Assuring System Reliability in Wireless Sensor Networks Via Verification and Validation

Zhun Shen
Department of Computer Science and Software Engineering
Xi'an Jiaotong-Liverpool University, China
Email: Zhun.Shen08@student.xjtlu.edu.cn

Ka Lok Man
Xi'an Jiaotong-Liverpool University, China
Myongji University, South Korea
Baltic Institute of Advanced Technology, Lithuania
Email: ka.man@xjtlu.edu.cn

Chi-Un Lei
The University of Hong Kong, Hong Kong
Email: culei@eee.hku.hk

Eng Gee Lim
Xi'an Jiaotong-Liverpool University, China
Email: enggee.lim@xjtlu.edu.cn

Joongho Choi
University of Seoul, South Korea
Email: jchoi@uos.ac.kr

Abstract—**Wireless sensor networks (WSNs) have been widely used for monitoring applications. However, due to the rigorous deployment environment, reliable operation of WSNs is difficult to guarantee. Thus, the assurance of WSN reliability should be concerned in order to measure physical quantities correctly and effectively, as well as to maximize the lifetime of the system. In this paper, concerns of WSN reliability and assurance measures have been discussed via a systematic reliability checking flow. Furthermore, issues about reliability assurance and certification are also raised for the future development of WSNs.**

Keywords-wireless sensor network; simulation; reliability

I. Introduction

Wireless sensor network (WSN) is one of the promising examples of pervasive computing [1]. Because WSNs are flexible to deploy in various situations, they have been widely used in different areas [2, 3], such as environmental monitoring [4], infrastructure monitoring, manufacturing monitoring, health care monitoring [5, 6] and home monitoring [7].

However, there are critical issues that deteriorate the deployment and the operation of WSN systems. For example, WSNs that are deployed in distant and isolated areas are usually difficult (sometimes even not practical) to repair and replace. Moreover, different WSN hardware systems often have different time scales, precisions and specifications. In addition, process variations and power densities in circuit systems as well as electromagnetic interference and other external disturbances from the surrounding obstruct the system operation. Meanwhile, conventional electrical components are often not designed for the extreme conditions associated with WSN applications. As a result, these issues threaten the reliability of WSNs, and may cause wrong measurement and even system failures in mission critical applications. Therefore, a detailed reliability study is needed before and after the deployment of the system.

This research is partially funded by the Xi'an Jiaotong-Liverpool University Research Development Fund, under grants 2010-26 and 10-02-03; and the Xi'an Jiaotong-Liverpool University Educational Development Foundation, under grant 201211.

Different approaches have been proposed to assure the reliability of WSN systems, such that WSN systems measure physical quantities correctly and effectively, operate correctly in veritable situations, and have a maximum lifetime of the system. These reliability studies cover topics from hardware to software, from devices to systems, from basic networks to large-scale sensor networks, and from ways of predicting behavior and effectiveness of systems to techniques for making systems better sustained.

In this paper, different issues related to system reliability of WSNs are discussed for obtaining a reliable WSN system. We first describe WSN reliability issues systematically in Section II. Then, the process of validation and verification is discussed in Section III. Finally, modeling and simulation is presented in Section IV and Section V, respectively.

II. Reliability Issues In Wireless Sensor Networks

From the functional perspective, WSNs are continuous and autonomous measurement systems that monitor space, objects and interactions of objects within the system and the space. In other words, WSNs can determine the intensity of some phenomena across the region, track the location and motion of an object in the region. From the hardware perspective, a WSN contains numerous distributed sensor node devices, a wireless data communication network and a monitoring base station. A sensor node is automatically operated by a micro-controller and supported by a power source (e.g. batteries and/or energy harvesting systems). Sensor nodes also contain sensors that examine physical quantities (e.g. temperature, sound, vibration and pollutants). Furthermore, there is a wireless transceiver in each sensor node to transmit measured quantities.

Meanwhile, reliability can be defined as "the duration or probability of failure-free performance under stated conditions" [8, 9]. A typical hazard function is shown in Fig. 1. In WSN applications, the system should be able to provide long-term monitoring services continuously and readily without any catastrophic consequences on users and environment. In addition, physical quantities measured by the system should be reliable and identical, and should not be disclosed without authorization. Moreover, a reliable WSN system should be convenient to modify and repair.

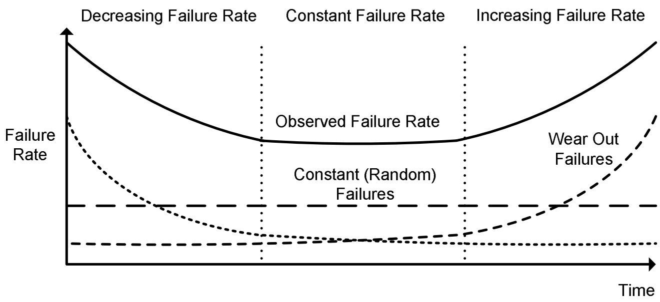

Figure 1. A typical bathtub-shaped hazard function.

WSN systems are time-dependent and application-aware systems that operate in a distributed environments and subject of a variety of physical, chemical and environmental damage. Thus, the function of deployed WSN system may be affected by noise and extreme dynamics of the environment. Furthermore, limitation of resource and power also expose the system to operation failure. These requirements can be accomplished through analysis and test of high level system architecture, hardware system and software system, in the design stage as well as the operational stage. Some typical faults that appear in WSNs [10] are shown in Table I.

TABLE I. TYPICAL FAULTS IN WSNS

Table	Table Column Head
Channel fault	The transmitted signal is disturbed by the physical environment (e.g. fading phenomena, interference and noise)
Replication fault	Multiple copies of measured signal are produced during the process of computation and communication
Preterm-it fault	A copy of measured signal is lost during the process of computation and communication
Struck at fault	No change in gradient of signals over a long period of time
Spike fault	A sudden and large change in gradient of signals over a short period of time

The reliability analyses rely on a risk management strategy based on identification, modeling, analysis and control/elimination of hazards throughout the life-cycle. A typical reliability assurance flow is shown in Fig. 2. Characteristics of objects can be identified by specifications of products or measured responses in the deployment site (**Response Characterization**). Models can then be constructed from given characteristics (**Modeling**). The model is used to determine whether the design meets a defined set of requirements, specifications, and regulations (**Verification**). If the system passes the verification test, the system is then tested to determine whether the design meets the needs of the user (**Validation**). The validation process can be done by statistical simulation with models and/or on-site pilot deployment with prototype sensor nodes. If the system passes the validation test (i.e., evidences have been provided that the design is valid through pre-defined standards), the WSN system is said to have met the standard (**Assurance and Certification**), and can be deployed.

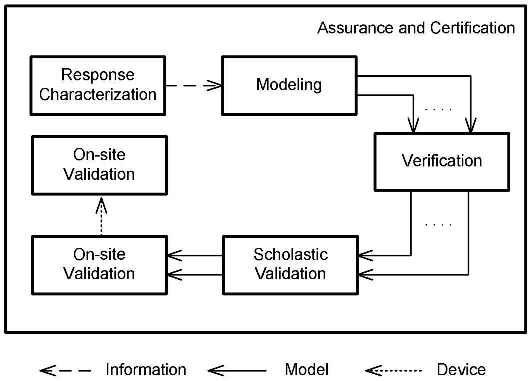

Figure 2. A Typical Reliability Checking Flow in WSNs.

III. VALIDATION AND VERIFICATION

A. Formal verification and probabilistic verification

Formal method is the most common technique used in WSN verification [11, 12]. Formal method provides theoretical guarantees on properties of the system, discovers hidden errors and analyzes the system design at different system development stages. In a formal verification process, requirements, regulations and specifications of the WSN system can be identified and formalized as properties in a property specification language. Meanwhile, the architecture of the system can be specified in a simulation language. Then, a model checker is used to verify each model property repeatedly. If the property is violated, then the output is tracked, such that the system model or the property can be refined. The checking process continues until all properties have been checked. Meanwhile, probabilistic verification can determine the probability that the proposed design can stay within operating parameters for all possible inputs. However, an adequate coverage of operating conditions, scenarios and system inputs is required, such that the reliability of the WSN system can be proofed statistically/probabilistically.

B. On-site validation

Although *a priori* verification approaches have been widely adopted, different studies showed that many on-site deployments did not match the expected performance in the design stage. Statistical validation has been proposed to determine the percentage of usage scenarios with a satisfactory user performance. Meanwhile, different on-site testing and validation approaches, such as deployment support networks and debugging tools, have been proposed.

1) Real time validation through an interface device: This approach [13] can detect early time problems that happen in sensor node devices (e.g. radio link, hardware, sensors and battery) and wireless network systems (e.g. connection to network of each node and base station and timesynchronization). Furthermore, a light and low-power interface device has been developed for ease of monitoring.

2) Self test case analysis: These procedures can be used to validate the performance of the system, individual system components [14] and high-level functionality of the application [15]. In the procedure, there will be a run-time verification, an application-level operation assurance and a correctness demonstration. However, validation methodologies have not been well-developed yet; therefore a comprehensive validation process is one of the bottlenecks in WSN design. Meanwhile, validation cannot be formalized because the validation process relates a system design to intent. For example, it is difficult to characterize complex physical environments such as human body. In particular, the formalization involves on-site experimentation, and thus limitations are exposed in the formalization process. For example, there are not sufficient test cases and test devices for a comprehensive analysis; the environment of the simulation is different from the real deployment due to the change of environment and equipments.

IV. MODELING

Models describe the Input-Output (I/O) characteristics of the physical environment (e.g. heat, pressure and temperature), computing units (hardware specifications) and interactions (e.g. heat transfer and air transfer). Given a set of object behaviors and model requirements, the model can be constructed through first principles (white-box approach) or system identifications (black-box approach). The model is then used for analysis and simulations, and verification/validation of systems. Thus, constructed models should be accurate, physically consistent, robust and of low complexity for simulation. In general, models can be classified according to their application domain, model structure, construction approach and metrics [16]. In this paper, three layers of models are discussed in the following subsections. A detailed discussion about models for other layers (i.e. link layer, network/transport layer, operating system layer and application layer) is shown in [16].

A. Hardware models

Sensor nodes measure and transmit signals through hardware; therefore performance of hardware is significantly related to the system performance. Most existing system-level models are used to estimate latency associated with sensing and data transmission [17]. Furthermore, these models are also used to estimate energy that dissipated in the operation period (including sensing and data transmission) and the idle period. Meanwhile, there are low-level circuit models for sensors, signal conditioning circuitries, microcontrollers, oscillators and analog/digital interferences. The complexity of the circuit model mainly depends on the accuracy, sampling spectrum, range of sensing and density of sensor nodes.

Because WSNs are often used for outdoor measurements, energy characterization of hardware devices becomes important and critical. Energy in the system is mainly consumed by both data transmission and hardware operation. Therefore, energy models for processing circuits have been developed for the estimation of energy estimation. Meanwhile, models for packaging [18, 19], batteries, power management circuits and energy harvesting/scavenging circuits have been proposed. For example, a model of battery management systems for outdoor deployment has been proposed for accurate energy estimation [20]. Furthermore, mechanisms for charging, self-discharging and self-recovery have also been modeled. These models have been used to predict the remaining energy for operation, and configure the system in order to prolong the operation time.

B. Radio signal propagation models

Radio signal propagation models also play an important role in modeling WSNs [21], because these models can be used to compute the communication range of nodes and implement an effective strategy for the deployment of WSNs. These models mainly characterize the attenuation of transmitted signals over space and time, in particular, the communication media (e.g. wireless spectrum and modulation techniques), as well as interference, fading and other disturbance from other sensor nodes and the ambient. Full models can be constructed through first principles (e.g. Maxwell equations). However, for an effective simulation process, full models are usually replaced by scholastic models to reduce computation load. Furthermore, specific signal propagation models have been proposed for node localizations and mobilized nodes.

C. Environment models

WSNs are used to monitor status and rate of change of the environment. Therefore, environments should be modeled for a realistic (thus accurate) simulation. The environment models includes the physical monitoring environment (e.g. light, sound and hazard indicators), as well as environments that affect the sensing and signal transmission.

V. SIMULATION

Simulation is the process of validating the design by imitating its behavior for a given set of inputs. Since on-site pilot validation is costly, time consuming and sometimes not practical, simulation becomes a necessary step to design WSNs [22, 23]. In general, designers can choose their simulation tools according to their required accuracy, scale of condition, simulation speed and functionality.

Simulation can be performed via generic computation engines (e.g. Matlab) or specific simulators. There are mainly two kinds of simulation approaches with tradeoff between precisions, scalability and computation speed: discrete-event simulation and instruction-level simulation. In discrete-event simulations, users are required to use high-level descriptions to construct a network of nodes. The simulation tool can analyze the communication traffic among the process. This simulation approach is efficient; however, it cannot simulate the low level performance of WSNs. In instruction-level simulations, the complete microcontroller programs/instructions instead of WSN models are run in simulators. These simulators can provide low-level information such as signals, timing and power dissipation in devices and communication channels. However, they often have a high computation complexity.

Although various simulation tools have been proposed, there are still some open research problems in the field of simulations, e.g. the co-simulation of diverse physical and hardware systems, as well as the co-simulation of systems expressed at different levels of abstractions and/or with different time scales, precisions and specifications.

VI. ASSURANCE AND CERTIFICATON

Assurance is the process of providing evidence that a design is valid through pre-defined standards. Meanwhile, certification is the process of obtaining approval for a design by a certificate authority. These practices have been widely adopted in the design of systems for mission critical applications [24] and concurrent systems, such as medical devices, avionic devices and military devices [25]. This quality assurance process has been recently introduced to WSN.

In software systems, most safety assurance standards are process-based, in particular, they list pre-determined activities that happen in a safe system. Through a clear specification, faults can be tracked and removed. Meanwhile, evidence-based standards, another kind of assurance standards, require developers to assure the safety through structured reasoning, with provision of a safety cases. These assurance approaches can be adopted for the reliability assurance of embedded systems and complex electronics, such as microprocessors and programmable logic devices. More discussions about the assurance of complex electronics are shown in [26]. Furthermore, peripheral tools, such as quality assurance checklists and tracing tools for hardware description languages can facilitate the quality assurance processes and help to define, compare and improve the design for a better reliability.

VII. CONCLUSION

Reliability issues in WSN become one of the bottlenecks in the WSN deployment. In this paper, different issues and measures related to the reliability of WSN systems have been discussed for the development of a reliable WSN system. In summary, in order to further improve the reliability of WSNs, advanced simulation methodologies should be developed, and certification process should be introduced to WSNs.

REFERENCES

[1] Frank Adelstein, Sandeep K. S. Gupta, Golden G. Richard III, and Loren Schwiebert, "Fundamentals of Mobile and Pervasive Computing," The McGraw-Hill companies, 2005

[2] Th. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," IEEE International Symposium on Intelligent Control, pp. 719-724, June 2005.

[3] Ning Xu, "A Survey of Sensor Network Applications," IEEE Communications Magazine, 2002

[4] R Jaichandran, and A. Anthony Irudhayaraj, "Specification verification and validation of wireless sensor network model for environment monitoring," Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief, pp.437-440, 2011

[5] Victor Shnayder, Borrong, Chen, Konrad Lorincz, Thaddeus R. F. FulfordJones, and Matt Welsh, "Sensor Networks for Medical Care," in Harvard University Technical Report, 2005

[6] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai, and S. K. S. Gupta, "Ayushman: a wireless sensor network based health monitoring infrastructure and testbed," DCOSS'05 Proceedings of the First IEEE international conference on Distributed Computing in Sensor Systems, pp. 406-407, 2005

[7] Helal S, Mann W, El-Zabadani H, King J, Kaddoura Y, and Jansen E, "The Gator Tech Smart House: a programmable pervasive space," Computer, Vol. 38, pp. 50-60, March 2005

[8] KK Aggarwal, "Reliability engineering," Kluwer Academic Publishers, 1993

[9] R.J. O'Dowd, "A Survey of Electronics Obsolescence and Reliability," Air Operations Division, DSTO Defence Science and Technology Organization, July 2010

[10] K. Ni, N. Ramanathan, M. N.l H. Chehade, L. Balzano, S. Nari, S.Zahedi, E. Kohler, G. Pottie, M. Hansen, and M. Srivastava, "Sensor network data fault types," ACM Transactions on Sensor Networks, vol.5, May 2009

[11] H. Turner, and Jules White, "Verification and Validation of Smartphone Sensor Networks," MOBILWARE 2011, pp.233-247, Feb 2011

[12] J. S. Dong, J. Sun, J. Sun, K. Taguchi and X. Zhang, "Specifying and Verifying Sensor Networks: An Experiment of Formal Methods," Lecture Notes in Computer Science, vol. 5256/2008, pp. 318-337, 2008

[13] H. Liu, H. Liu, and J. Stankovic, "SeeDTV: deployment-time validation for wireless sensor networks," Proceedings of ACM 4th workshop on Embedded networked sensors, pp. 23-27, 2007

[14] Chieh-Yih Wan, Shane B. Eisenman, and Andrew T. Campbell, "CODA: congestion detection and avoidance in sensor networks," Proceedings of ACM Intl. Conf. on Embedded networked sensor syst., pp. 266-279, 2003

[15] Yafeng Wu, Krasimira Kapitanova, Jingyuan Li, John A. Stankovic, Sang H. Son, and Kamin Whitehouse, "Run time assurance of application-level requirements in wireless sensor networks," IPSN '10 Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, pp. 197-208, 2010

[16] Phillip Stanley-Marbell, Twan Basten, Jérôme Rousselot, Ramon Serna Oliver, Holger Karl, Marc Geilen, Rob Hoes, Gerhard Fohler, and Jean-Dominique Decotignie, "System Models in Wireless Sensor Networks," Rapport Technique, May 2008

[17] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," ACM Mobile Computing and Communications Review, vol. 6, pp. 28-36, April 2002

[18] Chi-Un Lei, Hing-Kit Kwan, Yansong Liu, and Ngai Wong, "Efficient linear macromodeling via least-squares response approximation," IEEE International Symposium on Circuits and Systems, 2008. 2008, pp. 2993-2996, May 2008

[19] Chi-Un Lei, Yuanzhe Wang, Quan Chen, and Ngai Wong, "On Vector Fitting Methods in Signal/Power Integrity Applications," Proceedings of IAENG International MultiConference of Engineers and Computer Science, pp.1407–1412, March 2010

[20] C. Chen, K.L. Man, T.O. Ting, Chi-Un Lei, T. Krilavičius, T.T. Jeong, J.K. Seon, S.-U. Guan, and P. W.H. Wong, "Design and Realization of a Smart Battery Management System," Proc. of IAENG Intl. MultiConference of Engineers and Computer Science, pp. 1173-1176, March 2012

[21] Mukhopadhyay S, Schurgers C, Panigrahi D, and Dey S, "Model-Based Techniques for Data Reliability in Wireless Sensor Networks," IEEE Transactions on Mobile Computing, vol. 8, pp. 528-543, April 2009

[22] E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, P. Pavón-Mariño, and J. García-Haro, "Simulation Tools for Wireless Sensor Networks," Summer Simulation Multiconference, 2005

[23] Imran, M., Said, A.M., and Hasbullah, H., "A Survey of Simulators, Emulators and Testbeds for Wireless Sensor Networks," International Symposium in Information Technology, vol. 2, pp. 897-902, June 2010

[24] Andrew J. Kornecki, and Janusz Zalewski, "Hardware certification for real-time safety-critical systems: State of the art," Annual Reviews in Control, vol.34, pp. 163-174, April 2010

[25] Miner, P.S., Torres, W., Malekpour, M., and Carreno, V.A., "A case-study application of RTCA DO-254: design assurance guidance for airborne electronic hardware," Digital Avionics Systems Conference, 2000. Proceedings. DASC. The 19th, vol. 1, pp. 1A1/1 - 1A1/8, 2000

[26] Richard A. Plastow, "Fillig the Assurance Gap on Complex Electronics," Science Applications International Corporation, Cleveland, Ohio, March 14-16, 2007