An Overview of Development Problems in WSNs

A. Prayati*, F. Kerasiotis, C. Antonopoulos, S. Giannoulis, T. Stoyanova, G. Papadopoulos
*Research and Innovation Center in Information,Communication, and Knowledge Technologies -ISI, Greece
Department of Electrical & Computer Engineering, University of Patras, Greece
{ prayati, kerasiwtis, cantonop, sgiannoulis, tsstoyanova, papadopoulos}@ece.upatras.gr

Abstract[1] *- As wireless sensor networks (WSNs) are being developed for a wide range of application fields of real-time monitoring and control, a design overview seems important so as to investigate alternative communication aspects while treating the WSN as a whole system. As applications become more demanding the need to consider also deployment constraints and application particularities on top of the commonly used network factors, leads to new integrated design methodologies for addressing all complexity degrees of such systems. In this paper, problems concerning the design aspect of today's WSN applications are presented, which are reasoned to multiple impact factors, to accent design directions and options.*

Keywords-WSN network protocol design, WSN deployment, security, health application scenarios

I. INTRODUCTION

Complex and demanding applications are more and more associated with the application of WSN technology. Starting from the lower level of communication algorithms to the higher application level and its associated functionality requirements and constraints, WSNs are used in a variety of application domains such as environment, health, security, military or urban. Each scenario may require collaborative sensing, communication and computation among multiple sensors that observe moving objects, physical effects and/or environmental events and it is commonly structured in tasks named deployment, application functionality and information exchange.

Meeting the application requirements could greatly depend on optimal and energy-efficient nodes placement [16]. The actual deployment affects network properties such as node density and topology but may also predetermine the data collection and routing mechanisms by providing connectivity degree and sensing coverage. Prudent planning and analysis of different deployment strategies could lead to network efficiency with respect to energy, cost, speed and lifetime.

From the network point of view, there is a variety of protocols trying to enhance the performance of the network. Still no standard one has been established. Metrics used in route selection, such as power awareness and disconnection management are issues that still need a lot of research. However, a good routing strategy requires an efficient underlying Medium Access Protocol (MAC) to support network performance [1]-[6]. Reliable and efficient sharing of the wireless transmission medium, scalability and mobility are critical issues when designing a network protocol, introducing design problems difficult to overcome [6]. Cross-layer optimization intends to improve the existing approach that a layer in isolation does not lead to efficiency, since it ignores critical interactions and correlations that should be exploited [7].

Last but not least security is a challenging demand in complex data-intensive WSN applications. Ensuring data confidentiality, integrity and authentication are some issues in WSN communication security [11][12].

The above issues are discussed in this paper revealing the different aspects of WSN particularities when designing demanding distributed applications. Section 2, the variety of WSN application domains is analyzed. Deployment techniques used in WSN design are presented in Section 3. Section 4 reviews existing network communication approaches with respect to routing and security aspects and identifies the open issues and their interrelations. Finally, conclusions are presented in Section 6.

II. WSN APPLICATIONS OVERVIEW

The WSN application scenarios can be categorized on the basis of their major functional commonalities into four application domains: environment, health, security and other. Each domain with corresponding scenarios is presented in **TABLE 1**. These scenarios may be clustered in terms of their functional characteristics with respect to the

[1] The work reported here was performed as part of the ongoing research Program uSWN FP6-2005-IST-034642 and funded by the European Social Fund (ESF).

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5982
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5982

network demands into four entities, namely *tracking, surveillance, time-critical monitoring of events or people and environmental monitoring.* Analysis of a demanding application scenario abstracts the major tasks that need to be performed for its functionality to be successful. Summarizing and generalizing, a WSN system must provide the following major functional components: data sensing, data processing, continuous monitoring, localization, inter-node communication, interconnection to other infrastructure, additional functionality like event handling or priority scheduling to handle alarms.

TABLE 1. CATEGORIZATION OF APPLICATION SCENARIOS

Environment domain	Health domain	Security domain
Weather forecast	Hospitalized patient monitoring	Indoor / outdoor surveillance
Shipping forecast	Athletes monitoring	
Tropical storm prediction	Disability assistance with implanted sensors	
Earthquake prediction		
Landslide prediction	People rescue in emergency situations / disaster areas	**Other domains**
Volcanic eruption prediction		Structural health monitoring
Fauna monitoring	Bio-surveillance for early disease prediction	Building monitoring and control
Flora / Agriculture farming monitoring		Automotive monitoring
Livestock farm monitoring	Smart home environment	Traffic monitoring
Fish farming monitoring		Industrial process monitoring
Air / water pollution monitoring		Asset and warehouse management

III. ANALYSIS OF DEPLOYMENT PARAMETERS

Sensor node deployment is a very important and critical issue reflecting WSN features as final cost and detection capability. A good sensor network deployment should address a variety of problems such as sensing coverage, network connectivity, sensing and communication ranges, deployment method etc.

Coverage requires that every location in the sensing field is monitored by at least one sensor. Some applications may require greater degrees of coverage [17] [15]. A network has a coverage degree k if every location is within the sensing range of at least k sensors. Networks with a higher coverage degree possess higher sensing accuracy and are more robust to sensor failure [16]. *Connectivity* requires that any active node can communicate with any other active node, possibly using intermediate nodes as relays. To maintain coverage and connectivity the important factor is the *sensing and communication ranges*. In a particular WSN, the relation between sensing range (Rs) and communication range (Rc) of the sensor nodes must be maintained in order to ensure sensing coverage and connectivity [15].

Coming to the WSN *deployment methods*, a deterministic sensor placement may be feasible in accessible environments, with a minimum number of sensor nodes required to cover a given region. On the other hand, random sensor distribution is considered in military applications, in remote areas and hazardous environments.

Another deployment objective is the trade-off between the network lifetime and the number of sensor nodes. One approach for maximizing network lifetime is by reducing the number of working nodes, when the redundancy degree is free enough [18]. However, the deployment with minimal or optimal number of sensor oppose to that idea.

The deployment of networked sensor nodes for certain application scenarios like tracking of moving residents inside a bounded area [19] consider the following points:

- *Terrain specifics:* the area of interest contains obstacles such as trees and buildings.
- *Static nodes assumption:* sensor nodes are assumed to be homogeneous, with fixed and equal sensing range.
- *Moving object characteristics:* the application must be able to handle numerous moving objects.
- *Application requirement:* sensors must be deployed in such a way as to allow for optimal system performance.

The efficiency of alternative deployment schemes is evaluated based on harmonization between application requirements, the routing protocol, and system requirements as lifetime, end-to-end delay, number of nodes, etc.

IV. ANALYSIS OF WSN COMMUNICATION ASPECTS

Three major requirements are the target of every network protocol design: bounded delay, power awareness and low overhead imposed to the network. These three requirements however seem to be contradictory to each other, thus demanding a trade-off in order to enhance one aspect of network performance at the expense of the rest.

A. Network Layer

Routing protocols are basically grouped by the proactive or reactive way they create routes. Both approaches can be applied in WSNs depending on the application data creation pattern, establishing one or multiple routes. In case of multiple routes, the protocol selects one of them based on a link-route metric. Some approaches relate this metric to power [4] and some others to the real-time performance of the network either indirectly by hop-count or directly by selecting the route that formed fastest after the initial route creation request [5]. However, no standard metric exists, since each application imposes different requirements on the routing protocol.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5982
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5982

Hierarchical protocols like Leach [6] try to minimize protocol overhead through localization of data transmission using clusters and cluster heads. Leach includes distributed cluster formation, local processing to reduce global communication, and randomized rotation of the cluster-heads to minimize the possibility of premature energy exhaustion of nodes having this role. Although it is a promising routing protocol, it is not always suitable, since the mechanism to elect cluster-heads imposes overhead to the network and local processing cannot be used in cases of tracking, where data aggregation is needed. The only functionality provided is the grouping of data of several packets to one, in order to minimize the packets sent to the WSN sink. In this way, the possibility of collisions in a contention based MAC is lowered, but larger packets are transmitted degrading network performance.

SPIN [7] is a family of protocols used to efficiently disseminate information in a WSN using data negotiation and resource-adaptive algorithms. Nodes running SPIN assign a high-level name to data, called meta-data, and perform meta-data negotiations before any data transmission, assuring that there is no redundant data sent throughout the network. In addition, SPIN is adapted based on the remaining energy and uses data aggregation, which is dependant on the application requirements and nature. For health data-intense application, data is deterministic in nature, providing data that cannot be aggregated without losing vital information.

PEGASIS [8] is a greedy chain protocol that is promising for data-gathering problems in WSNs. Nodes take turns to transmit the fused data to the base station to balance the energy depletion in the network, whilst preserving its robustness as they die at random locations. Distributing the energy load among the nodes increases the lifetime and quality of the network. PEGASIS uses controlled transmission power in order for nodes to be able to alternatively transmit to the base station but implying long transmission range which most of the times is not the case for WSN platforms. Even more, data fusion is not applicable to health applications that demand localization because of possible loss of vital information, and mobility of nodes is not supported, which is important for other applications too.

Another interesting routing approach is FloodNet Adaptive Routing (FAR) [5], designed for use in the Floodnet project. FAR examines the impact of diverse reporting rates on protocol design. It incorporates mechanisms for interest diffusion, neighbor status maintenance, a routing algorithm that uses the above mechanisms and a mathematic weight formula to select routes to the WSN sink. The mathematic nature of the route selection metric allows for further fine tuning or partial redesign that could fit best in any application. However, studies made on FAR until now, don't take into consideration mobility or dynamic topology, which are basic characteristics for most of today's WSN applications.

B. MAC Layer

Sensor network MAC layer protocol has major problems to face as far as resources waste is concerned [1]-[3]. Identification and handling of collisions impose serious delay penalties and lead to power consumption overhead. In order for a WSN to be configured, a considerable number of packets not carrying user data must be maintained and managed. These are control packets and minimization of their number leads to power conservation and reduction of unnecessary workload. Additionally, a considerable percentage of power consumption of a node is due to overhearing when receiving and processing a packet not intended for the specific node. Finally, idle listening is also a major problem of a MAC protocol.

In order to face these problems, MAC protocols follow certain techniques, with CSMA being quite popular utilized by SMAC [3] and BMAC [1]. CSMA algorithms are decentralized, without any control needed from a single entity, which is more suited to the distributed nature of a WSN. Of course, in this case no bounded delay is guaranteed, but if the network data load is kept within limits, then average delays will be low, even when collisions and hidden-exposed node problems hinder the network performance.

To face the problem of collisions [6], a typical TDMA approach promises deterministic delays at the expense of higher access times and low bandwidth usage in low data traffic state, like in cases of environmental monitoring. However, in health applications with many mobile nodes entering and exiting wireless domains, where vital-signs need to be continuously monitored, this is not possible.

Hybrid techniques, like Z-MAC [5], follow the CSMA technique in low traffic conditions, whilst when traffic increases adapts its functionality to TDMA. Finally CrossMAC [2] follows the cross-layer approach, with control packets containing routing information and facilitating considerably the scheduling of sleep-wake period of each node. There have been many approaches for cross-layer design, among Network, MAC and PHY layers. In [9]-[12] some of the dominant approaches in cross-layer design for WSNs are presented. Using information from MAC and PHY, routing algorithms can enhance their performance while minimizing the overhead imposed by them. Collision detection information from MAC layer can pinpoint possible broken links resulting in links and routes deletion at the Network layer. Transmission power manipulation in the PHY can be used to control connectivity of each node, resulting in avoiding network partitioning while maintaining a good connectivity degree for each node. All the above techniques are open to evaluation as far as WSN application specifics are concerned with cross-layer design being the most promising.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5982
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5982

C. Security

With respect to security provisioning, different techniques exist varying the characteristics and demands of such mechanisms [13][14]. All security mechanisms are based upon cryptographic algorithms, discriminated in two major categories: private (symmetric) and public (asymmetric). Private cryptography is less demanding on computational power, but this imposes considerable control overhead. Public cryptography solves the key number issue, but it affects negatively the node performance and results into larger cipher data, burdening memory usage.

Efficient management of the keys is crucial for security and the respective key management techniques can be indicated by the chosen cryptographic algorithm. Bootstrapping key management is in accordance with the WSN application nature, since each node shares a key only with the base station (BS) and all other keys are derived from this. However, this introduces a single point of failure, which is a very significant disadvantage for WSNs. Key management pre-distribution is very interesting, according to which a subset is chosen from a symmetric-key pool and distributed to each node. In this way, not all nodes can communicate with each other, but by utilizing smart distribution and by exploiting statistical research, full connectivity across the network can be guaranteed. Polynomial-based, Blom's matrix-based, deterministic and pure probabilistic key pre-distribution are modifications of the pre-distribution algorithm, presenting a clear trade-off between efficiency and sensor node needs.

In WSNs, the main trade-off is between security level and energy cost. However for this trade-off, no optimal solution for each application scenario exists. Instead, general guidelines can be given, which combined with the criticality of the application can provide the best solution. Thus, public and private cryptography can be combined by utilizing the former for setting up a private key between the communicating parties, while exploiting the latter characteristics of less computational demands to transfer the actual data. Additionally, indicative analysis of security levels can be achieved by varying major cryptographic algorithm parameters [20].

V. CONCLUSIONS

This paper surveys the multiple WSN dimensions spanning from application level to the lower layers of communication capabilities and constraints or security aspects. A WSN design should address all these aspects for supplying security- and energy-aware communication to meet the application requirements. Deployment should also consider the integration of this mosaic of options into a multi-criterion optimization methodology, necessary to support an optimal WSN operation and performance.

REFERENCES

[1] J. Polastre, J. Hill, D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks", SenSys '04, ACM, November 3-5, 2004, Baltimore Maryland, USA

[2] Ch. Suh, Y-B. Ko, D-M Son, "An Energy Efficient Cross-Layer MAC Protocol for Wireless Sensor Networks" APWeb 2006, LNCS 3842, pp. 410–419, 2006. Springer-Verlag Berlin Heidelberg 2006

[3] A. Warrier, J. Min, I. Rh, "Z-MAC: a Hybrid MAC for Wireless Sensor Networks" SIGCOMM '05 ACM, USA

[4] Y.-S. Chen, S.L.g Lee, T.-H..Lin, "PCAR: A Power-Aware Chessboard-Based Adaptive Routing Protocol for Wireless Sensor Networks," Journal of Internet Technology, Special Issue on "Wireless Ad Hoc Network and Sensor Networks", April 2005.

[5] Jing Zhou, De Roure D. "Designing Energy-Aware Adaptive Routing for Wireless Sensor Networks" , Proc. International Conference on ITS Telecommunications Proceedings, June 2006, pp.680-685

[6] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-Efficient Communication Protocols for Wireless Microsensor Networks", Proc. Hawaaian Int'l Conf. on Systems Science, January 2000.

[7] W. Heinzelman, J. Kulik, H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", Proc. 5th ACM/IEEE Mobicom Conference, Seattle, WA, August 1999.

[8] S. Lindsey and C. S. Raghavendra, .PEGASIS: Power-Ef_cient Gathering in Sensor Information Systems,. in IEEE Aerospace Conference Proceedings, vol.3, 2002, pp.1125-1130.

[9] R. Madan, S. Cui; S. Lall, A. Goldsmith, "Cross-layer design for lifetime maximization in interference-limited wireless sensor networks," in Proc. IEEE INFOCOM '05, vol.3, pp.1964 - 1975, 2005.

[10] S. Cui, R. Madan, A. Goldsmith, S. Lall, "Joint routing, MAC, and link layer optimization in sensor networks with energy constraints," Proc. IEEE ICC '05, vol.2, pp.725-729, 2005

[11] J. P. Walters, Z. Liang, W. Shi, V. Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing, 2006 Auerbach Publications, CRC Press

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", Mobile Computing and Networking 2001 Rome, Italy (ACM)

[13] S. Dong-Mei, HE Bing, "Review of Key Management Mechanisms in Wireless Sensor Networks", Acta Automatica Sinica, Vol. 32, No. 6, November 2006

[14] S. A. Camptepe, B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", Technical Report TR-05-07, March 23, 2005

[15] H. Zhang, J. C. Hou, "Maintaining Sensing Coverage and Connectivity in Large Sensor Networks", Ad Hoc & Sensor Wireless Networks, Vol. 1, pp. 89–124, 2005

[16] M. Cardei, J. Wu, "Energy-efficient coverage problems in wireless ad-hoc sensor networks", Computer Communications 29, 413–420, 2006

[17] Chi-Fu Huang, Yu-Chee Tseng, "The Coverage Problem in a Wireless Sensor Network" WSNA'03, September 19, 2003, San Diego, California, USA.

[18] Y. Gao, K. Wu, F. Li, "Analysis on the Redundancy of Wireless Sensor Networks",WSNA'03, San Diego, USA.

[19] uSWN: Solving Major Problems in MicroSensorial Wireless Networks, FP6-2005-IST-034642

[20] N. R. Potlapally, S. Ravi, A. Ranghunathan, N. K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols", IEEE Transaction on Mobile Computing, Vol. 5, No. 2, February 2006

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5982
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5982