison study of many cryptographic schemes in terms of energy consumed by both computation and communication. [BOM10] shows how to increase security in Ad hoc networks by using multipath routing. If one route is damaged or not enough secure, another is chosen. In [GMT12], a smart technique to monitor denial of service (DoS) over WSNs is proposed. It shows how to detect DoS over WSNs using clustering techniques. In [BF10], we have designed an efficient MAC protocol based on reducing useless communications between

nodes.

In all these studies, there is a lack of mixing all layers to consider security performances of any WSN. In our case, we consider all layers and intend to provide mechanisms to tailor with precision the choice of relevant factors in order to reach more secure WSN network.

3 Usual Protocols

This section is dedicated to detail all usual protocols that we use in our comparative scheme.

3.1 IEEE 802.15.4

The IEEE 802.15.4 standard defines the features of the physical and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPAN) [BPC+07]. It supports short-range operation, reasonable battery life, while maintaining a simple and flexible protocol stack.

3.1.1 Physical Layer

The physical layer uses the Direct Sequence Spread Spectrum (DSSS) access mode in three frequency bands 2450 MHz (with 16 channels), 915 MHz (with 10 channels) and 868 MHz (with 1 channel). Besides radio on/off, the physical layer gives some functionality for channel selection, link quality estimation, energy detection measurement and clear channel assessment to assist the channel selection.

3.1.2 MAC layer

The IEEE 802.15.4 MAC layer defines two types of nodes: FFDs (Full Function Devices) equipped with a full set of MAC layer functions and RFDs (Reduced Function Devices) equipped with a reduced set of MAC layer functions and they can communicate only with a single FFD. The standard considers two main topologies a Star topology and a Peer-to-Peer topology. The MAC layer has two modes for medium access: Non beacon mode is purely based on CSMA/CA and beacon enabled mode operates with a Superframe which contains an active and an inactive portion for energy conservation.

The IEEE 802.15.4 standard has two main topologies: **Star topology** based on a master-slave model. The PAN coordinator represents the master, and slaves are other nodes such as FFDs or RFDs. Slaves can only communicate with the PAN coordinator. A **Peer-to-Peer topology** where the PAN coordinator can communicate with other FFDs, and they relay messages to others outside of their radio coverage. This topology forms a multihop network where the PAN coordinator is an administrator.

The MAC layer has two modes for medium access:

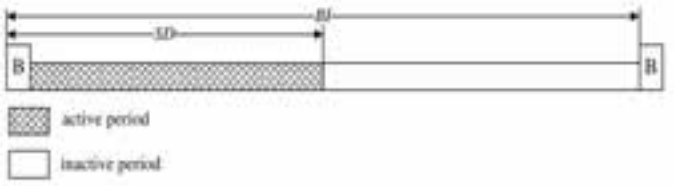


Figure 1: Superframe with SD and BI

1. **Nonbeacon mode:** The medium access is purely based on the CSMA/CA (Carrier Sense Multiple Access) /(Collision Avoidance) mechanism.

2. **Beacon mode:** The PAN coordinator operates with a Superframe. It starts the Superframe with beacon for node synchronization. The Superframe contains an active and an inactive portion where nodes may move to the sleeping status and then save energy. The active portion contains fixed size slots which represent two period: a Contention Access Period (CAP) where nodes use CSMA/CA mechanism, and a Contention Free Period for large packets or time-critical data deliveries assigned by the PAN coordinator. Synchronization and sending (non GTS) operations are executed in the CAP period. Informations for pending delivery are in the beacon frame.

However, the durations of the Superframe are called *beacon interval* (*BI*) ranges from 15ms to 245s. And the durations of an active period are called *SD* (see Figure 1). But the length of *BI* and *SD* can be determined by the parameter *macBeaconOrder* (*BO*) and respectively *SuperFrameOrder* (*SO*). These values can be derived as:

$BI = aBaseSuperframeDuration \times 2^{BO}$

$SD = aBaseSuperframeDuration \times 2^{SO}$

$0 \leq SO \leq BO \leq 14$

where aBaseSuperframeDuration is the minimum duration of a Superframe i.e.

$aBaseSuperframeDuration = aBaseSlotDuration \times aNumSuperframeSlots$

$aBaseSlotDuration = 60 symboles$

$aNumSuperframeSlots = 16$

So in 2400MHz, rate may be $250Kb/s$ or $62.5Ksymb/s$. Thus for $BO = 0$, we have $BI = 960symb$ then $BI = 15.36ms$

The proportion of time where a system can operate represents a duty cycle. For 100% duty cycle, nodes are always on, that represents $BI = SD$ so $BO = SO$. For less than 100%, duty cycle nodes can turn off their transceiver to reduce power consumption. Duty cycle can be calculated as:

$$duty\ cycle = \frac{SD}{BI} = (\frac{1}{2})^{BO-SO}$$

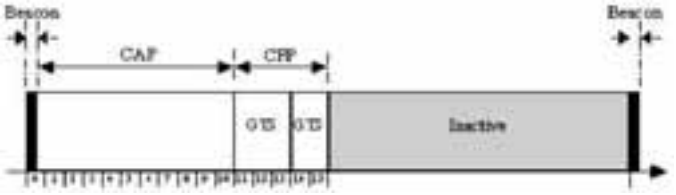


Figure 2: Superframe with active and inactive period

According to [HP07], different pairs values of *BO* and *SO* (in the same duty cycle) will provide various low-power attributes, and will have different impacts on throughput and energy consumption. That means it will definitely influence the network security.

3.2 Routing Layer

Routing protocols are required to ensure multihop communications. Indeed, if the wireless nodes are within the range of each other, a routing protocol is not necessary. But, nodes can move or would communicate with a node out of this range. Then, intermediate nodes are needed to organize the network which takes care of data transmission.

Routing protocols algorithms must choose some criteria to make routing decisions, for instance the number of hops, latency, transmission power, bandwidth, etc. Thus routing protocols are divided into two classes:

- Proactive routing protocols
- Reactive routing protocols

In the following, we present briefly the routing protocol that we used in our study:

3.2.1 AOMDV Protocol

The Ad Hoc On-demand Multipath Distance Vector Routing extends the prominent AODV to discover multiple link-disjoint paths between the source and the destination in every route discovery. It is designed mainly for highly dynamic ad hoc networks where link failures and route breaks occur frequently. The AOMDV protocol has two main features:

- a route update rule to establish and to maintain multiple loop-free paths at each node.
- a distributed protocol to find link-disjoint paths.

Multipath routing protocols, such as AOMDV, try to reduce the high latency of route discovery which can decrease performance.

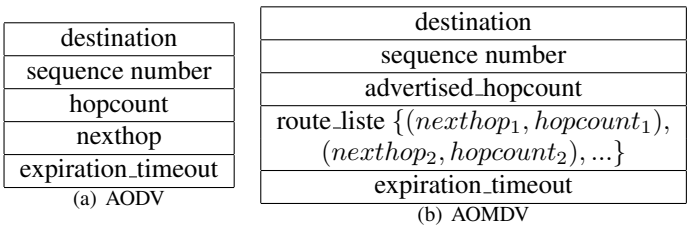


Figure 3: Structure of routing table entries for AODV and AOMDV

Fig. 3 shows the structure of the routing table entries for AODV and AOMDV. In AOMDV $advertised\_hopcount$ replaces $hopcount$ in AODV. A $route\_list$ replaces the $nexthop$, and essentially defines multiple next hops with respective hopcounts. However, all next hops still have the same destination sequence number. The $advertised\_hopcount$ is initialized each time the sequence number is updated.
A node i updates its *advertised_hopcount* for a destination d whenever it sends a route advertisement for d.

3.3 Application Layer

We have classified applications in three types of applications:

1. Regular applications, which characterize those which send low-data with large intervals. In NS-2 we represent this kind of application in a CBR (Constant Bite Rate) stream with 2 seconds intervals. This CBR stream generates UDP traffic according to a deterministic rate. Packets have constant size.

2. High rate applications characterize applications which have large streams. In the NS-2 tool, we use CBR stream with 0.2 seconds to represent the overload of the network.

3. Burst based applications, characterize applications which send data on burst time and sleep during the remaining time. In order to represent this kind of applications in NS-2, we use a Poisson stream with $0.5s$ on period, $2.5s$ for off period and $50kb$ rate. The Poisson stream generates traffic according to an Exponential On/Off distribution. Packets are sent at a fixed rate during a period, and no packet is sent during off periods.

4 Contributions

In this section, we observe the impact of application layer with the different protocols parameters on the network security.

4.1 Working Environment

In the following, we detail the parameters which have been investigated:

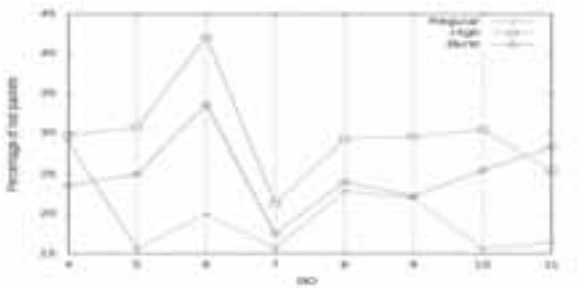
- The network size with 300 nodes. We use a Peer-to-Peer topology with one PAN coordinator.
- The physical layer with all nodes are FFDs using $2400MHz$ band frequency and $250kps$ bandwidth.
- The MAC layer could be in a non-beacon mode and in a beacon-enabled mode.
- For routing, we use AOMDV protocol.

Nodes can reach their neighbors located in the transmission range. We have to follow two steps for simulation. One for synchronization between nodes, and another one for executing the application job. The total duration is different for each simulation because nodes are synchronizing in different duration in beacon-enabled mode. In all simulations, application time is $250\ seconds$. We use a $interval\_sync$ to start nodes at different intervals to reduce the synchronization time, according to BO and SO values, synchronization time varies between 20 and 10000 seconds. For the power consumption, we adopt the data sheet in [SKKW07] where transmission mode is $76.2mW$ and reception mode is $83.1mW$, and nodes start with high energy level ($2.5J$).

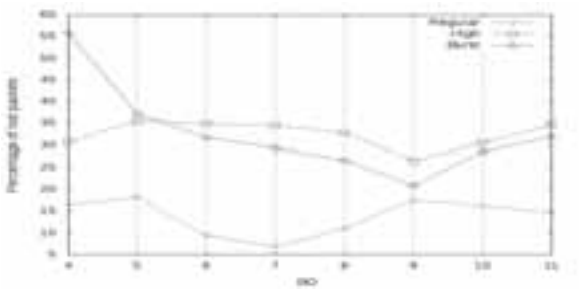
For each application class, we consider some end-device nodes which send messages. The numbers of devices which send data depend on the kind of application load and network load. For example, with 25 nodes, we use 8 nodes to send data to represent regular applications. All messages are sent to the PAN coordinator which is located in the middle of the network.

4.2 Experimental Results

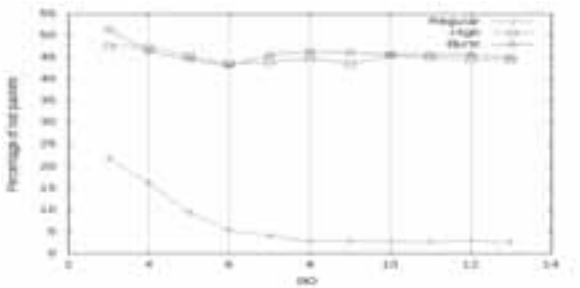
At the end of all simulations, we analyze the rate of lost application packets. We have studied some duty cycle values such as: 6.25%, 12.5%, 25%, 50% and 100% and Non-beacon mode. But we show only 25%, 50% and 100% duty cycle and Non-beacon mode, since under 25%, we have bad results related the complexity of the network to communicate. Indeed, under 25%, the active period is very short between two successive inactive periods. All generated packets will be buffered, and these packets will be transmitted in a burst period during the beginning of the active period, and the collision probability at that time will increase, then the number of received packets decreases. For these values of duty cycle, we use *BO* value between 4 and 11. Values under 4 are not considered in our experiments, because in NS-2, it is harder to simulate scenario with limited bandwidth resources.



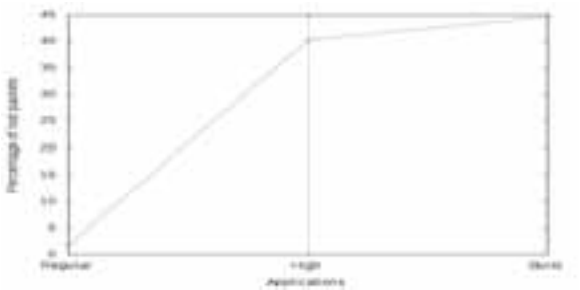
(a) 25% duty cycle



(b) 50% duty cycle



(c) 100% duty cycle



(d) Non Beacon mode

Figure 4: Average rate for all applications with 300 nodes

4.3 Result Analysis

We only comment about 300 nodes results due to the number of graphics. In the first case, we can see that lost packets of burst based and high rate applications is higher than in regular applications in 50%, 100% duty cycle and non-beacon mode. These results show that these applications are more critical than a regular application, which can compromise the security of the network when nodes are mostly on. Indeed, the number of lost packets is higher than the increase of retransmission, collision, and energy consumption. Theses consequences decrease the level of security about the network and may increase attacks of man in the middle.

In the second case, we can see that for all applications the values of MAC layer (BO and SO) impact in a different way. For regular applications, we observe that the best results are obtained when $6 \leq BO \leq 10$ for 100% duty cycle, $6 \leq BO \leq 8$ for 50% duty cycle and when $BO = \{5, 7, 10, 11\}$ for 25% duty cycle. However, the best choice is for non-beacon mode which obtained best results. For high rate applications and burst based applications in 100% duty cycle and non-beacon mode, nodes are always on and lost packets rate is high. Results are similar in these two cases. But when nodes turn off their transmission radio during a period, that reduces lost packets. Indeed for burst based we obtain interesting results when $BO = 9$ for 50% duty cycle and $BO = 7$ for 25% duty cycle. For high rate it is roughly the same results.

So, these results show for a regular application, the security level increases for "on" periods. but in most cases of "off" periods, the security decreases.. Whereas, burst based and high rate applications need off periods to reduce lost packets to improve the level of network security.

5 Conclusion

In this paper, we have shown that the application layer has a real impact on WSN security. We have observed the security of a WSN for many kinds of applications and have measured a metric in terms of packets lost rate.

We have conducted a set of experimentations with 300 nodes executing 3 different types of applications. All simulations have been achieved using the well-know NS-2 simulator. We have presented numerical results of the network performance in each case. We have given what are the best practices for each configuration depending on the application layer type.

We are currently working on extension of this work in order to observe other impacts on WSN security and performances:

- Higher network sizes and much more detailed transmission range values
- Symetric data encryption mechanisms

Our main future work about this study is to justify our results by a theoretical approach

which could be based on stochastic techniques or a qualitative evaluation methods.

References

[AK05] Younis Mohamed Akkaya Kemal. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(5):325–349, 2005.

[AkK04] Jamal N. Al-karaki and Ahmed E. Kamal. Routing Techniques in Wireless Sensor Networks: A Survey. *IEEE Wireless Communications*, 11:6–28, 2004.

[AY05] Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3:325–349, 2005.

[BF10] Thibault Bernard and Hacène Fouchal. Efficient Communications over Wireless Sensor Networks. In *Proceedings of the IEEE Global Communications Conference (Globecom-2010)*, pages 1–5, Miami, USA, December 2010 2010.

[BMJ+98] Josh Broch, David A. Maltz, David B. Johnson, Yih chun Hu, and Jorjeta Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *Mobicom 1998*, pages 85–97, 1998.

[BOM10] J. Ben-Othman and L. Mokdad. Enhancing Data Security in Ad hoc Networks based Multipath Routing. *Journal of Parallel and Distributed Computing (JPDC)*, 70(3):309–316, March 2010.

[Bou04] Azzedine Boukerche. Performance evaluation of routing protocols for ad hoc wireless networks. *Mob. Netw. Appl.*, 9:333–342, August 2004.

[BOY10] J. Ben-Othman and B. Yahya. Energy Ecient and QoS based Routing Protocol for Wireless Sensor Networks. *Journal of Parallel and Distributed Computing (JPDC)*, 70(8):849–857, Aug 2010.

[BPC+07] Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications*, 30(7):1655 – 1695, 2007. Wired/Wireless Internet Communications.

[BPSM09] Rajashree V. Biradar, V.C. Patil, S. R. Sawant, and R. R. Mudholkar. Classification And Comparison Of Routing Protocols In Wireless Sensor Networks. *UbiCC Journal*, 4:704 –711, 2009.

[BYAH06] Michael Buettner, Gary V. Yee, Eric Anderson, and Richard 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.

[CoSKM04] Rachel Cardell-oliver, Keith Smettem, Mark Kranz, and Kevin Mayer. Field Testing a Wireless Sensor Network for Reactive Environmental Monitoring. In *In International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pages 14–17, 2004.

[DP00] Samir R. Das and Charles E. Perkins. Performance comparison of two on-demand routing protocols for ad hoc networks. pages 3–12, 2000.

[GMT12] M. Guechari, L. Mokdad, and S. Tan. Dynamic Solution for Detecting Denial of Service Attacks in Wireless Sensor Networks. In *IEEE International Conference on Communications (ICC'2012)*, June 2012.

[GS09] Dr Aditya Goel and Ajaii Sharma. Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol. *International Journal of Computer Science and Security*, 2009.

[HP07] Yu-Kai Huang and Ai-Chun Pang. A comprehensive study of low-power operation in ieee 802.15.4. In *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, MSWiM '07, pages 405–408, New York, NY, USA, 2007. ACM.

[KC12] Joseph Kabara and Maria Calle. MAC Protocols Used by Wireless Sensor Networks and a General Method of Performance Evaluation, 2012.

[KKHH06] Mikko Kohvakka, Mauri Kuorilehto, Marko Hännikäinen, and Timo D. Hämäläinen. Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications. In *Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks*, PE-WASUN '06, pages 48–57, New York, NY, USA, 2006. ACM.

[LLW08] Po-Chiang Lin, Tsungnan Lin, and Chiapin Wang. Performance analysis of a cross-layer handoff ordering scheme in wireless networks. *IEEE Transactions on Wireless Communications*, pages 5166–5171, 2008.

[MD01] Mahesh K. Marina and Samir R. Das. On-demand Multipath Distance Vector Routing in Ad Hoc Networks. In *in Proceedings of IEEE International Conference on Network Protocols (ICNP*, pages 14–23, 2001.

[NJ10] Amit N.Thakare and Mrs. M. Y. Joshi. Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks. *IJCA Special Issue on MANETs*, pages 211–218, 2010. Published by Foundation of Computer Science.

[SKKW07] D. Schmidt, M. Krämer, T. Kuhn, and N. Wehn. Energy Modelling in Sensor Networks. Bundesrepublik, Deutschland, 2007. Copernicus Publications on behalf of the URSI Landesausschuss.

[SRDV08] Pablo Suarez, Carl-Gustav Renmarker, Adam Dunkels, and Thiemo Voigt. Increasing ZigBee network lifetime with X-MAC. In *Proceedings of the workshop on Real-world wireless sensor networks*, REALWSN '08, pages 26–30, New York, NY, USA, 2008. ACM.

[YBO09] B. Yahya and J. Ben-Othman. Towards a Classication of Energy-Aware MAC protocols for Wireless Sensor Networks. *Wireless Communications and Mobile Computing (WCMC)*, 12(3):1572–1607, Feb 2009.

[ZHL11] Xueying Zhang, Howard M. Heys, and Cheng Li. Energy efficiency of encryption schemes applied to wireless sensor networks. *Security and Communication Networks*, 2011.