On Synthesis of Dependable MAC Protocol for Two Real-world WSN applications

Evgeny Osipov, Laurynas Riliskis
Department of Computer Science and Electrical Engineering
Luleå University of Technology
971 87 Luleå, Sweden

Abstract—Currently, when matter comes to engineer a communication system for a new WSN application with a unique set of dependability requirements, the developer should undergo a lengthy process of analysing the existing solutions in order to select appropriate functionality. In this article we argue that because of variety of wireless sensor network applications there is a clear need for a systematic approach to develop application-tailored communication solutions. The core of this methodology constitute functional components with known reliability and security properties and the rules of combining these components in a communication system. On the example of engineering MAC protocol for two real world applications, we demonstrate a line of dependable reasoning and identify components satisfying the dependability requirements of the applications.

I. INTRODUCTION

Dependability of communications in wireless sensor networks (WSN) is the key property in life-critical applications, e.g. connected to public safety, protection of critical infrastructures and intelligent transportation systems. Dependability of a computing system in general is an integrated property jointly characterized by its attributes: availability, reliability, security and maintainability [1]. The definition of dependability includes *justification* of an ability of the system to perform according to the requirements on the above listed attributes given in the system specification.

The diversity of WSN applications with different performance requirements so far generated several tens of competing communication protocols on MAC, network and transport layers. It is well understood that designing a universal set of protocol suitable for all WSN applications is infeasible. Due to the diversity of WSN applications it might well happen that none of the existing protocols addresses application-specific combination of dependability requirements. In this case the obvious engineering choice would be to select functional

Fig. 1: Systematic engineering of WSNs.

primitives or components (further in this article we will use these terms interchangeably) from different protocols which together would deliver the desired service. Currently, however, there is no systematic methodology for performing this task. Instead, developers should go through a very time consuming manual process of navigating through the vast pool of existing approaches, many of which are specified in form of research publications. The latest requires special expert skills from the developer diverting him from the main task of time efficient engineering.

In this article we argue for a need of creating a systematic framework illustrated in Fig. 1, where the selection of functional components for the particular communication system is intuitive. In order to enable such a framework the existing communication solutions should be analyzed with respect to identification of atomic functional components. These components should further be characterized and classified with respect to

addressing particular dependability properties in different scenarios.

To this end we present the process of identification such components *prior to implementation and testing phases*. In this article we present the protocol synthesis process by navigating through the pool of existing MAC protocols in order to identify components achieving the dependability requirements of two real world applications. As the result we define *Primitive Implicit Consensus Scheduling* component and assess its suitability for target applications using identified properties. As the next step we specify a new MAC protocol which is suggested for implementation and further evaluation in the target applications. The implementation itself and the pre-deployment testing is currently ongoing and will be reported outside the scope for this article.

The paper is organised as follows. In Section II we describe the methodology in general terms. In Section III we describe the applications and state their dependability requirements. In Section IV we present the steps of dependable reasoning which lead to identification of a candidate functional component. In Section V we verify the conformance of its performance to the requirements of the target applications *prior to the actual specification and deployment* and outline the specification of the resulting MAC protocol. The article concluded in Section VI.

II. METHODOLOGY

Fig. 2 describes our methodology for dependable protocol synthesis. A specific WSN application is in the root of the analysis and design chain. The parameters of the particular installation site characterize both the physical environment of the site and the function to be implemented by the sensor and actuator network. We identify the following classes of site parameters: Physical security procedures; Radio properties of the environment; Energy properties; Topography and the Application function. The site parameters are assessed at the first stage of the WSN design process. This is because they play a dual role in the design chain. On the one hand they dictate specific configuration of the communication system along topology, hardware and software axes. On the other hand the site properties are natural enablers of different types of natural and security threats. It is well known that securing an initially insecure communication protocol is a complex task. In many cases this process would lead to modification of the protocol functionality. Therefore, the design of a dependable protocol should start from selection of

Fig. 2: Application specific synthesis of dependable protocols.

communication components, which address the security requirements.

The selected subset of functional protocol components are then analysed with respect to their applicability to the topological specifics of the installation site and information flow of the target application. The result of this analysis is yet narrower subset of functional blocks suitable to the particular WSN application.

The performance of the resulting subset of components is further assessed on satisfaction to the performance requirements of the application. At the end the components showing the best estimated performance are suggested as a candidate protocol for implementation and pre-deployment testing.

III. CONSIDERED WSN APPLICATIONS

The two target applications considered in this article are under development in the scope of EU FP7 project

WSAN4CIP¹ and Swedish national project iRoad². Both applications are currently under the deployment.

¹WSAN4CIP - Wireless Sensor and Actuator networks for Critical Infrastructure Protection. [Online]. Available: <http://www.wsan4cip.eu>.

²iRoad - Intelligent Road. [Online]. Available: <http://www.iroad.se>.

³Geveko ITS. [Online.] Available: <http://www.gevekoits.dk/en/>.

Fig. 3: WSAN for protecting drinking water mains near Frankfurt-Oder in Germany.

Fig. 4: “Running light” ITS application in Luleå, Sweden.

farthest from the roundabout node in the chain of signalling LED-Marks generates a signal (≤ 30 B) to actuate the running light function, while the other nodes in the chain relays the message to the coordinator node.

For the vehicle with the cruise speed of 50 km/h the running light activation distance, to allow comfortable deceleration (-3 m/s^2), is $x_{on} = 30\text{m}$. The detecting node is placed $x_d = 60 \text{ m}$ away from the round about which allows 2 seconds end-to-end propagation delay. In order to account for eventual packet losses and possible retransmission of messages on the multihop path, the system should be dimensioned for $d_{end-to-end} \leq 1$ second.

Placement of the nodes along the road, limits the transmission range. Therefore, the relay nodes are placed on distance 7.5 m from each other, which forms the forwarding chain of 7 hops.

TABLE I: Analysis of security threats in target WSN applications.

Attack type	Risk in drinking water CIP	Risk in running light ITS	Countermeasure, <i>implementation place</i>
Dismounting and stealing nodes (including destruction of nodes)	Medium	High	Periodic network self-diagnostic, reporting the fault in presence of connectivity to the control center, graceful WSN service degradation. <i>Network management component using support from network and MAC layers.</i>
Jamming	High	High	Channel hopping combined with packet fragmentation and redundant encoding [3] are only efficient in the case when the attacker has limited energy resources and does not use full transmission power to perform the attack. <i>MAC layer.</i>
Eavesdropping	Medium	Low	Encryption of the message content (medium risk). <i>Application layer.</i>
Replay of protocol messages	High	High	Authentication <i>Network layer (routing) or MAC layer.</i>
Injection of crafted protocol messages	High	High	Authentication <i>Network layer (routing) or MAC layer.</i>
Remote code injection including installing rogue software on nodes	Medium	Medium	Secure code distribution. <i>Network layer (routing) Application layer, network management component with authentication support from the MAC layer.</i>
Deployment of rogue nodes	High	High	Authentication, secure bootstrapping procedures. <i>Network layer (routing) and MAC layer.</i>

A. Summary of dependability requirement analysis

In this section we present the results of the dependability analysis with respect to security, reliability, availability and maintainability attributes specific for the target applications. We identify the requirements needed to be implemented by the MAC layer. The **availability** requirement for the target applications concerns maximizing the energy efficiency of the communication system for prolonging the time of autonomous network operation. With respect to **maintainability** requirements, the target communication system *should possess self-* properties* excluding as much as possible human involvement in its configuration and management, since the network will be deployed by non-experts in communication systems. Table I presents the results of the **security analysis**. Table II summarizes the identified **reliability** requirements. In summary, it is important to note that with respect to reliability the optimization objective function for the two applications is bounding the packet loss rate and the end-to-end delay. *Due to the specifics of the topologies and the absence of the requirements on in-order data delivery, it is decided to address the reliability requirements inside MAC protocol on a hop-by-hop basis.*

IV. DEPENDABLE REASONING WHEN SELECTING MAC PROTOCOL COMPONENTS FOR TARGET APPLICATIONS

A. Selecting functional components

Amongst the attacks presenting the highest risk for the target applications (see Table I) jamming and deployment of rogue nodes require active involvement of the MAC layer for implementing the countermeasures. The resulting MAC protocol should implement secure bootstrapping and message authentication as means of protecting the network from illegitimate nodes. These procedures, however, do not have specific dependencies on the choice of the medium access technique. Protection against jamming attacks, however, requires a specific support from the MAC and physical layer. If jamming is done with the highest power and the attacker does not care to be detected, the MAC layer does not have any active countermeasures. The MAC layer at nodes located at the edge of the jammed region can notify upper layer protocols about permanent link failures. For the target protocol this implies an inclusion of the link-quality reporting functionality. When dealing with sophisticated jamming attacks, channel hopping, message fragmentation and redundant encoding are possible

TABLE II: Analysis of reliability requirements in target WSN applications.

Application	Drinking water CIP	Running light ITS
Packet loss rate, %	≤ 1	≤ 1
Data delivery order	Not applicable	Not applicable
End-to-end delay, s	≤ 120	≤ 1
Throughput, b/s	≤ 500 (much less than the available end-to-end capacity)	≤ 100 (much less than the available end-to-end capacity)

countermeasures⁴ [3]. Several protocols e.g [6]–[8], and references therein, are multichannel schemes designed specifically for single radio WSN networks.

Firstly, it is important to understand the dependency of security mechanisms on functionality of communication layers. Not all security requirements could be addressed by means of communications. For example, message integrity is achieved by local computation of the message digest and remote verification of its correctness. On the other hand security operations which require an exchange of messages not necessarily implemented on all communication layers. For example, secure key distribution might be implemented by a security management component residing on the network layer and using insecure MAC layer communications. Later on the MAC layer might use the established keys for its own operations, however, the message exchange mechanism of the MAC protocol *does not depend* on the functionality of the security management component.

In the scope of our discussion it is important that multi-channel MAC schemes (further on referred commonly as FDMA schemes) *depend on* slotted transmission in the time domain (further on referred to as TDMA schemes). The performance properties of either separate FDMA and TDMA components or of their combination are determined by the quality of the established access schedules. The scheduling procedures fall into two major classes: centralized and distributed. The centralized approach requires the presence of a dedicated coordinator node. Since in our applications these nodes are not present we did not develop this thread further and concentrated on the analysis of distributed approaches. The distributed approaches could be in their turn divided into *eavesdropping* methods, *cooperative assignment of exclusive schedules* and *implicit consensus*

methods (see [8] for more elaborative description). In the scope of our discussion it is important that the first class requires continuous monitoring (at least during certain time) of activities on available communication channels, this obviously results in energy wastage in the “Listen” state of the transceiver. The cooperative negotiation requires an exchange of candidate schedules in the two-hops neighbourhood, which also consumes energy. The most energy efficient way from the point of view of the communication overhead is suggested in [9]. There, the nodes independently agree on the communication channel number by computing common to all nodes hash function based on their own ID and the IDs of the neighbouring nodes. We choose this approach as a candidate for schedule establishment both in frequency and time domains based on its both lowest overhead and low implementation complexity properties.

B. Definition of a primitive Implicit Consensus Scheduling component and its properties

The original protocol was suggested to minimize the collisions in a two-hop neighbourhood of a node. This involved extra communication overhead (at least two broadcast rounds are required) when resolving the collisions. *Our primary goal*, however is to identify the simplest possible mechanism that achieve defined by the target applications dependability requirements. We therefore define a *primitive implicit consensus scheduling* component as follows.

- **Input:** N - number of resources to distribute, M - number of contenders, Q - number of requested resources;
- **Output:** R - allocated resource id;
- **Parameters:** P_R - probability of selecting resource R ;
- **Default values:** $P_R := 1/N$ (according to property of hash function), $Q := 1$;
- **Operation:** WHILE (M) DO WHILE (Q) DO
 $R := \text{CALL HashComponent}; M--; Q--;$
 $OD; OD;$
- **Default properties:**

⁴There exist several approaches to defend against jamming attacks on single channel MAC protocols, e.g. [4], [5]. It is, however, known that multi-channel MACs make jamming attacks more complex, placing higher requirements on the attacker’s hardware. The degree of criticality of the target applications motivated us to explore the multi-channel approach to medium access as the first option.

- **Reliability: Packet loss** (collision probability for $Q = 1$): $P(R_{\text{collided}}) = 1 - P(R_{\text{not_collided}}) - P(R_{\text{not_empty}}) = 1 - (1 - P_R)^M - M \cdot P_R \cdot (1 - P_R)^{M-1}$;
- **Availability: Energy efficiency** (Probability of empty resource⁵ for $Q = 1$): $P(R_{\text{empty}}) = (1 - P_R)^M$
- **Availability: Energy efficiency** (Communication overhead): 0 (zero)

The function of this component is simply Q executions of another component that performs computation of a hash function for each of M contenders. On top of this component one could add a collision resolution procedure resulting in functionality of the original protocol [9]. In fact, the described component functionally equivalent to the well known Slotted Aloha channel access [10]. The only difference between the primitive Implicit Consensus Scheduling and the Slotted Aloha is the system-enforced assignment of resources. While in Slotted Aloha the slot selection probability is determined by a user configured probability of accessing the channel, here the system allocates time slots or communication channels with a-priori known probability, which is determined by the property of the hash function. As such the analysis of default properties⁶ boils down to the well-known probability analysis of Slotted Aloha.

V. DEPENDABILITY ASSESSMENT FOR THE TARGET APPLICATIONS AND SPECIFICATION OF MAC PROTOCOL

For further discussion we impose the following time structure for protocol operations. The time line is divided into epochs, superframes and subframes as illustrated in Figure 5a. The duration of one epoch is configurable and may span over the duration of one or several superframes. A superframe contains a broadcast subframe during which the transceivers of all nodes are on and a slotted unicast subframe during which only communicating nodes are on. The length of the broadcast subframe is a configurable parameter. In the case of

⁵While in Slotted Aloha this property is considered as the main contributor to protocol's inefficiency in terms of throughput in the saturated case, in our case this property characterizes the energy efficiency of the component, since the transceiver can be switched off during these periods.

⁶In this article we presented only the properties of the Implicit Consensus Scheduling component needed for dependability analysis in the scope of the target applications, identification of other properties is a subject for future investigation. Example of other properties would be execution time for different types of hash functions linked to specific hardware platform, throughput etc..

the drinking water CIP application it has a non-zero length in order to enable slot reservations from multiple concurrent sources. In the case of the running light ITS application the broadcast subframe is not needed since messages from a single data source are transmitted serially. The duration of a unicast slot equals the time to transmit one maximum size data unit plus a short acknowledgement generated by the recipient of the data packet.

1) *Drinking water CIP application:* For the calculation of the superframe size recall that the end-to-end delay in this application should be less than two minutes. According to the specification of the used radio transceiver the maximum communication distance at the lowest rate is around 6 km. It is therefore safe to assume that at 1.8 km distance (the distance between the relay nodes in the application) the expected physical layer transmission rate is 20 kb/s. For further calculations it is also important to note that at maximum we have 4 contenders for the channel at the last three relay nodes before the processing center. This means that in order to compute the transmission schedule in the time and the frequency domains we need to perform 8 modulo operations. According to our measurements it may take up to 400 milliseconds to perform one modulo operation on the target platform. Recall also that each station generates 30 bytes of data per transmission event. Each relay node generates a 4 bytes acknowledgement on each successfully received data packet.

Using the information above the dimensioning of the superframe structure is straightforward. The duration of the broadcast subframe is set to 5 seconds, where the stations may submit transmission request during first 1.5 seconds and the rest of the time is taken for computation of the transmission schedule. In order to ensure the target end-to-end propagation delay the per-hop delay must less than or equal to 12 seconds. This is achieved when the unicast part of the superframe consists of 73 slots (each sufficient to transmit one data packet and receive an acknowledgement) and the data being received during the first possible slot of the one superframe is relayed during the last slot of the subsequent superframe.

Having only four contenders at maximum the collision probability due to operation of MAC protocol is 0.1%. The energy efficiency of the scheme in this case is between 94% (a probability of having empty slots during the active transmission phase) and 98% (the percentage of the sleep time due to duty cycling operation).

2) *Running light ITS application:* In order to assess the suitability of the identified component to the “running

light” ITS application we first compute the minimum number of time slots needed to ensure 1 second end-to-end propagation delay for a given transmission rate at the physical layer. In this application the relay nodes do not inject new traffic into the network, therefore the duration of the broadcast subframe is set to zero. In order to reduce the per-hop delay we specify that each node will reserve Q slots in each superframe for receiving and transmitting messages. The signal message (5 B), therefore, can be sent/relayed during any of the Q slots. Having 7 hops as the maximum distance between the vehicle detecting LED-Mark and the roundabout coordinator the per-hop delay should be less than 142ms. In order to satisfy the target per-hop delay the superframe must consists of $N = 20$ unicast slots assuming the lowest (20 kb/s) transmission rate at the physical layer. With this number of slots each relay node may reserve 2 slots for reception of messages from an upstream node and 2 transmission slots to the downstream node. This makes the number of contending entities for a superframe $M = 4$. With 4 contenders for 20 slots the collision probability in time is 1%, which makes an error free relay probability sufficiently high. With this parametrization of the scheme the energy efficiency is 81%. For higher transmission rates at the physical layer the expected performance of the scheme is even better. For the same number of contending entities (4) the collision probability at 40kb/s is 0.3%, at 100kb/s and higher rates is negligible. The expected energy efficiency at the same time rises to 90% at 40 kb/s, 96% at 100kb/s and 98% at 200kb/s.

A. MAC Protocol

This section presents selected parts of the full specification presented in technical documentation of the corresponding projects. For the sake of further discussion we assume that the nodes share a pre-deployed secret and their clocks are synchronized with one-second precision. This initialization is made off-line before the deployment of nodes at a centralized point. During the protocol’s operations all nodes re-synchronize with substantially higher precision in the bootstrap phase. The protocol is designed for low-power radio transceivers with 16 available radio channels (out of which 8 are orthogonal). Each node is equipped with only one radio interface and is pre-configured with a unique identifier.

1) *Establishment of the channel hopping and time division patterns:* The FDMA and TDMA schedules are constructed in each node independently in probabilistic manner. As a consequence the schedules in

(a) Epochs, superframes, subframes and slots.

(b) MAC operations in time and frequency domains.

Fig. 5: Summary of protocol operations.

one node may partially overlap with other schedules in the two-hop neighbourhood. The schedules’ establishment happen at the beginning of each epoch and is based on computation of a cryptographic hash function $f_1 = Hash(e, ID_s, ID_d) \bmod N$. Note that we use the same hash function both for computation of the transmission schedules and for authenticating data packets as described below. For computation of the transmission schedule we construct a data block which includes the epoch number e , identifiers of the source and destination nodes ID_s and ID_d correspondingly. The resulting hash value maps either into a channel number $CH \in [1, N_{ch}]$ or a slot number $S \in [1, N_{slots}]$, depending on the purpose of its computation, by taking $hash \bmod N$. The broadcast channel is computed similarly using function $R_{BCAST} = Hash(e, 0xFF) \bmod N_{ch}$. In the time domain the broadcast communications always happen in the beginning of the superframe. Fig. 5b presents an

overview of separating the concurrent transmissions both in frequency and the time domains.

2) *Protocol operations*: In order to allow self-configuration of the new nodes during the protocol operation the *bootstrapping phase* repeats with a configurable period of N_{conf} epochs. During the bootstrapping phase, the entire superframe is replaced with the configuration frame, and the application operates in a default safe mode (not specified in this article). The exact specification of the bootstrapping phase procedures falls outside the scope for this article. The two major outcomes of the bootstrap phase are: 1) Synchronization of nodes' clocks with the highest precision, and 2) the securely exchanged current epoch number. As soon as a new node is deployed it turns its transceiver on and tunes it to the bootstrap channel computed as $CH_{BOOT} = Hash(round(t_{cur}, (N_{conf} \cdot t_{epoch})), Secret) \bmod N_{ch}$. There t_{cur} is the current pre-configured time on the node; t_{epoch} is the duration of one epoch, specific for the particular application; and $Secret$ is the shared pre-established secret. The computation of $round(t_{cur}, (N_{conf} \cdot t_{epoch}))$ rounds the current time to the precision of the size of the interval between the subsequent bootstrap phases. The transceiver remains in the ON state until the configuration of the node is complete. Assuming that the new node is deployed at the end of the current bootstrap phase its configuration will end within N_{conf} epochs.

During the *main operation phase* the actual exchange of control and data messages happen. The MAC communications are guided by a forwarding table, with the following format of the entries $\langle \text{Slot number}, \text{Channel number}, \text{Node ID}, \text{Direction} \rangle$. The *direction* field indicates whether the transceiver will transmit or receive data in the particular time slot over a specific channel. The *Node ID* field is used as an index field when looking up the time slot and the transmission channel for locally generated packets. When receiving a packet this field uniquely identifies the source node since the joint probability of collision in time and frequency domains is negligible. This allows not to include the source and destination addresses in the header of each protocol data units. The message authentication procedure described below enables an extra control on the identities of the communicating nodes.

By default we specify that all nodes compute FDMA and TDMA schedules and fill in the forwarding table at the beginning of each epoch. This means that the nodes will be in the active state during all scheduled slots even

if there is no data to transmit (or receive). This operating mode does not require exchange of any messages and minimizes the protocol's reaction time when the data to transmit becomes available. This is the essential property of the protocol for the "running light" ITS application.

In order to improve the energy saving properties (in the "drinking water" CIP application) the developer *may* enable explicit transmission request scheme using non-zero broadcast subframes. In this case the entries in the forwarding table will be computed on demand, leaving the transceiver in the OFF state when there is no packets to transmit or receive.

3) *Message identification and authentication*:: Packet sequence numbering is left to the upper layer services directly adjacent to the MAC protocol. Therefore, this field should be present in the structure of upper layer payload. In the specified MAC protocol all messages are authenticated by means of AEAD security services, i.e. Simultaneous Combined Mode Algorithm, SCMA, [11] running on the ID's of the source and destination nodes and the payload. The SCMA provides the means for both encryption and message authentication. Therefore, we reuse functionality for message authentication to compute hash for establishment of channel-hopping and time division patterns. The message authentication code is truncated to 32 bits, which represents a trade-off between security and byte overhead. The size of the MAC field can of course be increased, however at the cost of increasing the communication overhead.

VI. CONCLUSIONS

In this article we presented an instance of dependable reasoning when constructing a new MAC protocol tailored to specific dependability requirements of two real world applications. The goal of this reasoning was to identify the simplest communication components which satisfy these requirements. So far this reasoning was done manually, through an extensive analysis of existing approaches. This lengthy process requiring special expert skills from a developer of WSN communication systems is, in our opinion, the major stumbling block which prevents from an efficient development of commercial WSN applications. We conjecture that given the vast pool of existing communication protocols on all communication layers, the research effort should be directed on their systematization and identification of suitability of functional components for addressing different patterns of dependability requirements. The reasoning presented in this article is feasible to automate by formally describing the components, their dependency on functionality

of other components and their effect on dependability attributes using known techniques for knowledge management. This automated reasoning will be a part of our future work.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement 224621.

REFERENCES

- [1] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, and M. Vytutas, "Basic concepts and taxonomy of dependable and secure computing," *Dependable and Secure Computing, IEEE Transactions on*, vol. 1, no. 1, pp. 11–33, 2004.
- [2] R. Hostettler, W. Birk, and M. L. Nordenvaad, "Surface mounted vehicle property sensing for cooperative vehicle infrastructure systems," in *16th World Congress and Exhibition on Intelligent Transport Systems and Services*, 2009.
- [3] A. Wood, J. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, 2007, pp. 60–69.
- [4] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," *ACM Trans. Sen. Netw.*, vol. 5, no. 1, pp. 1–38, 2009.
- [5] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, pp. 1119–1133, 2010.
- [6] Y. Kim, H. Shin, and H. Cha, "Y-mac: An energy-efficient multi-channel mac protocol for dense wireless sensor networks," in *IPSN '08: Proceedings of the 7th international conference on Information processing in sensor networks*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 53–63.
- [7] O. D. Incel, L. van Hoesel, P. Jansen, and P. Havinga, "Mc-lmac: A multi-channel mac protocol for wireless sensor networks," *Ad Hoc Networks*, vol. In Press, Uncorrected Proof, pp. –, 2010. [Online]. Available: <http://www.sciencedirect.com/science/article/B7576-507BHS4-1/2/a77e6fa11d311fb6317bd56c1d437bf9>
- [8] G. Zhou, Y. Wu, T. Yan, T. He, C. Huang, J. A. Stankovic, and T. F. Abdelzaher, "A multifrequency mac specially designed for wireless sensor network applications," *ACM Trans. Embed. Comput. Syst.*, vol. 9, no. 4, pp. 1–41, 2010.
- [9] L. Bao and J. J. Garcia-Luna-Aceves, "A new approach to channel access scheduling for ad hoc networks," in *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2001, pp. 210–221.
- [10] L. G. Roberts, "Aloha packet system with and without slots and capture," *SIGCOMM Comput. Commun. Rev.*, vol. 5, no. 2, pp. 28–42, 1975.
- [11] A. Adekunle and S. Woodhead, "An efficient authenticated-encryption with associated-data block cipher mode for wireless sensor networks," in *Wired/Wireless Internet Communications*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2010, vol. 6074, pp. 375–385.