AIST4998/AIST4999: Background Study

Submitted on September 9, 2022

Prof. Wei Meng

YUEN Yu Ching
1155143580

I am submitting the assignment for:

☑ an individual project or

□ a group project on behalf of all members of the group. It is hereby confirmed that the submission is authorized by all members of the group, and all members of the group are required to sign this declaration.

I/We declare that:

(i) the assignment here submitted is original except for source material explicitly acknowledged/all members of the group have read and checked that all parts of the piece of work, irrespective of whether they are contributed by individual members or all members as a group, here submitted are original except for source material explicitly acknowledged;

(ii) the piece of work, or a part of the piece of work has not been submitted for more than one purpose (e.g. to satisfy the requirements in two different courses) without declaration; and

(iii) the submitted soft copy with details listed in the ⟨Submission Details⟩ is identical to the hard copy(ies), if any, which has(have) been / is(are) going to be submitted.

I/We also acknowledge that I am/we are aware of the University's policy and regulations on honesty in academic work, and of the disciplinary guidelines and procedures applicable to breaches of such policy and regulations, as contained in the University website http://www.cuhk.edu.hk/policy/academichonesty/.

In the case of a group project, we are aware that all members of the group should be held responsible and liable to disciplinary actions, irrespective of whether he/she has signed the declaration and whether he/she has contributed, directly or indirectly, to the problematic contents.

I/we declare that I/we have not distributed/ shared/ copied any teaching materials without the consent of the course teacher(s) to gain unfair academic advantage in the assignment/ course. I/We also understand that assignments without a properly signed declaration by the student concerned and in the case of a group project, by all members of the group concerned, will not be graded by the teacher(s).

	September 9, 2022
Signature(s)	Date
YUEN Yu Ching	1155143580
Name(s)	Student ID(s)
AIST4998/AIST4999	AIST Final Year Project
Course code(s)	Course title

1 Problem

LPWAN (Low Power Wide Area Network) is a type of IoT network that enables low-power devices (e.g. remote sensors) to send small amounts f data over long distances. However, since the devices are low-power and computationally constrained, the computational cost and size of each message need to be kept low, which is not ideal for security. Moreover, in contrast to traditional cyberattacks, attacks on IoT devices can compromise entire networks.

LoRaWAN is one such implementation of LPWAN, and is considered relatively robust compared to other solutions [1] due to its flexibility. However, there are still some security concerns with it. Some possible attacks on both generic IoT systems and LoRaWAN networks has been outlined by Torres *et al.* [2]:

1.1 Physical attacks

This type of attack is performed physically: for example, stealing end nodes, inserting malicious nodes, or changing the environment to "confuse" IoT sensors. For LoRaWAN, the attacker may be able to disconnect all connected nodes if they can gain access to a LoRaWAN gateway.

1.2 Bit-Flipping attacks

This attack can be performed when the plaintext has the same order as the ciphertext, or with other ciphers where each field in the plaintext correspond to specific bits in the ciphertext. The attacker only needs to change certain fields in the ciphertext (by modulating the bits in the same position in the ciphertext) to change the deciphered plaintext. This attack is relatively easy, as the attacker doesn't even need much knowledge about the cipher itself to execute it.
For LoRaWAN, a malicious network server can execute this attack when the ciphertext for sensor data are passed through them. The malicious actor can then send the manipulated ciphertext to the application server(s), resulting in incorrect deciphered plaintext.

1.3 Jamming attacks

Jamming attacks works by interfering network signals. For example, a malicious actor can place a radio transmitter between an end node and a gateway and have it send out large amount of radio noise, thereby interfering the radio signals in the LoRaWAN/IoT network, and thus "jamming" the normal flow of data.

1.4 Replay attacks

Replay attack are done by first recording a legitimate sent message (e.g. join request from an end node to a gateway), then replaying it from a malicious device.
In LoRaWAN, the frame counters on both the end-device and the network server are reset to zero. Each transmission from the end node will contain an incremented counter value, and the network server will only accept messages with a counter value greater than the current server-side counter value; accepted messages will increment the server-side counter value to the message counter value. This means that attackers who record a message from the current session will generally fail to launch the replay attack, since the counter value of the recorded message will be lower than the server-side counter value and thus will be rejected. However, in the case of counter value overflow or end-device reset, the server side counter value will be reset to zero, thus providing an opportunity to attack with a message recorded prior to the overflow/reset (since its counter value is likely to be greater than zero) [3].

2 Significance and Impact

In [4], it is stated that there are 12.2 billion connected IoT decvices globally, with a forecasted growth to 27 billion devices by 2025. This represents a pervasive presence of IoT globally, with its presence in many diffferent fields such as Smart Homes and healthcare. It also has a correspondingly large market: [5] forecasted the global IoT market to grow to 1,567 billion USD by 2025. This is a clear sign that IoT technology is widely adopted across different regions and sectors.

Hence, the security of IoT networks are certainly of high importance, as the attacks can leverage against both the vitality of the services provided by the IoT networks, as well as the raw computational/networking power provided by the device inside the network. One such example is the Mirai botnet [6]: by launching dictionary attacks against BusyBox IoT devices, the attackers were able to obtain control of a large amount of such devices, which were then used to launch a Distributed Denial of Service attack to a target server (with methods such as TCP and HTTP flooding).
Another malware listed in [6] is the BrickerBot: instead of utilizing the victim nodes' compuatational power, it instead "bricks" the node by modifying device firmware, deleting files in memory, and reconfiguring network parameters, rendering the device permanently useless. Such attacks can likewise be harmful: monetary cost replacing affected devices notwistanding, such an attack on healthcare-related devices may lead to delays or disability to report correct statistics, leading to delayed or missed treatments, thus harming the patient's health.

3 Existing Approaches and Limitations

Currently, there are some ways of detecting and stopping the attacks. However, there are also some limitations for each of these approaches.

3.1 Physical attacks

To protect against such attacks, end devices should be physically protected. [7] provides a possible solution in the form of Hardware Security Module (HSM), which contains security keys and cryptographic functions, and should be tamper-proof such that the keys are inaccessible by attackers. However, [7] also shows that HSM is not (yet) infailible, as [8] has demonstrated a side-channel attack-based method of extracting keys, which cannot be blocked by HSM.

3.2 Bit-Flipping attacks

Bit-flipping attacks are possible due to an insecurity in the LoRaWAN protocol: [9] and [10] have concluded that since messages from the network server to the application server are not authenticated at the application server, it is possible for a malicious actor positioned between the network server and the application server to execute this attack with a variety of methods.
[9] suggests the usage of secure transmission methods between the network server and the application server as a potential mitigation against such attacks, and also for the Message Integrity Code (MIC) to be preserved through the whole node-application server transmission such that the application server can perform further checking; while [10] proposes a shuffling method to make bit-flipping attacks impractical. However, the LoRaWAN Security Whitepaper [11], which is online at time of writing and thus assumed to be current, does not mention the adoption of the above suggestions, and lists the usage of AES in CTR mode as the payload encryption method, which is asserted as insecure against bit-flipping attacks by [1].

3.3 Jamming attacks

Multiple methods of defending against jamming attacks has been outlined in [1] and [2]. In [1], three approaches are suggested:

- A smaller payload size could decrease the air time, thus making the attack window smaller while also forcing the attacker to constantly recalculate the time to launch the attack. However, this method may not be useful in production scenarios, as the payload size usually have a lower limit for useful messages to be sent, and further decrease in payload size would render the data useless even if the transmission become more secure.
- A random delay between messages sent from the end node would make predictive jamming infeasible, due to the unpredictable offsets from the predicted attack windows; the attacker would be unable to plot out the best attack time in this scenario. However, should the duty cycle time for two legitimate devices overlap, it becomes possible for them to send out messages at the same time, resulting in at least one device being blocked. A possible mitigation would be to ensure that the start and end times of duty cycles does not overlap for any two devices in the network.
- Multi-channel data transmission would increase the difficulty of jamming attacks, as the attacker would need to know the pattern of channel hopping and the corresponding slots to jam all data. However, since the header information about the source and the destination are generally not encrypted, it would be easy for an attacker to learn the above information with minimal effort.

[2] provides further methods against jamming attacks:

- A denser LoRa network could be created, with overlapping coverage regions. As each end node would connect to multiple gateways if available in a network, this would make jamming attacks more difficult, as jamming attacks would need to ensure no gateway receive the transmission. With only one end node-gateway connection, this is relatively trivial, but becomes at least proportionally harder as the number of end node-gateway connections increase. However, this also means that the area covered by the same amount of end node and gateway devices would be smaller due to the higher density required for this defense.
- The network could adopt a higher Spreading Factor (SF) to beat the jammer RSSI. With a higher SF, the gateway would have a higher sensitivity towards received signals, thus forcing the jammer to use more precise/higher-powered signals to successfully jam the transmission.
- The system should also take note of the normal transmission rate of the end devices. Should the transmission rate deviate significantly, the system can then respond accordingly.

3.4 Replay attacks

To protect against replay attacks under the current LoRaWAN specifications, end devices should be physically protected, so that attackers cannot reset the devices; thus giving them less opportunities to trigger a counter reset via device reset.

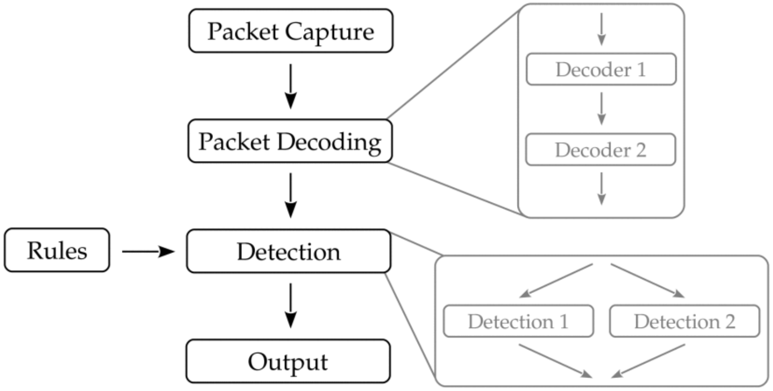
[2] also suggests some adjustments in the LoRaWAN specifications to mitigate against replay attacks. One proposed change is to let the server retain the counter value after an end-device reset: the network server will reject all messages until the message counter value is greater than the one reacher prior to the reset, which means all pre-recorded message (after the last counter overflow) remains useless for replay attacks.

Another proposed amendment is to add a function to end devices which forces a re-activation after each reset, or when the counter value reaches its maximum. Functionally, it would force the end node to disconnect and reconnect (i.e. experience the ”Join request-Join accept” procedure) before any counter value can be reused. Since each session uses unique NwkSKey and AppSKey to encrypt the messages, with the application of this function any messages recorded in a prior session would be useless (since the keys used to encrypt it are no longer valid).

3.5 Suricata

Suricata is an intrusion detection system developed by the Open Information Security Foundation (OSIF). Its architecture is shown in the below figure.

Figure 1: Architecture of the Suricata IDS. [12]



After capturing a network packet, it will be processed by decoding functions, then passed on to the detection module(s). The decoding pipeline will start from the source of the packets, then protocols on incrementally higher layers will be decoded (i.e. L2, L3 including TCP/IP etc.). It can be extended by implementing a new decoding function and adding it to the decoding pipeline.

After decoding, the packet will be passed to the detection module(s). This stage is parallelized, and so a single packet can be processed by multiple modules at the same time. The modules are governed by the user-defined rules. Similar to the decoding module, the detection module can also be extended by implementing a new module and registering it in the table of detection methods [12].

In IoT environments, it is possible for the Suricata IDS to be run on a host computer (for example, the network server in a LoRaWAN network), thus bypassing the power limitations of the end nodes [13].

4 Conclusion

There are some security weaknesses both in LoRaWAN networks and IoT technologies in general; while most of them can be mitigated, some of them require changes to protocol and/or specifications. IDSs such as Suricata can be employed to detect anomalous network activity and handle it reactively.

References

[1] D. B. Max Ingham, Jims Marchang, "Iot security vulnerabilities and predictive signal jamming attack analysis in lorawan," *IET Information Security*, vol. 14, no. 4, pp. 368–379, 2020.

[2] S. I. L. Nuno Torres, Pedro Pinto, "Security vulnerabilities in lpwans—an attack vector analysis for the iot ecosystem," *Applied Sciences*, vol. 11, no. 3176, 2021.

[3] 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)*, 2018, pp. 129–140.

[4] M. Hasan, "State of iot 2022: Number of connected iot devices growing 1814.4 billion globally," IoT Analytics, May 18 2022, accessed 2022/09/06. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[5] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020–2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 449–453.

[6] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[7] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, "Security issues in internet of things: Vulnerability analysis of lorawan, sigfox and nb-iot," in *2019 Global IoT Summit (GIoTS)*, 2019, pp. 1–6.

[8] J. Liu, Y. Yu, F.-X. Standaert, Z. Guo, D. Gu, W. Sun, Y. Ge, and X. Xie, "Small tweaks do not help: Differential power analysis of milenage implementations in 3g/4g usim cards," in *Computer Security – ESORICS 2015*, G. Pernul, P. Y A Ryan, and E. Weippl, Eds. Cham: Springer International Publishing, 2015, pp. 468–480.

[9] X. Yang, "Lorawan: Vulnerability analysis and practical exploitation," Master's Thesis, Delft University of Technology, Delft, The Netherlands, 07-28 2017. [Online]. Available: http://resolver.tudelft.nl/uuid:87730790-6166-4424-9d82-8fe815733f1e

[10] J. Lee, D. Hwang, J. Park, and K.-H. Kim, "Risk analysis and countermeasure for bit-flipping attack in lorawan," in *2017 International Conference on Information Networking (ICOIN)*, 2017, pp. 549–551.

[11] A. Gemalto and Semtech, "Lorawan security whitepaper," LoRa Alliance, East Lansing, Michigan, Tech. Rep. MSU-CSE-06-2, July 2016. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

[12] I. Ghafir, V. Prenosil, J. Svoboda, and M. Hammoudeh, "A survey on network security monitoring systems," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 2016, pp. 77–82.

[13] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for iot-based smart environments: a survey," *Journal of Cloud Computing*, vol. 7, no. 1, p. 21, Dec 2018. [Online]. Available: https://doi.org/10.1186/s13677-018-0123-6