Secure and Efficient Management Architecture for the Internet of Things

Jun young Kim
School of Computer Science and Engineering, UNSW Australia
junyoungkim@cse.unsw.edu.au

ABSTRACT

The capability to securely manage embedded devices is arguably a fundamental functionality for the emerging Internet of Things (IoT). Current Wireless Sensor Networks (WSNs) approaches are not applicable directly for IoT deployments due to new challenges from emerging IoT applications. We propose to address this shortcoming and enhance the process while providing a sufficient level of security. This work proposes to design, implement and evaluate an *efficient and secure* software update/manage architecture for the IoT. We plan to conduct an extensive experimental study on a public testbed to evaluate the design tradeoff and quantify the performance of our architecture.

1. INTRODUCTION

Internet of Things (IoT) encompass a wide range of devices enabling the interconnection of the physical world to the Internet. An efficient, secure, and long-term management system is necessary, as it is studied/used in the Wireless Sensor Networks (WSNs). Since the emerging IoT applications pose a different set of characteristics, existing WSNs solutions may not work efficiently. We address these differences in terms of managing IoT applications, then provide proper solutions.

The Thread group [1] is organized by major IT companies such as ARM, Qualcomm, and Samsung. The main goal of the IoT project is to securely connect/manage a large number (+250) of various devices in home networks. Another goal is to design an energy friendly security in which, even battery powered devices can run for years. Low power and secure management functionality is a necessity to achieve the goals. In this project, communication and computation are two premium resources for the secure/energy friendly design, as radio activities and security operations consume the majority of energy on constrained devices.

2. PROBLEM DEFINITION

Managing remotely deployed sensors has been thoroughly studied in the context of WSNs. However, existing WSNs solutions exhibit poor efficiency due to a wide variety of emerging IoT issues such as mobility, heterogeneity, scale, connectivity, security and privacy, energy, and the ease of management. Among other IoT security and efficiency issues, below three are the baseline issue that make these problems challenging to solve [2]:

Heterogeneity: It is challenging to design a framework that can manage various types of devices. Existing solutions coherently become more complex and suffer from performance degradation while supporting the heterogeneity.

Mobility: Having a coherent and stable view of the network topology is a significant factor for managing IoT applications. Mobility related dynamics make this process difficult and result into inefficiency. Existing solutions experience an extreme resource degradation from constantly tracking the topology view and neighbor information.

Connectivity: IoT applications naturally include the Internet connection capability, and this results in exposure to a wider types of adversaries. It is desirable to identify these threats and provide efficient solutions.

3. DESIGNING THE ARCHITECTURE

3.1 Secure and Efficient Code Dissemination Protocol for the IoT

Many IoT devices are launched in the market without considering security during the design phase and hence can be easily compromised [2]. This makes IoT devices an easy target for attackers. This problem will exacerbate when the number of such poorly designed, faulty, or malicious devices start to wreck havoc in future. Once deployed, IoT devices require secure code dissemination for multiple purposes such as code update, security patch, and parameter change.

3.1.1 Methodology on Group Key Distribution

Existing secure over-the-air (re)programming protocols for WSNs are based on the epidemic communication [5], which assumes homogenous sensor nodes in the network with all nodes participating in the (re)programming process. Epidemic code dissemination approaches perform efficiently and provide security in homogenous networks by exploiting *spatial multiplexing*, i.e., parallel transmissions in different parts of the network. Given the multitude of systems in an IoT network, the epidemic approach would require non-target nodes to participate in the propagation resulting in unnecessary cryptographic operations and additional packet forwarding overhead.

SenSys'15, November 1–4, 2015, Seoul, South Korea..
ACM 978-1-4503-3631-4/15/11.
DOI: http://dx.doi.org/10.1145/2809695.2822522.

As an alternative for the IoT context, we explore multicast communication primitives, known to be more efficient and better suited for heterogenous nodes. In a multicast communication approach, only target nodes involved in the code-image update actively take part in the process. We can significantly reduce the communication and computation overhead compared to epidemic approaches by avoiding unnecessary computation-intensive cryptographic operations. In order to enable the secure multicast approach, a secure group key distribution is a significant pre-condition. Existing group key distribution schemes, however, assume known/fixed group sizes or neighbor pairing for efficient key distribution.

We propose to use a public key cryptography broadcast encryption scheme (BGW_t [3]), which efficiently distributes the shared group key to a dynamic number of target nodes, but results in additional storage with following benefits.

The shortest ciphertext size: Shorter or fixed size ciphertext is desirable, as it is directly proportional to the communication overhead.

Lower decryption complexity: On a dissemination protocol, encryption is performed at a resource-rich trusted server while decryption is performed at constrained nodes. BGW_t has higher encryption complexity of $O(n)$ while lower decryption complexity of $O(1)$, which enhances energy consumption/latency on the constrained nodes.

Fixed size private key: IoT nodes are vulnerable to physical node capture attack, where adversaries compromise nodes to extract pre-installed keys. BGW_t's $O(1)$ private key can be stored in the tamper resistant storage to effectively mitigate physical attacks.

3.1.2 Expected Contribution

We develop a secure over-the-air code dissemination protocol for the IoT, which adopts a multicast communication to improve the protocol efficiency in networks with heterogeneous devices. Our design process will involve the selection and implementation/optimization of a public key cryptographic broadcast encryption scheme. Then allows to distribute a fresh shared key to a dynamic number of target nodes efficiently, and provides authenticity, integrity and confidentiality to the program image update process. Our security analysis will demonstrate that our security properties are not compromised against identified adversary models. We will experimentally validate our system through a prototype IoT platform and demonstrate the efficiency in practical settings. We plan to publicly release our implementation as an open-source code.

3.1.3 Current Status

My poster submission on this work to the Sensys'15 is accepted. We are going to submit a full paper to IPSN'16.

3.2 Reliable and Secure Multicast Protocol

We addressed the open issues on the existing code dissemination approaches. Since we propose to adopt a multicast propagation for efficient code disseminate, providing reliability in the multicast protocol becomes another open problem. Based on our research, achieving a reliable multicast in the IoT environment is challenging due to the feedback implosion problem, which occurs when a large number of receivers sends feedback to the sender.

We propose to design a reliable multicast protocol by using a combination of techniques and evaluate the trade-off between communication overhead and energy to meet the application requirements.

3.2.1 Expected Contributions

Designing a practical reliable multicast protocol is a necessary task for efficient code dissemination in IoT applications. We will investigate the existing reliable multicast protocols suitable or adaptable for IoT applications, and investigate various associated mechanisms and assess their security vulnerability. This will result in a secure reliable multicast protocol for IoT applications.

3.3 Policy Management on IoT Gateways

A secure gateway which can detect mis-configurations and any policy conflict is extremely important for successful deployment of IoT at scale. Also as from the mobility and heterogeneity, the management process becomes complex and suffers from the performance degradation.

Since IoT applications consist of various network services/devices, many policies conflict to each other, which results in various performance degradation and security threats. Unfortunately, in many practical settings, the detection and resolving on-the-fly are commonly a NP-hard problem and they are categorized as different tasks.

3.3.1 Expected Contributions

To address the policy conflict detection/resolution problem, we take advantage of the distinguished modeling and reasoning capacities of Answer Set Programming (ASP) [4]. Our goal is to provide ASP solutions for reasoning over influence graphs and experimental profiles. We believe logic based algorithms can detect and resolve conflicts in predictable and reliable ways. In the end, this will enhance the policy development/management environments.

4. CONCLUSION

In this proposal, we proposed a secure and efficient management system for the emerging IoT applications. We plan to enhance the efficiency of the secure code dissemination process caused by the emerging IoT issues such as heterogeneity and mobility.

Jun young Kim received the M.Eng. degree in computer science from Hanyang University, Seoul, Korea, in 2004. After 12 years of embedded software developer career, he is currently working toward the Ph.D. degree in mid 2017 at the UNSW, Sydney, Australia supervised by Wen Hu and Sanjay Jha. His main research interest is securing the Internet of Things and Wireless Sensor Networks.

5. REFERENCES

[1] The thread group. `http://threadgroup.org/`, 2015.

[2] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 2010.

[3] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO 2005*. Springer, 2005.

[4] M. Gebser, R. Kaminski, B. Kaufmann, and T. Schaub. Answer set solving in practice. 2012.

[5] P. A. Levis, N. Patel, D. Culler, and S. Shenker. *Trickle: A self regulating algorithm for code propagation and maintenance in wireless sensor networks*. Computer Science Division, University of California, 2003.