AIP Conference Proceedings

RESEARCH ARTICLE | APRIL 02 2019

Encryption protocols on wireless IoT tools FREE

Onder Sahinaslan

AIP Conf. Proc. 2086, 030036 (2019)
https://doi.org/10.1063/1.5095121

View Online Export Citation

Articles You May Be Interested In

Cryptographic methods and development stages used throughout history
AIP Conf. Proc. (April 2019)

Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions
AIP Conf. Proc. (April 2018)

Cross-object information security: A study on new generation encryption
AIP Conf. Proc. (April 2019)

11 July 2025 11:01:02

AIP Publishing

Encryption Protocols on Wireless IoT Tools

Onder Sahinaslan

Maltepe University, Information Technology, Istanbul, Turkey

ondersahinaslan@maltepe.edu.tr

Abstract. Internet of Things and Security (IoT) is now prevalent in every aspect of our lives. Moreover, the number of wireless electronic devices which can be controlled remotely has proliferated. However, a range of varied difficulties such as data transfer, energy supply, and security may occur in IoT devices; therefore, it is imperative that the most suitable connection type be chosen for the sake of the efficiency and security of the process. The choice of cryptological keys exerts direct influence on data security, instant data density, and the length of the encryption time, and excess processing power, on the other hand, shortens battery life. This study has been conducted in order to inspect the preferable cryptological keys, for wireless smart-devices equipped with latest technology, in terms of speed and reliability.

Keyword: Wireless IoT Security, Cryptography, IoT Protocols, Encryption Algorithms
Mathematics subject classification: 11T71, 14G50, 94A60

INTRODUCTION

By interconnecting devices; standardized, administrable, scaleable, end-to-end ecosystems which are able to work conjointly through cloud computing. IoT accounts for the body of systems which modulate and control how tangible objects detect and transmit data, see, think, decide, and communicate with each other[1]. Corporations and users acquire valuable data swiftly, and the market share of IoT has been growing exponentially. These innovations will advance and eventually become more prevalent through practical solutions. Smart gateways stretching from end-devices to cloud services must be protected by means of powerful cryptological encryption protocols, the data transfer must be concealed, and each datum must be consistent. The established body must not effect any delay or malfunction in the process of transfer between the sender and the receiver. Devices which connect to the internet, apart from the computer, are called things, and the network manifested by these objects is called The Internet of Things. The likes of smartphones, tablets, GPS trackers, home automation systems, electricity-gas etc. meters are embedded electronics. Performance matters in IoT, to which myriads of objects, and by which several platforms and technologies are connected. It is estimated that people will be able to economise on energy, time, and monetary things owing to The Internet of Things, and that it will become essential. According to the latest report published by IDC, the total volume of expenditures of The Internet of Things, a new paradigm which rapidly makes its mark in the domain of telecommunication, will be nearing a sum of $800 billion in 2018[2]. Therefore, in this context, it is pivotal that the protocols of inter-object such as 6LoWPAN, 6TiSCH, CoAP, WPA3 be formulated with paramount regard for security. Next, the communication inter se the devices, the amount of power consumption, routing protocols, security compatibilities, encrypted connections, and appropriate switching models will be expounded.

LITERATURE REVIEW

There exist various protocols used in communication among the objects. Transfers of package and message on the network are provided by the protocols defined in the device. Each protocol has its respective unique means of encryption, compression, and error checking/correction, in which domain lots of research and laboratory studies are conducted on a regular basis. IEEE 802.15 is a convenient standard for domains compatible for low-power consumption and rapid transfer[3]. The 6LoWPAN standard enables small devices with the IEEE 802.15.4 physical layer to connect to the internet via IPv6 addressing[4,5]. The devices must exchange some security parameters in order to ensure the safety of the data[6]. Some preexisting means of encryption are not compatible for IoT due to high-energy requirements, transaction costs, and security[7]. The determination process of the protocol which is going to be used hinges on application needs[8]. In the IoT device, CoAP is employed owing to its simple interface and use[9]. The new WPA3 standard is further fortified by means of strong encryption of data protocols[10].

11 July 2025 11:01:02

International Conference of Mathematical Sciences (ICMS 2018)
AIP Conf. Proc. 2086, 030036-1–030036-4; https://doi.org/10.1063/1.5095121
Published by AIP Publishing. 978-0-7354-1816-5/$30.00

WIRELESS ACCESSORIES USED IN IOT VEHICLES

Objects communicate with each other through embedded software on wireless devices. Many devices are required to communicate by wired or wireless means within smart structures, and there is a soaring interest in wireless networks due to the mobility and practicality of contemporary technology. Wireless connections -many of which are powered by cell batteries and expected to operate continually for years without having it replaced- such as Wi-Fi, GPRS, Bluetooth, RFID, LPWAN, Z-Wave, Zigbee, Infra-Red are employed among smart objects. It is not conventional for devices such as Wi-Fi, Ethernet and GPRS to connect to the internet; however, 6LoWPAN is a recently developed technology which enables devices operating with cell batteries to establish a connection to the internet. 6LoWPAN technology is a short-ranged technology operating on low power, and is also capable of IPv6 addressing [11].

In the domain of IoT, LPWAN is employed in wide networks that operate on low power. The most appropriate option of network should be selected, pertinent to the application, after having considered factors such as battery life, power demand, security, and data requirements[12]. Electronic devices gradually get smaller in size, more powerful in capacity; and endeavours to optimize the power usage are in progress. Zigbee network, which is based on the principle of minimizing power consumption for low data usage, enables low-end devices which operate on cell batteries to connect to the internet. Not only does it activate sleep mode when there is no exchange of data in order to preserve its modest levels of power consumption, but it also does not transfer large data[13]. ZigBee is also able to protect the device in the event of exchange by encrypting each and every datum. Moreover, it can be used for IoT devices which demand more memory and superior security. However, it is not that prevalent as of yet[14].

ENCRYPTION IN WIRELESS IOT DEVICES

It is often SSL and TLS encryption layers which are generally used to provide security for the objects in the internet; the former is used as the secure layer, whereas the latter takes on the role of the transport layer - which empowers the former. TLS, which has recently become the regular protocol for secure internet applications, supports a variety of symmetrical encryption systems including one which has RC4 streaming encryption as its foundational basis[15]. Although TLS provides secure communication, the likelihood of encountering cyber-attacks still persists due to a number of deficits in the core algorithm. The Markov Chain model is recommended to ensure the confidentiality and integrity of the data transmitted in Secure Sockets Layer / Transport Layer Security (SSL / TLS) connections[16]. In IoT data transmission, any discrepancy or latency likely to occur is detected through a formula which calculates the possibility of error.

Discrete-time random variable Xt for any t = t0, t1, ..., tn ∈ T. It takes values it ∈ {1, ..., s}, where it is either an SSL/TLS message type or a sequence of the SSL/TLS message types transmitted in a single TCP segment, Xt is a first-order Markov chain;

$$P(X_t = i_t | X_{t-1} = i_{t-1}, X_{t-2} = i_{t-2}, \ldots, X_1 = i_1) = P(X_t = i_t | X_{t-1} = i_{t-1}).$$

In the formula above, the events at the time of t + 1 are dependent on the time t. It is ensured that each datum is seamlessly and continually transferred to the receiver object owing to the statistical nature of Markov models[16].

RSA is known as the most prevalent method which allows both encryption and digital signatures. Since RSA is an asymmetrical encryption technique, sharing the encryption key is not obligatory, hence the encryption key of neither party needs concealing, which relieves the system of a substantial storage load as it is fairly difficult to deal with large numbers. AES, which is an advanced encryption standard, is the symmetrical counterpart of RSA, and it being common is another commonality they share. So, the receiver and the transmitter use the same key to encrypt and decrypt the message - provided that it is only them who have possession of the key. AES is often used with a 128-bit switch in IoT devices. MAC session key is yet another algorithm which both allows cryptographic control over the information, and detects the intended and unintended alterations within the message sent. Since it is a one-way algorithm, the reciprocation of inputs is not possible.

11 July 2025 11:01:02

FAST SWITCHED IOT ENCRYPTION PROTOCOLS

Devices in the Internet of Things technology can either generate data according to their capabilities, or both generate data and process this data to the border router. In switch selection, it is important to pay attention to safe and fast encryption that is compatible with the routing protocols defined on the device. Nowadays, WPA3, CoAP and Wi-Fi Easy Connect are preferred as fast encryption protocols in IoT tools.

IEEE 802.15.4 is an important standard in the development of the communication protocols which are used for the Internet of Objects. The data transfer rates are between 20kbps and 250kbps. It is preferred to be used with low speed wireless networks. It supports AES encryption method. Wireless smart objects use 6LoWPAN, LR-WPAN, ZigBee infrastructures for network access.

WPA3 is the new wireless encryption standard released after WPA2. A poor access to the network in previous Wi-Fi accesses was also a threat to other connected objects. With WPA3, a different security protection has been created according to each device in the network. It has 192-bit encryption. WPA3 uses a new switch exchange protocol called Simultaneous Authentication of Equals (SAE). SAE, also known as Dragonfly Key Exchange Protocol, is a safer key exchange method that fixes the KRACK vulnerability.

Dragonfly Key Exchange Structure; In a message which is transferred from Object A to Object B, After elliptic curve parameters are shared and the PE is derived, both parties will then generate a private r and mask m, which are randomly chosen large numbers in the range {1...q}. They will then use those values to calculate a scalar s and, along with the PE, calculate an element E using the given Equations [7,17]

$$s_A = r_A + m_A \mod q$$

$$E_A = (m_A \times PE)^{-1}$$

$$ss = r_A \times (E_B + (s_B \times PE))$$

$$ss = r_A \times ((m_B \times PE)^{-1} + ((r_B + m_B) \times PE))$$

$$ss = r_A \cdot ((m_B \times PE)^{-1} + (r_B \times PE) + (m_B \times PE))$$

$$ss = r_A \times r_B \times PE = r_B \times r_A \times PE$$

$$confirm_A = H(kck + s_A + s_B + E_A + E_B + A)$$

The security of this protocol lies in the intractable nature of the dot product operation in discrete logarithmic computation. By knowing EA and PE, it is computationally intractable to find mA. This level of security strength allows for the user to have a less complicated password for ease of use [16].

Especially, it is resistant to offline decoding attacks by establishing advanced privacy. Advanced privacy prevents an attacker who decrypted a previously saved Internet connection even if they know the WPA3 password. In addition, the WPA3 SAE uses a peer-to-peer connection to exchange and eliminate the possibility of a malicious middle attacker who has seized keys. CoAP is an application layer messaging protocol developed to enable IoT devices to be connected to the Internet. The difference from the HTTP protocol is that it is developed for the devices which are small and have a limited capacity. CoAP enables communication over UDP while providing communication over HTTP, UDP or TCP. Wi-Fi Easy Connect technology is a standard which is designed for easy connection and simple configuration of Wi-Fi devices. It provides a strong encryption for IoT products which don't have a user interface at all. It uses public key encryption to secure authentication. One of the most important roles for the Wi-Fi Alliance is to ensure that the industry is staying ahead of emerging threats. The Wi-Fi Alliance is one of the most important companies in the world

CONCLUSION

This study has been conducted having taken into account the encryption and access protocols which ought to be in the Internet of Things networks. The importance of infrastructure was remarked upon. As much strong of an encryption as WPA 3 provides, it is still not compatible with contemporary devices. Dragonfly is a powerful encryption structure of WPA3, and CoAP, on the other hand, is a dedicated web transfer protocol for use with limited networks on the Internet of Things - which is also suitable for machine-to-machine (M2M) applications such as smart

11 July 2025 11:01:02

energy and building automation[18]. The purpose of 6LoWPAN is to implement the IPv6 protocol by taking into account the fundamental characteristics of IEEE 802.15.4 such as low-power consumption, low data rate and humble cost. However, it is only provided that connected devices be compatible with IPv6.

When security mechanisms are being designed, each layer of Internet of Things must be double-checked taking into account the security requirements of device layers, and an infrastructure which is able to support a range of different protocols must be established, considering the heterogeneous body of devices. Information acquired through IoT might be crucial. Probable protocol vulnerability and latency occur at an intolerable rate. This study has provided insight into the strength and robustness of protocols and means of encryption, both of which are considered to be standard as of today.

REFERENCES

1. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communication surveys & tutorials vol. 17, No 4, fourth quarter, pp. 2347-2376, 2015.
2. D. Evans, "The Internet of things: How the next evolution of the Internet is changing everything," *CISCO, San Jose, CA, USA, White Paper,* 2011.
3. Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). The Internet of Things: A survey from the data-centric perspective. In C. C. Aggarwal (Ed.), *Managing and mining sensor data* (pp. 383–428). US: Springer.
4. Kushalnagar N., Montenegro G., IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. https://tools.ietf.org/pdf/rfc4919.pdf. Yayın tarihi Ağustos 2008. Erişim tarihi Temmuz 17, 2016.
5. Hui J., Thubert P., Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks. Yayın tarihi Eylül 2011. Erişim tarihi Ağustos 10, 2016.
6. Roman R., Alcaraz C., Lopez J., Sklavos N., Key management systems for sensor networks in the context of the Internet of Things, Comput. Electric. Eng., 37 (2), 147-159, 2011.
7. Lida Xu, Wu He, Shancang Li., Internet of Things in Industries: A Survey, Published 2014 in IEEE Transactions on Industrial Informatics, DOI:10.1109/TII.2014.2300753
8. Palattella M.R., Accettura N., Vilajosana X., Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutorials, 15 (3), 1389 – 1406, 2013.
9. Rahman R.A., Shah B., Security analysis of IoT protocols: A focus in CoAP. 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), IEEE, Umman, 1-7, 15-16 Mart, 2016.
10. Junqing Zhang, Alan Marshall, Roger Woods, Trung Q. Duong., Design of an OFDM Physical Layer Encryption Scheme, IEEE Transactions on Vehicular Technology (Volume: 66 , Issue: 3 , March 2017), DOI: 10.1109/TVT.2016.2571264
11. Xiong X, Zheng K, Xu R, Xiang W, Chatzimisios P. "Low power wide area machine-to-machine networks: Key techniques and prototype". IEEE Communications Magazine, 53(9), 64-71, 2015.
12. Hayder AA Al-Kashoash, Andrew H. Kemp. "Comparison of 6LoWPAN and LPWAN for the Internet of Things", Australian Journal of Electrical and Electronics Engineering · December 2017 with 5,140 Reads, DOI: 10.1080/1448837X.2017.1409920
13. Prodromou, Agatoklis. "TLS/SSL Explained – Examples of a TLS Vulnerability and Attack, Final Part". 2017. https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/
14. ZigBee Alliance (2012). ZigBee Light Link Standard. San Ramon, United States. Version 1.0, ZigBee Document 11-0037-10.
15. Nadhem AlFardan, Royal Holloway, University of London; Daniel J. Bernstein, University of Illinois at Chicago and Technische Universiteit Eindhoven; Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt, Royal Holloway, University of London
16. Maciej Korczynski, Andrzej Dud. "Markov Chain Fingerprinting to Classify Encrypted Traffic", DOI: 10.1109/INFOCOM.2014.6848005, Conference: IEEE INFOCOM 2014
17. Kohlios, C.P.; Hayajneh, T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics 2018, 7, 284. Journal reference, 2018, 7, 284, DOI: 10.3390/electronics7110284
18. Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

11 July 2025 11:01:02