A Framework for Modeling Sensor Networks

Raja Jurdak*, Cristina Videira Lopes*, Pierre Baldi†
School of Information and Computer Science, University of California, Irvine CA 92697
*Center for Pervasive Communications and Computing
†California Institute for Telecommunications and Information Technology Cal-(IT)^2
{rjurdak, lopes, pfbaldi} @ics.uci.edu

***Abstract*— Recent technological advances are likely to increase sensor network development and deployment efforts. The expected growth in sensor network deployment requires efficient sensor network modeling techniques to facilitate initial programming of the sensor nodes and their eventual reprogramming once the network is deployed. The myriad of sensor network application scenarios, physical deployment media, communication technologies, and performance requirements complicates the efficient modeling of sensor networks. This paper proposes a framework for sensor network modeling based on general features identified through a careful analysis of existing sensor networks. This framework facilitates the modeling of new sensor networks by characterizing them according to these general features and providing a set of performance goals. The specification of each network's performance requirements within this framework enables the appropriate selection of communication protocols. The discussion in this paper focuses on sensor network routing protocols, but the approach applies to any kind of communication protocols.**

I. INTRODUCTION

Advances in processor, memory, communication and sensing technology have fueled increased interest in sensor networks. Sensor networks have a wide range of applications, such as tracking and intrusion detection for military purposes, pollutant and habitat monitoring for environmental purposes, and traffic and location systems for civilian use.

In addition to their application diversity, sensor networks may be deployed in a variety of physical media, including air [1], liquids [2, 3], and physical structures [1]. Providing efficient communication in diverse physical media may require alternative technologies to traditional Radio Frequency (RF) communication, such as acoustics [4] for underwater networks [2, 3] or location systems [5], and Ultra Wide Band (UWB) Radio [6, 7] for networks embedded in physical structures.

Many communication protocols have been developed to perform well for specific subsets of sensor network scenarios. Selecting the appropriate protocols for a particular network scenario is a challenge in itself. Additionally, customizing communication protocols is a hard but central programming task to optimize the behavior for each sensor network application.

In the next few years, it is likely that the number of deployed sensor networks will experience an exponential increase. Most of these networks will require application-specific functionality and performance requirements [8]. Modeling sensor network behavior before implementation and deployment is therefore crucial in order to efficiently program the network application. This paper proposes a framework for sensor network modeling based on general features identified through a careful analysis of existing sensor networks. This framework facilitates the modeling of new sensor networks by characterizing them according to these general features and providing a set of performance goals. The specification of each network's performance requirements within this framework enables the appropriate selection, and eventual customization, of communication protocols. The discussion in this paper focuses on sensor network routing protocols, but the approach applies to any class of communication protocols. For each feature, the framework also identifies the key high level network mechanisms that need to be programmed.

The work in [9] provides a survey of current sensor network routing protocols. He et al. [10] have proposed a programmable routing framework for sensor networks that adapts to the requirements of particular sensor network applications and settings. The main distinction of our effort from the work in [10] is that we consider a global and flexible framework for modeling sensor networks rather than a framework that provides generic interfaces for programming a single communication layer. Directed diffusion [11] provides a common query processing framework that interfaces with different routing protocols depending on the network scenario. Our work involves the selection and customization of routing protocols based on the features that impact the sensor network system as a whole.

The rest of this paper is organized as follows. First, we define an ontology of sensor network features. Next, we discuss how the specification of these features is used in modeling a network scenario. We also evaluate the impact that features have on the choice of suitable routing protocols. Finally, we consider a case study to illustrate how communication protocols can be chosen for a particular network scenario.

II. CUSTOM MODELING FRAMEWORK FOR SENSOR NETWORKS

Figure 1 presents our proposed ontology for sensor networks. This ontology integrates sensor network features described in several works [12–15]. Although we realize that the set of features for sensor networks is potentially open-ended, this ontology aims at pinpointing the main high level features that characterize sensor networks mainly for customizing routing behavior.

A. *Topology*

The topology of a sensor network has impacts on several network aspects, including power consumption, battery life and routing mechanisms. The network organization feature includes the physical and logical organization of the network as well as the sensor density. In general, the physical shape of sensor networks aims at efficiently covering the deployment area. Careful power considerations and specialized routing protocols can benefit networks with specific physical organization, such as a grid [16, 17] or a chain [18].

The logical and hierarchical organization of the network also impacts power consumption and protocol choices. Sensor networks can have a distributed organization or a clustered organization, where selected nodes handle data forwarding. Depending on the logical network organization, nodes in the network can use specialized routing protocols for clustered [18–20] or distributed [21] networks to determine with which physical neighbors to communicate.

Sensor density is another sub-feature of the network organization feature. Dense sensor networks benefit from routing protocols that balance the communication load [19, 22] and incorporate sleep modes [16].

The data sinks feature deals with the number of sinks and the relative number of sensor nodes in the network. The availability of multiple sinks could reduce power consumption, since the average distance that the data must travel to reach a sink is reduced. A suitable routing protocol for a network scenario should support the number of sinks and scale of sensor deployment for that scenario.

Mobility of sensors or data sinks causes the internode distances to change and thus complicates network modeling. Modeling mobile sensor networks requires the definition of mobility patterns along with statistical techniques for approximating internode distances. Some routing protocols support mobile sinks [17], while others support only node mobility [23].

Finally, two closely related topology features are location-awareness (i.e. whether or not the sensors are aware of their relative locations) and sensor deployment (i.e. the process by which the sensors are deployed). Location-aware sensors can optimize routes and transmission power based on neighbor location information. In controlled network deployments, it is relatively simple to initially load each sensor with its location information. Ad hoc sensor networks may require the sensors to discover their relative locations in the network. Thus, routing protocols that need location awareness are less favorable for ad hoc sensor networks, unless the underlying communication technology facilitates localization (e.g. UWB or acoustic).

B. *Network Setting*

The network setting has significant implications for the power modeling of the network. Sensor networks will be deployed in various physical media. Because RF waves have unfavorable propagation characteristics in certain media (e.g. water), some sensor networks may use alterative communication technologies, such as acoustics or UWB. The combination of transmission medium and communication technology of a particular network setting determines transmission loss, signal spreading, multi-path propagation, background noise and interference.

The operating environment feature determines whether the network operates in a hostile, adverse, or benign environment. In case of a hostile military environment, the sensor network should include security mechanisms to encrypt or hide the existence of communication. In an adverse environment (e.g. forest fire monitoring), some sensors may be damaged or destroyed, which requires redundant data paths and possibly error detection and correction mechanisms to ensure data delivery.

C. *Sensor Description*

The properties of individual sensors also impact network modeling and protocol choices. In homogeneous networks, all the sensors have the same resources, so spreading the processing and communication loads evenly among the nodes is beneficial. A homogeneous sensor network benefits from protocols that attempt to

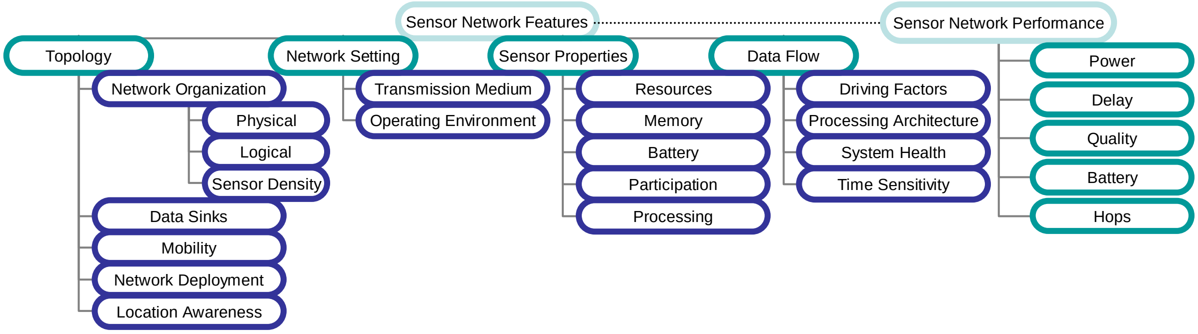

Fig. 1. Proposed Ontology for Sensor Networks

prolong network battery lifetime by rotating the role of cluster heads [18–20] and from protocols that enable sensor nodes to take turns in turning off their transceivers [16]. In heterogeneous sensor networks, a routing protocol should enable nodes with more battery, processing, or memory resources to participate more in network coordination, data aggregation and processing, and data dissemination.

The memory size at each sensor is another important feature, regardless of whether the network is homogenous or heterogeneous. Protocols that use complex state information at each node require more memory at each sensor and thus drive up the cost of the network. Consequently, routing protocols for a sensor network must minimize storage of state information in order to adhere to sensor storage capacity.

The battery is one of the most important resources of the sensors. Depending on the network performance requirements, the choice of routing protocol can trade off battery efficiency for performance. For example, in Two Tier Data Dissemination (TTDD) [17], sensor nodes send their data to dissemination nodes, where the data is stored until a query requests it. These dissemination nodes are kept idly waiting, so that when a query comes in, they can promptly send the data. This protocol significantly reduces the latency of access to sensed data, which may be important for delay-sensitive applications, but involves an overhead in terms of power consumption.

Advances in processor technology have outpaced advances in memory or battery technology. Thus, the processing capacity of a sensor node remains a secondary issue unless the communication protocols require intensive computation at individual nodes.

The participation feature indicates the signal interaction between the sensor and the sensed entity. Sensor nodes can sense data either by sending a signal and awaiting a reply, as in radars, or by sensing signals from the sensed entity. At the other end, the sensed entity can either cooperate to achieve the sensing task by sending a signal to the sensor, such as in location systems, or be passive, such as in intrusion detection systems.

D. Data Flow

Data acquisition and dissemination in sensor networks can be time-driven, event-driven, or demand-driven. Some sensor networks combine more than one of the above data acquisition approaches. In time-driven networks, sensor nodes collect and report data from the physical environment periodically. The periodicity of information flow provides for efficient scheduling of communication and subsequently efficient bandwidth use. Event-driven sensing is useful for sensor networks that perform positioning, intrusion detection, and notification of specific events. Some events, such as forest fires, require immediate data reporting, so low latency is key for event-driven sensing. Finally, demand-driven sensor networks provide a framework for the human operator, or software components within the network, to send SQL-style queries to the sensors. Only the sensors that satisfy the query conditions report their sensed data.

The processing architecture feature describes the nature of data processing and aggregation in the sensor network. In networks with a distributed processing architecture, individual sensors fuse their data with the data of other sensors in order to reduce communication overhead. In networks with a centralized processing architecture, data aggregation and processing occur at the data sink. Networks with a hybrid processing architecture provide a compromise by forming clusters and allowing cluster heads to process data.

The system health feature defines what conditions result in unacceptable network operation, and subsequently provides a semantic definition of network lifetime. In addition, this feature specifies whether network health is monitored continuously or on-demand, and whether it relies on explicit or implicit signals.

The setup feature indicates the data urgency requirement of the network. Most of the current sensor network routing protocols involve an initial transient phase before reaching steady state paths, which is undesirable for urgent situations that require immediate data reporting. Modifying current protocols to include flooding or greedy mechanisms may be more suitable for urgent situations.

III. CASE STUDY

In this section, we consider a coastal underwater sensor network for environmental monitoring [3]. In addition to demonstrating the applicability of our ontology to real world networks, the case study demonstrates how our model determines the suitable routing protocol from network specifications.

This underwater sensor network can monitor environmental indicators, such as the level of pollutants, off the coast of a densely populated area. The concrete features of our underwater network are described in the top part of Table I. Most of them are self-explanatory. Because this network's goal is to monitor both small and large time scale variations in the underwater medium, data acquisition and dissemination is time-driven with a period of several minutes. The network has a distributed processing architecture, where each node fuses incoming data with its own data and forwards the fused data to the next hop. The system is considered healthy as long as data from all active nodes arrives at the base station.

A protocol's suitability for a particular network scenario is determined by matching the protocol's features to the network specifications. However, it is common that only some of a protocol's features fit the network scenario, whereas other features may be unfavorable to the scenario, or unspecified. To choose the best protocol for a network scenario, we propose a matrix structure, as shown in the bottom part of Table I, where the rows correspond to existing protocols. The values in this matrix are derived from our own analysis of the protocols, which has yielded an extensive feature classification [25]. For feature classification purposes, we assign a score of 1, 0 or -1 to denote favorable, neutral or unfavorable behavior. As new protocols appear, we can include them in our analysis.

The entries of each row are summed and the row with the highest aggregate score corresponds to the best protocol. Power Efficient Gathering in Sensor Information Networks (PEGASIS) emerges as the protocol with the most favorable features for this network scenario with a total score of 12.

The only mismatch between PEGASIS and the network scenario is that PEGASIS requires location-awareness, but the network application does not provide any mechanisms for location-awareness. Because the sensors in the underwater network are immobile after their controlled deployment, it is relatively simple to provide each sensor node with the network topology before deployment. Alternatively, PEGASIS can be enhanced with mechanisms of other protocols that do not require location-awareness. For example, Low Energy Adaptive Clustering Hierarchy (LEACH) [20] has several common features with PEGASIS, and it relies on local coordination messages to gather information about the neighboring nodes. A modified version of PEGASIS can use similar messages with an expanded range so that nodes can initially discover their neighbors, and subsequently the network topology.

IV. DISCUSSION AND FUTURE WORK

The ontology in this paper covers high level features that characterize sensor networks mainly for customizing routing behavior. We expect this ontology to expand both in breadth and depth in order to obtain a full cross-layer ontology of sensor networks that accommodates any network scenario. For example, customizing the Medium Access Control (MAC) layer behavior requires the specification of many of the same features in the current ontology, as well as additional features, such as synchronization, transmit power control or hello messages.

Scoring protocols using the protocol selection matrix raises interesting issues regarding protocol suitability. The protocol with highest total score may have several mismatches with the network specifications. To address this issue, the protocol can be modified to incorporate suitable mechanisms of other similar protocols, as we already described in Section III. In some cases, protocol modification may not be possible because the new mechanisms do not fit with the protocol's structure. Instead, a new protocol should be developed specifically for the network scenario. The details for developing a new protocol are beyond the scope of this paper, but the protocol can build on the knowledge base of existing protocols. The modeling framework in this paper thus serves as the basis for efficiently customizing sensor networks for a wide range of applications and deployment areas. We envision that the features identified here will map to standard mechanisms in sensor networks. Programming these mechanisms into components that can be easily connected will enable the composition of new custom protocols that suit each network scenario.

In sum, we have proposed an ontology for sensor networks as the building block for feature based modeling of sensor networks. The framework enables the selection and customization of appropriate communication protocols for specific sensor network scenarios. We expect

Routing Protocol	*Underwater Network Specifications*																	
	Topology							*Network Setting*		*Sensor Description*				*Data Flow*				
	Network Organization			*Data Sinks*	*Mobility*	*Location Aware*	*Network Dep.*	*Trans. Medium*	*Operating Env.*	*Platform Uniformity*	*Memory*	*Battery*	*Partici-pation*	*Dissemi-nation*	*Process. Arch.*	*System Health*	*Setup*	
	Physical	*Logical*	*Density*															
	Chain	Clustered	Low	Single Sink	Not Mobile	No	Controlled	Shallow Seawater	Benign	Homo-geneous	Limited State	Off-the-Shelf	Passive Uncoor.	Time driven	Dist.	Implicit	Not Urgent	Total Score
LEACH [20]	-1	1	0	1	1	1	1	0	1	1	0	1	0	1	1	1	1	11
PEGASIS [18]	1	1	0	1	1	-1	1	0	1	1	1	1	0	1	1	1	1	12
GAF [16]	-1	1	0	1	1	-1	1	0	1	1	0	1	0	-1	0	1	1	6
SPIN [23]	0	-1	0	1	1	1	1	0	1	-1	1	1	0	-1	1	1	1	7
RR [22]	0	-1	-1	1	1	1	1	0	1	0	-1	0	0	-1	1	1	1	4
MCF [21]	0	-1	0	1	1	1	0	0	1	1	1	1	0	1	-1	1	1	8
TEEN [19]	0	1	-1	1	1	1	1	0	1	1	1	-1	0	-1	1	1	1	8
TTDD	-1	1	0	-1	0	-1	1	0	1	1	-1	-1	0	-1	0	1	1	0

TABLE I

PROTOCOL SELECTION MATRIX

that developing this framework into a software modeling tool will provide for more efficient modeling of sensor networks.

REFERENCES

[1] N. Xu. A Survey on Sensor Network Applications. available: http://enl.usc.edu/ ningxu/papers/survey.pdf.

[2] X. Yang et al. Design of a Wireless Sensor Network for Long-term, In-Situ Monitoring of an Aqueous Environment. *Sensors*, 2:455–472, 2002.

[3] R. Jurdak, C. V. Lopes and P. Baldi. Battery Lifetime Estimation and Optimization for Underwater Sensor Networks. *Sensor Network Operations*, IEEE Press, September 2004.

[4] C. Lopes and P. Aguiar. Aerial Acoustic Communications. In Proc. *IEEE (WASPPA'2001)*, 2001.

[5] R. Jurdak, C. V. Lopes, and P. Baldi. An Acoustic Identification Scheme for Location Systems. In Proc. *IEEE/ACS ICPS'04*, 2004.

[6] M. Z. Win and R. Scholtz . "Impulse Radio: How it Works," *IEEE Communications Letters*, 2:1, 1998.

[7] IEEE 802.15.4 WG. Low-Rate Wireless Personal Area Networks. Draft Standard.

[8] A. Woo, S. Madden, and R. Govindan. Networking Support for Query Processing in Sensor Networks. *Comm. of the ACM*, 47(6):47–52, 2004.

[9] Q. Jiang and D. Manivannan. Routing Protocols for Sensor Networks. In Proc. *IEEE (CCNC)*, 2004.

[10] Y. He et al. A Programmable Routing Framework for Autonomic Sensor Networks. In Proc. *The Autonomic Computing Workshop IEEE AMS '03*, 2003.

[11] C. Intanagonwiwat et al. Directed Diffusion for Wireless Sensor Networking. *IEEE/ACM Trans. on Networking*, 11:2-16, 2003.

[12] C. Chong and S. Kumar. Sensor Networks: Evolution, Opportunities, and Challenges. In Proc. IEEE, 91(8):1247–1256, 2003.

[13] D. Estrin et al. Instrumenting the World with Wireless Sensor Networks. In Proc. *ICASSP*, 2001.

[14] J. Zhu, S. Papavassiliou, and S. Xu. Modeling and Analyzing the Dynamics of Mobile Wireless Sensor Networking Infrastrucures. In Proc. *IEEE VTC*, 2002.

[15] R. Szewczyk et al. Habitat Monitoring with Sensor Networks. Comm. of the ACM, 47(6):34-40, 2004.

[16] Y. Xu, J. Heidemann, and D. Estrin. Geography informed Energy Conservation for Ad Hoc Routing. In Proc. *Mobicom*, 2001.

[17] F. Ye et al. A two-tier data dissemination model for large-scale wireless sensor networks. In Proc. *Mobicom*, 2002.

[18] S. Lindsey and C. Raghavendra. PEGASIS: Power-Efficient Gathering in Sensor Information Systems. In Proc. *ICC*, 2001.

[19] A. Manjeshwar and D. Agrawal. TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. In Proc. *IPDPS*, 2001.

[20] W. Heinzelmann, A. Chandrakasan, and H. Balakrishnan. Energy-Efficient Communication Protocol for Wireless Microsensor Networks. In Proc. *HICSS*, 2000.

[21] F. Ye et al. A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks. In Proc. ICCCN, 2001.

[22] D. Braginsky and D. Estrin. Rumor Routing Algorithm for Sensor Networks. In Proc. *1st ACM Int. Workshop on Wireless Sensor Nets and Applications*, 2002.

[23] W. Heinzelmann, J. Kulik, and H. Balakrishnan. Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks. In Proc. *Mobicom*, 1999.

[24] R. J. Urick. *Principles of Underwater Sound*. Mcgraw-Hill, 1983.

[25] Routing Protocol Feature Classification. available: http://www.ics.uci.edu/∼rjurdak/Features.xls.