On Standards for Wireless Sensor Networks in the application of Structural Health Monitoring

Peter Edge
Faculty of Health Engineering and Sciences
The University of Southern Queensland (UniSQ) West Street, Toowoomba
QLD Australia
U1068436@umail.usq.edu.au

Hossein Akarinejad
Department of Engineering and Architectural Studies
Ara Institute of Canterbury/Te Pukenga
Christchurch, New Zealand
Hossein.Akarinejad@ara.ac.nz

Zhongwei Zhang
School of Mathematics, Physics and Computing
The University of Southern Queensland (UniSQ) West Street, Toowoomba
QLD Australia
Zhongwei.Zhang@usq.edu.au

Abstract— This paper presents the view of The Internet of Things (IoT) from the perspective of Wireless Sensor Networks (WSN) in the application of Structural Health Monitoring (SHM). Automation of building data collection over time, detecting prolonged or rapid changes in physical structure properties offers financial and time saving opportunities. SHM has attracted a great deal of interest from the research community in recent years. Regulatory frameworks, security, and guidance for manufacturers have not evolved in parallel for the WSNs supporting IoT. In this context it is important to consider the effectiveness of WSN for IoT and its ability to deliver accurate, secure and reliable service to the civil and structural engineering SHM application. The number of research projects to consider the security and integrity of collecting data from critical sites is negligible. Based on these considerations, we present the idea of SHM systems designed in partnership with structural engineers. In this way, we propose regulated, secure WSN classified into SHM categories based on current information technology (IT) standards.

Keywords—Internet of Things (IoT), Wireless Sensor Networks (WSN), 802.11 ah, Structural Health Monitoring (SHM). Extended Abstract Research Paper.

I. INTRODUCTION

The Internet of Things (IoT) [1] is an infrastructure that aggregates Wireless Sensor Networks (WSNs) with gateway nodes and provides connectivity to the internet. WSNs are regarded as one anatomical element of the Internet of things (IoT) infrastructure and platform. Security of WSNs has been identified as an important and imperative issue as it may significantly impact the application and hence the acceptance by communities and industry [2]. A continued profit driven approach with a shortage of regulation and guidance for manufacturers could potentially erode confidence in the technology.

IoT services are presented in cloud computing and dashboards on smartphones or Human Machine Interfaces (HMI). [3] E.g., Industrial IoT (IIoT) can create an awareness of the environment through collecting information and flow back to devices such as actuators to manipulate industrial processes. For critical real-time applications of the IoT, gateway devices form a [4] fog layer and therefore remove round trip latency to the cloud. However, security of such applications of the IoT remains a challenging area [5]. Traditional network security schemes which require encryption, storage, and high CPU cycles, are unsuitable for resource constrained sensing devices with low or ultra-low power supplies [6]. For instance, in the case of civil structure monitoring, integrity of transmitted data through the network to analytical applications, is critical in making real-time decisions affecting public health and safety.

The remainder of the paper is organized as follows: Section II gives a background of issues deploying SHM and the gap between research and real-world deployment of systems. Section III describes motivation and research goals. Finally, conclusions are drawn, and future work is defined in section IV.

II. BACKGROUND

A recent application of the WSNs is Structural Health Monitoring (SHM), which is an approach for identifying changes in the integrity of various structures including buildings, bridges, and pipelines etc. [7],[8],[9]. SHM is an important asset management tool for engineers. The opportunities for WSN integrated SHM are extensive. However, IoT systems as an industry are largely underregulated in many countries. There exists a significant gap between the benefits automation of SHM could offer and the capability to do so in its current form. Structural and civil engineering bodies as highly regulated professional entities, require precision in planning, construction, maintenance, and eventual replacement of infrastructure. Structures are monitored throughout their life span. We argue IoT systems based on WSN are unable to achieve these processes in the current state. This is a critical point for the industry and requires attention from both researchers and industry in achieving global and local regulatory standards in manufacturing, identification, and management of IoT devices. Most devices currently do not meet standard definitions of information technology (IT) security. Typically, IT devices, smartphones, servers, laptops, are the basis of what is known as device cybersecurity. Conversely, ordinary household consumer appliances that lacked any computing functionality are now consumed as smart devices, connected to the internet as a thing, with an attack surface introduced. The life cycle of asset managed IT equipment achieves a standard of security through security policy based on the Confidentiality, Integrity, and Availability (CIA) triad. On the other hand, in a poorly regulated IoT industry, millions of low-cost IoT sensors are manufactured without standards, never receive a firmware update, and potentially remain in service for years. In addressing device management, manufacturers of IoT sensors and solutions need to generate a lifecycle

roadmap for updating their products and end-of-life control strategies to align with the rest of IT. Unfortunately, doing so would dramatically increase the cost of devices and consumers would continue to seek a cheaper version.

Automated collection of modal analysis data is relatively new to engineering disciplines. Wired sensor networks have produced promising results over the last decade. Peiris et al [10] discuss SHM of six bridge systems in the state of Kentucky over a period of 12 years. United States regulations specify 600,000 highway bridges should be examined at regular intervals not exceeding 24 months catogorised as (1) short-term, (2) long-term, and (3) extreme event monitoring. Typically, in the absence of automated SHM, examinations would be of the manual visual method. The analysis comprised of multiple wired instrumentation sets capable of sensing tilt, strain, and acceleration, etc. The paper comprehensively outlines the lessons learned in the 12-year period. Sub-optimal choice of sensor placement, environmental noise issues, prohibitive budgets. At one site, vandalism disrupted monitoring to the extent no data was ever collected via telemetry. It is clear from the authors comments, considering the wide-ranging body of research available around sensor based SHM, there are very few papers outlining the lessons learnt from the difficulties faced by researchers when deploying monitoring systems. Knowledge which would have saved substantial amounts of time and money. One such recent paper [11] by Apaydin et al detail problems and adversities experienced through modern SHM deployments on multiple long-span bridges throughout Turkey. Live extreme events, 5.8 magnitude earthquake, during the experimental research project provided data on extreme loads at the bridge sites. Hence, recommendations are provided for future applications. The authors of [12] may have benefited from recommendations in seismic sensor sleep modes on the Golden Gate bridge (GGB) in 2006, considering the installation failed to register 3 earthquakes of magnitude 4.4 soon after installation. These publications emphasize the difficulty in deploying wired and wireless SHM. Unfortunately, very few such papers exist. In addition, with reference to proprietary monitoring installations. Despite documented success of these systems, they do not make it into the research domain due to closed algorithms and methods.

Considering WSN for SHM, wireless communication technology provides a natural eavesdropping and intervention capability to an adversary due to its broadcast nature [13]. Based on long-range wireless communication technology, WSNs utilised by IoT operating at sub-Gigahertz frequencies are capable of transmitting at extended ranges in a 10 - 15 km radius of the receiver. Anyone within the radius can observe an adequate signal and an adversary may eavesdrop. Comparatively, the attack surface of wired SHM is significantly smaller. Subsequently, WSNs are prone to traditional security risks, attacks and additionally, those exclusive to the resource constrained [14], often sparsely deployed networks further exacerbate security efforts. Moreover, retrofitting security mechanisms designed for wired networks into WSN is not scalable where computational security methods place high demands on devices. Considerable research efforts for information-theoretic security or physical (PHY) [15],[16] security techniques exist. Identified as a promising option for constrained device networks, forming a key through exploitation of state information on fading channels exchanged in establishing communication between transmitter and receiver warrants deeper research [17].

III. MOTIVATION AND RESEARCH GOALS

The motivation for this paper emerges from the observation that despite sharing a common philosophy on the benefits of SHM, a knowledge void exists. Engineering disciplines strive to automate time consuming and critical inspection tasks within their domain. To provide full coverage of structure requires deep knowledge about the nature of the structure to be monitored and the types of readings to be collected. E.g., “temperature plays a detrimental role in static (strain) and dynamic (modal) analysis of bridges. Therefore, a robust SHM strategy cannot disregard temperature compensation methods” [18]. The technological methods of measuring and collecting data from critical points provided by structural engineers are in the domain of communication and networking engineers, for developing, deploying, and advancing the sensor infrastructure. Through a partnership of these disciplines, the primary aim of the project is to accurately design and build sensing elements capable of interfacing with 802.15.4 LoRa and 802.11 ah wireless transmitters. The 802.11 ah wireless standard remains primarily untested for SHM but is strongly positioned as a technology to fill the gap [19] between Low power wide area networks (LWPAN). A superior data rate makes it possible to interrogate and collect a larger amount data from WSN nodes over the wireless network including video at a reasonable quality.

A. Method and Contribution

A medium to long-range monitoring network capable of supporting WSN infrastructure has been deployed on the campus of Ara Institute of Canterbury, Christchurch New Zealand. 802.15.4 LoRa (capable of approximately 15 kms sensing radius) and 802.11 ah (Halow) (capable of 1km radius with greater distances achieved through mesh configuration) The network is utilised to collect data from surrounding civil structures. Network engineers are responsible for access points (AP) and stations (STA) comprising the WSN. In consultation with structural and civil structure engineers for optimal monitoring locations, circuit board design will follow specifications for the Newracom evaluation board NRC7292 draft for 802.11 ah standard. Negotiations are complete on two initial civil monitoring sites less than 1 kilometer from the campus. To the south, rail infrastructure and specifically rail health will be monitored. To the north lies the construction of a 35,000-seat multi-purpose covered stadium. The stage of ground construction is almost completed. The focus here is to monitor vertical deformation due to sinking as the ground works bear the weight of the stadium under construction including the roof. We envisage expanding the monitoring networks across the city, creating numerous multi-disciplinary projects for network, electronic design, software development and structural engineering candidates from across the campus. At the time of writing, to the best of our knowledge, very few real-world

evaluations of 802.11 ah for SHM exist [20]. Furthermore, overall actual installations of 802.11 ah versus bench tests and simulations strongly favors the latter. This is partly due to delays in ratification of the standard and therefore slowing release of evaluation hardware. The Newracom NRC7292 System on a chip (SOC) is the first of its kind incorporating the 802.11 ah draft wireless standard. Subsequently, the few evaluation boards on the market utlilise the Newracom Chip. Our objective in evaluating 802.11 ah for SHM is to provide hardware testing environments designed to be flexible and adaptable for various SHM projects. However, ultimately the primary focus is to produce a trustworthy seismic evaluation infrastructure complete with analytical capabilities to firstly, accurately measure acceleration of the event. Secondly, provide accurate damage detection methods to measure vibrational response of the structure and show sensor damage evaluation in real-time. Christchurch, situated over a relatively active earthquake zone, experiences moderate shaking on a regular basis. The acceleration data is critical to our project. Additionally, in developing custom sensing elements, experimental research will include further development on the adoption of OpenFlow managed flow control for IoT security discussed in [21]. Physical layer security methods utilizing design concepts of Nain et al [22] for a Phase-Encryption transceiver design incorporating physical unclonable functions (PUF) as discussed in [23].

IV. CONCLUSION AND FUTURE WORK

In this paper, the relationship between those responsible for the ongoing development of IoT supported WSNs and the role of structural and civil engineering practitioners in designing SHM solutions was examined. Whilst the body of research on adaptation of IoT for SHM is vast, the number of works providing guidance to engineers is trivial. We concede all WSN monitoring for structures are different. Including variance from bridge to bridge. However, forming a partnership with those responsible for designing, constructing, maintaining, and eventually deconstructing is key in understanding how best to optimize WSNs for SHM. Future work and research will target development of a SHM standard in deploying IoT supported WSN.

[1] J. A. Stankovic, "Research Directions for the Internet of Things," in IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, Feb. 2014.

[2] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616-644, Firstquarter 2020

[3] Hugh Boyes, Bil Hallaq, Joe Cunningham, Tim Watson, The industrial internet of things (IIoT): An analysis framework, Computers in Industry, Volume 101, 2018

[4] Butun, I., Sari, A., & Österberg, P. (2019, January). Security implications of fog computing on the internet of things. In 2019 IEEE international conference on consumer electronics (ICCE) (pp. 1-6).

[5] Rytel, M.; Felkner, A.; Janiszewski, M. Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources. Sensors 2020, 20, 5969

[6] Mustapha, S., Lu, Y., Ng, C.-T., & Malinowski, P. (2021). Sensor Networks for Structures Health Monitoring: Placement, Implementations, and Challenges—A Review. Vibration 2021, Vol. 4, Pages 551-585

[7] Jeong, S., & Law, K. (2018). An IoT Platform for Civil Infrastructure Monitoring. Proceedings - International Computer Software and Applications Conference, 1, 746–754.

[8] Luo, Y., Chen, Y., Wan, H. P., Yu, F., & Shen, Y. (2021). Development of laser-based displacement monitoring system and its application to large-scale spatial structures. Journal of Civil Structural Health Monitoring, 11(2), 381–395.

[9] Askarinejad, Hossein & Chakraborty, A & Williamson, I. (2018). Application of IoT-based systems in seismic monitoring of structures.https://www.researchgate.net/publication/329698697

[10] Peiris A, Sun C, Harik I. Lessons learned from six different structural health monitoring systems on highway bridges. Journal of Low Frequency Noise, Vibration and Active Control. 2020;39

[11] Memisoglu Apaydin, N., Zulfikar, A.C. & Cetindemir, O. Structural health monitoring systems of long-span bridges in Turkey and lessons learned from experienced extreme events. J Civil Struct Health Monit 12, 1375–1412 (2022)

[12] L. Cheng and S. N. Pakzad, "Agility of wireless sensor networks for earthquake monitoring of bridges," 2009 Sixth International Conference on Networked Sensing Systems (INSS), Pittsburgh, PA, USA, 2009, pp. 1-4

[13] Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A Security Framework for the Internet of Things in the Future Internet Architecture. Future Internet 2017, 9, 27

[14] W. Trappe, R. Howard and R. S. Moore, "Low-Energy Security: Limits and Opportunities in the Internet of Things," in IEEE Security & Privacy, vol. 13, no. 1, pp. 14-21, Jan.-Feb. 2015, doi: 10.1109/MSP.2015.7.

[15] Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. Entropy 2017, 19, 420

[16] Poor HV, Schaefer RF. Wireless physical layer security. Proc Natl Acad Sci U S A. 2017 Jan 3;114(1):19-26

[17] J. Zhang, A. Marshall, R. Woods and T. Q. Duong, "Design of an OFDM Physical Layer Encryption Scheme," in IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2114-2127, March 2017, doi: 10.1109/TVT.2016.2571264

[18] Rizzo, P.; Enshaeian, A. Challenges in Bridge Health Monitoring: A Review. Sensors 2021, 21, 4336

[19] Baños-Gonzalez, V.; Afaqui, M.S.; Lopez-Aguilera, E.; Garcia-Villegas, E. IEEE 802.11ah: A Technology to Face the IoT Challenge. Sensors 2016, 16, 196019

[20] Adhiatma, F. N., Perdana, D., Adriansyah, N. M., & Raharjo, R. H. (2020). IEEE 802.11ah Network Planning for IoT Smart Meter Application: Case Study in Bandung Area. Jurnal Pekommas, 5(1), 11–22

[21] Edge, P., Davar, Z. and Zhang, Z., 2019, July. Software Defined Networking Managed Hybrid IoT as a Service. In ICNS 2019 The Fifteenth International Conference on Networking and Services (pp. 17-20). International Academy, Research, and Industry Association (IARIA).

[22] A. K. Nain, J. Bandaru, M. A. Zubair and R. Pachamuthu, "A Secure Phase-Encrypted IEEE 802.15.4 Transceiver Design," in IEEE Transactions on Computers, vol. 66, no. 8, pp. 1421-1427, 1 Aug. 2017, doi: 10.1109/TC.2017.2672752.

[23] M. N. Aman, K. C. Chua and B. Sikdar, "Mutual Authentication in IoT Systems Using Physical Unclonable Functions," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1327-1340, Oct. 2017, doi: 10.1109/JIOT.2017.2703088.