A Pattern for Sensor Network Architectures

Mihaela Cardei, Eduardo B. Fernandez, Anupama Sahu, and Ionut Cardei
Department of Computer and Electrical Engineering and Computer Science
Florida Atlantic University, Boca Raton, FL 33431, USA
mihaela@cse.fau.edu, ed@cse.fau.edu, asahu1@fau.edu, icardei@cse.fau.edu

Abstract—Wireless sensor networks provide rapid, untethered access to information and computing, eliminating the barriers of distance, time, and location for many applications in national security, surveillance, healthcare, area/target monitoring, and many more. In this paper we use patterns to present an abstract view of the structure and general architecture of a wireless sensor network. Using a sensor network pattern makes the design of such a network simpler and more convenient, and can facilitate their integration with the rest of the IT system when applicable. The security aspects of a wireless sensor network are also addressed.

Keywords: Wireless sensor networks, architecture, patterns, security.

I. INTRODUCTION

A wireless sensor network (WSN) is a deployment of a large number of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information, used to make global decisions about a physical environment. Research on sensor networks was originally motivated by military applications, such as acoustic surveillance and target detection. However WSNs have many other applications such as [Cho03]:

- Infrastructure security: instrument critical buildings and facilities such as power plants with networks of acoustic, video, and other sensors in order to provide early detection of any potential threat.
- Environmental and habitat monitoring: environmental sensors can be used to study vegetation response to climatic changes and diseases, while acoustic and imaging sensors can be used to identify, track, and measure the population of birds and other species.
- Traffic monitoring: sensors are deployed in intersections for traffic monitoring and control, and to control traffic lights. Another concept is deploying sensors along the highways and attached to each vehicle. Such a network can be used to avoid traffic jams and plan alternative routes.

The main components of a sensor node and a pattern of a sensor node are presented in [Sah10]. A WSN consists of large number of sensors and one or more sinks where data is collected [Aky02]. Each sensor node is able to sense the physical environment, process data locally, and participates in data forwarding to a sink, from where data are retrieved by users.

WSNs are application specific, thus sensors nodes are equipped with sensors accordingly. Some applications (e.g. building monitoring) require a smaller number of sensors that can be placed individually. Others (e.g. surveillance of a battlefield) require a large number of sensors (e.g. thousands or even millions) that will be deployed ad hoc. Using a larger number of sensors increases network robustness and fault-tolerance. The IrisNet (Internet-scale Resource-Intensive

Sensor Network Services) project [Gib03] at Intel Research is envisioning a worldwide sensor web of millions of widely distributed, heterogeneous sensors.

Sensor nodes have limited resources: they have finite battery resources, low CPU speed , little memory, and small transmission range. For example, the Crossbow MICAz mote [Cro10] operates on the 2.4GHz ISM band, uses two AA batteries, and has an ATmega 128L processor at 8 MHz, 4 K bytes RAM, and a transmission range up to 30 m (indoor) /100 m (outdoor).

In this paper we present an architecture that describes the generic structure of most sensor networks. To make this description more useful, we present it as a pattern. A pattern is a solution to a recurrent problem in a given context. Our final result can be considered a reference architecture or composite pattern for a wireless sensor network. A reference architecture provides a generic solution for a family of systems intended for a particular domain [Tay10], while a composite pattern is a composition of simpler patterns [Rie05]. We also consider how to add security to this pattern, although we do not provide a complete solution for that extension.

Usually, sensor networks are not designed in isolation but are part of a larger system, e.g. a medical system for patient monitoring. Information systems are often designed using UML and patterns. Having a similar model for sensor networks can facilitate their integration with the rest of the IT system. Another advantage is that by having appropriate patterns to describe sensor networks makes the design of these networks simpler and more convenient, especially for inexperienced designers. If we need to comply with regulations, the policies defined by the regulations can be described as patterns and then combined with the functional patterns. Combining the functional aspects of the networks with security patterns along the development lifecycle can produce a secure version of the network. Simulation is used extensively in networks in order to evaluate performance and traffic properties; patterns can be used to define in a generic way different topologies for simulation as well as to assign parameters to the network nodes.

Our contribution is not a new architecture but an abstraction of any sensor network architecture that describes its important architectural properties and can be the basis to apply security, reliability, or performance optimizations. In this paper we develop a pattern for sensor network architectures, following the POSA template [Bus96]. Section II presents the Sensor Network Architecture pattern and Section III concludes the paper.

II. THE SENSOR NETWORK ARCHITECTURE PATTERN

A. Intent

Many applications use sensors to monitor various physical parameters. This pattern describes architectures used by wireless sensor networks, which allow sensor nodes to transmit their collected data to users and users to send commands to the sensor nodes.

B. Example

We are fighting an enemy in a large area. We have put sensor nodes for detecting the presence of enemies. Having the troops patrol the field periodically may be dangerous and sometimes

infeasible. Sensors can detect the presence of enemies but their collected information must be sent to us or they are not useful.

C. Context

Physical environments need to be often monitored for the presence of living beings, for recording some physical attributes, or for detecting specific conditions. Areas to be monitored may be larger or smaller, depending on the application. These environments could be inside a building or could be external areas. The covered areas may be inaccessible at times. Some applications may also require monitoring of environments that can be accessible by adversaries as well (e.g. monitoring of a battlefield).

D. Problem

Sensors are being used by many applications to monitor various parameters. For applications requiring a large number of sensor nodes or a dangerous environment, it is infeasible to have the user physically located in the communication range of each sensor node for communicating with it. How can we provide a system that allows users to interact with sensors (e.g. gather sensor data) remotely ?

The possible solution is constrained by the following forces:

- The data collected by sensors must be sent to a sink or to a set of sinks to be processed or integrated with a larger system. Without reaching the sink, this data collection is wasted.
- Most nodes have limited resources and may not be able to reach the sinks directly.
- For management or security purposes we may need to logically divide the network into groups which are independent in some sense.
- Some applications may have specific optimization objectives. For example, consider an application where sensors are deployed for environmental monitoring. It may be infeasible or impossible to recharge or change the sensors batteries. Such applications require that the sensor nodes lifetime to be prolonged as much as possible with regard to the target application.
- Various applications use different number and types of nodes. The system must be able to accommodate different types of nodes.
- Only authorized users can access data and the data transmission must be secure.
- The cost of the system must be relatively small, otherwise the system may become too expensive to implement and operate.

E. Solution

Sensor nodes can be organized in a wireless sensor network (WSN). The main functions of a sensor node are data sensing, local data processing, and data forwarding. Figure 1 shows the general architecture of a WSN.

WSNs can be classified as homogeneous and heterogeneous. Homogeneous WSNs contain only one type of devices, the sensor nodes. On the other hand, heterogeneous WSNs contain devices of different capabilities. Typical sensor nodes are resource-constrained nodes and another type, called supernodes here, are more resource rich than the standard sensor nodes; they can have, for example, more energy resources, larger transmission range, higher data rate, etc. These

supernodes are also be found in the literature under the name of gateways, masters, microservers, shepherds, and macronodes.

In addition, a sensor network can be logically organized in clusters. Each cluster has a cluster head which has a certain role within the cluster (e.g. aggregates data received from the nodes in the cluster).

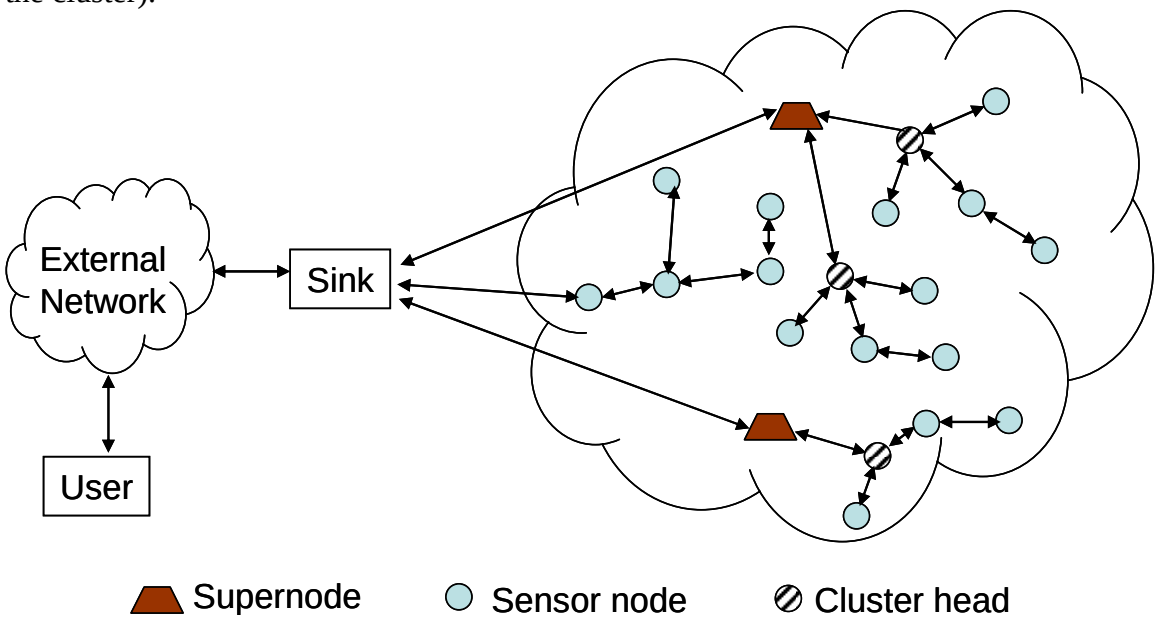

Figure 1. Wireless Sensor Networks

Structure

Figure 2 shows a **Network** composed of several **Nodes** and one or more **Sinks**. Networks can be connected to other networks. Nodes may be connected to other nodes and all are connected to the sinks. A sink can be fixed or mobile (e.g. smartphone). Nodes can be Sensor nodes (regular data-collection nodes) or Supernodes (that collect data from other nodes). Nodes can be organized into clusters, and each cluster has a Cluster Head that controls the data collection within the cluster.

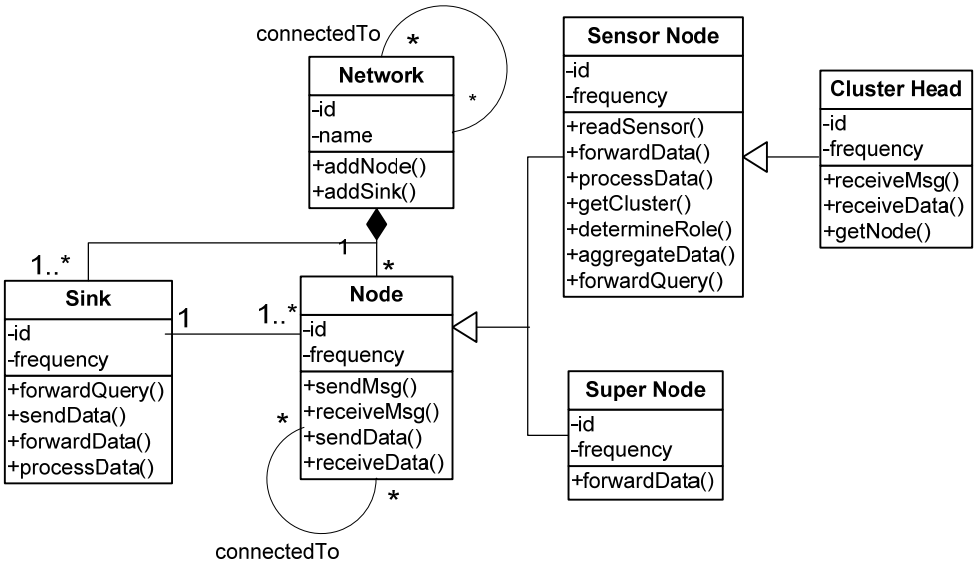

Figure 2. Class Diagram of a Wireless Sensor Network

Dynamics

Several use cases are possible with this network architecture, which include Initialize Network, Reconfigure Network, Query Request, Data Gathering, Create Cluster, and Forward Data. Figure 3 shows a sequence diagram for the use case Data Gathering.

UC: Data Gathering
Precondition: Sensor nodes store routing tables and execute routing protocols in order to route data from one node to another. The WSN is distributed and consists of sensor nodes, cluster heads, super nodes, and a sink. All sensor nodes in a cluster are within direct communication range with the cluster head.

- Sensor nodes collect data and forward the data to the nearest cluster head.
- Cluster heads aggregate the data received from sensor nodes and forward them to the nearest super node.
- Supernodes forward the data to the sink.
- The user can access the data from the sink (the sink forwards the data to the user or the user requests data from the sink)

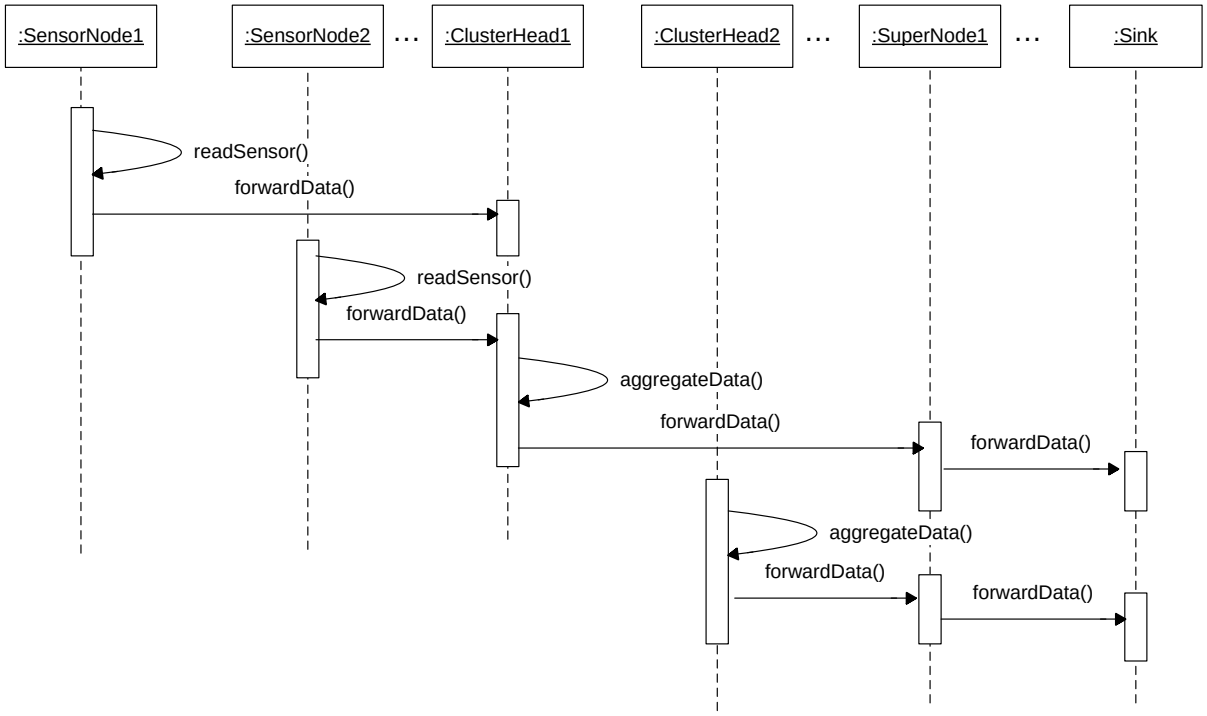

Figure 3. Sequence Diagram for Use Case “Data Gathering”

Figure 4 describes the sequence diagram for the use case “Query Request”

UC: Query request
Precondition: The sink is interested in retrieving some data from sensor nodes, so it requests the sensor nodes to collect the required data and send it to the sink. Since a WSN is distributed and not all the sensor nodes are within direct communication with the sink, the nodes forward the query request hop by hop. The nodes return the collected data in the same way. In other scenarios, data can be returned on different paths as well.

- The sink sends a query request to the network
- The first sensor node that receives the request stores it in the memory, and then forwards the request to its next hop, decision based on the routing protocol .
- The first node then starts collecting the data as per the request and then processes the collected data.
- Each node receiving the request behaves in a similar manner.
- The farthest node sends its processed data to the node from which it received the query. This node then aggregates the received data with its own data and sends it to previous hop.
- This process continues until the sensed data reaches back the sink.

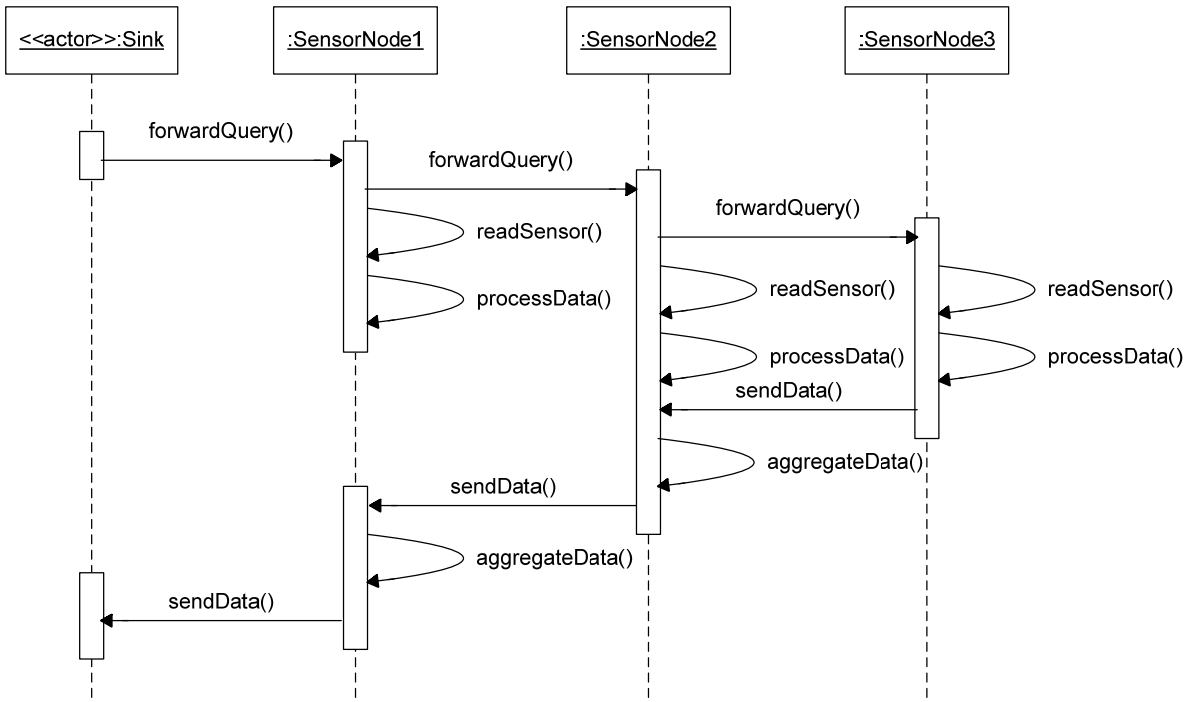

Figure 4. Sequence Diagram for Use Case “Query Request”

Figure 5 describes the sequence diagram for the use case “Forward Data”.

UC: Forward data
Precondition: The sink is interested in retrieving data from a particular area of the WSN, so it directs the sensor nodes to collect data from that region. Since the WSN is distributed, some nodes behave as cluster heads and forward data from their cluster to the nearest super node which in turn forwards data to the sink.

- Sensor node 1 forwards the data to sensor node 2.
- Sensor node 2 aggregates the received data with its own data and forwards it to sensor node 3.
- Sensor node 3 forwards the data according to a routing protocol to the next sensor node, and so on, until the data reaches a sensor node within communication range with the cluster head. That sensor node forwards the data to the cluster head.
- The cluster head aggregates all the data from its cluster and forwards it to the supernode.
- If the supernode is within direct communication range with the sink, then it forwards the data directly to the sink. Otherwise, data is transmitted using supernode-to-supernode communication until it reaches the sink. Note that supernodes are resource rich nodes, therefore it is more efficient to transmit data using supernodes than using sensor nodes which are resource constraint.

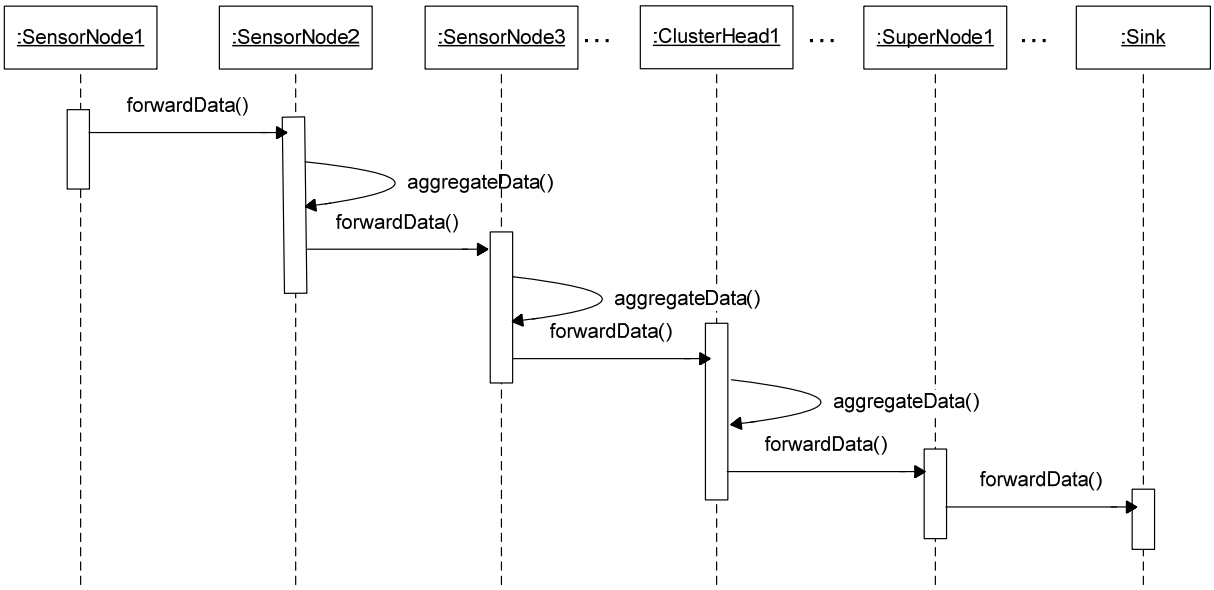

Figure 5. Sequence Diagram for Use Case Forward Data

F. Implementation

A group of sensor nodes can be used to build a WSN that can be implemented inside buildings or in external environments.

- Sensor nodes can be programmed using a general purpose programming language such as C or a specialized language such as NesC or LabVIEW. Crossbow MICA motes [Cro10] uses TinyOS and are programmed using NesC [Gay03].
- After the sensors are programmed, they are deployed inside buildings or external environments. Once they are deployed, they initialize and perform operations such as neighbor discovery, data sensing, local data processing, and data transmission [Cho03]. Sensed data can be transmitted periodically or event based.
- A wireless communication protocol is used to specify message relaying between nodes. For example, IEEE 802.15.4/Zigbee standard [IEE03] specifies the Physical and MAC layer of the wireless communication.
- A WSN implementation must also specify a routing protocol. Operations such as query request (from a sink) and data gathering (to one or more sinks) have to be supported. One such mechanism is Directed Diffusion [Int00].
- In addition, other mechanism for security, data aggregation, quality of service, etc. can be implemented.

G. Example Resolved

The isolated sensor nodes deployed in the battlefield have been organized into a network. Now the information of all active sensors can reach long distances with the help of other sensors that can relay data. If a sensor is destroyed or runs out of power its function can be replaced by a

nearby sensor. Using multiple hop communication, sensor data can reach the sink which can be remotely located. From the sink, the data is accessed by users.

H. Variants: Secure Sensor Network Architecture

We can analyze threats and superimpose security patterns to control these threats [Fer06]. We do not enumerate here all possible threats for sensor networks but only show the approach. We indicate where the patterns for the relevant mechanisms can be found. Some specific threats and their possible defenses include:

- A network or node impersonating another node. This threat can be prevented by mutual authentication. The Authenticator pattern [Sch06] can be used in the Network class of Figure 2, indicating that communications between networks require authentication to prevent impostors.
- Illegal access to the data in a sensor node. This threat requires the use of some type of access control, e.g. Access Matrix or Role-Based Access Control [Sch06].
- Message interception. The objective can be illegal reading or writing of a message in transit. This attack can be controlled through cryptography.
- Repudiation. Can be controlled using digital signatures.
- Some other attacks such as node capture, physical tampering, denial of service attacks, and traffic analysis are discussed in [Per04].

The activities in each use case of the network must be analyzed to enumerate threats systematically. The threats are then handled by selecting an appropriate security pattern that can stop or mitigate them. Each pattern has a context and this must be considered before applying the pattern.

I. Known Uses

We will illustrate examples of WSNs that contain no clusters/supernodes, examples that contain clusters, and examples that use supernodes.

The next two examples show uses of WSNs that contain no clusters and no supernodes. In August 2005, scientists deployed a WSN on Volcan Reventador in Northern Ecuador [Wer06]. The array consisted of 16 nodes, each equipped with a microphone and seismometer, deployed over 3 km. Over three weeks, the network captured 230 volcanic events. Another example is the deployment of a WSN for structural health monitoring of the Golden Gate Bridge [Kim07]. The network had 64 nodes and measured ambient structural vibrations at 1kHz rate and it was deployed and tested on the 4200ft (1280m) long main span and the south tower of the bridge.

There are many articles that explore a clustered WSN architecture. In [Hei00], authors proposed LEACH, a clustered WSN where sensor nodes alternate to take the role of cluster heads. A cluster head has the role to collect data from sensors in its cluster, process it locally, and then transmit it to the sink. Another clustered WSN is proposed in [You04]. Here cluster heads are chosen among the sensor nodes, based on the residual energy, proximity to its children, and node degree.

Various research works refer to resource-rich *supernodes* with different names: *gateways* by work [Jol03], *masters* by the Tenet architecture [Gna06], *microservers* by work [Gre06], *shepherds* by work [Sta05], *macronodes* by work [Wan03], and *supernodes* by work [Awa06]. In all these works, supernodes refer to nodes that have more capabilities than a sensor node, such as memory, computational capability, transmission range, etc. Such nodes can perform local data processing, can run various security protocols, data aggregation, and can help in forwarding the data to the sink.

J. Consequences

The pattern has the following **benefits:**

- If some nodes cannot reach the sink directly, other nodes can help them by relaying their data.
- Clusters allow the management or securing of sections of the network by defining a cluster head that can control different functions.
- Specialized, resource-rich nodes (called supernodes in this paper) can be inserted in the network. For example they can have more processing power to do filtering, to keep logs, or to store authentication information, or they can have a larger communication range. Using supernodes, the WSN could achieve better performance such as longer network lifetime, better latency, and reliability [Sta05].
- UML provides a standard and unified description of network topology and functions. If the other parts of the system are also described in UML their model integration becomes simpler. Also the integration of the lower architectural levels can be simpler since the classes define the interface contracts to be used by the rest of the system. For example, patterns such as Wrapper Façade allow the designer to encapsulate lower-level functions [Sch00]. Associations such as aggregation or relationship allow any type of network combinations. The model is also suitable for simulations.
- Depending on the application requirements, a WSN can have more or less number of sensor nodes and it can be homogeneous or heterogeneous. Architectures using clusters or supernodes are scalable with the number of sensor nodes. The number of supernodes deployed will depend on the network size.
- Depending on the application requirements, the WSN can be extended with security mechanisms.
- Organizing the sensors in a WSN provides a cost efficient solution, since the same sensor nodes are used both in data sensing and data relaying.

The **liabilities** of the pattern include:

- This structure may be too complex for simple applications.
- This pattern does not include any security mechanisms.

K. Related Patterns

- A pattern for a sensor node is presented in [Sah10]. This describes the structure of each network node.

- The structure of the network which describes the network as composed of nodes and sinks, follows the Whole-Part pattern [Bus96].
- Patterns addressing various security aspects are described in [Sch06]. They can be used to apply security to this pattern.

III. CONCLUSIONS

The Sensor Network Architectures pattern abstracts the architectural aspects of a wireless sensor network. Object diagrams can describe specific networks and can be used to study for example, forensic aspects.

We are now writing a Secure Sensor Network Architecture pattern following the ideas of Section H.

ACKNOWLEDGMENTS

We thank our shepherd Eric Platon, for his careful comments that helped improve the paper.

REFERENCES

[Aky02] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A Survey on Sensor Networks, *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-116, Aug. 2002.

[All06] G. Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. B. Johnson, J. Lees, and M. Welsh, Deploying a Wireless Sensor Network on an Active Volcano, *IEEE Internet Computing*, pp. 18-25, Mar.- Apr. 2006.

[Awa06] W. Awada and M. Cardei, Energy-Efficient Data Gathering in Heterogeneous Wireless Sensor Networks, *IEEE Intl. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob'06)*, Jun. 2006.

[Bus96] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerland, and M. Stal, *Pattern-oriented Software Architecture*, Wiley, 1996.

[Cho03] C. -Y. Chong and S.P. Kumar, Sensor networks: Evolution, Opportunities, and Challenges, *Proceedings of the IEEE*, Vol. 91, No. 8, pp. 1247-1256, Aug. 2003.

[Cro10] Crossbow Technology, http://www.xbow.com, last accessed on May 28, 2010.

[Gay03] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler. The *nesC* language: A holistic approach to networked embedded systems, *Proc. of the ACM SIGPLAN 2003 conference on Programming language design and implementation* (PLDI '03).

[Fer06] E. B. Fernandez, M.M. Larrondo-Petrie, T. Sorgente, and M. VanHilst, "A methodology to develop secure systems using patterns", Chapter 5 in "*Integrating security and software engineering: Advances and future vision",* H. Mouratidis and P. Giorgini (Eds.), IDEA Press, 2006, 107-126.

[Gib03] P. B. Gibbons, B. Karp, Y. Ke, S. Nath, and S. Seshan, IrisNet: An Architecture for a Worldwide Sensor Web, *IEEE Pervasive Computing*, pp. 22-33, Oct.-Dec. 2003.

[Gna06] O. Gnawali, B. Greenstein, K.-Y. Jang, A. Joki, J. Paek, M. Vieira, D. Estrin, R. Govindan, and E. Kohler, The Tenet Architecture for Tiered Sensor Networks, *ACM SenSys*, Nov. 1-3, 2006.

[Gre06] T. Schoellhammer, B. Greenstein, D. Estrin, Hyper: A Routing Protocol to Support Mobile Users of Sensor Networks, in *CENS Technical Report #63,* Jan. 2006.

[Hef09] M. Hefeeda and M. Bagheri, Forest Fire Modeling and Early Detection using Wireless Sensor Networks, *Ad Hoc and Sensor Wireless Networks*, Vol. 7, No. 3-4, pp.169-224, Apr. 2009.

[Hei00] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-efficient Communication Protocols for Wireless Microsensor Networks, *Hawaaian Int'l Conf. on Systems Science (HICS'00)*, Jan. 2000.

[IEE03] IEEE 802.15.4 specification, May 2003, *http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf*.

[Int00] C. Intanagonwiwat, R. Govindan, and D. Estrin, Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks, *Proc. ACM MobiCom'00*, pp. 56-67, 2000.

[Jol03] G. Jolly, M. C. Kuscu, P. Kokate, and M. Younis, A Low-Energy Key Management Protocol for Wireless Sensor Networks, *IEEE International Symposium on Computers and Communications (ISCC '03)*, 2003.

[Kar05] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*, Willey 2005.

[Kim07] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks, *Procs. of the 6th International Conference on Information Processing in Sensor Networks (IPSN'07)*, pp. 254-263, Apr. 2007.

[Luk07] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, MiniSec: A Secure Sensor Network Communication Architecture, *Sixth International Conference on Information Processing in Sensor Networks (IPSN 2007),* Apr. 2007.

[Mai02] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, Wireless sensor networks for habitat monitoring, *Proc. Of the 1st ACM International Workshop on Wireless Sensor Networks and Application*, 2002.

[Per04] A. Perrig, D. Wagner, and J. Stankovic, Security in Wireless Sensor Networks, *Communications of the ACM*, Vol. 47, No. 6, pp. 53-57, Jun. 2004.

[Rie97] Dirk Riehle., "Composite design patterns", in *Proceedings of the 1997 Conference on Object-Oriented Programming Systems, Languages, and Applications* (OOPSLA '97). ACM Press, 1997. 218-228.

[Sah10] A. Sahu, E. B. Fernandez, M. Cardei, and M. VanHilst, A Pattern for a Sensor Node, *Procs. 17th Conference on Pattern Languages of Programs (PLoP'10)*, Oct. 2010.

[Sch00] D. Schmidt, M. Stal, H. Rohnert, and F. Buschmann, *Pattern-oriented software* architecture, vol. 2 , *Patterns for concurrent and networked objects*, J. Wiley & Sons, 2000.

[Sch06] M. Schumacher, E. B.Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, Wiley 2006.

[Sta05] T. Stathopoulos, L. Girod, J. Heidemann, and D. Estrin, Mote Herding for Tiered Wireless Sensor Networks, in *CENS Technical Report* #58, Dec. 2005

[Tay10] R.N. Taylor, N. Medvidovic, and E.M. Dushofy, *Software architecture: Foundations, theory, and practice*, Wiley 2010.

[Wal06] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, Wireless Sensor Network Security: A Survey, Chapter 17 in *Security in Distributed, Grid, and Pervasive Computing*, Yang Xiao (Ed.), Auerbach Publications, CRC Press, 2006.

[Wan03] H. Wang, D. Estrin, L. Girod, Preprocessing in a Tiered Sensor Network for Habitat Monitoring, *EURASIP Journal on Applied Signal Processing*, Vol. 4, pp. 392-401, 2003.

[Wir] Wireless Sensor Networks Security Website: *http://www.wsnsecurity.info*.

[You04] O. Younis and S. Fahmy, HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks, *IEEE Transactions on Mobile Computing*, Vol. 3, No. 4, pp. 366-379, Oct-Dec 2004.