International Journal of Engineering & Technology, 7 (4) (2018) 4918-4921

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.19850
Research paper

ECC Based Data Retrieval Using LoRaWAN Technology

Nibras Raad Abdallah[1*], Taha Mohammed Hasan[1] and Ahmed Chalak Shakir[2]

[1]*Department of Computer Science , College of Science , University of Diyala , Iraq*
[2]*Department of Computer Science , College of Science , University of Kirkuk , Iraq*
[*]*Corresponding author E-mail:nibras98246@gmail.com*

Abstract

LoRaWAN is a low-bandwidth network technology (LPWAN) that enables low-cost and low-power communications for Internet-connected devices even in dense urban areas. This paper aimed to adds an additional encryption layer plus with an electronic signature to transferred data through the Elliptic Curve Cryptography(ECC). Although this technology has important benefits such as a provides the security in data transmission where it uses the AES 128 in the process of encryption and decoding, but many studies have reported a safety vulnerability that can be exploited by brute force attack in the LoRaWAN technology termed 'Bit-flipping attack'. Accordingly, an additional layer of protection has been added to the proposed system.

Keywords: *Bit-Flipping Attack ; LoRa/LoRaWAN ; ECC ; ECCDH ; ECCDSA;bit-flipping attack .*

1. Introduction

More and further objects are connecting to the web a day, through the Internet of Things (IoT) paradigm. At 2020 further than 26-50 billion intelligent devices are connecting to the web as expected[1]. The areas of IoT applications this new connectivity are including multiple fields as manufacturing, healthcare, smart homes, transportation, urban infrastructure management, and agriculture. In addition. too many various other fields, as predictable, the health care and industrialization are the predominant markets figure1[2].

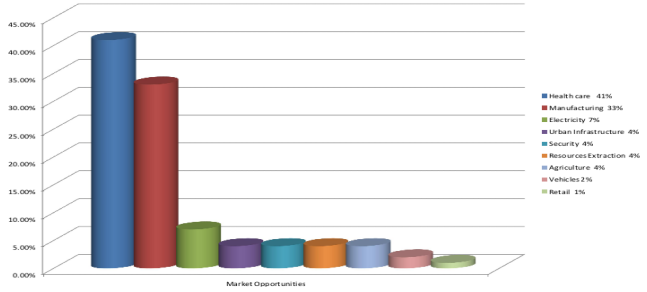

Figure 1: Market Opportunities IoT applications

Currently, one architecture is particular for IoT networks it is the Low-Power Wide Area Network (LPWAN) model, which is still evaluating in the community of researchers have [3]. Understanding these networks and if it has the ability to live with other networks standards, it's an important idea for the community of researchers. In specific, this paper aims to do possibility of worked a private network among distances of up to more than three kilometers in a civilian environment situation and data interchangeability for one important of the prominent LPWAN technologies, LoRaWAN™[4]. LoRaWAN has able to the deployment of private and public networks. The work of these networks similar to cellular ones. LoRAWAN (Long Range Network Protocol) [3], mainly developed in January 2015 through LoRa Alliance to facilitate IoT applications[5][6][7]. This guarantees a full compatibility between the IoT objects, with no need the complicated applications[8]. LoRa (Long Range), it is a radio frequency layer, worked on unlicensed bands (EU 868 MHz, US 915 MHz) and it has unique modulation depended on Chirp Spread Spectrum (CSS) modulation. in addition, LoRa does several improvements on Frequency Shift Key (FSK) modulation, and more advantage of the LoRa is detailed in[9]. LoRaWAN is used by various applications, such as infrastructure communication (e.i.agriculture [10] security[11], and smart metering) these just few examples of applications that depend effectively over this technology, and can be successfully used by other applications in different fields. Recently, many studies have said found a security vulnerability in this technique that may be can be exploited through a flurry attack termed it a bit-flipping attack by doing changes in some fields in an encrypted text without decryption[12]. This type of attack, in simple its form, it changes certain fields in a cryptographic text without decoding[13]. Therefore, in this paper, the data will be sent and received through LoRaWAN network with the addition of an additional encryption layer and a digital signature by using the ECC system as a suggestion to prevent dealing with the data that has been manipulated by this attack. A single gateway connected with a central database and a simple device which represents the end-node LoRa combined with a computer is used. Structure of the paper, information about LoRaWAN technology, and ECC system discussing in section II, while the design of the system will be discussed in section III, the experimental results will be discussed in section IV. The paper closes in section V with our remarks.

2. LoRa & LoRaWAN

LoRaWAN is a MAC layer built upon modulation of LoRa, which is based on the chirp spread spectrum (CSS) modulation. Which are within the standard IEEE standard 802.15.4 Low Rate Wireless Personal Area Networks (LR-WPANs) is described[14].

2.1. Network Architecture

The LoRa modulation runs on industrial, scientific, and medical radio band (ISM band) . The system of LoRaWAN has three major components; (i) network servers (ii) end devices) and gateways. LoRaWAN networks are deployed as star-of-stars topology,and gateways relay messages between network server and end-devices . All Gateways connecte to the central network server by standard IP technology, while single-hop LoRa communication used for end-devices to one or many Gateways. The communication between end devices and Gateways can be FSK or LoRa modulation by different data rates and channels.Overview of LoRaWAN architectural in Figure2 [15].

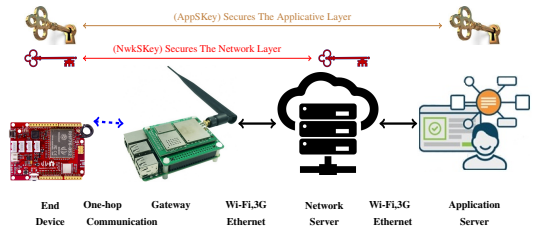

Figure 2: Seeeduino LoRaWAN Network Architecture module RHF0M301

In return,the network server connects data to one or a group of application servers through IP such as the https,MQTT , and ... etc; Security technique relies upon the shared root key AppKey between the network server and the end device through that key, each device will compute two primary keys for the session. The first key is an application session key AppSKey that will assure information confidentiality amongst an AS and an end devices, while another key is a network session key NwkSKey that will guarantee an integrity of information between an network server and end devices. Through that, there is no guarantee the integrity of information between an end devices and an AS. The NwkSKey provides confidentiality and integrity of information between an network server and an end devices when frames transportation between them. The confidentiality provides with use AES128 for encryption in CTR mode[16]and the integrity of information are given by AES128 NwkSKey in CMAC[12][17].

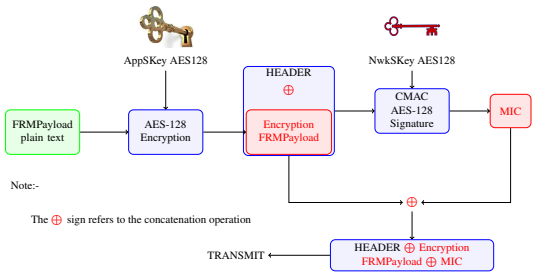

Figure 3: LoRaWAN Data Encryption

In the LoRaWAN, because there is no guarantee for data integrity between end devices and AS and the message by using the CTR mode is vulnerable to the bit-flipping attack. The encrypted message that was created using CTR mode is exposed to a bit-flipping attack because it was executed by Xor operation [12]. A Message Integrity Code (MIC) using in LoRaWAN protocol guarantees data integrity[5].For data integrity, The LoRaWAN verifies the MIC before decrypting for the received frame payload.The small size of MIC which is a four bytes, therefore,the frame payload can be exposed to a brute-force attack easily[18].The attacker will be an attempt to attack about 2,147,483,648 times to obtain the correct MIC according for calculation the average case[12].

2.2. Elliptic Curve Cryptography

In 1985, Neal Koblitz with Victor Miller ware proposed the Elliptic Curve Cryptography (ECC). ECC can improve the existed encryption systems because it has smaller parameters, usage bandwidth is lower, public-key smaller for certificates, implementations is the faster, low power and need it small hardware processor. So, The ECC using to build a crypto system is laudable for the reasons an efficiency and high security[19].Further, very fitting to the environment of the Wireless Network like smart cards and cellular phones [20], Wireless Sensor Networks (WSN's) [21],etc; The ECC offers security at higher levels than other public key cryptographic standards like RSA because it provides higher security with lower key sizes and therefore reduces the cost of processing. Diffie-Hellman key exchange algorithm of elliptic curve cryptography (ECCDH) provides a safe means of exchanging keys among communicating hosts[22].The ECC heart is a discrete logarithm problem (ECDLP) that is mean d value cannot be calculated, such that, q= dp, where p and q are known points on the curve. But it's easy to find q where d and p are known.

3. Scenario of Communication

Now a day the most communication technologies are Zigbee, Bluetooth, and WiFi among IoT devices. Currently, the candidate used as an alternative to these platforms is LoRaWAN. This paper will focus on the most widely used and primary wireless platform of the ISM-band. This paper will use dual Xor proposed method of ECC to encoding and decoding the message which will be transmitted over the channel because it is suitable for the devices used inside a paper, where it will use Raspberry Pi 3B with RHF0m301 as a hat installed upon, which is Gateway connected to the network server. The network server connected to the central database, and from the other party RHF76-052 as an end device sender. Dual Xor proposed method of encoding typically consumes time response less than any of the other ECC encoding techniques, which generally use the encoding process. Since encoding involves Xor operations, therefore it consumes less computational time and power with efficient security.

3.1. Preliminary Configuration

The initial configuration of the network by two phases, the first one is the end device will create an "active"(any session) with network server via one of two methods.

1. Personal Activation(ABP) the device contains two session keys and other parameters (not AppKey in root) before it is published.
2. Over the Air Activation(OTAA)consists of providing the device with an AppKey root and other parameters, allowing key exchanges with network server via the radio interface as soon as they are deployed.

The second phase proposes use Elliptic Curve Cryptography Diffie–Hellman(ECCDH) to derive symmetric keys from the key exchange of public keys between EN and network server for beginning their communication.The procedure is described below and summarized in Figure 4.To protect data sent between two hosts (end device(A) and network server(B)) against modification and eavesdropping,all parameters needed to create the elliptic curve are Figure .To protect data sent between two hosts (EDs(A) and NS(B)) against modification and eavesdropping,all parameters needed to create the elliptic curve are pre-configured such as (all parameters needed to

create the elliptic curve are pre-configured such as (the base point G(x,y),two parameters a,b for core equation$y^2 = x^3 + ax + b$ and q is a prime number of prime fields GF (q)) in the two nodes A,B. The node A will generate private a random integer numbers a,a1 and two public keys P=aG, P1=a1G, as well as node B will generate a couple of public and private keys (b,b1 as private and Q=bG, Q1=b1G as public). Node A computes two a secret keys S = aQ, S1=a1Q1 where Q, Q1 is node B's public keys. Also, node B can compute two a secret keys S=bP, S=b1P1 where P, P1 is node A's public keys. The two secret keys are used to encoding and decoding data by using a dual Xor proposed method.

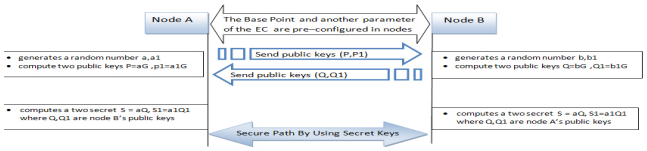

Figure 4: ECCDH Key Exchange

3.2. Application processing

• Clint send data to Server and (Server send data to Clint) :- The procedure of A will be described by next steps and figure 5.
Input: Private key (d) ,message (m),n (Order point on the Curve), Output: Signature (r,s).

- A Clint send data to Server and D(Server send data to Clint) :- The procedure of A will be described by next steps and figure 5. Input: Private key (d) ,message (m),n (Order point on the Curve), Output: Signature (r,s)

  1. Compute z=hash (m) {sha512} .
  2. Generate a onetime Key-pair. (U,V) {U is Private key,V is a public Key}.
  3. Compute r=integer (Vx) mod n.
  4. Compute s=((z+r*d)u-1)mod n.
  5. If r or s =zero then go to step 2.
  6. Output (r,s).

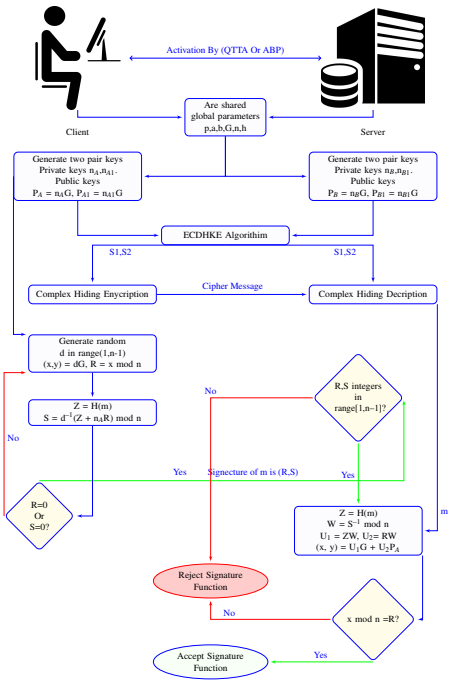

Figure 5: Phase1 Client to Server Sending Cipher Message and Digital Signature

Before sending the message will be encoding to a series in a dual Xor proposed method and combine with digital signature, in next steps of algorithm :-
Input : Two Secret Key (S1,S2),message(m) , Output : Cipher message

1. Compute D is a distance between S1x and S2x.
2. Give v1=S1x,v2=S2x .
3. Compute cipher message = v1⊕v2⊕m.
4. Send cipher message combined with digital signature.
5. For next section change value v1 to v1+D ,v2 to v2+D.
6. Output cipher message

- (Server received data from Clint) and (Clint received data from Server) At this stage, the validity of the data received will be verified in several steps which can be summarized in figure 6.
Input : Singer's public Key (W), Message(m),signature (r,s),G(base point on the Elliptic curve),n (Order point on the Curve), Output : Valid (Accept) or Invalid (Reject)

  1. Separate the digital signature from the received message.
  2. Decoding received cipher message by complex hiding method ,the decryption steps are the same as the encryption.
  3. Compute z=hash (m) {sha512} .
  4. Compute w=s-1 mod n.
  5. Compute u1=w*z mod n.
  6. Compute u2=w*r mod n.
  7. Compute p=u1*G+u2*W.
  8. If Px mod n =r mod n (signature Accepted) otherwise (signature rejected).

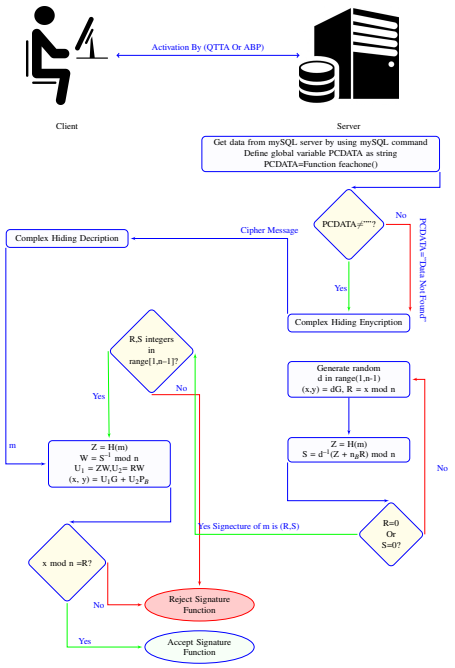

Figure 6: Phase2 Server to Client Sending Cipher Message and Digital Signature

In both stages when the digital signature is refused, the counterparty will be notified of the rejection. In the case of accepting the digital signature, stage displays the received message after decrypted to the end user while in stage the application will connect to the central database connected with the server and return the data associated with the required field, then encoding the data and will be sent to the second party with the digital signature.

4. Experimental result

The difference between the method used in this paper to encoding the data and the traditional method used to encode data using the Koblitz's method is shown in the figure 7. In addition, it shows a faster response time for the proposed method, with a similar message(like '7' with a deferent size of a finite elliptical curve such as(2011,4093,..,etc.), and the device (Raspberry Pi 3 Model B) used in this paper. The remarks recorded on a device with 1.2GHz 64-bit quad-core ARMv8 CPU, 1 GB RAM.

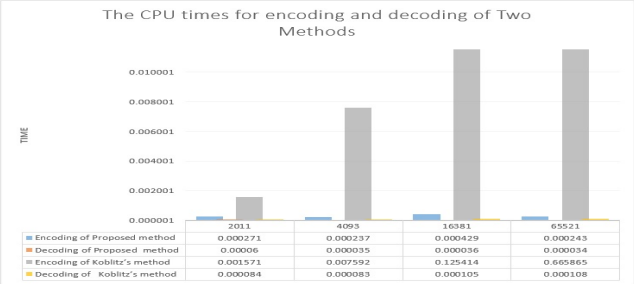

Figure 7: The CPU times for encoding and decoding of two methods

5. Conclusion

Nowadays, the world's great companies(Cisco, IBM, Microchip and Semtech, etc.) have opened up new horizons to deal with this technology by forming large networks that contain many gateways and end-node devices to cover all zone. For instance, these end-node devices are supported by this technology can monitor the movement of vehicles by sending the site using GPS. This paper demonstrates how anyone can easily acquire and set up their own servers and end-node devices, creating long-distance networks for exchange data without the need to use Internet technology, obtain licenses from an agency, saving both time and cost, where the programming of these machines is not very difficult because of its open source. In addition, this paper suggested increasing a reliability for dealing with the data sent within this network. It occurs by adding an additional encryption layer with a digital signature using the elliptic curves cryptography system which added more reliability and security to this network.

References

1. Mekki, K., Bajic, E., Chaxel, F. & Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express.* ISSN: 24059595. doi:10.1016/j.icte.2017.12.005. http://linkinghub.elsevier.com/retrieve/pii/S2405959517302953 (2018).
2. Al-Fuqaha, A, Guizani, M, Tutorials, M. M.. . . S. &. & undefined 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *Ieeexplore.Ieee.Org* **17,** 2347–2376. ISSN: 2316-9451 (2015).
3. Petajajarvi, J., Mikhaylov, K., Roivainen, A., Hanninen, T. & Pettissalo, M. *On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology* in *ITS Telecommunications (ITST), 2015 14th International Conference on* (2015), 55–59.
4. Mikhaylov, K., Petajajarvi, J., Haapola, J. & Pouttu, A. D2D communications in LoRaWAN Low Power Wide Area Network: From idea to empirical validation. *2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017,* 737–742 (2017).
5. LoRa Alliance. LoRaWAN™ 1.1 Specification. *LoRaWAN™ 1.1 Specification,* 97331 (2017).
6. Bor, M. C., Roedig, U., Voigt, T. & Alonso, J. M. Do LoRa Low-Power Wide-Area Networks Scale? *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWiM '16,* 59–67 (2016).
7. Centenaro, M., Vangelista, L., Zanella, A. & Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications* **23,** 60–67. ISSN: 15361284 (2016).
8. Alliance, L. What Is LoRa. *Available (accessed on 5.1. 2017): https://www. loraalliance. org/What-Is-LoRa/Technology.*
9. Semtech Corporation. LoRa Modulation Basics, 1–26 (2015).
10. Stočes, M., Vaněk, J., Masner, J. & Pavlík, J. Internet of Things (IoT) in Agriculture - Selected Aspects. *Agris on-line Papers in Economics and Informatics* **VIII,** 83–88. ISSN: 18041930 (2016).
11. Bjelcevic, S., Jemson, J., Karusala, N. & Purcell, D. LAMBS: Light and Motion Based Safety, 1–5 (2015).
12. Lee, J., Hwang, D., Park, J. & Kim, K.-H. Risk analysis and countermeasure for bit-flipping attack in LoRaWAN. *2017 International Conference on Information Networking (ICOIN),* 549–551 (2017).
13. Paterson, K. G. & Yau, A. K. *Cryptography in theory and practice: The case of encryption in IPsec* in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (2006), 12–29.
14. Committee, I.L. S. *et al.* IEEE Standard for Information technology-Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendmentl: Radio Resource Measurement of Wireless LANs. *http://standards. ieee. org/getieee802/download/802.11 n-2009* (2009).
15. Sinha, R. S., Wei, Y. & Hwang, S. H. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express* **3,** 14–21. ISSN: 24059595 (2017).
16. Fips, N. 197: Announcing the advanced encryption standard (AES). . . . *Technology Laboratory, National Institute of Standards . . .* **2009,** 8–12. ISSN: 13534858 (2001).
17. Lorawan, R. & Avoine, G. Rescuing LoRaWAN 1.0. *N.a.* https://eprint.iacr.org/2017/651 (2016).
18. Zulian, S. Security threat analysis and countermeasures for lorawan join procedure (2016).
19. Dhanashree, M., Kuthe, M, Avinash, P. & Agrawal, J. Implementation of Blind Digital Implementation of Blind Digital Implementation of Blind Digital Implementation of Blind Digital Signature Signature Signature Signature U U U Using Sing Sing Sing Ecc Ecc Ecc Ecc. *International Journal of Computer Science and Network* **1,** 2277–5420 (2012).
20. Lauter, K. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications* **11,** 62–67 (2004).
21. Tian, X., Wong, D. S. & Zhu, R. W. Analysis and improvement of an authenticated key exchange protocol for sensor networks. *IEEE Communications letters* **9,** 970–972 (2005).
22. Kodali, R. K. & Sarma, N. N. in *Emerging Research in Electronics, Computer Science and Technology* 471–478 (Springer, 2014).