Location-Based Services for Security Analysis of IoT Testing Framework

Dr.P.Srimachari, Assistant Professor & Head,
Department of Computer Applications
Erode Arts and Science College (Autonomous), Erode – 638001

Dr.G.Anandharaj, Associate Professor & Head
Department of Computer Science
Adhiparasakthi College of Arts and Science,
Kalavai, Vellore – 632 506

ABSTRACT

Location information is one of the most crucial pieces of information required to achieve intelligent and context-aware IoT systems. Recently, positioning and localization functions have been realized in a large amount of IoT systems. However, security and privacy threats related to positioning in IoT have not been sufficiently addressed so far. In this paper, we survey solutions for improving the robustness, security, and privacy of location-based services in IoT systems. Typically, a WSN consists of a large number of tiny, low-cost sensor nodes that are limited in terms of their capabilities of computation, communication, memory, and power. In WSNs, energy-efficient algorithms are of paramount importance for a long lasting high throughput network. MAC protocol plays a prominent role in extending the life-time of WSNs. MAC protocols provide various schemes on how multiple nodes access a common wireless medium. To achieve a longer lifetime for the nodes and the networks, MAC protocols need to be energy-efficient and reduce the sources of energy wastage. Energy conservation in sensor nodes is generally achieved by duty cycling the radios and it is the MAC layer protocol that controls when to switch ON and OFF the radio. In this paper, we discuss the essential properties of MAC protocols, the MAC for IoT and the common causes of energy consumptions. Thereafter, we categorize the MAC layer protocols and discuss several protocols under each category in depth, emphasizing their strengths and weaknesses, giving a detailed comparison of MAC protocols. First, we provide an in-depth evaluation of the threats and solutions related to both global navigation satellite systems (GNSS) and non-GNSS-based solutions. Second, we describe certain cryptographic solutions for security and privacy of positioning and location-based services in IoT.

Keywords: IoT System, MAC protocol, GNSS, Network

I. INTRODUCTION

Internet of Things (IoT), which is the concept of pervasive interconnected smart objects operating together to reach common goals [1], has become particularly popular with the rapid development of small low-cost sensors, wireless communication technologies, and new Internet techniques. A typical application of IoT techniques includes intelligent transportation and logistics, smart home/building, environmental monitoring, medical and health care, etc. Extensive surveys of architectural elements, features and development tendencies in IoT are provided in [1] and [2].Key applications and, in particular, applications of IoT in industry are reviewed in [3] and [4]. Security has often had a low priority for vendors of IoT devices and this has led to a situation where IoT is filled with security vulnerabilities in practice. Hence, also the security and privacy of location information and an IoT enabled Location-Based Service (LBS) are often exposed to attacks. In IoT systems, context-awareness has been recognized as a significant property. Within the entire context sensing information, the location information plays important roles [5]. During the last two decades, researchers and engineers have developed a significant amount of prototypes, systems, and solutions using positioning and localization modules in IoT sensor nodes.

The *IoT device*. The device whose location is determined or used by the system. It can be smart or dumb; smart IoT devices can have a positioning engine on themselves and can support device-centric passive positioning (i.e., without sending their location to the network); dumb IoT devices can be positioned only in a network centric active approach (i.e., the network computes the device location and it either sends it back to the device or uses it for various location-based or location-aware services).

The *network* part. The part of the network that is involved in positioning and LBS. It can be further split into two either collocated or distinct parts:

- The *Location Aggregator (LA)*. This is the network part providing the location information (in network centric approaches) or the location databases (in device-centric approaches).
- The *Service Provider (SP)*. This is the network part providing the location-aware or LBS to the end-user/IoT device.

II. RELATED WORKS

Several threats are related to the training database in RSS-based localization. The database includes information about the Access Nodes (AN), i.e., the static nodes of the network. In its simplest version the information is just the location of the AN and its unique Media Access Control (MAC) address [1], while the more sophisticated versions include also information about signal propagation environment, such as coverage areas of ANs [2] or location dependent information on the probability distribution of the RSS from each of the MAC addresses [3]. The category of databases is usually based on extensive data collection.
However, the database can also be generated automatically from AN locations and taking into account the signal propagation properties of the environment, e.g., _oor and wall attenuations obtained from path-loss models and map or floor plan information [4] Cellular-based positioning solutions, covering all digital cellular standards from 2G to 4G and beyond, e.g., to the proposed 5G, have been increasingly offering more accuracy and more robustness for the positioning functionality. Most of the cellular-based approaches work in a network-centric mode, where the network, based on the measurements from the IoT device, computes the device location. More recently, standards speci_cally dedicated to IoT communications, such as LoRa [5], NB-IoT [6], eMTC or other Low Power Wide Area Network (LPWAN) standards [7], support positioning of the nodes to a certain extent. For example, in LoRA, the positioning is supported via proprietary chirp spread spectrum with time stamping of packet arrivals, plus a combination of TDOA, RSS, and Differential RSS (DRSS) estimators.

The target positioning error in LoRa is 3 m, with coverage up to 5 km range urban and up to 15 km range suburban. In NB-IoT and Narrowband Cellular IoT (NB-CIoT) standards, only the basic positioning inherited from LTE/4G is supported, such as Cell-ID and Positioning Reference Signals (PRS)-based. In Machine-to-Machine/Machine Type Communications (M2M/MTC) standards, collaborative positioning methods have been proposed [8], which may introduce an additional layer with possible vulnerabilities, the one of the inter-communication between the IoT devices. Outlier detection methods developed by statistics and signal processing communities [9] can be used to find possible problems in the training database. As the data in databases with location dependent RSS information or coverage areas include mutual dependences, the consistency of the database can be analyzed by using various outlier detection methods. With simple database including only MAC addresses and location information of the ANs, the consistency checks can be done when RSS measurements are available by comparing simultaneous measurements from multiple ANs and using theoretical coverage or path loss models and the geometry of the AN locations. For localization based on databases with RSS information, the authors of [8] propose an outlier detection method that is based on non-iterative Random Sample Consensus (RANSAC) to detect ANs from which the measured RSS is severely distorted. A crowd sensing-based management scheme for the training database is proposed in [9] where the coverage and the accuracy of the initial database are enhanced by collaboratively collected user data. Localization system for WSNs that localizes the nodes, uses outlier detection to monitor the quality of the RSS database, and updates the RSS database is proposed in [10]. The authors of [11] propose a localization scheme for RSS fingerprinting where the user's location and the ANs with erroneous measurements are jointly estimated by an online algorithm. For detecting outliers without the RSS information in the database, [12] proposes a method where distance is estimated from RSS and trilateration residuals and hypothesis testing is used.

ThingML is developed as a domain-specific modeling language which includes concepts to describe both software components and communication protocols. The formalism used is a combination of architecture models, state machines, and an imperative action language [5]. ThinkML is supported by a set of open source tools that are built using the Eclipse Modeling Framework. APPARATUS was developed for security analysis of IoT systems. As such it requires concepts that can be used to express “things”, services, threats but also the social aspects of IoT systems. On the other hand, ThingML was developed to model the hardware, software components and communication protocols of IoT systems. It does not have concepts to model social or security components of IoT, such as users, stakeholders, threats or vulnerability. ASSIST is an agent-based simulator of Social Internet of Thing (SIoT) [6]. The idea behind SIoT is that smart objects will connect with each other to form social networks. ASSIST uses an agent-based approach by defining three types of agents. Device Agents, Human Agents, and Task Agents. While ASSIST can be used to express the social components, it was not designed with security analysis in mind. As such it cannot be used to express security components. SenseSim is an agent-based and discrete event simulator for IoT [7]. It can be used to simulate heterogeneous sensor networks and observe the changing phenomena. The simulator using a perception model understands phenomena such as weather changes, fires or car traffic and can react according to them. SenseSim was developed to augment the perception of sensor networks. While those networks can be configured to react to security threats, the tool was not designed to facilitate security analysis.

III. PROPERTIES OF MAC PROCEDURE FOR INSTRUMENT SYSTEMS

A. Attributes of MAC Protocols

Energy efficiency is the most important attribute of MAC protocols for sensor networks. With the limited volume of energy storage, sensor nodes are required to function for a very long time. MAC protocols achieve energy efficiency by turning off the radio when the node is not transmitting or receiving. An ideal energy-efficient node would be one that sleeps most of the time and wakes up just to transmit or receive user data without any overheads.

Energy efficiency directly influences network lifetime. Scalability and adaptability refer to the ability to accommodate changes in network size, node density, and topology. These changes can be attributed to mobility and failure of nodes. End-to-end latency refers to the delay from when a sender has a packet to send to the time it is received by the final receiver. Throughput refers to the amount of data that is successfully received by a receiver from a sender.

B. Causes of Vitality Inefficiency

Energy is wasted when a radio is active while it is actually not doing anything useful or doing something redundant. As an example suppose two nodes A and B are communicating with each other where node A is a sender and node B is a receiver node. After a certain period of time node B assumes that the transmission from node A is finished and it goes to sleep mode. While node A has not finished with the data transmission and still has data packets for node B.

In this case, energy wastage will occur as the node A will keep transmitting while the node B is in sleep mode. These activities of radio's are redundant when nothing useful is done and energy is simply wasted. There are a few sources of energy wastage that may be attributed to the MAC protocol scheme.

The collision causes corruption in data transmission and therefore the corrupted packets need to be discarded. These packets need to be re-transmitted, consuming energy and may cause another round of collisions. Collision increases latency as well. *Idle listening* refers to listening to a channel without actually receiving data. This happens when the radio is awake just listening to an idle channel. *Overhearing* refers to nodes receiving packets that are intended for other nodes.

To implement this idea, the test system provides an *agent* which is a secured communication wrapper for the *IUT*. When the *IUT* connection is established through the agent, the test system creates an isolated room for testing. When the configuration of the environment is finished, *test execution script*, generated from the test description, is executed. This execution consists of three phases: STIMULI to trigger *IUT* to initiate a specific behavior CHECK to validate communication, for example, to capture contents of a packet, and VERIFY so that *IUT* would reflect the desired result.

The *Testing Analysis Tool* veri_es the output data and behavior after communication. The tool then generates a verdict for the test from PASS, FAIL, and INCONCLUSIVE. The test system has its own packet generator for input generation and provides a web interface to allow status checking and testers to manually input decisions or commands when needed as part of a test. The architecture of F-Interop is designed to handle the entire process of IoT interoperability testing, with a focus on the testing administration and related tasks including capturing a trace and reporting the verdicts.

All of these operations are controlled and coordinated by *Orchestrator* which administrates the cooperation of different testing components: test session, message broker, and access control. Communications are encrypted and managed by Event Bus. They include control messages, data, and log packets being transmitted to the central Event Bus which is implemented in RabbitMQ.

This centralized communication architecture ensures the independence of each component, with the messages containing routing keys and topics to indicate how to route messages to the relevant input queues of the components.

C. Testing models of IoT interrupt.

To reflect the scale and heterogeneity of IoT deployments, the IoT test system has to support different configurations which can be handled by the tested federation. Five test configurations have been identified as follows:

Simple Conformance Testing. Tests the conformance of a single IUT. Only functional behavior of an IoT device or platform interfaces are checked. This model is suitable for individual testing of an IUT.

Simple Conformance and Interoperability Testing. Tests conformance and interoperability of a single IUT with a unique testbed in the test system. This is the basic model for testing a new IUT within a standardized tested providing a reference implementation.

Simple Conformance and Compound Interoperability Testing. Tests conformance and interoperability of a single IUT with multiple tested in the test system. This is a suitable model for testing a new IUT when no reference implementation has been identified.

Compound Conformance Testing. Tests conformance and interoperability of multiple IUTs with no tested. This is a model for testing cooperative and collaborative behavior of multiple IUTs.

Compound Conformance and Compound Interoperability Testing. Tests conformance and interoperability of multiple IUTs with multiple tested in a test system. This is a model for highly interconnected environments between IUTs and tested.

IV. SECURE AND PRIVACY-PRESERVING POSITIONING IN IoT

This surveys cryptographic techniques that can be used for protecting location information and secure localization in IoT. Although work designed specifically for secure IoT localization is still mostly missing, we can utilize existing schemes originally designed for applications that are closely related or included in the IoT framework, such as (military) WSN or RFID.

The IoT inherits many of the threats of the previous applications but, e.g., the heterogeneity of devices that are connected into the same worldwide network and the sensitive nature of location information (e.g., persons' movements) handled in applications also set new challenges.

LOCATION INFORMATION

Assume that a device (e.g., a beacon node or a user's personal device) knows its location (e.g., has a GNSS chip), which it and the network trust to be correct up to necessary precision, and the device wants to share this information with some other devices (e.g., regular nodes or cloud service provider) over the network (i.e., the Internet) in a secure manner. In this case, location information can be treated similarly as any other critical piece of information and standard cryptographic techniques can be used for securing communication. The other devices can trust the correctness of the location information only if they can verify its authenticity and integrity. The former means that the location information was truly sent by the device claimed to be the source and not by a malicious party claiming to be the correct source.

The latter means that the information has not changed on the way. The former implies the latter, but not vice versa. The authenticity and integrity of location information can be ensured with standard cryptographic techniques. Computing a check sum by using a (cryptographic) hash function (e.g., SHA-256 [126]) gives integrity, but without additional techniques only against transmission errors (i.e., no security). If the parties have a shared secret key, they can use cryptographic message authentication to ensure both integrity and authenticity (see, e.g., HMAC [127]). Digital signature schemes based on public-key cryptography (e.g., (EC)DSA [128]) allow verification of authenticity and integrity without shared secrets. Additionally, digital signatures provide non-repudiation, which prevents a sender from later challenging sending the message. This can be an important feature also in the context of location information because it ensures that a device that has claimed to be at a specific location cannot later refuse this claim. The above schemes provide only authenticity and integrity of location but the location information itself is, by default, transferred as plain text and is available to anyone observing traffic in the network.

The simplest form of privacy of location information (i.e., privacy in respect to third parties) can be achieved by ensuring confidentiality of location information transferred in the network. Confidentiality can be achieved by encrypting the location information, again, with standard cryptographic techniques. Encryption can be performed either with secret-key cryptosystems, which require that the communicating parties have securely shared a secret key, or with public-key cryptosystems, where the key used for encrypting is public (anyone can encrypt) but decryption is possible only with the secret key of the receiver.

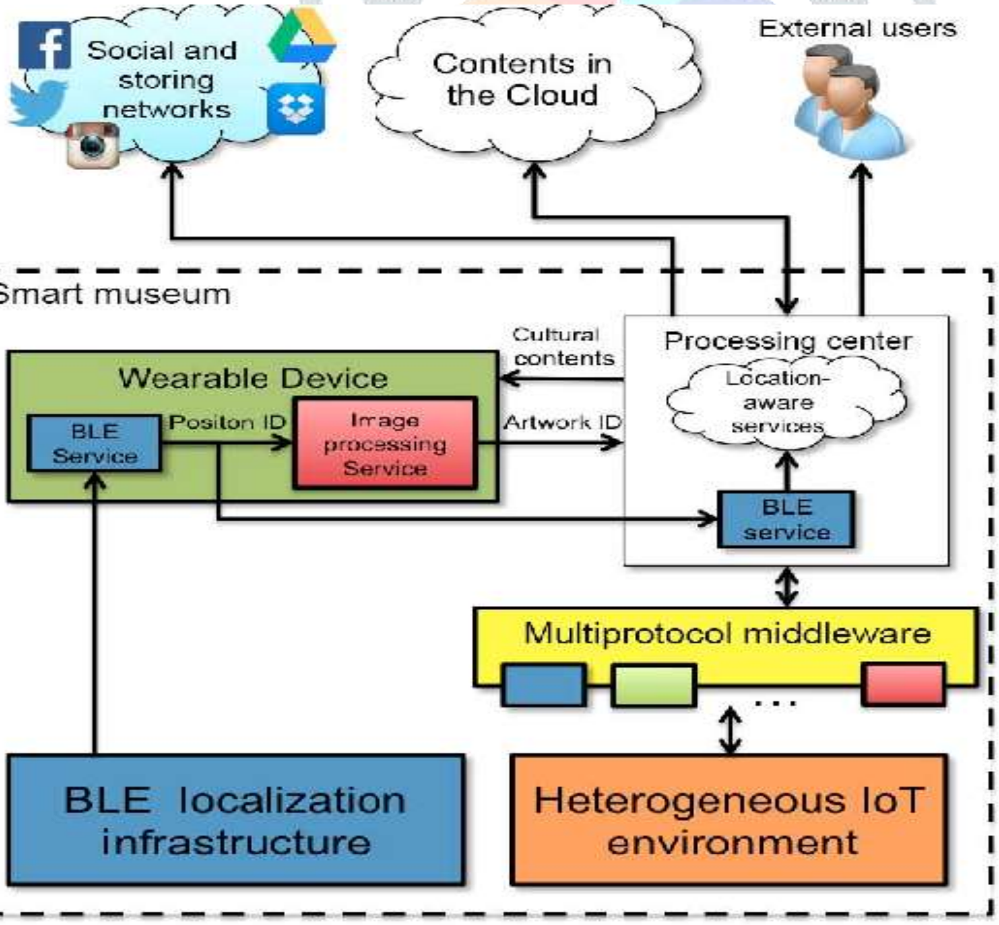

Figure 4.1 Location – aware system

V. FUNCTIONALITY OF ASTO

The tool is developed using a modular approach. Each module contains everything necessary to execute only one aspect of the desired functionality. The packages are divided into Global packages, Design phase packages and Implementation phase packages. The Global packages are shared between the design and implementation phase analysis. The Design phase packages can only be used for the design phase analysis, while the Implementation phase packages are used only for the implementation phase analysis. Design phase and Implementation phase packages provide similar functionality to the tool but use different meta-models as an input for their analysis.

- ***Global packages:*** Global packages provide the majority of the functionality of the Tool. Global packages are divided into two parts. Style and Analysis packages. Style packages are used to configure the appearance of the tool. This was made to enable users with disabilities to configure the tool according to their needs. Analysis packages are used to perform analysis on the IoT graphs.
- ***GUI configuration:*** every element in the GUI of the application is configurable. A user can change the color values of the elements, the font style, and size or choose to which elements of the GUI to display.
- ***Graph configuration:*** the style of the graph is configurable. A user can change the size, color, and shape of the nodes. The size, style, and color of the edges, along with the font style, size and color of graph's labels can be changed.
- ***Graph manipulation:*** the tool supports manipulation of the graph in a graphical manner. The user can move nodes, add nodes and edges and make changes on the properties of the nodes.
- ***Highlight nodes:*** the desired nodes are highlighted while the rest of graph has its opacity reduced.
- ***Highlight modules:*** the nodes that are part the same meta-model module are highlighted. For example, the engineer can choose to highlight only the network module nodes or the security module nodes.
- ***Highlight neighbors:*** the neighbors of the selected node are highlighted.
- ***Attribute search:*** the nodes with the selected attribute are highlighted.
- ***Flag properties:*** the nodes that have the specified properties are highlighted. This functionality is useful when looking for patterns in the graph. For example, we might be interested in all the *Devices* that use *wireless network connection* which support the *telnet* communication protocol.
- ***Hover node information:*** while covering a node, its properties are displayed in an adjacent container.
- ***Layout placement:*** the layout of the graph can be configured using placement algorithms. Those algorithms are provided by the Cityscape library
- ***Export/import models:*** the graphs can be exported or imported as JavaScript Object Notation (JSON) files.
- ***Threat verification:*** the tool can verify if the identified Threats are mitigated by Constraints. The package displays an overview of the number of Threats of the graph along with the mitigated Threats number.
- ***Model checking:*** graphs are validated according to the rules of meta-models of the tool in an asynchronous manner.

VI. CONCLUSION

In IoT, various devices are exchanging information with each other without human interaction and computing the information intelligently. Context-awareness is a significant property of IoT and location information and LBS play important roles in such systems. We then described certain cryptographic solutions for security and privacy of location information, localization and LBSs in IoT. Furthermore, we discussed the state-of-the-art of policy regulations regarding security of positioning solutions and legal instruments to location data privacy. We also reviewed our concerns and gave recommendations for developing more secure and privacy-preserving localization and LBSs for the future IoT. Our survey shows that many solutions are available for improving robustness, security and privacy of LBSs in IoT. Often they come with significant overheads and require specialized expertise to be implemented correctly which, arguably are reasons why they are not included at the moment. Nevertheless, certain open problems also exist, in particular, in topics such as adapting existing solutions to the IoT framework of interconnected heterogeneous devices, secure localization in presence of powerful malicious adversaries, and privacy-preserving LBSs. TDMA and FDMA, in depth, emphasizing their strengths and weaknesses. This classification of WSN MAC protocols aims at identifying recent research trends in the design of MAC protocols. We have also presented design trade-offs between some of the MAC protocols with respect to various matrices such as mobility, energy awareness, QoS, scalability and so on.

REFERENCE:

[1] L. Atzori, A. Iera, and G. Morabito, ``The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787_2805, Oct. 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ``Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645_1660, 2013.

[3] E. Borgia, ``The Internet of Things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, pp. 1_31, Dec. 2014.

[4] L. Da Xu,W. He, and S. Li, ``Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233_2243, Nov. 2014.

[5] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, ``Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414_454, 1st Quart., 2014.

[6] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for iot," in *2011 International Conference on Multimedia Technology*, 2011, pp. 747 –751.

[7] W. Miao, L. Ting-lie, L. Fei-Yang, S. Ling, and D. Hui-Ying, "Research on the architecture of internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, vol. 5. Chengdu: IEEE, 2010, pp. 484–5. F-Interop_Online platform of interoperability and performance tests for the Internet of Things," in *Proc. Int. Conf. Interoperability IoT*, 2016, pp. 49_55

[8] P. Cousin, ``White Paper on _exible approach for semantic validation in the context of Internet of Things," Easy Global Market, Valbonne, France, White Paper, 2016. [Online]. Available: http://www.eglobalmark. com/white-paper-_exible-approach-semantic-validation-context-internetthings

[9] E. S. Reetz, D. Kuemper, K. Moessner, and R. Tönjes, ``How to test iotbased services before deploying them into real world," in *Proc. 19th Eur.Wireless Conf. (EW)*, 2013, pp. 1_6.

[10] S. De, F. Carrez, E. Reetz, R. Tönjes, and W. Wang, ``Test-enabled architecture for IoT service creation and provisioning," in *The Future Internet Assembly* (Lecture Notes in Computer Science), vol. 7858, A. Galis and A. Gavras, Eds. Berlin, Germany: Springer, 2013, pp. 233_245.

[11] Gluhak, S. Krco, M. Nati, D. P_sterer, N. Mitton, and T. Raza_ndralambo, ``A survey on facilities for experimental Internet of Things research," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 58_67, Nov. 2011.

[12] Shala, P. Wacht, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, ``Framework for automated functional testing of P2P-based M2M applications," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 916_921

[13] P. Rosenkranz, M. Wählisch, E. Baccelli, and L. Ortmann, ``A distributed test system architecture for open-source IoT software," in *Proc. Workshop IoT Challenges Mobile Ind. Syst.*, May 2015, pp. 43_48.

[14] D. Kuemper, E. Reetz, and R. Tönjes, ``Test derivation for semantically described IoT services," in *Proc. Future Netw. Mobile Summit (FutureNet-workSummit)*, 2013, pp. 1_10.

[15] M. Vögler, J. Schleicher, C. Inzinger, S. Nastic, S. Sehic, and S. Dustdar, ``LEONORE_Large-scale provisioning of resourceconstrained iot deployments," in *Proc. IEEE Symp. Service-Oriented Syst. Eng. (SOSE)*, Mar. 2015, pp. 78_87.

[16] S. Moseley, S. Randall, and A. Wiles, ``Experience within ETSI of the combined roles of conformance testing and interoperability testing," in *Proc. 3rd Conf. Standardization Innov. Inf. Technol.*, Oct. 2003, pp. 177_189.

[17] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[18] Z. Qin, Y. Gao, and C. G. Parini, "Data-assisted low complexity compressive spectrum sensing on real-time signals under sub-Nyquist rate," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1174–1185, Feb. 2016.

[19] Z. Quan, S. Cui, A. H. Sayed, and H. V. Poor, "Optimal multiband joint detection for spectrum sensing in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 57, no. 3, pp. 1128–1140, Mar. 2009.

[20] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116–130, 1st Quart., 2009.

[21] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[22] W. Zhang, R. K. Mallik, and K. B. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5761–5766, Dec. 2009.

[23] C. J. Miosso, R. Von Borries, and J. H. Pierluissi, "Compressive sensing with prior information: Requirements and probabilities of reconstruction in $l0$-minimization," *IEEE Trans. Signal Process.*, vol. 61, no. 9, pp. 2150–2164, May 2013.

[24] N. Vaswani and W. Lu, "Modified-CS: Modifying compressive sensing for problems with partially known support," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4595–4607, Sep. 2010.

[25] P. Feng and Y. Bresler, "Spectrum-blind minimum-rate sampling and reconstruction of multiband signals," in *Proc. IEEE Int. Conf. Acoust Speech Signal Process. (ICASSP)*, vol. 3. Atlanta, GA, USA, May 1996, pp. 1688–1691.

[26] J. Matoušek, "On variants of the Johnson–Lindenstrauss lemma,"*Random Struct. Algorithms*, vol. 33, no. 2, pp. 142–156, Sep. 2008.

[27] O. E. B. Nielsen and D. R. Cox, *Asymptotic Techniques for Use in Statistics*, 1st ed. London, U.K.: Chapman and Hall, 1989.

[28] Ning Xu *et al.*, "A Wireless Sensor Network for Structural Monitoring," presented at the Proceedings of The 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004,

[29] K. Langendoen and G. Halkes, "Energy-Efficient Medium Access Control," in *Embedded Systems Handbook*, R. Zurawski, Ed.: CRC press, 2005.

[30] L. Lin, K.-J. Wong, A. Kumar, Z. Lu, S.-L. Tan, and S. J. Phee, "Evaluation of a TDMA-based energy efficient MAC protocol for multiple capsule networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, p. 54, 2011.

[31] P. Naik and K. M. Sivalingam, "A Survey of MAC Protocols for Sensor Networks," in *Wireless Sensor Networks*, C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Eds. Boston, MA: Springer US, 2004, pp. 93-107.

[32] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 115-121, 2006.

[33] K. Kredo Ii and P. Mohapatra, "Medium access control in wireless sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 961-994, 3/14/ 2007.

[34] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC Essentials for Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials,* vol. 12, no. 2, pp. 222-248, 2010.

[35] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 15, no. 1, pp. 101-120, 2013.

[36] M. Zhao, P. H. J. Chong, and H. C. B. Chan, "An energy-efficient and cluster-parent based RPL with power-level refinement for low-power and lossy networks," *Computer Communications,* vol. 104, pp. 17-33, 2017/05/15/ 2017.

[37] R. Oma, S. Nakamura, T. Enokido, and M. Takizawa, "An Energy-Efficient Model of Fog and Device Nodes in IoT," in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2018, pp. 301-306.