Security Analysis of IoT Networks and Platforms

Stephen Ugwuanyi
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

James Irvine
Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—With the recent increase in the adoption of Internet of Things (IoT) technology globally, cybersecurity-related issues have been raised, particularly with the limitations of IoT devices, privacy and other security standards guiding IoT development as wireless technology evolves. With the enterprise and the massive IoT market expected to reach $7.6 B and $1.2 B in 2024 respectively, according to Gartner, and several operational vertical IoT use cases and platforms experiencing cyber vulnerabilities. Based on the findings from our recent LPWANs IoT testbeds and their operational performance in certain use case scenarios, this paper summarizes the key wireless technology security requirements for IoT deployments. We first compare the security requirements of legacy and emerging IoT technologies as it relates to smart city applications and examined the effectiveness of the existing countermeasure opportunities as it affects the overall system performance in critical and non-critical machine type communications. We concluded by recommending countermeasures opportunities and frameworks to secure industrial IoT platforms to cope with future cybersecurity vulnerabilities.**

Keywords—Deployment, Industrial, Internet of Things, Narrowband, Platforms, Security

I. INTRODUCTION

There is a global drive to adopt the Internet of Things (IoT) technology in every aspect of human life in recent time, as it tends to facilitate efficient and reliable information exchange and data sharing. Various physical devices and communication protocols have been used to facilitate communication in Human-to-Human (H2H), Human-to-Device (H2D), and Device-to-Device (D2D) interactions. In most of these applications, known and emerging issues of privacy and security vulnerabilities puts IoT security at the centre of cybersecurity researchers. In this paper, we will be making references to IoT enabling technologies from different perspectives: consumer and industrial domains; critical and non-critical applications; local and international; each with specific security challenges and countermeasure opportunities examined.

Generally, IoT technology has been widely used in various sectors for several reasons. In the health care sector to detect medical severity of patients [1] and [2]. Similarly, IoT has been used in the transport sector [3], utilities and smart cities [4], and smart agriculture [5], etc to tackle specific use case challenges. In [6], an IP-based next-generation open smart grid measurement and visualization platform are used to obtain real-time data from Phasor Measurement Units (PMUs). Such real-time information presents an opportunity to predict future anomalies in the grids, analyze the grid generation mix, and ascertain demand levels. The platform has the potential to expose the grid to a wide range of external exploits without any aspect of the implementations involving security. The growing roles of constrained physical devices like industrial PMUs, sensors and actuators in the IoT communication architecture cannot be overemphasized especially in critical applications.

Security remains one of the biggest issues today in the IoT world and it is yet to be addressed both in the cloud and at the edge. In the IoT network, the tasks of guarding totally against an exploit are becoming more complicated. The security lapses are driving research into identifying vulnerability types as they evolve. Security threats such as BadRabbit [7], Wanna Cry [8] and Petya/Goldeneye [9] often grouped as cybersecurity attacks (external), malicious attacks (internal), and aided by human errors or negligence (internal) are always targeted at the critical infrastructure to compromise their operational efficiency, safety, productivity, asset control and reliability. These attacks have usually focused on the industrial network router links and edge IoT devices.

Various security algorithms have been proposed as ways of combatting known/emerging IoT security attacks, but past and recent successful attacks which can emanate from human errors depict otherwise. Towards the end of 2019, Wyze exposed around 2.4 million private IoT cloud data database online unnoticed for a few weeks as a result of Amazon Web Services platform security protocol being turned off in error [10]. To ensure a high level of security in IoT networks, we outlined and compared the different security requirements for known IoT technologies and platforms, establishing a baseline for securing constrained IoT modules in a network.

The paper focuses on the security of wireless technology for enabling large scale IoT deployment and it is structured as follows: Section I presents the background information on IoT security; Section II discusses the general security requirements for industrial and consumer-based IoT applications; Section III presents security analysis of IoT platform technologies with focus on LoRaWAN and NB-IoT/LTE-M for industrial application; Section IV analyses the general IoT security countermeasures; Section VI presents the IoT security benefits in a smart grid; and Section VI concludes the paper with key IoT security findings.

II. IOT SECURITY REQUIREMENTS

The growing number of cybersecurity disruptions globally is partly due to more industrial IoT devices such as sensors and actuators increasingly connected to the internet with the deployment scaled differently in different literature. Estimated to surpass 20 billion devices [11] and [12]; 30 billion [13]; 10 billion [13]; and 50 billion [14], [15] and [16]. The varied assertions on the future capacity of IoT deployment indicate the need to develop a good security framework considering the huge potential market value and the growing complexity of IoT technology [17].

The general concept of IoT security is to successfully bridge the connectivity, vulnerability and compatibility gaps between Operational Technology (OT) and Information Technology (IT). An industrial framework for increasing IoT visibility that has introduced security issues such as link

This research is funded by the Nigerian Petroleum Technology Development Fund (PTDF) award number PTDF/ED/PHD/USO/1092/17

978-1-7281-5628-6/20/$31.00 ©2020 IEEE

establishment, authentication, key agreement and encryption method in IoT applications and services. Security in the industrial domain was initially referred to as '*safety'* (meaning, the protection of industrial workers and machines) [17], [18] when not associated with the IT world. Implying that the development of IoT solutions for Cyber-Physical Systems (CPS) should be a convergence of OT and IT requirements. IT domain has been identified as a dangerous platform [19] such that smart connected devices can be used to compromise industrial systems. The security procedure in such a network environment should capture the hardware, networking, application-specific requirements and third parties' aspects of the ecosystem.

Research exists in the field of IoT that focuses on addressing some of these security issues. In [18], the cryptographic algorithms and security protocols such as microkernels, sandboxes and virtualization tools failed to tackle notable security breaches in the industrial environment as new IoT solutions are mostly developed for companies to offset their resource limitation without prioritizing security. Security is seen as the major component to be considered by the industrial sectors before the full deployment of IoT [20]. This view is perceived differently on the consumer-based IoT solutions where security is mostly not a priority. The security requirements of the industrial IoT network are not limited to, as categorized in the following literature [15], [13], [21] and [22]. The order of IoT security requirement is different from the IT perspective. However, previous studies have adopted the IT requirements into the OT IoT security domains. [23] adopted the Confidentiality, Integrity and Availability (CIA) IT model of security analysis and countermeasures. To secure IoT network, we recommend that the following security requirements should apply:

A. Confidentiality

The idea of confidentiality in the IoT context is the restriction of access to IoT data to authorized devices and users only. The cryptographic goal of IoT device data confidentiality is to encrypt all data and restrict access to only the desired recipient using strong encryption schemes like Advanced Encryption System (AES).

B. Integrity

Integrity ensures that IoT configurations, software and data logs/updates are verifiable, remains unchanged, be in the correct format and are not compromised over time at any point across the network. The accuracy, consistency and trustworthiness of IoT data may be difficult to guarantee throughout the IoT life cycle. In [18], the integrity check could only secure the system during the boot process. A hybrid approach ensures that industrial IoT nodes-to-node data is not tampered with by any malicious code injections [24]. The computational limitations of IoT modules affect how Secure Hash Algorithm (SHA) which provides integrity checks are implemented. Edge computing enabled by parallel processing is what we see as the research direction.

C. Availability and Reliability

Making IoT technology part of a process control network should accommodate a very small amount of downtime. IoT devices must be available at all time irrespective of whether the system is compromised or not. Asymmetric scheduling policy and interrupt sources can provide a high-level of IoT service availability and reliability.

D. Mutual Authorization and Authentication

Industrial IoT devices must have a reliable means of authorizing and authenticating themselves in a network. From our LoRaWAN test network, see Fig. 1, server-generated keys are used to authenticate and authorize D2D communication. To avoid malicious node injections, the IoT devices on the other side of the communication channel must in turns generates cryptographic keys based on the received security features to validate each other before sharing data. In our narrowband IoT network, see Fig. 2, the random-access authentication procedure is one security scheme used to prevent malicious node injections. It affects the IoT module power consumption and the data transmission overhead, which is a problem in the large-scale IoT environment for economies of scale. Quantum resistance access authentication and data distribution have been used to provide stronger privacy in large scale NB-IoT D2D communication [25]. D2D authentication is necessary to maintain a legitimate communication link between entities and enforces non-repudiation.

E. Privacy

Privacy in the IoT ecosystem has a wide definition. Privacy is needed to protect the backward and forward secrecy of new and existing IoT devices in a network. The privacy of IoT devices participating in a group-based communication managed by Service Network (SN) is achieved using User Equipment (UEs) pseudonym [26]. The emergence of many SNs and IoT devices with mobility needs will affect the performance of the scheme.

III. IoT Platforms

IoT platforms are the user-centric visualization middleware of the IoT value chain that has found increased application in all fields. They provide opportunities for IoT users to carry out data analytics of virtualised device. IoT Platforms needs and objectives vary from one use case to another and depend on several factors such as the hardware capabilities, the cloud infrastructure, the wireless technology on which the network is built, the nature of deployment, management strategy, etc.

IoT platform development has not been standardized. However, IoT platform visibility is seen in various fields becoming very relevant in the domestic and international domains leveraging on MQTT, Web socket, and other protocols. Interest group such as the Web of Things is developing a standard for a common IoT platform that is open to all use cases. IoT platform security framework differs for both local and international platforms and is mostly encryption-based for authentication and authorization. The current Local IoT platforms as outlined in [10] are Thingplug, GiGa IoT Maker and ARTIK developed based on Open Connectivity Foundation (OCF) – based authentication and oneM2M. The international commercialized IoT platforms include the Google Cloud, Microsoft Azure, Ayla Agile, SAP Cloud, PTC Thing Worx, Amazon Web Service, etc. [27] that provides data aggregation, visualization and analytics services.

Web platforms are few of either in an open and closed solution and the choice is mostly based on the application needs and costs. The selection of the right platforms is based on various reasons. In [28], the basis of IoT platform selection criteria was based on the technical offerings, strategy, market presence and compliance. We present the security

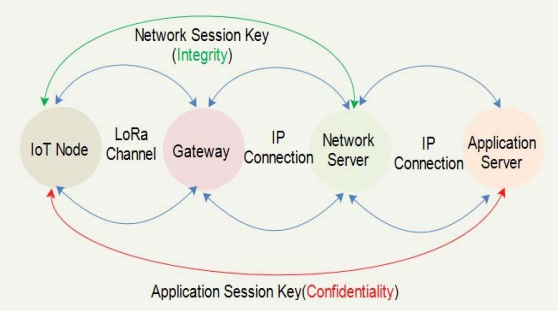

Fig. 1 LoRaWAN IoT Platform

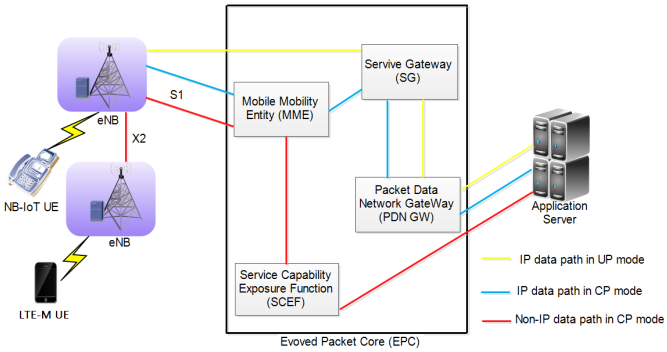

Fig. 2 NB-IoT/LTE-M Platform

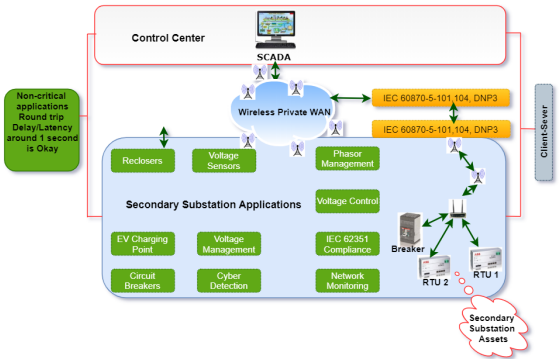

Fig. 3 Smart Grid Platform

considerations in our IoT test platforms based on LoRa and cellular technologies.

A. LoRaWAN

A standard LoRa platform consists of two major parts; the front-end and the back-end. LoRaWAN platforms are built based on two different technologies; Over the Air Activation (OTAA) and the Activation by Personalization (ABP). The security of a LoRaWAN platform as presented in Fig.2 ensures that D2D authentication, integrity and confidentiality is delivered. However, there is a distinction in the security vulnerability surfaces for applying public or private deployment scenario. Public LoRAWAN IoT Cloud Platforms such as the thethings.io, hIOTron, ResIoT, (open source: ThingsBoard, MAINFLUX) uses HTTPS, MQTT-S and CoAP protocols. Integrating LoRaWAN and 4G/5G platforms require the modification of the gateway [13]. The concept of USIM will improve how the security keys will be stored.

B. NB-IoT/LTE-M

Narrowband Internet of Things (NB-IoT) and Long-Term Evolution for Machine (LTE-M) are LPWAN technologies for connecting low bandwidth (non-critical) requirement IoT devices. NB-IoT is a special Cellular Radio Access (CRA) interface in the 3GPP Releases 13 and 14 [29] that comes with a small modification of a legacy LTE and GSM networks. It shares the basic radio principles with the regular LTE system which helps with the integration of NB-IoT carriers with the LTE cells. Examples of the shared principles are the duration of the radio frames, the time slots, the communication between the core networks and the number of symbols. Elements of the technology such as synchronization signals and broadcast of the System Information Block (SIB) are done differently, introducing a new radio interface in the Evolved-UMTS Terrestrial Radio Access Network (E-UTRAN).

Similarly, LTE-M is an industrial IoT technology designed for enhanced Machine-Type Communication (eMTC) specified in the 3GPP studies provisioning different LTE categories: Cat-0 in Release 12, Cat-M1 in Release 13 and Cat-M2 in Release 14. It relies on existing LTE infrastructure and design actions such as a software upgrade in the base station and the EU to thrive. With LTE-M data rates higher than LoRa and NB-IoT networks at both the uplink and downlink channels, LTE-M platform has the potential to be adopted more widely. In most of the implementations, LTE-M and NB-IoT support data transmission at a Maximum Coupling Loss (MCL) of 156 dB in 1.4 MHz bandwidth and 164 dB in 200 kHz bandwidth respectively [30].

Our cellular NB-IoT/LTE-M platform as shown in Fig.2 employed a functional Amarisoft wireless protocol stack based LimeSDR (LMS7002M) hardware as the radio front-end to generate the standard core LTE and NB-IoT base station physical signals on the same processor and pycom IoT modules as the UEs. The security features of the platform are based on multiple Non-Access Stratum (NAS) and Access Stratum (AS) ciphering and integrity algorithms existing between the UE and the eNB and MME respectively as inherited from LTE system. The security architecture as specified in the 3GPP Release 10 [31], indicates that the security configuration level depends on the UE capabilities [32] in addition to other requirements as described below:

1) Security Requirements: In [27], NB-IoT security relied on SNOW 3G encryption to provide data confidentiality and on ATR-128 for secure inter-mobile network data transfer. In our platform, the UE supports Secure Hash Algorithm (SHA), Message Digest 5 (MD5), Digital Encryption System (DES) and Advanced Encryption System (AES). AES is used for encrypting sensor payload before transmission, guaranteeing IoT security attributes such as privacy, confidentiality, data freshness, authorization and integrity as they are crucial in all sensitive IoT use cases. Alleged Rivest Cipher 4 (ARC4), Hash-based Message Authentication Code (HMAC), Random Number Generator (RNG), Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) are other IoT security schemes at the silicon and code level. The cellular IoT platform security framework relates to hardening of IoT products, securing communication links, complying with international standards, enforcing management policy, trusting of third-party services and software, implementing key management frameworks and embedded security techniques. Following from [34] classifications, we present the general IoT platforms security into three layers:

a) Perception Layer: Perception layer is the actual location of the IoT modules where their interconnectedness, energy consumption, data gathering and communication capabilities are handled. An attack targeted at this part of the network can modify IoT device programs or steal the device information. This can occur in the forms of reverse engineering, traffic analysis, node replication, message tampering, social engineering, eavesdropping, physical compromise, and Radio Frequency (RF) interference. An attack can also occur through the wireless network connecting all the devices. In [34], these types of attack are classified into active and passive with the active attack having far-reaching implications. Security measures such as encryption, authentication and integrity verification are commonly used. Stream cipher and block cipher are proposed for this layer in [35] to preserve the battery life and reduce processing delays at the terminals. In our test network, the IoT modules communicate with the NB-IoT/LTE-M enabled base station depending on the configuration contrary to the multiple gateways that introduce routing problems in the other IoT network such as in LoRa and Sigfox. The concern around this implementation is the potential impact of pseudo-IoT base stations in a bidirectional communication between base stations and IoT terminals.

b) Transmission Layer: This is probably where the second most types of attack experienced in IoT networks occur. The attacker is usually miles away from the target system relying on the knowledge of routing and security protocols for traffic, node, and routing exploits. Routing and transmission problems differ in NB-IoT/LTE-M from other LPWANs. In NB-IoT, multi-networking and extra cost introduced by the gateways is eliminated. On the other hand, the single base station providing support for thousands of nodes means that node authentication and access control if not properly managed will give room for malicious code injection. Similarly, the total dependence on an open wireless network presents challenges such as network interferences, end-to-end authentication since the terminals are not user-assisted. Having an intrusion detection and protection system added to the based station will reduce these risks. We recommend the profile establishment of a certain group of IoT nodes in a network from their previous, normal and abnormal operation scenarios.

c) Application Layer: The data generated by the heterogeneous network of IoT devices are aggregated at this service layer. A great deal of these data originates from memory, power and processing constrained device that cannot be pre-processed on the node. Edge computing technologies allow IoT devices to process their heterogeneous data logs, ensuring authenticity, confidentiality and integrity. Virtualization technology such as Docker containers is increasing used to enable edge computing. Data security mechanisms, Access Control List (ACLs) policies and permissions, firewalls, security software and layers trust management are the application layer countermeasure opportunities.

C. 5G

The Fifth Generation (5G) technology is an evolving wireless platform designed to meet the security requirements of protecting ubiquitous IoT devices from all forms of vulnerabilities, deliver services at low latency and improves user experience at a higher data rate. 5G platform evolved with new security and privacy issues at the MAC and PHY layers different from the radio bearer security in the older generations [36]. In 5G environment, massive machine-type communication with higher user density and capacity is achieved, hence, presenting new security requirements and challenges when compared to other wireless technologies. Among the core requirements of 5G design is an improvement on the security as applied to the internet of things.

Some of the security benefits of the platform include; infrastructure and service user metadata protection, information filtering, application security, user/infrastructure security and privacy, and multi-context security encryption. The core 5G security challenges revolve around how Network Function Virtualisation (NFV), Edge Computing (EC), Network Slicing (NS), Multi-Input Multi-Output (MIMO) and Software Defined Networking (SDN) are implemented [37]. Other issues are the cost of delivering the required security at high bandwidth and low latency with high-security requirements, Control and User Plane Separation (CUPS), Security Computational Overheads (SCO), Spectrum Congestion (SC) and interferences. Spectral Efficiency Frequency Division Multiple (SEFDM) is a new bandwidth compression technology explored for efficient use of wireless spectrum in meeting the connectivity vision of the Internet of Things in 5G and 6G era. In [38], a novel SEDM study achieved a 60% compression of signal bandwidth, but with significant inter-carrier interference and multi-path effects.

IV. KEY SECURITY COUNTERMEASURES

The layer 3 state-of-art security measures for data transmission in IoT networks are discussed in this section. This is to ensure secure remote communication between IoT modules over platform types which will rely on IP networks for economies of scale.

A. IP Security

Internet Protocol (IP) Security (IPSec) is a layer-3 end-to-end tunneling security scheme for encapsulating, authenticating and encrypting data payloads when connecting industrial IoT infrastructure through public or private networks. IPSec algorithm functions by encapsulating data overheads (headers and trailers) on the data payload adequately in the form of Encapsulating Security Payload (ESP), authenticating transmitted payloads in the form of the Authentication Header (AH), and encrypting the payloads in the form of Internet Key Exchange (IKE), thereby ensuring end-to-end Confidentiality, Integrity and Authenticity (CIA) in data transmission [39]. The size of the payload and the type of higher layer protocols like the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) affects the overall encryption payload, hence, considered in the overhead computation. For adequate protection from Man-in-the-Middle attack, resisting replay attack and data exposure, we highly recommend IPSec as most of the encryption algorithms are supported by the IoT modules.

B. Transport Layer Security (TLS)

Transport Layer Security (TLS) provides user and device authentication, connection encryption and guarantee data integrity. The negative impact of TLS is latency and power consumption [40]. Because TLS has higher overhead, we recommended it for remote access application with high transmit intervals.

C. Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation (GRE) is also a layer-3 security standard specified by the Internet Engineering Task Force, RFC 2784. Just as the name implies, it encapsulates data payloads in the form of header-only with checksum, Key, and Sequence security flags [41] without payload encryption. Running GRE over other Layer 3 protocols would result in offering better protection against spoofing and man-in-the-middle attack.

D. Cryptography

Cryptographic security algorithms in the form of a private key (symmetric) and public key (asymmetric) is the most used security techniques at the time of writing this paper. Cryptography in the IoT context is the methods of protecting user/device data from unauthorized access. This is mostly realized by encryption; to protect the data readability. Decrypting the encrypted data recovers the original data and ciphertext, the recovered data [43]. One key (private) is used for encryption and decryption in symmetric keying while in asymmetric keying, a public key is used for encryption and a private key is used for decryption. The security level of the encryption algorithm is dependent on the size of the cypher key used. Various cryptographic algorithms have been proposed as a solution to the emerging cases of attacks on critical infrastructure. To ensure a high level of confidentiality, integrity and availability in IoT network, we recommend different combinations of AES, ARC4, HMAC, RNG, RSA, ECC security schemes during implementation.

E. Tunneling

Tunneling creates a virtual connection between two communicating entities through a public network. This concept will allow an encapsulated data packet to be sent across a network protected from attacks such as man-in-the-middle. Using GRE on MPLS network improves the security since the packet is visible to the intermediate nodes [41].

V. Internet of Smart Grid

Security is one of the challenges facing the deployment of IoT devices in the smart grid. The benefits of IoT in smart grid are not limited to, advancing Metering Infrastructure (MI), enhancing the reliability of power network protocols like SCADA, advancing the management of load demand in the grid, facilitating reliable interaction mechanisms with end-users, and monitoring of the health and operation of the grid. Most of the grid equipment is largely a legacy traditional power system devices running on legacy protocols such as SCADA, Modbus, and DNP3 and cannot enforce end-to-end encryption and message-by-message authentication [44]. The IEC 62351 is the security standard that offers security objectives of confidentiality, integrity and availability in smart grid networks [45]. To understand the security requirements of the smart grid over Wide Area Networks (WAN), we analyzed TLS and IPSec as countermeasure opportunities, see Fig. 3.

The demand for communication integration and cybersecurity compliance in the utility networks has become more important, especially with the advent of IoT. We refer to such an evolutionary change as the Internet of Smart Grid (IoSG). An innovation that is increasing the number of Intelligent Electronic Devices (IEDs) and Remote Terminal Units (RTUs) being used for digital connectivity, automation, and remote monitoring of utility assets safely and cost-effectively. Various types of wireless technologies such as the NB-IoT discussed above, are used to support IoT deployment in smart grid. A dedicated wireless network is however considered more appropriate from a security perspective. This will ensure secure communication and better quality of service owing to any changes in the existing infrastructure due to capacity expansion, digitization, network redesign, deployment and management of cyber-related attacks.

In a typical TCP/IP based Information Technology (IT) networks, data overhead attributed to security implementation are major concerns as a result of bandwidth limitations. Also, implementing power system security standards using these wireless technologies will scale the bandwidth required by a high margin. Spectrum has become the core element of wireless solutions for the smart grid and the power utility companies desire a secure and cost-effective wireless communication protocol that can be integrated into their legacy power system efficiently.

The requirements of wireless networks in the smart grid should also include the ability to accommodate long-term security needs, meet the demands for substation assets monitoring and control and be capable of supporting remote access. The measurement of bandwidth which translates to spectrum management will be achieved with the accurate information on the number of connected IoT devices, the type of service rendered in each of the grid entities, network topology implemented and the location of the devices among others. The additional overhead in each service layer of the chosen protocol as a result of implementations of standards such as IEC 62351 (cybersecurity standard for smart grid networks) will affect the network average rate of transmission.

The Distribution Network Operators (DNOs) have employed the services of Mobile Network Operators (MNOs) to meet their communication needs. It is an expensive option and the DNOs will have to accept the cost per bytes of data per month as determined by the MNO's pricing on each carrier. The carrier is most cases do not support full security suite and with incidences of service outages in hard to reach locations. However, the DNOs have recommendation plan in upgrading the security and management suites for different Remote Terminal Units (RTUs), IEDs, Private Network Service (PNS) and services using satellite communication systems. Generally, adding any security feature to the grid would increase the data overhead, but the additional cost of disruption and technical failure arising from such improvement in the power network cannot be overemphasized.

VI. Conclusion

Internet of Things related services and application has witnessed extensive growth worldwide. We present and analyze the general security requirements and countermeasure opportunities in LoRaWAN and other IoT technology platforms based on recent literature and findings from our test networks. The security overview of 5G to guide platform integration and consumer and industrial use case.

We also highlighted many layer-3 state-of-art security measures that would drive IoT deployment in smart grid and how integrating wireless technology will affect the security.

References

[1] A. Limaye and T. Adegbija, "HERMIT: A Benchmark Suite for the Internet of Medical Things," *IEEE Internet Things J.*, vol. 5,

no. 5, pp. 4212–4222, Oct. 2018.

[2] R. K. Pathinarupothi, P. Durga, and E. S. Rangan, "IoT-based smart edge for global health: Remote monitoring with severity detection and alerts transmission," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2449–2462, Apr. 2019.

[3] S. Chavhan, D. Gupta, B. N. Chandana, A. Khanna, and J. J. P. C. Rodrigues, "IoT-based Context-Aware Intelligent Public Transport System in a metropolitan area," *IEEE Internet Things J.*, pp. 1–1, Nov. 2019.

[4] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 716–723, Apr. 2018.

[5] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4890–4899, Dec. 2018.

[6] Q. Hong *et al.*, "Design of an Open Platform for Real-Time Power Grid Monitoring," 2019.

[7] Alex Hern, "Bad Rabbit: Game of Thrones-referencing ransomware hits Europe | Technology | The Guardian," 2017. [Online]. Available: https://www.theguardian.com/technology/2017/oct/25/bad-rabbit-game-of-thrones-ransomware-europe-notpetya-bitcoin-decryption-key. [Accessed: 06-Nov-2018].

[8] S.-C. Hsiao and D.-Y. Kao, "The static analysis of WannaCry ransomware," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 1–1.

[9] A. Batcheller, S. C. Fowler, R. Cunningham, D. Doyle, T. Jaeger, and U. Lindqvist, "Building on the Success of Building Security In," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 85–87, 2017.

[10] "Techmeme: IoT device vendor Wyze says a server leak exposed data, including email addresses, camera user IDs, and WiFi SSIDs, of ~2.4M customers from Dec. 4 to Dec. 26 (Catalin Cimpanu/ZDNet)." [Online]. Available: https://www.techmeme.com/191229/p1#a191229p1. [Accessed: 07-Jun-2020].

[11] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and Privacy in Device-to-Device (D2D) Communication: A Review," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[12] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," *2014 Int. Conf. Sci. Eng. Manag. Res.*, pp. 1–8, 2014.

[13] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 60–67, 2018.

[14] L. Chen, "Security Management for The Internet of Things," *ProQuest Diss. Publ.*, 2017.

[15] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016-Febru, pp. 180–187, 2016.

[16] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks & defenses," *Int. Conf. Commun. Technol. ComTech 2017*, pp. 104–110, 2017.

[17] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proc. 52nd Annu. Des. Autom. Conf. - DAC '15*, pp. 1–6, 2015.

[18] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices," *IEEE Internet Comput.*, vol. 21, no. 1, pp. 40–47, 2017.

[19] D. Pishva, "Internet of Things: Security and privacy issues and possible solution," *2017 19th Int. Conf. Adv. Commun. Technol.*, vol. 5, no. 2, pp. 797–808, 2017.

[20] N. Newmeyer, "The Impact of IoT Devices on Network Trust Boundaries," *Cyber Assur. Internet Things*, pp. 163–174, 2016.

[21] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of things security," *2017 Int. Conf. Wirel. Technol. Embed. Intell. Syst. WITS 2017*, 2017.

[22] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012.

[23] D. Pietro, "Security and Trust Challenges in the Area of IoT," *Innosummit*, 2012.

[24] C. Lesjak, D. Hein, and J. Winter, "Hardware-security technologies for industrial IoT: TrustZone and security controller," *IECON 2015 - 41st Annu. Conf. IEEE Ind. Electron. Soc.*, pp. 2589–2595, 2015.

[25] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9794–9805, Dec. 2019.

[26] M. Wang, Z. Yan, and S. Member, "Privacy-Preserving Authentication and Key Agreement Protocols for D2D Group Communications," vol. 3203, no. c, 2017.

[27] J. B. Hoffmann, P. Heimes, and S. Senel, "IoT platforms for the internet of production," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4098–4105, Jun. 2019.

[28] P. Ganguly, "Selecting the right IoT cloud platform," in *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 2016, pp. 316–320.

[29] J. Schlienz, D. R.-W. Paper, undefined Rohde&Schwarz, and undefined 2016, "Narrowband internet of things whitepaper," *pdfs.semanticscholar.org*.

[30] M. Lauridsen, I. Z. Kovács, P. Mogensen, M. Sørensen, and S. Holst, "Coverage and capacity analysis of LTE-M and NB-IoT in a rural area," *IEEE Veh. Technol. Conf.*, vol. 20, pp. 2–6, 2017.

[31] TSGS, "TS 133 401 - V10.3.0 - Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 10.3.0 Release 10)," 2012.

[32] B. Martinez, F. Adelantado, A. Bartoli, and X. Vilajosana, "Exploring the performance boundaries of NB-IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5702–5712, Jun. 2019.

[33] K. K. Nair, A. M. Abu-Mahfouz, and S. Lefophane, "Analysis of the narrow band internet of things (NB-IoT) technology," *2019 Conf. Inf. Commun. Technol. Soc. ICTAS 2019*, pp. 1–6, 2019.

[34] M. Chen *et al.*, "Narrow Band Internet of Things," vol. 3536, no. c, pp. 1–19, 2017.

[35] M. Martonosi, "Keynotes: Internet of Things: History and hype, technology and policy," *2016 49th Annu. IEEE/ACM Int. Symp. Microarchitecture*, pp. 1–2, 2016.

[36] C. B. Mwakwata, H. Malik, M. Mahtab Alam, Y. Le Moullec, S. Parand, and S. Mumtaz, "Narrowband Internet of Things (NB-IoT): From Physical (PHY) and Media Access Control (MAC) Layers Perspectives," *Sensors*, vol. 19, no. 11, p. 2613, Jun. 2019.

[37] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3682–3722, Oct. 2019.

[38] W. Ozan, H. Ghannam, P. A. Haigh, and I. Darwazeh, "Experimental implementation of real-time non-orthogonal multi-carrier systems in a realistic fading channel," in *IEEE Radio and Wireless Symposium, RWS*, 2018, vol. 2018-January, pp. 121–124.

[39] J. Guo, C. Gu, X. Chen, and F. Wei, "Model learning and model checking of ipsec implementations for internet of things," *IEEE Access*, vol. 7, pp. 171322–171332, 2019.

[40] R. Tataroiu, F. A. Stancu, and D. C. Tranca, "Energy considerations regarding transport layer security in wireless iot devices," in *Proceedings - 2019 22nd International Conference on Control Systems and Computer Science, CSCS 2019*, 2019, pp. 337–341.

[41] K. A. Ogudo, "Analyzing generic routing encapsulation (GRE) and IP Security (IPSec) tunneling protocols for secured communication over public networks," in *icABCD 2019 - 2nd International Conference on Advances in Big Data, Computing and Data Communication Systems*, 2019.

[42] M. Shankar and P. Akshaya, "Hybrid Cryptographic Technique U Sing Rsa," vol. 6, no. 6, pp. 39–48, 2014.

[43] K. Sharma, "Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing," 2017.

[44] J. G. Wright and S. D. Wolthusen, "Limitations of IEC62351-3's public key management," *Proc. - Int. Conf. Netw. Protoc. ICNP*, vol. 2016-Decem, no. HotPNS, pp. 1–6, 2016.

[45] "DS/IEC/TS 62351-5:2013 - Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives." [Online]. Available: https://webstore.ansi.org/Standards/DS/DSIECTS623512013. [Accessed: 07-Feb-2020].