Resilient Wireless Sensor Networks for Cyber-Physical Systems

Waseem Abbas*, Aron Laszka†, and Xenofon Koutsoukos‡

Vanderbilt University, Nashville, TN 37212

Abstract

Due to their low deployment costs, wireless sensor networks (WSN) may act as a key enabling technology for a variety of spatially-distributed cyber-physical system (CPS) applications, ranging from intelligent traffic control to smart grids. However, besides providing tremendous benefits in terms of deployment costs, they also open up new possibilities for malicious attackers, who aim to cause financial losses or physical damage. Since perfectly securing these spatially-distributed systems is either impossible or financially unattainable, we need to design them to be resilient to attacks: even if some parts of the system are compromised or unavailable due to the actions of an attacker, the system as a whole must continue to operate with minimal losses. In a CPS, control decisions affecting the physical process depend on the observed data from the sensor network. Any malicious activity in the sensor network can therefore severely impact the physical process, and consequently the overall CPS operations. These factors necessitate a deeper probe into the domain of resilient WSN for CPS. In this chapter, we provide an overview of various dimensions in this field, including objectives of WSN in CPS, attack scenarios and vulnerabilities, notion of attack-resilience in WSN for CPS, and solution approaches towards attaining resilience. We also highlight major challenges, recent developments, and future directions in this area.

1 Introduction

A wireless sensor network is a collection of sensor devices organized into a wireless network. Traditionally, wireless sensor networks have been used as cost-effective means of monitoring spatially-distributed processes and phenomena. Their potential applications include military applications, such as battlefield surveillance and chemical attack detection, environmental applications, such as forest-fire detection and precision agriculture, and health applications, such as monitoring human physiological data [1].

A cyber-physical system is an integrated system of *computational elements* and *physical processes*, in which the physical processes are controlled by the computational elements [2]. Since the computational elements must have reliable information about the evolving state of the physical processes in order to control them, every practical cyber-physical system has to include *sensor devices*. These sensor devices monitor the physical processes, providing the computational elements with information that can be used for various tasks, such as state estimation and fault identification.

*waseem.abbas@vanderbilt.edu

†aron.laszka@vanderbilt.edu

‡xenofon.koutsoukos@vanderbilt.edu

Finally, the output of the computational elements is fed into actuator devices that can influence the physical processes in the desired way, which closes the loop between the physical and cyber parts of the system.

In the case of *spatially-distributed physical processes*, however, the sensing task can prove to be challenging, as the sensor devices may need to be deployed over a larger area. For example, in order to provide intelligent traffic control for a whole city, we must have reliable information about the current traffic situation in various parts of the city. In order to have such information, we must deploy a large number of traffic sensors over vast area. With wired sensors, the cost of deployment could be prohibitively high and in some cases, it may even be physically or legally impossible. Consequently, wireless sensor networks, whose deployment is much simpler and more cost-effective, may act as a key enabling technology for spatially-distributed cyber-physical systems.

The rest of the chapter is organized as follows: In the remainder of this section, we illustrate the role of WSN in the context of CPS along with information-security goals in CPS. In Section 2, various applications of WSN for CPS are stated along with examples. An overview of different attack scenarios and vulnerabilities in WSN along with instances of such attacks in practical networks is provided in Section 3. In Section 4, the notion of attack-resilience in WSN is discussed along with the modeling issues and related challenges. Different approaches towards making WSN resilient against attacks, as well as a couple of detailed examples, are presented in Section 5. Finally, some future directions in this field are outlined in Section 6.

1.1 Cyber-Physical Systems and Sensor Networks

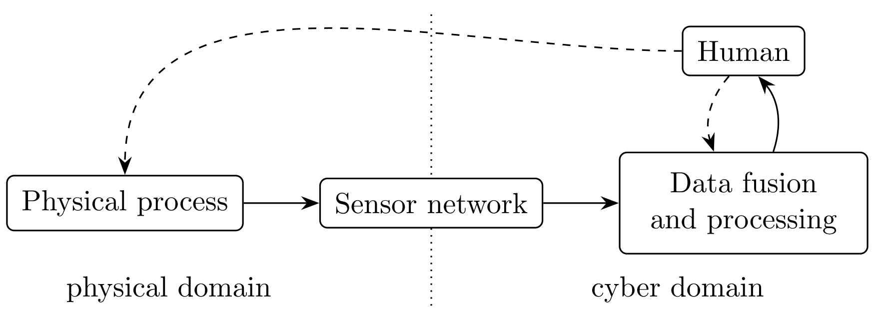

Figure 1: Wireless sensor networks for monitoring and surveillance applications.

Monitoring and Surveillance Applications Traditional sensor network applications focus on acquiring, transmitting, and fusing data. In these applications, the physical and cyber parts do not form a closed loop, or in some cases, form a closed loop which includes human element. See Figure 1 for a simple illustration of the system architecture of such applications.

For example, in a typical habitat-monitoring application [3], sensors measure environmental properties, such as light, temperature, humidity, and barometric pressure, and transmit their data through the sensor network to a gateway. Then, the gateway transmits the data through a transit network to a base station, which provides WAN connectivity. Finally, the processed data is displayed on a user-friendly interface to scientists. As another example, in a forest-fire surveillance application [4], sensors collect temperature, humidity, and illumination data and transmit it through the sensor network to a gateway node. The gateway node then forwards the data to a middleware, which stores the measurements in a database server and calculates forest-fire risk-levels from real-time and historical data. Finally, the results are displayed in a web application and if a forest fire is detected, alarms are automatically sent to fire stations or nearby residents.

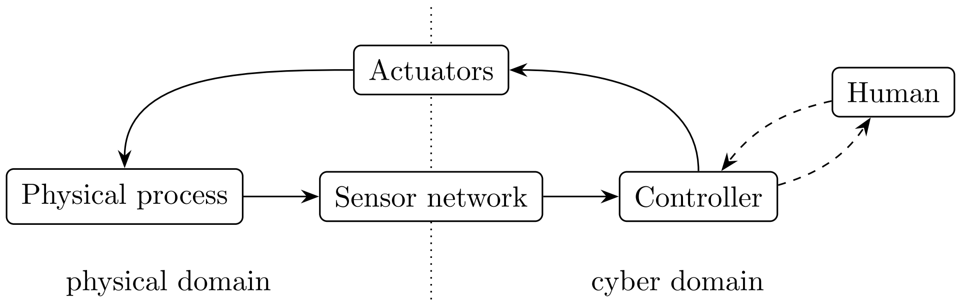

Figure 2: Wireless sensor networks for cyber-physical systems.

Cyber-Physical Systems In cyber-physical systems, on the other hand, physical processes and computational elements are tightly integrated: physical processes, sensors, controllers, and actuators form a *closed loop*. Note that cyber-physical systems can still be supervised by human operators; however, there is a closed, real-time control loop which does not contain a human element. See Figure 2 for a simple illustration of the architecture of cyber-physical systems using wireless sensor networks.

Since sensor networks in cyber-physical systems are part of closed, real-time control loops, ensuring their security is more critical than in traditional sensor-network applications. In a CPS, malicious sensor data will result in incorrect control decisions, which are immediately executed by the actuators. Consequently, an attacker who has compromised a sensor network has some level of control over the physical process and may cause physical damage or financial losses using malicious control. For example, in a smart electric grid, an attacker who can tamper with real-time power-consumption data may be able to cause physical damage by simulating a rapid increase in consumption.

Therefore, security is a crucial issue for wireless sensor networks in cyber-physical systems. In the following subsection, we summarize the traditional goals of information security and how they can be applied to cyber-physical systems. For a general overview of WSN in CPS, we refer readers to the other book chapters and a survey of Wu et al. [5].

1.2 Information-Security Goals and Cyber-Physical Systems

Traditionally, the three key goals of information security are *confidentiality*, *integrity*, and *availability* (CIA). For cyber-physical systems, however, these properties are often listed in reverse order to emphasize that in many CPS, availability and integrity requirements have priority over the confidentiality objective [6, 7].

Acknowledgment

This work was supported in part by the National Science Foundation under Award CNS-1238959.

References

[1] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Computer networks. 2002;38(4):393–422.

[2] Lee EA. Cyber physical systems: Design challenges. In: Proceedings of the 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC). IEEE; 2008. p. 363–369.

[3] Mainwaring A, Culler D, Polastre J, Szewczyk R, Anderson J. Wireless sensor networks for habitat monitoring. In: Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications. ACM; 2002. p. 88–97.

[4] Son B, Her Y, Kim JG. A design and implementation of forest-fires surveillance system based on wireless sensor networks for South Korea mountains. International Journal of Computer Science and Network Security. 2006;6(9):124–130.

[5] Wu FJ, Kao YF, Tseng YC. From wireless sensor networks towards cyber physical systems. Pervasive and Mobile Computing. 2011;7(4):397 – 413. Available from: http://www.sciencedirect.com/science/article/pii/S1574119211000368.

[6] Cardenas AA, Amin S, Sastry S. Secure control: Towards survivable cyber-physical systems. In: 28th International Conference on Distributed Computing Systems Workshops. IEEE; 2008. p. 495–500.

[7] Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. Proceedings of the IEEE. 2012;100(1):210–224.

[8] McDaniel P, McLaughlin S. Security and Privacy Challenges in the Smart Grid. IEEE Security Privacy. 2009 May;7(3):75–77.

[9] Rial A, Danezis G. Privacy-preserving smart metering. In: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society (WPES'11). ACM; 2011. p. 49–60.

[10] Sankar L, Rajagopalan SR, Mohajer S, Poor HV. Smart meter privacy: A theoretical framework. IEEE Transactions on Smart Grid. 2013;4(2):837–846.

[11] Alemdar H, Ersoy C. Wireless sensor networks for healthcare: A survey. Computer Networks. 2010;54(15):2688–2710.

[12] Haykin SS, Haykin SS, Haykin SS. Kalman filtering and neural networks. Wiley Online Library; 2001.

[13] Olfati-Saber R. Distributed Kalman filtering for sensor networks. In: 46th IEEE Conference on Decision and Control. IEEE; 2007. p. 5492–5498.

[14] Hernandez L, Baladrón C, Aguiar J, Carro B, Sánchez-Esguevillas A, Lloret J, et al. A survey on electric power demand forecasting: Future trends in smart grids, microgrids and smart buildings. IEEE Communications Surveys & Tutorials. 2014;16(3):1460–1495.

[15] Mirowski P, Chen S, Kam Ho T, Yu CN. Demand Forecasting in Smart Grids. Bell Labs Technical Journal. 2014;18(4):135–158.

[16] Amin S, Schwartz G, Cardenas A, Sastry S. Game-Theoretic Models of Electricity Theft Detection in Smart Utility Networks: Providing New Capabilities with Advanced Metering Infrastructure. IEEE Control Systems. 2015;35(1):66–81.

[17] McLaughlin S, Holbert B, Fawaz A, Berthier R, Zonouz S. A multi-sensor energy theft detection framework for advanced metering infrastructures. IEEE Journal on Selected Areas in Communications. 2013;31(7):1319–1330.

[18] Fang X, Misra S, Xue G, Yang D. Smart grid – The new and improved power grid: A survey. IEEE Communications Surveys & Tutorials. 2012;14(4):944–980.

[19] Gungor VC, Lu B, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. IEEE Transactions on Industrial Electronics. 2010;57(10):3557–3564.

[20] Ghena B, Beyer W, Hillaker A, Pevarnek J, Halderman JA. Green lights forever: Analyzing the security of traffic infrastructure. In: Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT'14). USENIX Association; 2014. p. 1–10.

[21] Tubaishat M, Zhuang P, Qi Q, Shang Y. Wireless sensor networks in intelligent transportation systems. Wireless Communications and Mobile Computing. 2009;9(3):287–302.

[22] Smith BL, Demetsky MJ. Traffic flow forecasting: Comparison of modeling approaches. Journal of Transportation Engineering. 1997;123(4):261–266.

[23] Xie Y, Zhao K, Sun Y, Chen D. Gaussian processes for short-term traffic volume forecasting. Journal of the Transportation Research Board. 2010;2165(1):69–78.

[24] Raymond DR, Midkiff SF. Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing. 2008;7(1):74–81.

[25] Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials. 2006;8(8):2–23.

[26] Wood A, Stankovic JA. Denial of service in sensor networks. Computer. 2002;35(10):54–62.

[27] Xu W, Ma K, Trappe W, Zhang Y. Jamming sensor networks: attack and defense strategies. Network, IEEE. 2006;20(3):41–47.

[28] Maheshwari R, Gao J, Das SR. Detecting wormhole attacks in wireless networks using connectivity information. In: Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM'07). IEEE; 2007. p. 107–115.

[29] Poovendran R, Lazos L. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Networks. 2007;13(1):27–59.

[30] Gu Q, Ferguson C, Noorani R. A study of self-propagating mal-packets in sensor networks: Attacks and defenses. Computers & Security. 2011;30(1):13–27.

[31] Francillon A, Castelluccia C. Code injection attacks on harvard-architecture devices. In: Proceedings of the 15th ACM Conference on Computer and Communications Security. ACM; 2008. p. 15–26.

[32] Yang Y, Zhu S, Cao G. Improving sensor network immunity under worm attacks: A software diversity approach. In: Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing. ACM; 2008. p. 149–158.

[33] Wang Y, Wen S, Xiang Y, Zhou W. Modeling the propagation of worms in networks: A survey. IEEE Communications Surveys & Tutorials. 2014;16(2):942–960.

[34] Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security. 2011;14(1):13.

[35] Xie L, Mo Y, Sinopoli B. False data injection attacks in electricity markets. In: Proceedings of the 1st International Conference on Smart Grid Communications. IEEE; 2010. p. 226–231.

[36] Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks: analysis & defenses. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks. ACM; 2004. p. 259–268.

[37] Parno B, Perrig A, Gligor V. Distributed detection of node replication attacks in sensor networks. In: IEEE Symposium on Security and Privacy. IEEE; 2005. p. 49–63.

[38] Amin S, Cárdenas AA, Sastry SS. Safe and secure networked control systems under denial-of-service attacks. In: Hybrid Systems: Computation and Control. Springer; 2009. p. 31–45.

[39] Amin S, Litrico X, Sastry S, Bayen AM. Stealthy deception attacks on water SCADA systems. In: Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control. ACM; 2010. p. 161–170.

[40] Amin S, Litrico X, Sastry S, Bayen AM. Cyber security of water scada systemspart I: analysis and experimentation of stealthy deception attacks. IEEE Transactions on Control Systems Technology. 2013;21(5):1963–1970.

[41] Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on scada systems. IEEE Transactions on Control Systems Technology. 2014;22(4):1396–1407.

[42] Mo Y, Sinopoli B. Secure control against replay attacks. In: Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing. IEEE; 2009. p. 911–918.

[43] Rezvani M, Ignatovic A, Bertino E, Jha S. Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. IEEE Transactions on Dependable and Secure Computing. 2015;12(1):98–110.

[44] Kushner D. The real story of Stuxnet. IEEE Spectrum. 2013;50(3):48–53.

[45] Kaspersky Lab. Kaspersky Lab provides its insights on Stuxnet worm; 2010. Accessed: May 1st, 2015. http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm.

[46] Kelley MB. The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought; 2013. Accessed: Apr 27th, 2015. *Business Insider*, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

[47] Cerrudo C. Hacking US (and UK, Australia, France, etc.) traffic control systems; 2014. Accessed: May 3rd, 2015. *IOActive Labs Blog*, http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html.

[48] Zetter K. Hackers can mess with traffic lights to jam roads and reroute cars; 2014. Accessed: May 3rd, 2015. *Wired*, http://www.wired.com/2014/04/traffic-lights-hacking/.

[49] ICS-CERT. Sensys Networks Traffic Sensor Vulnerabilities; 2014. Advisory (ICSA-14-247-01A).

[50] Mouawad J. Conflict narrows oil options for West; 2008. Accessed: May 3rd, 2015. *The New York Times*, http://www.nytimes.com/2008/08/14/world/europe/14oil.html.

[51] Robertson J, Riley MA. Mysterious '08 Turkey pipeline blast opened new cyberwar; 2014. Accessed: Apr 27th, 2015. *Bloomberg*, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[52] Cobham A. The intrinsic computational difficulty of functions. In: Proceedings of the 1964 Congress for Logic, Methodology, and the Philosophy of Science; 1965. p. 24–30.

[53] Kerckhoffs A. La cryptographie militaire. Journal des Sciences Militaires. 1883 January;9:5–83.

[54] Pita J, Jain M, Tambe M, Ordóñez F, Kraus S. Robust solutions to stackelberg games: Addressing bounded rationality and limited observations in human cognition. Artificial Intelligence. 2010;174(15):1142–1171.

[55] Freund Y, Kearns M, Mansour Y, Ron D, Rubinfeld R, Schapire RE. Efficient algorithms for learning to play repeated games against computationally bounded adversaries. In: Proceedings of the 36th Annual Symposium on Foundations of Computer Science, (FOCS). IEEE; 1995. p. 332–341.

[56] Deng J, Han R, Mishra S. A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In: Proceedings of the 2nd International Workshop on Information Processing in Sensor Networks (IPSN). Springer; 2003. p. 349–364.

[57] Al-Karaki JN, Kamal AE. Routing techniques in wireless sensor networks: A survey. Wireless Communications. 2004;11(6):6–28.

[58] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks. 2005;3(3):325–349.

[59] Younis M, Akkaya K. Strategies and techniques for node placement in wireless sensor networks: A survey. Ad Hoc Networks. 2008;6(4):621–655.

[60] Cardei M, Wu J. Coverage in wireless sensor networks. Handbook of Sensor Networks. 2004;p. 422–433.

[61] Wang YC, Tseng YC. Distributed deployment schemes for mobile wireless sensor networks to ensure multilevel coverage. IEEE Transactions on Parallel and Distributed Systems. 2008;19(9):1280–1294.

[62] Dhillon SS, Chakrabarty K. Sensor placement for effective coverage and surveillance in distributed sensor networks. In: Proceedings of the 2003 IEEE Wireless Communications and Networking Conference (WCNC). IEEE; 2003. p. 1609–1614.

[63] Abbas W, Egerstedt M. Robust graph topologies for networked systems. In: 3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems; 2012. p. 85–90.

[64] Dekker AH, Colbert BD. Network robustness and graph topology. In: Proceedings of the 27th Australasian conference on Computer science-Volume 26. Australian Computer Society, Inc.; 2004. p. 359–368.

[65] Laszka A, Buttyán L, Szeszlér D. Designing robust network topologies for wireless sensor networks in adversarial environments. Pervasive and Mobile Computing. 2013;9(4):546–563.

[66] Santi P. Topology control in wireless ad hoc and sensor networks. ACM Computing Surveys. 2005;37(2):164–194.

[67] Wagner D. Resilient aggregation in sensor networks. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. ACM; 2004. p. 78–87.

[68] LeBlanc HJ, Zhang H, Koutsoukos X, Sundaram S. Resilient asymptotic consensus in robust networks. IEEE Journal on Selected Areas in Communications. 2013;31(4):766–781.

[69] Sundaram S, Hadjicostis CN. Distributed function calculation via linear iterative strategies in the presence of malicious agents. IEEE Transactions on Automatic Control. 2011;56(7):1495–1508.

[70] Marano S, Matta V, Tong L. Distributed detection in the presence of byzantine attacks. IEEE Transactions on Signal Processing. 2009;57(1):16–29.

[71] Olfati-Saber R, Franco E, Frazzoli E, Shamma J. Belief consensus and distributed hypothesis testing in sensor networks. In: Antsaklis PJ, Tabuada P, editors. Networked Embedded Sensing and Control. Lecture Notes in Control and Information Science. Springer; 2006. p. 169–182.

[72] Vempaty A, Tong L, Varshney P. Distributed inference with byzantine data: State-of-the-art review on data falsification attacks. IEEE Signal Processing Magazine. 2013;30(5):65–75.

[73] Rasmussen CE, Williams CKI. Gaussian Processes for Machine Learning. MIT Press; 2006.

[74] Das A, Kempe D. Algorithms for subset selection in linear regression. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. ACM; 2008. p. 45–54.

[75] Abbas W, Vorobeychik Y, Koutsoukos X. Resilient consensus protocol in the presence of trusted nodes. In: 7th International Symposium on Resilient Control Systems. IEEE; 2014. p. 1–7.