GE-International Journal of Engineering Research
Vol. 5, Issue 1, January 2017 Impact Factor- 5.613
ISSN(O): 2321-1717, ISSN(P): 2394-420X
© Associated Asia Research Foundation (AARF) Publication
Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

A PROBLEMS AND ISSUES IN WIRELESS SENSORS NETWORKS EXISTING IN EFFICIENCY CRITERIA

[1] Kamaljeet Singh
Assistant Professor

[2] Umesh Sehgal
Research Scholar

ABSTRACT

Network security refers to the protection of information and resources from loss, corruption, and improper use. With WLANs, security vulnerabilities fall within the following areas .

- *Passive monitoring*
- *Unauthorized access*
- *Denial-of-service attacks*

The limited capabilities of a sensor node, such as restricted processing capabilities and a limited amount of energy, have an impact on all the parameters of a WSN. Taking into account the energy characteristics of transmitters in sensor nodes and their high susceptibility to interference, the quality of communication between sensor nodes can vary significantly with time. That is why the information loss and substantial delays often occur in WSNs. And their impact is closely associated with the size of a WSN.

Keywords: WSNs, Task Monitoring.

1. Introduction

Also, in order to save energy, sensor nodes in most WSNs are in the low power state (the sleep mode) most of the time, as mentioned in Section 2.2. At the low power state, all the components of a sensor node except the microcontroller are switched off and inside the microcontroller only a small portion of internal blocks are switched on. Moreover, in most applications, the amount of calculations, performed by the microcontroller at a sensor node, is reduced to minimum. This technique allows to extend the WSN lifetime up to several months or even several years.

For a typical monitoring applications information losses and shortage of the processing capabilities are not crucial, because dropping of one or several measurements does not have a strong influence on the result of the processing of the data from the whole WSN. Tolerance to partial loss of information due to the low communication quality is the main difference between common WSN applications and WSN applications for critical tasks. The critical tasks here and later will reference to such applications where the data received from the WSN is used as basis for responsible decision-making. The exact criteria for determining whether task is critical or not, are out of scope of this technical paper. This we describe only the main

peculiarities and give a few examples of critical tasks. Applications of WSNs for critical tasks in comparison with applications for common tasks have stronger reliability, information security and quality of service (QoS) requirements. Clauses 7.2, 7.3 and 7.4 describe some relevant applications of WSNs for critical tasks.

2 Security and privacy

Wireless media is much more vulnerable than wired media for attackers. In critical tasks information security problems are particularly important since a security breach can result in a variety of negative effects. WSN applications for critical tasks are required to support integrity and confidentiality of the data exchanged during the application operations. These applications are required to provide security of exchanged data against malicious attacks. It is recommended to provide a secure channel to protect the data flows.

Data encryption and authentication are common information security techniques used in WSNs [50]. Restriction of access to the WSN settings and to the collected information is also a necessary measure of protection. These techniques in conjunction with the appropriate organization of interaction of sensor nodes in the WSN allow to achieve required level of security and privacy.

3 Fault tolerance

Errors in a WSN can occur for the following reasons: malfunction of one or more of sensor nodes, the change of environmental conditions, the actions of the attacker. According to most common practices, sensor node can be considered as failed if it sends measurements which significantly deviate from the results of the neighbor sensor nodes [51]. A faulty sensor node can be identified by the WSN as workable but provide bad measurement results.

A WSN intended for critical tasks has to operate well even if some nodes fail. In order to ensure a given level of fault tolerance, appropriate error correction mechanism must be provided. Besides, the WSN is required to ensure reliability and availability of the WSN infrastructure in order to handle a single sensor node failure. In case of such failures, the capabilities of the failed sensor nodes can be dynamically delegated to sensor nodes in order to provide consistent functioning and to prevent failure of the critical task.

3.1 Context Awareness

Context involves the information which can be used to describe the state of some physical object. This information has to be considered when making responsible decisions based on WSN measurements. For example, many of the processes are affected by temperature and time of day (especially in e-health applications). Without consideration of such dependencies, the data obtained from the WSN can be interpreted incorrectly. Data processing and decision-making systems of the WSN should also take into account the natural noise in sensor nodes, possible node failures and other sources of context information. For this purpose, context information is required to be collected, stored and used for decision making.

3.2 Quality of Service

The strict reliability requirements are often a key challenge for WSN utilization for critical tasks. Some applications require low latency in updating sensor readings, others may require high accuracy of measurements. Time response and accuracy characteristics of a WSN affect the accuracy and timeliness of the decision-making. Critical tasks ordinary need high levels of both of these parameters. Appropriate QoS mechanism must be implemented to make sure that QoS requirements are satisfied [52].

3.3 Emergency management

Emergency management is a good example of critical tasks where WSN can find its application [53]. Telecommunications during an emergency play crucial role in rescue coordination. And WSNs, and, in particular, sensor control networks (SCNs) which are considered in Section 6.4, are well applicable in this field because of easy deployment and self organization features. Besides monitoring the state of emergency and providing communication in emergency situations, WSNs have another potentially important application concerning emergency situations and saving people's lives. This application was described in [54].

An indoor emergency management system is based on SCNs. The main goal of the system is to provide everyone in the building with instructions concerning the appropriate way of evacuation. The system uses a personal mobile phones or tablet computers to deliver information to their owners. So every mobile device turns into a terminal of the rescue system in case of emergency. It is very reasonable due to the wide spread of mobile devices and because of the presence of additional communication channels in today's mobile devices.

At the entrance to the building a mobile user terminal automatically connects to the SCN infrastructure and obtains data from the SCN motes. While normal operation, system uses SCN motes to observe the physical conditions inside the building (temperature, smoke, etc.) as shown in Figure 1.1. When an emergency occurs, SCN motes automatically detect it. Then the information about the detection of signs of disaster spreads throughout the SCN and user terminals. Each user terminal automatically launches software for guidance in emergency cases. It gives instructions on the safest way of self-evacuation from the building. For example it can show one of the following: evacuation plans or maps; step-by-step sound commands and visual hints (e. g. interior photos with arrows towards the exit overlaid); videos showing how to use safety equipment. Especially important that the information displayed varies depending on the location of the user.

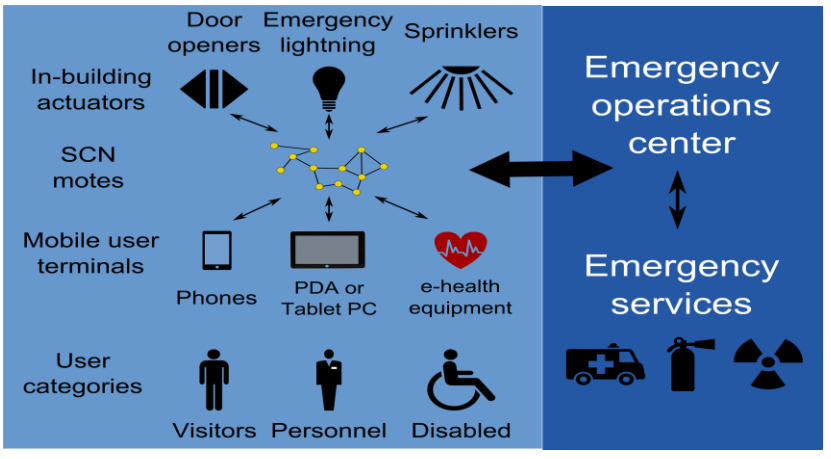

Figure 1.1: Emergency management system

The content of the instructions, which the system gives through the device to the owner, depends on various factors, for example:

- State of the building like accessibility and hazard level of rooms and escape routes. The state is determined by SCN motes;
- Position of the user determined by the nearest network node or using the GPS or GLONASS;

- User's health state determined by the e-health equipment.

User peculiarities awareness is a crucial feature of system. It means that while the personal mobile equipment is used the owner can chose appropriate customization options in software. These options will have impact on the instructions shown by the system. For example, a person with disabilities will receive special self-evacuation route, equipped with necessary facilities. Another example of customization is special instructions for building personnel. The system will remind them if they have specific duty responsibilities in case of emergencies. Also, the system will point to location of people with disabilities who need help.

In-building actuators (e. g. automotive door openers, emergency lightning and sprinklers) should also be equipped with SCN motes. Such actuators will also get commands from the system and start working if necessary.

4. Solution and Verification networks

Verification networks [55] are intended for the systems that operate automatically without human intervention. For a machine actuation unit in such automated system there exists a set of critical operations. Such operations can cause considerable negative consequences when carried out in improper system state. To avoid this for each critical operation a set of verification rules should be defined, which must be checked up before this operation and/or while the operation is in progress. Verification network can be designed to test these conditions. This type of critical task can be solved by using WSNs or SCNs. In this case the WSN should provide some kind of addition context awareness for automated systems.

To check verification rules the values of a number of parameters must be determined. Such parameters can be:

- Aggregate values, reference values, sensor readings presenting in SCN as part of normal flow of decision-making;
- Aggregate values, reference values, sensor readings presenting in SCN which are only intended to support verification;
- Sensor reading obtained from the machine actuation unit's own sensors;
- Values obtained by request from SCN server or other servers in NGN.

Verification network may have much more strict requirements concerning the reliability, security and performance. Data processing and transmission in a SCN for the purpose of verification may have higher priority in QoS in comparison with other activities in the SCN.

In Figure 1.2 a normal SCN decision-making flow is shown (see Section 6.4), but as soon as decision sets a machine actuation unit in motion, the verification process starts up by the verification network. If some of the check-ups of the verification process fail, some safe action (or no action) is performed instead of the action supposed in the decision.

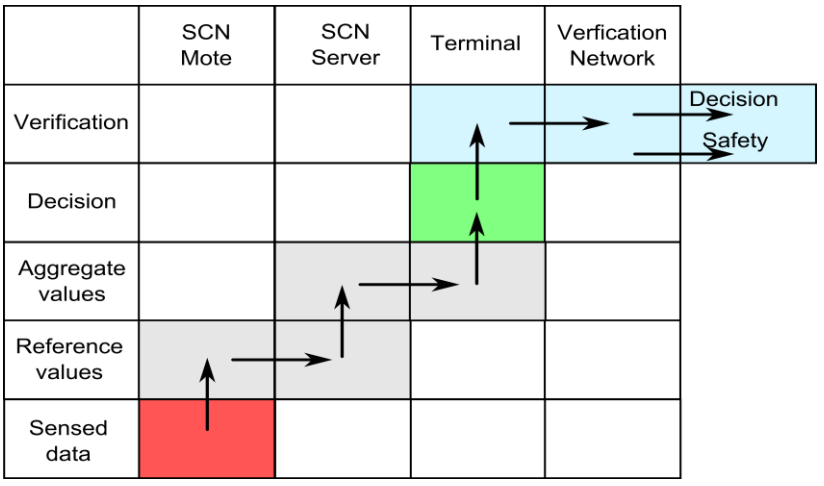

Figure 1.2: Verification network's decision-making flow

5. Conclusion:

A large private company in California implemented a WLAN to support enterprise mobility. The system was seemingly working great and providing significant benefits to its users. Over a year after the system went operational, the IT department noticed, through a routine network security audit, that several of its printers in the financial department had been configured to send all printed data to a file at a suspicious IP address. Unfortunately, the IT department had not locked down the administrative access ports on these printers. Even though all the details of what happened here are not known, it is likely that a hacker gained unauthorized access to the WLAN (which did not implement any form of authentication) and ran a port scan to find the open printer administration port. With the open port's IP address (resulting from the scan), the hacker could easily log in to the administrative port and set the printer to send all print jobs to a file located on the hacker's laptop. The printer would then continue to print on paper and also send the print data to the hacker's laptop. Of course this would send to the hacker everything that the printer would print, such as internal goals and objectives, company sales information, employee salaries, and so on. After discovering this issue, the company promptly implemented an authentication system to disallow all unauthorized people from accessing the WLAN.

6. References

[1] S. Glazyev, "The global economic crisis as a process of technological shifts," *Problems of Economic Transition*, vol. 52, no. 5, pp. 3–19, 2009.

[2] C.-Y. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[3] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*. Wiley. com, 2010.

[4] R. T. Lacoss, "Distributed mixed sensor aircraft tracking," in *American Control*

Conference, 1987, pp. 1827–1830, IEEE, 1987.

[5] G. J. Pottie, "Wireless integrated network sensors (WINS): the web gets physical," in *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2001 NAE Symposium on Frontiers of Engineering*, p. 78, National Academies Press, 2002.

[6] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, no. 5, pp. 51–58, 2000.

[7] S. Vardhan, M. Wilczynski, G. Portie, and W. J. Kaiser, "Wireless integrated network sensors (WINS): distributed in situ sensing for mission and flight systems," in *Aerospace Conference Proceedings, 2000 IEEE*, vol. 7, pp. 459–463, IEEE, 2000.

[8] W. J. Kaiser, K. Bult, A. Burstein, D. Chang, *et al.*, "Wireless integrated microsensors," in *Technical Digest of the 1996 Solid State Sensor and Actuator Workshop*, 06 1996.

[9] G. Asada, A. Burstein, D. Chang, M. Dong, M. Fielding, E. Kruglick, J. Ho, F. Lin, T. Lin, H. Marcy, *et al.*, "Low power wireless communication and signal processing circuits for distributed microsensors," in *Circuits and Systems, 1997. ISCAS'97., Proceedings of 1997 IEEE International Symposium on*, vol. 4, pp. 2817–2820, IEEE, 1997.

[10] J. Rabaey, J. Ammer, J. da Silva Jr, and D. Patel, "PicoRadio: Ad-hoc wireless networking of ubiquitous low-energy sensor/monitor nodes," in *VLSI, 2000. Proceedings. IEEE Computer Society Workshop on*, pp. 9–12, IEEE, 2000.

[11] J. Da Silva Jr, M. JS, C. G. Ammer, S. Li, R. Shah, T. Tuan, M. Sheets, J. Ragaey, B. Nikolic, A. Sangiovanni-Vincentelli, *et al.*, "Design methodology for Pico Radio networks," *Berkeley Wireless Research Center*, 2001.

[12] J. M. Kahn, R. H. Katz, and K. S. Pister, "Next century challenges: mobile networking for Smart Dust," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 271–278, ACM, 1999.

[13] K. S. Pister, J. M. Kahn, B. E. Boser, *et al.*, "Smart dust: Wireless networks of millimeter-scale sensor nodes," *Highlight Article in*, p. 2, 1999.

[14] "μAMPS research." URL: http://www-mtl.mit.edu/researchgroups/icsystems/uamps/research/overview.shtml, 2004. Accessed: 2013-11-08.

[15] B. H. Calhoun, D. C. Daly, N. Verma, D. F. Finchelstein, D. D. Wentzloff, A. Wang, S.-H. Cho, and A. P. Chandrakasan, "Design considerations for ultra-low energy wireless microsensor nodes," *Computers, IEEE Transactions on*, vol. 54, no. 6, pp. 727–740, 2005.

[16] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, "IEEE 802.15. 4: a developing standard for low-power low-cost wireless personal area networks," *network, IEEE*, vol. 15, no. 5, pp. 12–19, 2001.

[17] "The ZigBee alliance." URL: http://www.zigbee.org/About/AboutAlliance/TheAlliance.aspx, 2014. Accessed: 2014-02-26.

[18] "HART communications foundation official website." URL: http://www.hartcomm.org/, 2014. Accessed: 2014-02-26.

[19] "6LoWPAN working group." URL: http://www.ietf.org/dyn/wg/charter/6lowpan-charter.html, 2014. Accessed: 2014-02-26.

[20] “Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.” ITU-T Recommendation Y.2221 (2010).

[21] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[22] G. Simon, M. Mar´oti, ´ A. L´edeczi, G. Balogh, B. Kusy, A. N´adas, G. Pap, J. Sallai, and K. Frampton, “Sensor network-based countersniper system,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 1–12, ACM, 2004.

[23] J. Yick, B. Mukherjee, and D. Ghosal, “Analysis of a prediction-based mobility adaptive tracking algorithm,” in *Broadband Networks, 2005. BroadNets 2005. 2nd International Conference on*, pp. 753–760, IEEE, 2005.

[24] T. Gao, D. Greenspan, M. Welsh, R. Juang, and A. Alm, “Vital signs monitoring and patient tracking over a wireless network,” in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pp. 102–105, IEEE, 2006.

[25] K. Lorincz, D. J. Malan, T. R. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, “Sensor networks for emergency response: challenges and opportunities,” *Pervasive Computing, IEEE*, vol. 3, no. 4, pp. 16–23, 2004.

[26] M. Castillo-Effer, D. H. Quintela, W. Moreno, R. Jordan, and W. Westhoff, “Wireless sensor networks for flash-flood alerting,” in *Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on*, vol. 1, pp. 142–146, IEEE, 2004.

[27] G. Wener-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. Walsh, “Deploying a wireless sensor network on an active volcano. data-driven applications in sensor networks (special issue),” *IEEE Internet Computing*, vol. 2, pp. 18–25, 2006.

[28] C. Buratti, A. Conti, D. Dardari, and R. Verdone, “An overview on wireless sensor networks technology and evolution,” *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[29] R. Hartley, “Transmission of information,” *Bell System Technical Journal*, 1928.

[30] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, *et al.*, “TinyOS: An operating system for sensor networks,” in *Ambient intelligence*, pp. 115–148, Springer, 2005.

[31] “Wireless Medium Access Control (MAC) and physical layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).” IEEE 802.15.4 Standard. Part 15.4 (2006).

[32] D. R. Green, “Geospatial tools and techniques for vineyard management in the twenty-first century,” in *The Geography of Wine* (P. H. Dougherty, ed.), pp. 227–245, Springer Netherlands, 2012.

[33] A. Galloway, “An Internet of Cows (and Sheeps!),” *Design Culture Lab*, 07 2011. URL: http://www.designculturelab.org/2011/07/20/an-internet-of-cows-and-sheeps/.

[34] “Requirements for the support of machine-oriented communication applications in the next generation network environment.” ITU-T Recommendation Y.2061.

[35] W. Huiyong, W. Jingyang, and H. Min, “Building a smart home system with WSN and service robot,” in *Measuring Technology and Mechatronics Automation (ICMTMA),*

2013 Fifth International Conference on, pp. 353–356, IEEE, 2013.

[36] P. Waide, J. Ure, G. Smith, and B. Bordass, "The scope for energy and CO2 savings in the EU through the use of building automation technology," final report, Waide Strategic Efficiency, 08 2013.

[37] K. Jaafar and M. K. Watfa, "Sensor networks in future smart rotating buildings," in *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pp. 962–967, IEEE, 2013.

[38] S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, "Health monitoring of civil infrastructures using wireless sensor networks," in *Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on*, pp. 254–263, 2007.

[39] W.-Z. Song, R. Huang, M. Xu, A. Ma, B. Shirazi, and R. LaHusen, "Air-dropped sensor network for real-time high-fidelity volcano monitoring," in *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pp. 305–318, ACM, 2009.

[40] G. Liu, R. Tan, R. Zhou, G. Xing, W.-Z. Song, and J. M. Lees, "Volcanic earthquake timing using wireless sensor networks," in *Proceedings of the 12th international conference on Information processing in sensor networks*, pp. 91–102, ACM, 2013.

[41] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 5, no. 1, p. 5, 2009.

[42] T. Saaty, *Decision Making with Dependence and Feedback: The Analytic Network Process: the Organization and Prioritization of Complexity*. Analytic hierarchy process series, Rws Publications, 2001.

[43] L. Yu and Z. Heng, "Measuring agility of enterprise using analytic hierarchy process and bayesian belief networks," in *Management Science and Engineering, 2006. ICMSE'06. 2006 International Conference on*, pp. 551–556, IEEE, 2006.

[44] C.-x. Chen, Z.-w. He, J.-g. Jia, J.-m. Kuang, and Z.-y. Zhang, "Fuzzy evaluation algorithm for system effectiveness of wireless sensor networks," in *Global High Tech Congress on Electronics (GHTCE), 2012 IEEE*, pp. 43–48, IEEE, 2012.

[45] N. Kamiyama and D. Satoh, "Network topology design using analytic hierarchy process," in *Communications, 2008. ICC'08. IEEE International Conference on*, pp. 2048–2054, IEEE, 2008.

[46] N. Ruan, Y. Ren, Y. Hori, and K. Sakurai, "Performance analysis of key management schemes in wireless sensor network using analytic hierarchy process," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pp. 1739–1744, IEEE, 2011.

[47] M. R. Ahmad, E. Dutkiewicz, *et al.*, "Performance analysis of MAC protocol for cooperative MIMO transmissions in WSN," in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, pp. 1–6, IEEE, 2008.

[48] Y. Yin, J. Shi, Y. Li, and P. Zhang, "Cluster head selection using analytical hierarchy process for wireless sensor networks," in *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*, pp. 1–5, IEEE, 2006.

[49] N. Yang, T. Liqin, S. Xueli, and G. Shukai, "Behavior trust evaluation for node in WSNs

with fuzzy-ANP method," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, vol. 1, pp. V1–299, IEEE, 2010.

[50] I. M. Khan, N. Jabeur, M. Z. Khan, and H. Mokhtar, "An overview of the impact of wireless sensor networks in medical health care," in *The 1st International Conference on Computing and Information Technology (ICCT)*, pp. 576–580, 2012.

[51] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*. Wiley. com, 2010.

[52] M. Souil and A. Bouabdallah, "On QoS provisioning in context-aware wireless sensor networks for healthcare," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pp. 1–6, IEEE, 2011.

[53] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner, "Design challenges for an integrated disaster management communication and information system," in *The First IEEE Workshop on Disaster Recovery Networks (DIREN 2002)*, vol. 24, 2002.

[54] "Personal safety in emergencies." ITU News, 3 2012.

[55] "Sensor Control Networks and related applications in Next Generation Network environment." ITU-T Recommendation Y.2222 (2013).

[56] T. Gao, C. Pesto, L. Selavo, Y. Chen, J. G. Ko, J. H. Lim, A. Terzis, A. Watt, J. Jeng, B.-r. Chen, *et al.*, "Wireless medical sensor networks in emergency response: Implementation and pilot results," in *Technologies for Homeland Security, 2008 IEEE Conference on*, pp. 187–192, IEEE, 2008.

[57] D. of Engineering and H. U. Applied Sciences, "Sensor networks for medical care," in *Technical Report TR-08-05*, 2005.

[58] K. Lorincz, B.-r. Chen, G. W. Challen, A. R. Chowdhury, S. Patel, P. Bonato, M. Welsh, *et al.*, "Mercury: a wearable sensor network platform for high-fidelity motion analysis.," in *SenSys*, vol. 9, pp. 183–196, 2009.

[59] J. A. Weaver, *A wearable health monitor to aid parkinson disease treatment*. PhD thesis, Massachusetts Institute of Technology, 2003.

[60] B. Lo, S. Thiemjarus, R. King, and G.-Z. Yang, "Body sensor network-a wireless sensor platform for pervasive healthcare monitoring," in *The 3rd International Conference on Pervasive Computing*, vol. 13, pp. 77–80, 2005.

[61] "Open service environment functional architecture for next generation networks." ITU-T Recommendation Y.2020.

[62] "Open service environment capabilities for NGN." ITU-T Recommendation Y.2234.

[63] "Requirements and capabilities for ITU-T NGN." ITU-T Recommendation Y.2201.

[64] "Requirements and framework allowing accounting and charging capabilities in NGN." ITU-T Recommendation Y.2233.

[65] Y. B. Kim, "u-healthcare service based on a USN middleware platform," *Networked Computing and Advanced Information Management, International Conference on*, vol. 0, pp. 673–678, 2009.

[66] M. Kim, Y. Lee, and J. Park, "Trend of USN middleware technology," *ETRI: Trend Analysis of Electronic & Telecommunication*, vol. 22, pp. 67–79, 06 2007.

[67] Y. Kim, M. Kim, and Y. Lee, "COSMOS: A middleware platform for sensor networks

and a u-healthcare service," in *ACM SAC'08*, (Brazil), pp. 512–513, 03 2008.

[68] "Service description and requirements for ubiquitous sensor network middleware." ITU-T Recommendation F.744.

[69] W. Lee, A. Datta, and R. Cardell-Oliver, "Network management in wireless sensor networks," *Handbook of Mobile Ad Hoc and Pervasive Communications: American Scientific Publishers*, 2006.

[70] A. Smailagic, "Location sensing and privacy in a context-aware computing environment," *Wireless Communications, IEEE*, vol. 9, pp. 10–17, 10 2002.