International Journal of Sensors and Sensor Networks
2017; 5(6): 70-75
http://www.sciencepublishinggroup.com/j/ijssn
doi: 10.11648/j.ijssn.20170506.11
ISSN: 2329-1796 (Print); ISSN: 2329-1788 (Online)

Improvement of Security in IOT Sensor Network to Overcome Harmful Intruder by Optimizing the Existing Techniques

M. R. Arun[1], S. Selva Kumar[2]

[1]Department of ECE, Anna University, Chennai, India

[2]Department of CSE, G. K. M College of Engineering, Chennai, India

Email address:
researchonvideo@gmail.com (M. R. Arun)

To cite this article:
M. R. Arun, S. Selva Kumar. Improvement of Security in IOT Sensor Network to Overcome Harmful Intruder by Optimizing the Existing Techniques. *International Journal of Sensors and Sensor Networks*. Vol. 5, No. 6, 2017, pp. 70-75. doi: 10.11648/j.ijssn.20170506.11

Received: October 31, 2017; **Accepted**: November 13, 2017; **Published**: December 25, 2017

Abstract: Internet of Things is the web of physical devices acquired through the Internet. These devices contain entrenched technology to connect with both internal environment or the external status. Internets of Things (IoT) devices are directly becoming ubiquitous while IoT services are becoming global. Cyber-intruders are not unique to IoT, but as it will be deeply merged in our lives and humankind, it is becoming essential to step up and take cyber protection seriously. With increasing use of it in diverse fields has improved the demands of various parameters, for an excessive degree of security and applications. In this paper, we have compared the variance in security features of new technology like Low-Power Wide Area (LPWA) network technologies: LoRaWAN and NB-IoT. The security features of every technology are specified in a comparison to demonstrate that security won't be the determining aspect while choosing on a LPWA technology. We describe the exceptional contributions that every characteristic makes the general security of a device and emphasize how the security functions may not or might be appropriate in our option of a LPWA technology, based on the designed use case. We consider whether the security functions of each technology are appropriate for a fixed of use cases representing standard deployments for every technology. Based on an assessment of an appropriate feature, we have calculated the performance of the security in each technology and the each use instances. After identifying the security problems in IoTs, this paper suggest answers from present technologies as a start line for establishing a standardized security paradigm in IoTs.

Keywords: IOT Technology, LoRaWAN, NB-IoT, Intruder, Security

1. Introduction

The phrase Internet of Things (IOT) has acquired enormous fame with the eruption of wireless sensor networks, home automation devices, wearable electronics and smart meters. The IOT durations long-range outdoor systems such as the municipal lighting and smart grid, likewise shorter-range indoor systems which enable the affiliated home and residential security systems. Although the focal point of this paper is on security over the intruder, it should be mentioned that most of the major instances, security will no longer be the most important criterion on which a LPWA technology is chosen; there are additionally discriminate which might be possible to have a huge consequence such as: cost, availability of goal places, signal clout, content of implementation, correlated managed services and so on. We also endorse that specific user instances can have unique security requirement, and additional security features are not necessarily “better”; redundant security features will, in most instances, have a few related price, whether in bill-of-quantities strength or bandwidth intake, or just more complexity increasing the capability attack surfaces.

At a severe, we are ready to imagine user instances wherein there may be no perceived want for security:

(1) Transferring openly available data, with no solitude implications.
(2) If we don’t have confidence on for critical operations.
(3) Where there is no inducement or freedom for a mugger to tamper with it.

With generally very confined power and data rates, there can be a much less inducement to assault devices on LPWA networks for Denial-of-Service (DOS) botnet purposes, and the greater typical threats can be because of the data being processed by devices, even though there is quite a chance of DOS assaults supervised at the devices and the web. Devices the use of non-IP networks can also be hard for the mugger to reach from the cyberspace. Very easy sensors, deal with public domain data may use to have minimum security requirement.

Technologies under Consideration

The illustrated idiosyncratic of a LPWA network is the network which supports devices even at low power in both conditions like transmission power and processing power periodically, there is an objective of a battery span of 10 years or greater. This is generally coupled with a goal of minimizing cost, specifically in the recognize of the wireless module in the deep run devices. There is also a 3rd general goal which is to allow coverage in tough- to-reach areas (distance from base stations, inside buildings, or below ground level). The LPWA technologies distinguished the different comparison in the security features of most recent Low-Power Wide Area (LPWA) network technologies: LoRaWAN and NB-IoT [1].

LoRaWAN: LoRaWAN is a public specification for LPWA generation developed by way of individuals of the non-income LoRa Alliance. With a low-fee base station to be had, it's far getting used for self-managed private network installations in addition to by means of vendors of public networks. “LoRa” on my own describes the underlying, proprietary, physical radio layer which is also to be used for peer-to-peer communications, whereas “LoRaWAN” describes the link layer protocol.

NB-IoT: 3GPP Release thirteen also defines in addition, enhancement described by using UE class NB1 (NB for “Narrow Band”, honestly placed giving a lower records fee however extra penetration). Similarly to LTE-M, the characteristics are optimized for cheaper wi-fi modules and very long battery existence. The time period NB-IoT encompasses the use of this generation in the LTE bands and additionally includes use of the identical protocols in different, licensed radio spectrum outside the usual LTE bands.

2. Related Works

The issue of security is one of the most important issues considered as IoTs devices should be able to communicate in heterogeneous system to provide on the clock service in a long term deployment without having to perform regular checks. This setup leads to various intermittent and locale specific failures and could also lead to more permanent failures. Some of these failures in IoTs are covered by the obvious redundancy that is needed in such kind of deployments, but due to the demand for IoTs to perform consistently and have the ability to recover from security attacks to normal operations. Thus, the security solution should cover the possibility of security updates, easy connection, attack detection capabilities with a standardization in IoT architecture among all layers to operate in different modes to provide networking with the bare minimum use in order to convey and recover from various security attacks. These modes would be able to provide attack detection, diagnose, apply repairs and countermeasures, there is also the use to keep in mind the computational limitations of IoTs while constructing such a security solution [2]. With the growing miniaturization of smartphones, computer systems, and sensors in the Internet of Things (IoT) paradigm, strengthening the safety and stopping ransomware attacks have become key concerns. Traditional protection mechanisms are not relevant because of the involvement of useful resource-confined gadgets, which require more computation energy and sources. This paper affords the ransomware attacks and security concerns in IoT. We start to speak the upward thrust of ransomware assaults and description the related demanding situations. Then, we investigate, report, and highlight the research efforts directed at IoT from a protective attitude [3].

Identify security issues in the specific layers: [4, 5] Security challenges faced in perceptual layer are node authentication, confidentiality of information. Attacks like distributed denial of service and poor physical security with respect to the installation of its “things” cause a separate set of problems. In network layer security attacks like the man in the middle attack and counterfeit attack are experienced along with data congestion and other problems relating to network layer are consistent in this layer. As perceptual layer and network layer are very closely related, problems like exploiting devices through unsecure network services are common in this layer. In data fusion layer, malicious information, attacks from the internet due to lack of transport encryption, insufficient authentication are common along with the other insecure cloud interface. In Application layer privacy protection due to data sharing plays an vital role with respect to access control along with all the implications of data privacy. The data fusion layer works closely with application layer thus the issues from data fusion layer related to data integrity and corruptness creeps in this layer.

Access control in IoTs has to consider aspects such that limiting or granting access is at the discretion of the user. It should possible to give and remove access to various systems involved, on the fly with some kind of leasing. The type of access to data should also be a determent to context of data usage, that is the data available from IoTs should be categorized into various data sets with heuristic trust- so that data is only to be used in specific contexts. Certain assurances and certification could also be provided that data would not be used out of context of pre agreed terms (some legislations and other policies would be needed to be passed in order to fully realize this aspect) [6].

Influenced by existing solution, data distortion and data encryption are the driving force along with key management and authentication as IoTs integration is within heterogeneous, multi-layer networks. With the huge use of

IoT technology in the production and every day existence, the troubles of facts security and privacy safety had been regularly exposed. Based on the IoT technology structure, we made a deep evaluation of the safety troubles from the sensor layer, application layer and network layer respectively, and we attempt to locate the important thing technical factors and recommend the corresponding countermeasures and hints for the safety issues within the above three layers, as an example, the safety troubles of the terminal get entry to mechanism and the routing assaults of wi-fi sensor networks for the sensor layer. The address area shortage and the denial of the company due to network congestion for the network layer, personal privacy and unsound safety trendy for the application layer [7]. Internet of factors is a term coined by way of Kevin Ashton in one of his shows [8]. The time period describes an era of the destiny based on the Internet and involves sharing of information [8]. IoT is a revolt in the universe of technology and it is the next big thing in the universe of computing and communication. IoT permits the communication among all the things we see round us apart from the human-device interplay that already exists. Applications of IoT range of diverse fields from the obvious IT to the unexpected, saving energy using smart grids [9]. IoT may be considered as an extension of traditional wi-fi (wireless) sensor networks (WSN) that makes the entity-to-entity communication viable by using the generation called radio frequency identification (RFID). RFID allows the item to perceive other objects. RFID has long been used as an alternative to 6 barcode.

This technology to become awake of different entity and with the intention to connect to them. This technology, additionally detects entity in real time and provides important information inclusive of the region and status [10]. IoT is enabled by way of a robust RFID device. IoT additionally uses sensors to link the physical and information worlds [11].

The sensors are used to collect facts about the environment this data may be analyzed in line with different situations and elements to bridge the distance [9]. IoT additionally makes the aid of nanotechnology and miniaturization of region intelligence in various devices. These devices with intelligence are called capable devices and feature a crucial area within the architecture of IoT. These objects can configure themselves and take a decision on their very own. After which actual entity-to-entity communication could be performed [9].

3. Proposed Security Solutions of IoT

To deal with various security issues identified in the below section, a need for a framework specifically for IOT security and privacy which has layer specific attack detection and repair capabilities along with privacy constraints. It should be capable to determine and determine the framework of data in real time and dynamically propose privacy policies on the fly. It should be capable to facilitate secure inter domain data interaction and data fetching or querying in mark with the assorted aspects of data access control.

3.1. LoRaWAN

One scheme for addressing long range communication dedicated to Internet of things is recognized as LoRa. It benefits name from the fact that it is capable to produce 'Long Range' transmissions using very low power levels. It uses low power, high-range Wi-Fi connectivity in the broadly used sub GHz band. These are most suited for connecting devices that need small amount data and high battery span. Actually LoRaWAN is based on server-side operation of a numerous access protocol. It is specially performed to reduce collisions with a large number of endpoints. It needs a server utilization to run the MAC operations over a network connection. Its design is usually set out in a star-of-stars topology in which gateways are a translucent bridge transmitting messages between extreme devices and a main network server on the back end [12]. It is architecture basically for uplink simplest applications with abundant endpoints, or applications in which only a lean downlink messages are needed (defined neither by application nor by the sum of endpoints). In this type of architecture, the gateway in the similar network requires synchronization. The transmission between gateways and end-devices are extended out on various frequency data rates and channels. The options of the data rate are a deal-off between message duration and communication range. The contrasting data rates do not interfere with each other instead create a set of “virtual” channels increasing the capacity of the gateway. In this LoRaWAN network, server maintains the data rate and manage RF output for every end-device separately by method of an adaptive data rate (ADR) scheme which is usually refurbish once in every 24 hours. The numerous segments of security (encryption, EUI64 on web level and application level and EUI128 device specific key). AES CCM (128-bit) for encryption and authentication is available in this infrastructure. It endeavors inside the purview of the ETSI 1% and 10% work cycle at communication time in the 868 bands. The draft amendment of class B for downlink nodes that can count for a beacon at every 1s to 128s (2^n) where as n is 0 to 7. It also got antenna diversity. It is because of all gateways admitted to the similar uplink channels. LoRaWAN has ADR, which is compelling by the server, if a node’s link quickly fades, the server has no way of telling it to change spreading factors to compensate. ADR for LoRaWAN issued to optimize the capacity of the channel [13] [14].

3.2. NB-IoT

Low power wide area (LPWA) networks primarily need long and wide coverage, minimize power consumption and enormous connections. There are some basic characteristics of the NB-IOT technology, which form it the best for LPWA deployment. In addition, low power utilization is essential for almost 80% of all LPWA user cases, browsing from applications like smart parking, smart meter and wearables to smart grid [15]. Furthermore, with the opening of enormous connections it is attainable to prepare entirety around us smart. To recognize that it is optimal to have about 50,000

devices per cell; this is feasible by assuming that household density per each Sq.m is 1500 with 40 devices. When we analyze basic capacities of NB-IOT with other LPWA technologies like SigFox, Lora and e-MTC, we observed that NB-IOT offers better performance. In additionally, when we review at all the technologies in terms of network investment, uplink and downlink traffic, coverage scenario and network reliability, so obviously we recognize that NB-IOT is the best appropriate technology. Furthermore, in term of performance prospect, NB-IOT assurance 20+dB coverage, ~1000x connections, ~10 years using only 200 KHz bandwidth, whereas the other technologies like SigFox, eMTC provide far less in terms of performance. NB-IOT has entirely an extensive ecosystem, primarily due to its support from many worldwide top operators. Generally unlicensed results can't assurance of reliability and security [15].

4. Comparison in Terms of Security Features

There are many aspects that should be treated when we select the appropriate technology for an IoT application. The security facial characteristics of each technology are shown in a comparison table 1 to illustrate the contrasting contributions that every features makes the complete security of a device and describe how the security facial characteristics may or may not be significant to your choice of a LPWA technology [16] [17].

Table 1. *Security Features Of Lorawan And Nb-Iot.*

Security features	LoRaWAN	NB-IoT
Identity Protection	Partial	TMSI
End to Middle Security	Yes(APPS key)	No[5]
Replay Protection	Yes	Optional(with DONAS)
Reliable Delivery	No	Yes
Networking Monitoring and filtering	Limited	Yes
Key Provisioning	Pre-Provisional(ABP) or OTAA	Pre-Provosioned or RSP
IP Network	No	Optional
Updatability	Limited[10]	Possible

4.1. Identity Protection

Some protocols include privacy-preserving measures to minimize the usage of permanently allocated identifiers which could be intercepted and correlated with device activity over time. An example of this is the Temporary Mobile Subscriber Identity (TMSI) allocated by 3GPP networks to address the mobile device instead of the IMSI (International Mobile Subscriber Identity) which is only used once each time the device is powered on.

4.2. End-to-Middle Security

There will be greater than one communication "hop" between the end device and the server which is the destination or source of messages; the radio interface is just the first of them. For cellular networks, it is usual for there to be concentrators between the radio base stations and the core network, as shown in the below diagram, which is based on the GSM network design. The concentrators (Base Station Controllers in this example) have communications links which an intruder could potentially intercept, particularly where these are wireless (such as the microwave link shown) so we need to consider the security protections of these links as well as radio link between the access network and the device. This issue potentially arises for any network with a "star of stars" topology (e.g. LoRaWAN) where multiple gateways connect to a common network server. In such cases "end-to-middle" would indicate a security context established between the end devices and the network server. It is feasible to provide an end-to-middle security context for integrity protection, confidentiality protection, or both. Some networks may choose not to provide end-to-middle confidentiality protection due to a desire to provide local law enforcement agencies with lawful interception capabilities.

4.3. Replay Protection

Replay protection is a security property of a protocol such that messages recorded by an intruder will not be accepted by their recipient as legitimate if they are reinserted into the communications link later. This is important in scenarios where the content of the message is linked to some kind of commercial transaction, or, for example, where an intruder wishes to evade detection by a surveillance device by disabling it and replacing its transmissions with previously recorded normal activity.

4.4. Reliable Delivery

This is a security issue, as it directly pertains to the availability category of the Confidentiality / Integrity / Availability triad and indirectly affects other security characteristics as, without reliable delivery of messages, intruders could potentially block delivery of certain messages without the device and/or the network being conscious of it. This is a somewhat different issue than Denial of Service, as jamming at a large scale would be noticed due to the large change in the amount of network traffic, but selectively blocking a few messages could be unnoticeable and benefit an intruder, for example avoiding their being detected by a surveillance device. LPWA technologies with limited acknowledgement capabilities, such as LoRaWAN and Sigfox, may therefore be considered unsuitable for some use cases in which confirmation of successful delivery of

messages is required.

4.5. Network Monitoring and Filtering

Monitoring functions within a network can be important for security. One example of this is an Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) which inspect network traffic in order to look for and block malicious payloads. An IPS may be a necessary mitigation if a vulnerability is discovered in end devices and, for some reason, it is infeasible to update the devices to patch the vulnerability. If data is being encrypted end-to-end at the transport or higher layers, then the ability to inspect the network traffic in this way is severely restricted, preventing techniques such as long packet inspection.

4.6. Key Provisioning

Cryptographic techniques for certificating, confidentiality and uprightness, all rely on cryptographic keys being shared between the subject and the relying parties. For public keys, this can be as easy as downloading them from a known source, but secret and private keys must be distributed in a secure way. Often a "root of trust" public key is embedded in device firmware at manufacture time, which can then be used to authenticate keys which are distributed later, although the compute power and volume of data required for such distribution protocols could exceed the capabilities of some very low power devices used to LPWA technology. Secret keys are often pre-provisioned to devices as component of the manufacturing process, sometimes coupling a secure element for key storage and processing of the device (for example a UICC) with a Hardware Security Module (HSM) at the service provider. The HSM diminish the risk of a security breach at the service provider allowing an intruder to capture copies of secret keys for many devices in one go; this risk is similar in scope to that of a Class Break (see below). There may also be a need for secret keys to be renewed after manufacture, in cases that a long-term key has been in use for longer than its recommended lifetime (see Updatability (Keys / Algorithms) above) or if the device is to be re-personalized for a different network. The RSP (Remote SIM Provisioning) facility is a recently standardized mechanism for doing this for devices with an eUICC on a 3GPP network.

4.7. IP Networ

The choice of network layer protocol to run over the WAN (Wide Area Network) link layer has security implications. The most obvious choice is IP and, where it is used, it can be an enabler for implementation of well-tried and trusted standard security protocols, such as TLS, above the network layer; however, there is some potential downside as the use of IP may create an attack surface for Internet-borne threats such as botnets, if the device is usable from the social Internet. Threats from the public Internet when using IP can be much reduced by using a "Private APN" on 3GPP networks, so in effect the device is affiliated to a subscriber's intranet, and can be shielded by firewalls and other enterprise network security measures. A network operator may also use IP masquerading techniques such as Network Address Translation (NAT) to allow a device to make uplink connections to the public Internet while making it effectively inscrutable in the reverse direction.

4.8. Updatability (Device)

Device security vulnerabilities are a perennial issue, from the first PC viruses in the 1980s through to today's botnets of IoT devices (see Flashpoint report). New vulnerabilities are discovered every day, and the most effective response to such vulnerabilities is to patch affected devices with updated software or firmware. This is of course an issue for any type of connected device on any network, but the nature of LPWA technologies may make it harder to distribute such patches, given low data throughput and possible lack of reliable delivery (see above). If distribution of patches is infeasible, some other mechanism needs to be present to deal with serious vulnerabilities, such as network-based Intrusion Prevention Systems (IPSes) (see below) or, in the lowest case, blocking service to, or otherwise disabling, affected devices.

5. Representative Use Cases

To compare the effectiveness of the security features of the various LPWA technologies we will consider a set of example use cases. To avoid undue bias, we have selected two use cases which represent a typical deployment for each of the five LPWA technologies we are looking at. We will not be going through a comprehensive, risk analysis, but we will summarize some of the main and distinctive risks for example purposes.

5.1. Smart Street Lighting

The Street light Management System using LoRaWAN. It can be used with either public or networks, with private networks seeming to be the main target. The main benefits offered are energy saving (the lights run on an autonomous dimming schedule without requiring regular communication from the server) and monitoring for power efficiency and maintenance needs. There are a several potential threats to a street lighting control system: residents might wish to override the lighting schedule to provide brighter or longer illumination than the local government has budgeted for, and the safety implications of turning off street lighting might make it a potential terrorist target. Nevertheless, the feature of autonomous operation means that the risk of Denial of Service attacks is not a major concern and, as the operation of the network can be considered not be safety-critical, assurance needs are less. There does not seem to be any confidential data nor any personally identifiable information (PII) being processed.

5.2. Water Metering

NB-IoT is attractive for this use case because of the low

power requirements and good propagation to hard-to-reach locations. The main benefits are for the utility company to obtain more frequent meter readings and to obtain them without having to visit the meter location. There is a range of threats, including interference by the utility customer with the aim of reducing their bills. Assuming that there is no facility to disable the water supply, there may be no personal safety concerns, but there may be privacy concerns as fine-grained water usage data from a domestic property could be used to draw conclusions regarding the action of the occupants.

5.3. Security Suitability of LPWA Technologies

To produce the table below, we have considered the relative importance of the principal controls listed for each of the use cases above, and how strong the implementation of the supporting features is in each of the LPWA technologies we have covered. Rather than show the many individual comparisons involved, we have summarized them with a single grading for each use case and technology below.

Table 2. *Security Suitability By Use Case.*

Use Case	LoRaWAN	NB-IoT
Smart Street Lighting	Adequate	Good
Water Metering	Adequate	Good

6. Conclusion

In this paper, it's far shown that both LoRa and NB-IoT have their very own advantages and disadvantages according to its extraordinary technological standards. In well known, there is not a unique LPWA technology, but the maximum suitable stage for the unique application. Each utility has its specific necessities, which cause a selected generation choice. Both LoRa and NB-IoT have their place within the IoT marketplace. LoRa focuses on the decrease price packages. Meanwhile, NB-IoT is directed to programs that require high QoS and occasional latency.

References

[1] fhcouk.files.wordpress.com/2017/05/lpwatechnology-security-comparison.pdf

[2] Internet of Things – New security and privacy challenges: Rolf H. Weber - University of Zurich, Zurich, Switzerland, and University of Hong Kong, Hong Kong.

[3] The rise of ransomware and emerging security challenges in the Internet of Things (IOT). Available from: www.researchgate.net/publication/319527564_The_rise_of ansomware_and_emerging_security_challenges_in_the_Intern et_of_Things [accessed Oct 06 2017].

[4] John A. Stankovic, Life Fellow, IEEE “Research Directions for the Internet of Things”.

[5] www.owasp.org/index.php/Top_IoT_Vulnerabilities.

[6] H Suo, J. Wan Security in the internet of things: Review, 2012 International Conference on computer Science and Electronics Engineering.

[7] The Information Security for the Application of IoT Technology: Jia Jiang and Donghai Yang.

[8] Miao Wu; Ting-Jie Lu; Fei-Yang Ling; Jing Sun; Hui-Ying Du, "Research on the architecture of Internet of Things," Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference, vol. 5, pp. V5-484, V5-487, 20-22 Aug. 2010 doi: 10.1109/ICACTE.2010.5579493.

[9] Lu Tan; Neng Wang, "Future internet: The Internet of Things," Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference, vol. 5, pp. V5-376, V5-380, 20-22 Aug. 2010 doi: 10.1109/ICACTE.2010.5579543.

[10] Castellani, A. P.; Bui, N.; Casari, P.; Rossi, M.; Shelby, Z.; Zorzi, M., "Architecture and protocols for the Internet of Things: A case study," Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference, pp. 678-683, March 29 2010-April 2 2010.

[11] Huansheng Ning; Ziou Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?," Communications Letters, IEEE, vol. 15, no. 4, pp. 461-463, April 2011.

[12] Jonathande carvalhosilva, Joel J. P. C. Rodrigues, Antonio M. Alberti, Petar Solic, Andre L. L. Aquino, “ LoRa WAN-A Low Power WAN Protocol for Internet of Things: A Review and opportunies, Aug 02, 2017.

[13] Bhupjit Singh, Bipjeet Kaur, “Comparative study of Internet of Things Infrastructures & Security”, Oct 05, 2017.

[14] Aloÿs Augustin, Jiazi Yi, Thomas Clausen and William Mark Townsley, “A Study of LoRa: Long Range & Low Power Networks for the Internet of Things”, 9 September 16.

[15] Rashmi Sharan Sinha, Yiqiao Wei, Seung-Hoon Hwang, “A survey on LPWA technology: LoRa and NB-IoT”, d 4 January 2017.

[16] LoRa vs LTE-M vs Sigfox - www.nickhunn.com/lora-vs-lte-m-vssigfox/

[17] http://pages.silabs.com/rs/silabs/images/Wireless-Connectivity-

[18] http://link.springer.com/chapter/10.1007/978-3-662-43871-8_243?noaccess=true

[19] https://www.link-labs.com/what-is-sigfox/

[20] web.gdmec.cn/zlgcxm/2013/jxgg/xxljq/support/%E5%8

[21] http://www.radio-tronics.com/info/wireless/lora/basics-