A20-122 **APPLICATION GROUP**

作品名稱

具備超低功耗喚醒收發機之高安全性物聯網通訊技術

A Secure IoT Communication Technique
with Ultra Low Power Wake-Up Transceiver

隊伍名稱

物聯網不會誤連網 Internet-of-Right-Things

隊長

陳仕恩 成功大學電腦與通信工程研究所

隊員

張勝凱 成功大學電腦與通信工程研究所
李依潔 成功大學電腦與通信工程研究所
韋傑強 成功大學電腦與通信工程研究所

作品摘要

近年來基於物聯網設備的服務提升生活上的許多便利，因此在可見的未來，物聯網設備將快速增加，並且與人們的日常生活緊密結合並且無所不在。然而，物聯網的設備因其在能源與運算能力方面的限制，缺乏嚴謹地加密通訊及身份驗證，因此犧牲資安的防護，造成物聯網安全的嚴重威脅。因此如何在物聯網中同時達成安全防護與能源節省的兩項目標，是目前亟待解決的問題。

為了提升物聯網的安全防護，本作品設計一套嚴謹的多重安全防護系統，如Fig.1所示。本防護系統包含基於物理不可仿製功能 (PUF) 與可信任第三方 (TTP) 的雙向身分驗證機制、低計算量且安全的加密金鑰產生與更新機制、 以及一次性無線電喚醒碼產生與更新機制。首先，在雙向身分驗證機制中，陌生的設備欲加入網路需與閘道器透過 TTP 進行相互驗證，如此可避免攻擊者侵入網路發動攻擊，也可避免駭客偽裝成閘道器劫持整個物聯網。其次，為了避免通訊資料被竊取，我們提出基於 PUF 的加密金鑰產生機制可安全地產生加密金鑰並不斷更新，可大幅提升通訊安全。此外，設備在通訊過程中使用匿名 ID 而且也不斷更新，可避免被針對攻擊，有效確保隱私性。

此外，當物聯網設備運作時，其無線收發機消耗大部分能量。為了有效節能同時進一步提升其安全防護，本作品提出一個搭配喚醒收發機的安全喚醒機制。根據調查，目前市面上尚未有搭配喚醒收發功能的無線通訊設備，且市售之超低功耗無線收發機不能滿足規格需求，因此本作品自行開發一套低功耗喚醒收發機晶片（如 Fig.2 中之 WuTX/RX）。平時低功耗的喚醒接收機持續偵測通道，僅在收到特定喚醒碼時才喚醒高耗能區塊，如此可有效降低功耗，同時減低通訊延遲。此外，為了避免攻擊者竊聽喚醒碼，進而利用它來與物聯網設備建立連線並進行攻擊，本作品設計一次性喚醒碼的機制，在每次完成資料的傳輸後，雙方會各自同步產生新的喚醒碼作為下次通訊之用，如此本機制提供物聯網設備在硬體層級抵禦攻擊的防護。最後，本作品的收發機能夠支援多模調製技術，包括開關鍵控、頻率偏移、以及相位偏移調變，此三種調變方法廣泛的應用在現代低功耗的無線通信系統和無線傳感器網路當中，使其較易於整合進現存的通訊協定或產品當中。

本作品提出低功耗且高安全性智慧物聯網系統可強化資安防護並降低能源消耗，透過 Fig. 2 之實驗展示，可驗證本作品應可解決目前物聯網設備面臨的限制與瓶頸，進一步促進物聯網產業的蓬勃發展。

指導教授

林輝堂 成功大學電機工程學系

- 美國密西根州立大學電機博士，現為成功大學電機工程學系教授。曾任美國朗訊科技貝爾實驗室工程師及傑爾系統工程師。
- **研究領域：**網路安全、無線網路、軟體定義網路、網路編碼、網路服務品質演算法、光纖網路

鄭光偉 成功大學電機工程學系

- 美國華盛頓大學電機博士，現為成功大學電機工程學系副教授。
- **研究領域：**高效節能之射頻前端電路與系統設計、類比數位轉換器與鎖相迴路之低功耗技術、無線供電與獵能電路設計、生醫與感測器介面設計

Abstract

Recently, Internet of Things (IoT) has significantly improved our life quality through many convenient services it provides. While IoT continues ubiquitously integrating into our daily life, it is expected that the number of IoT devices will grow dramatically in the future. However, IoT devices are generally subject to limited computing power and energy budget. Thus, communication encryption and rigorous identity authentication are often neglected. This negligence posts a significant threat on the security of IoT. To resolve the aforementioned issues, this study designs a suite of secure and low-power communication schemes for IoT devices.

To safeguard the IoT security, based on Physical Unclonable Function (PUF) and Trusted Third Party (TTP), we have designed a mutual authentication scheme, a highly secure and low-complexity key generation and update scheme, and a one-time wake-up pattern generation and update scheme. With these proposed schemes as shown in the Fig.1, we are able to significantly enhance the IoT security and defend against various attacks from adversaries, such as Denial-of-Sleep attack, eavesdropping attack, replay attack, cloning attack and impersonation attack.

To dramatically reduce the energy consumption of IoT devices and prolong their operating time, we have designed a low-power wake-up transceiver (see the WuTX/RX in the Fig.2). With the wake-up transceiver, an IoT device is able to implement the wake-up scheme, which is a key technology in minimizing IoT's power consumption. Our wake-up receiver consumes significantly less energy than that of a main receiver up to one thousand times. Furthermore, the wake-up transceiver is designed to facilitate one-time wake-up pattern and mitigate the Denial-of-Sleep attack. The wake-up transceiver supports the popular OOK/FSK/PSK modulation schemes, allowing better integration with the current commercial products. The proposed IoT system has been implemented in the experimental system shown in Fig. 2. Through the demonstration of the experimental system, it is verified that the proposed system is able to significantly reduce the energy consumption of IoT systems while dramatically elevating the level of their security. It is expected that the growth of the IoT market will surge in the near future since the main concerns are resolved by our proposed system.

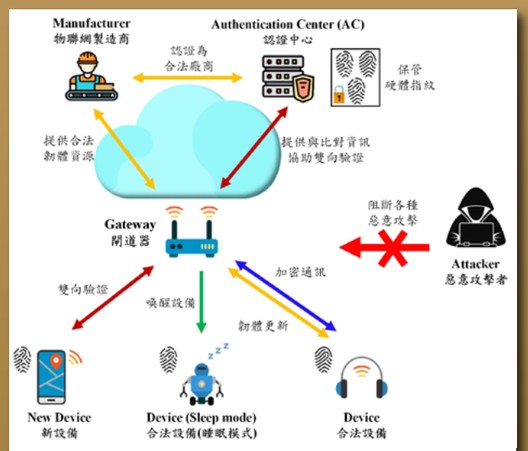

Fig. 1 A low power and high security IoT system architecture

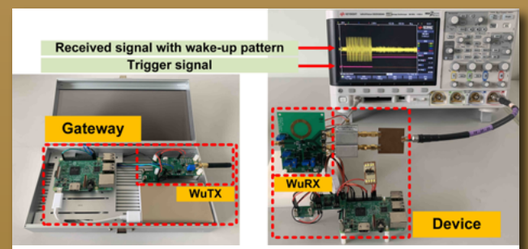

Fig. 2 VDemo architecture