Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications

Conference Paper · April 2019

DOI: 10.1109/WF-IoT.2019.8767250

CITATION
1

READS
671

3 authors, including:

Nilupulee Gunathilake
Edinburgh Napier University
6 PUBLICATIONS **3** CITATIONS

SEE PROFILE

William J Buchanan
Edinburgh Napier University
451 PUBLICATIONS **1,030** CITATIONS

SEE PROFILE

Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications

Nilupulee A. Gunathilake, William J. Buchanan and Rameez Asif

***Abstract*— High/ultra-high speed data connections are currently being developed, and by the year 2020, it is expected that the 5th generation networking (5GN) should be much smarter. It would provide great quality of service (QoS) due to low latency, less implementation cost and high efficiency in data processing. These networks could be either a point-to-point (P2P) communication link or a point-to-multipoint (P2M) communication link, which, P2M is also known as multi-casting that addresses multiple subscribers. The P2M systems usually have diverse nodes (also called as 'Things') according to services and levels of security required. These nodes need an uninterrupted network inter-connectivity as well as a cloud platform to manage data sharing and storage. However, the Internet of Things (IoT), with real-time applications like in smart cities, wearable gadgets, medical, military, connected driver-less cars, etc., includes massive data processing and transmission. Nevertheless, integrated circuits (ICs) deployed in IoT based infrastructures have strong constraints in terms of size, cost, power consumption and security. Concerning the last aspect, the main challenges identified so far are resilience of the deployed infrastructure, confidentiality, integrity of exchanged data, user privacy and authenticity. Therefore, well secured and effective cryptographic algorithms are needed that cause small hardware footprints, i.e. Lightweight Cryptography (LWC), also with the provision of robustness, long range transfer of encrypted data and acceptable level of security.**

In this paper, the implementation, challenges and futuristic applications of LWC algorithms for smart IoT devices have been discussed, especially the performance of Long-Range Wide Area Network (LoRaWAN) which is an open standard that defines the communication protocol for Low-Power Wide Area Network (LPWAN) technology.

***Index Terms*— Lightweight cryptography (LWC), Internet-of-Things (IoT), encryption**

I. INTRODUCTION

Cryptography is a well-established, secure information and communication technique derived from mathematical concepts and a set of rule-based calculations called algorithms. It transforms messages (cipher) in diverse ways, so that it is hard enough to decipher [1]–[3]. These algorithms are used for cryptographic key generation, digital signing and verification to protect data privacy, safe web browsing on the internet and confidential communications such as credit card transactions, email, etc. In parallel, cryptographic systems are being progressed with the improved performance of algorithms, i.e., Advanced Encryption Standard (AES) [4], [5], Rivest Shamir Adleman (RSA) and Data Encryption Standard (DES).

*This work is supported by the research grants from School of Computing, Edinburgh Napier University, UK

Nilupulee A. Gunathilake, William J. Buchanan and Rameez Asif are with Blockpass Identity Lab (BIL), School of Computing, Edinburgh Napier University, United Kingdom. Any correspondence related to this article can be sent to (nilupulee.gunathilake@napier.ac.uk).

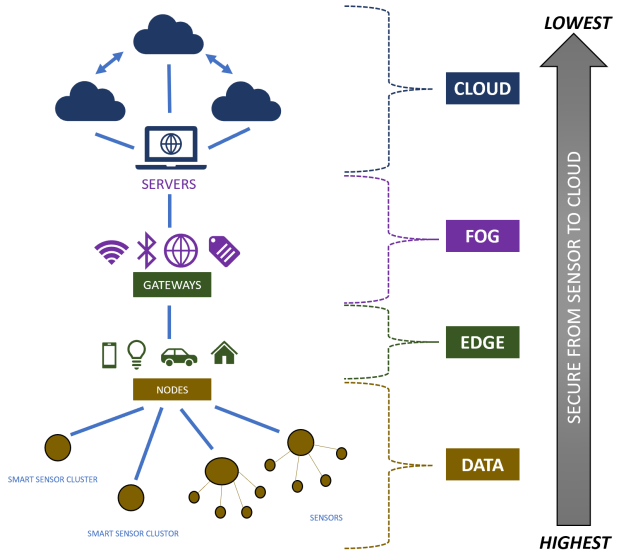

Fig. 1. Security levels of IoT architecture

According to the latest estimations, more than 18 billion IoT devices will be connected via cloud platform by 2020. Amongst, 57% will be industrial IoT (IIoT) applications [6]. Thus, the insurance of privacy and data protection is struggling at the moment to be solved. Generally, IoT devices target simple data processing, i.e, smartwatch, radio frequency identification (RFID) tags, mobile apps, etc. Therefore physical appearance as well as computational capacities are often small, i.e., low random access memory (RAM), low data rates, small internal memory, battery powered, etc. Because of that, unlike in desktop computers, tablets, and so on, IoT devices are unable to allocate considerable memory and processing energy just for security functions. That is when a need of lighter version of conventional cryptography arose, which is named as lightweight cryptography (LWC) [7]. This version expects to execute cryptographic algorithms with use of a few computational cycles providing high robustness against security attacks meanwhile.

LWC is yet in its emerging phase. Nevertheless, the necessity of efficient LWC methods is an urgent requirement in IoT to proceed with 5GN smart city demands of data processing. That includes ultra-high speed transmission, very low latency, affordability, open source capabilities, green networking with minimal power consumption and prevention of possible new threats or attacks. Hence our effort is to propose a novel LWC optimization that can rely on

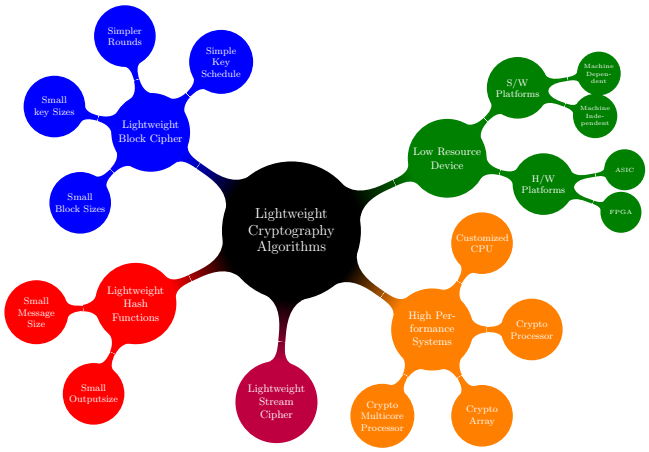

Fig. 2. Lightweight Cryptography (LWC) Classification

less on-board memory, less computing resources and longer battery life with the least possible power consumption. In addition, to deliver efficient security and confidentiality. As the initial state, this paper is a summary of the state-of-the-art findings. The paper structures theoretical as well as empirical approaches in academia and LWC predictability towards LoRaWAN which helps cover long-range IoT communications [8], [9].

II. State of the Art

The key features of an IoT prototype are the sensors which collect data, the edge which offers an entry point to the core network, the fog which is a supportive construction to process edge data, and lastly, the cloud which manages data distribution and storage. A comprehensive diagram for IoT security levels is shown in Fig. 1. The whole architecture operates integrated with different technologies and network protocols, i.e., near field communication (NFC), low energy Bluetooth, ZigBee, wireless fidelity (Wi-Fi) direct, etc. There are tremendous advantages of using IoT sensors in a smart city environment, but security and privacy concerns are enormously challenging at the moment. It has been investigated that the level of security deceases towards the cloud level from the data level, i.e. data in transit has more threats [10], [11].

A. Theoretical Approaches

For imparting a high level of security to IoT devices, few challenges do exist as:

- IoT devices operate on low power, but the least possible latency is expected.
- Current successful implementations of IoT devices work up to a maximum of 100-150 m distances only [12]. Thus improving the availability for longer distance transmission is essential.
- Huge number of networking nodes connects and disconnects simultaneously at the same time. Hence an insurance must be there that none of the node leaks information or gets attacked by, during handovers.
- Smart networks may create smarter threats/hazards that may be blind spots to researchers or security analyzers for some time. In fact, real-time access to the data of smart cities may give researchers more in-depth knowledge of the dynamics, but there should be a mutually agreed General Data Protection Regulation (GDPR) scheme in place.

For long-distance IoT networks, researchers are looking into LoRaWAN protocol which is ultimately a cost-effective implementation in the unlicensed frequency spectrum. Moreover, it is a media access control (MAC) layer based technique that can be used for communications up to 20-25 Km successfully under low power [13], [14]. As per concerns in any security mechanism in LoRaWAN, cryptography is highly responsible for validating heftiness against attacks, prevention of hazards and self-recovery having minimal risk of complete failure. In comparison, LWC is a novel tactic as in Fig. 2, although it does not have enough literature [15] to validate optimized performance nowadays. Especially, resource allocation and software-defined networking still are a necessity to be investigated. However, the literature proposes 2 core categories of LWC depending on the type of the application, its hardware (HW) and software (SW) aptitudes [7], [15], such as:

- **Ultra LWC:** Correspondence only to specific areas of the algorithms, i.e., selective micro-controllers (μC), selected cipher sections (block/stream/hash), etc.
- **Ubiquitous LWC:** Compatibility to wide variety of platforms, i.e., 8 bit to 32 bit μCs, field programmable gate arrays (FPGA), etc.

Existing research trials are primarily based on ubiquitous LWC. Nevertheless, ultra LWC is implementable with existing regular resources [16], [17]. The LWC further lies under 2 forms likewise in conventional cryptography, known as symmetric and asymmetric. Yet only symmetric developments are available [16]. Due to the complexities associated with asymmetric key generation, authentication and validation, it finds problematic to invent methods to share private-public key relationships by means of a few computation cycles that would cause small footprints. The categorization of LWC is shown in Fig. 2. In block ciphers, CLEFIA and PRESENT indicate promising grounding for practical systems at the moment [16]. Concurrently, sub versions of AES along with some modifications have proven successful approaches towards LWC block ciphers [13]. To specify, Grain v1, MICKEY v2 and Trivium are some LWC algorithms considered in stream ciphers [13], [14]. Correspondingly, a theoretical study mentions that hash functions are too immature to adopt its tasks individually, but a combination of LWC hash functions and LWC block ciphers would be a proper recommendation [16]. Amongst, some of the most common algorithms together with their performance parameters are shown in Table I.

B. Empirical Approaches

According to the existing literature published, a greater number of empirical analysis are biased on enhancing Lo-

TABLE I

COMPARISON OF LWC ALGORITHMS WITH CLASSICAL AES METHOD

Cipher	Block size (bit)	Key size (bit)	Security level	Target
AES	128	128	0.70	SW, HW
Fantomas	128	128	NA	SW
HIGHT	64	128	0.69	HW
LBlock	64	80	0.72	SW, HW
LED	64	80	NA	SW, HW
Piccolo	64	80	0.56	HW
PRESENT	64	80	0.84	HW
PRINCE	64	128	0.83	HW
RC5	64	128	0.90	SW
Robin	128	128	NA	SW
Simon	64	96	0.67	SW, HW
Speck	64	96	0.58	SW, HW
TWINE	64	80	0.64	SW, HW

Note: NA = Not Applicable

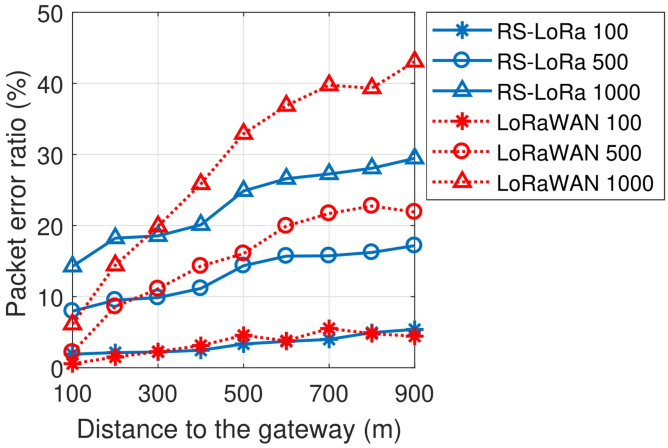

Fig. 3. Evaluation of RS-LoRa PER against distance to the GW [12]

RaWAN key management in order to afford sufficient security. Even though it has nothing to do with the expansion of LWC, optimization in traditional LoRa architecture now offers better cryptographic characterizes via its improved key management. More technical information together with result summary is available in [17], [18]. The objective they considered was to update the key once the key is leaked, however, it was impossible in the past. Therefore, each node is encouraged to have a different key, so once a key is known, only the particular node would be at risk. Moreover, the decreasing number of gateways (GW) progresses the energy efficiency [19]. The study states that LoRaWAN performs better when the nodes are closer to the GWs, as a result, reduced performance tends to occur in the middle nodes, as in Fig. 3. Regardless, several studies [13] emphasis on modifications of AES algorithm to gain small memory footprints, whereas a study [14] was able to minimize the encryption power down to 26.2%. All the referred efforts had targeted 3 types of attacks, which are known key, replay and eavesdropping [13], [14], [17]. Only one study [18] was able to reach up to 5 different attacks, including 'falsification' and 'battery exhaustion' in addition. The trials had been conducted on a simulation basis. To conclude the outcomes:

- Studies [15], [17] prove that the battery life can be maintained from 5-10 years via their LW scheduling in LoRaWAN.
- A trial [17] shows that fairness can be improved by 99.6% by reducing packet error ratio (PER) in 20%. Their method is named as RS-LoRa.
- A consequence occurred in an experiment [15] through the introduction of overheads when the security was better upgraded, but further optimization could reduce 43% of the overheads from the end devices and 48% from the network server side.
- Minimizing the encryption power by 26.2% [13] as mentioned above is also a great accomplishment.

III. DISCUSSION

According to the Tab. I, it is obvious that RC5 can be assumed to have the strongest security feature owning the highest security level of 0.90. In contrast, it has the lowest available block size, which is 64 bits while having 128 bits for the key size which is the longest amongst. However, long key generation technically improves the quality of security though, it tends to outbound the expectations of LWC slightly. Also, the targeted area of RC5 is towards SW attacks only. However, the 2nd strongest one being PRESENT retaining 0.84, it also has the same block size as RC5 and a lower key size, which is 80 bits, but targeted only HW attacks. Both SW and HW wise, AES, LBlock, LED, Simon, Speck and TWINE are available though, their strength varies from 0.58 to 0.72. Consequently, AES takes the highest block and key sizes that might not satisfy LWC objectives, because those are expected to be minimum. In comparison, LBlock, LED, Piccolo, PRESENT and TWINE satisfy the LWC expectations keeping the lowest block and key sizes. The predictions towards exact attack types of a device may be not accurate, also it increases the risk factor. Thus, robustness to both SW and HW attacks is a necessity. In the present, algorithms that are capable of handling both SW and HW targets comparatively have lower strength. Therefore, further work to strengthen security features is desired theoretically and practically. In addition, empirical trials would validate the accuracy of the methodologies if the experiments are scaled up beyond just simulations.

The ultimate level of LWC is only possible if security functions are capable of being executed through LW scripting languages, i.e., Io, wren, squirrel, etc. There is no available preliminary effort taken on the matter known to the authors at the moment. More on, the creation of LW scripting language libraries has the highest demand in the present due to the lack of concerns. The overall challenges and objectives of LWC can be concluded such that:

- Unavailability of the essential libraries in LW scripting languages, thus, initial work has to be started on the subject.

- Power drainage issues over introduced overheads by the adoption of conventional cryptography over smaller footprints for LW scale.
- Each individual case is based on different open system interconnection (OSI) layers, mainly on physical (PHY) layer and MAC of data link layer, hence, all 7 layers should be taken into account to investigate the overall performances.
- Security assurance of the whole four-layer IoT architecture, shown in Fig. 1.
- A proper measuring method is needed to validate research outcomes depending on the LWC categories, i.e., block, stream, hash, etc.
- Control mechanisms are essential to prevent privacy violations through open source IoT devices, defining privacy policies can be suggested as a solution.
- Cost efficiency may be deficient due to payments on cloud platforms.
- The assurance of cloud security is a must, which may be difficult when cloud companies are not transparent to clients or third parties.

Therefore, our aim is to propose or optimize LWC algorithms that would result in less on-board memory usage along with less computational resources, being more economical, that also helps support green networking by power saving. Meanwhile, to provide sufficient security and confidentiality to resource-limited 5G IoT devices. The objective is to design a method to include highly secured LWC mechanism in smart IoT devices, hence, the project will deal with theoretical analysis initially and empirical experiments lately. Thus, the attention should be given to:

- Consideration of the number of central processing unit (CPU) cycles for the number of algorithmic calculations and operations.
- Analysis of random access memory (RAM) and read-only memory (ROM) requirements.
- Mathematical algorithm adoption for enhancing security features.
- Real time experiments of the proposed LWC mechanism on actual HW.
- Verification of the proposed crypto system for all possible IoT attacks.
- Analysis of the results obtained and finalization.

IV. CONCLUSIONS

LWC is a novel approach headed for smart security applications in low-power constrained data-processing devices. Specifically, in IoT applications, provision of high-level security is challenging due to their in-built low-speed processors and low memory modules. Therefore, much lighter versions of conventional cryptography or new cryptologic algorithms are researched on to suggest durable security solutions. This paper has covered the necessity of LWC, its current status, compatible technologies and protocols, i.e., LoRaWAN, and also challenges in the present situation by evaluating existing theoretical and practical studies in academia. The overall analysis indicates promising capabilities in the direction of successful implementation of LWC and its performance towards 5GN smart cities. Yet, more theoretical, application-oriented and feasible empirical researches have to be further conducted in order to reach the ultimate optimization of security assurance and privacy protection in the IoT world.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, March 2002.

[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Phot.*, vol. 8, pp. 595–604, July 2014.

[3] W. Wootters and W. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, September 1982.

[4] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen, "Design and implementation of low-area and low-power aes encryption hardware core," in *9th EUROMICRO Conference on Digital System Design (DSD'06)*, Aug 2006, pp. 577–583.

[5] V. Dao, A. Nguyen, V. Hoang, and T. Tran, "An asic implementation of low area aes encryption core for wireless networks," in *2015 International Conference on Communications, Management and Telecommunications (ComManTel)*, Dec 2015, pp. 99–102.

[6] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431 – 440, 2015.

[7] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *Journal of Cyber Security Technology*, vol. 1, no. 3-4, pp. 187–201, 2017.

[8] J. Darivandpour and M. J. Atallah, "Efficient and secure pattern matching with wildcards using lightweight cryptography," *Computers & Security*, vol. 77, pp. 666 – 674, 2018.

[9] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems – a comparative analysis," in *Data Privacy Management and Autonomous Spontaneous Security*, J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 333–349.

[10] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544 – 546, 2018.

[11] C. C. Byers, "Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for fog-enabled iot networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 14–20, AUGUST 2017.

[12] O. Yassine, M. Baslam, and M. Oukessou, "Lpwanieee 802.11ah and lorawan capacity simulation analysis comparison using ns-3," in *2018 4th International Conference on Optimization and Applications (ICOA)*, April 2018, pp. 1–4.

[13] K. Tsai, Y. Huang, F. Leu, I. You, Y. Huang, and C. Tsai, "Aes-128 based secure low power communication for lorawan iot environments," *IEEE Access*, vol. 6, pp. 45 325–45 334, 2018.

[14] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Enhancing the security of the iot lorawan architecture," in *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, Nov 2016, pp. 1–7.

[15] R. Sanchez-Iborra, J. Snchez-Gmez, S. Prez, P. J. Fernndez, J. Santa, J. L. Hernndez-Ramos, and A. F. Skarmeta, "Enhancing lorawan security through a lightweight and authenticated key management approach," *Sensors*, vol. 18, no. 6, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/6/1833

[16] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in iot," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb 2017, pp. 887–890.

[17] B. Reynders, Q. Wang, P. Tuset-Peiro, X. Vilajosana, and S. Pollin, "Improving reliability and scalability of lorawans through lightweight scheduling," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1830–1842, June 2018.

[18] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in lorawan," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, April 2018, pp. 129–140.

[19] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of lorawan," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017.