基於物理不可仿造功能之輕量化身分驗證機制

林輝堂 教授

國立成功大學 電機工程學系

簡介

物聯網帶給人們生活的便利，同時也帶來資安威脅。由於物聯網設備配備有限的運算資源與能源，未加密通信傳輸，以及缺乏嚴謹身份驗證，導致攻擊者可輕易發動攻擊，造成重大資安危害。因此，如何在物聯網中達成安全防護、傳輸效率與能源節省的三項目標，是目前亟待解決的問題。本計畫的目的是研發一適用於物聯網網路安全防護機制。首先，本計畫基於設備的物理不可仿製功能(Physical Unclonable Function, PUF)設計一低耗能及低運算的雙向身份驗證機制。此機制可讓物聯網用較低計算量和耗能進行身份驗證，提供網路安全防護。另外，我們設計一資訊傳輸加密機制和驗證機制，提供資訊傳輸保密性和保障其完整性。

關鍵字： 物聯網、網路安全、物理不可仿製功能、加密

驗證流程:

步驟一：

物聯網設備欲加入一個新的物聯網時，會先產生一個隨機值N_D，並利用該數值與自己的PUF製作檢查值，接著將隨機值製作成加入請求。

步驟二：

管理節點收到加入請求後，亦會隨機產生一個數值N_G作為驗證請求，連同加入請求一起傳送給驗證中心。

步驟三：

驗證中心收到身分驗證請求後，解開請求取得相關資訊，然後搜尋資料庫取得該設備的PUF，利用PUF和隨機值N_G產生一個驗證值$Value_V$。接著再使用PUF和隨機值N_D產生回應值$Value_R$。最後將驗證值、回應值以及兩個隨機值加密後，回傳至物聯網管理節點。

Verify_Reply message: ID_G,$\{N_D, Value_V\}_{K_G}$,$\{N_G, Value_R\}_{K_{AC\_D}}$

步驟四：

管理節點收到訊息後，將部分的訊息留下做為驗證設備所用，並用訊息內的隨機數產生對稱式加密金鑰。而剩餘的訊息則作為身分驗證的挑戰訊息，傳給該物聯網設備，請求驗證。

步驟五：

設備收到挑戰訊息後，解開訊息確認回應值與檢查值是否相同，並使用訊息內的隨機值和自己的PUF產生驗證值。接著亦利用隨機值產生加密金鑰，再將驗證值使用該金鑰加密，回傳物聯網管理節點，作為挑戰的回覆訊息。

步驟六：

物聯網管理節點收到回覆訊息後，將訊息解密取得驗證值，並與來自驗證中心的驗證值比對是否相同。如果相同則此物聯網設備通過身分驗證，否則身分驗證失敗。

```
-------------Step 11-------------

Recv Respond Message

Unmodified!
authentication : INFO     140.116.177.120  38922   nsda00008   challenge message
 unmodified
respond:
 c20a4a641c12213c5419ff93e17cc535f443ffc17a9a599c12a17327043d3253
Device verification sucessful!!
authentication : INFO     140.116.177.120  38922   nsda00008   legal device
```

圖1、管理節點成功驗證物聯網設備

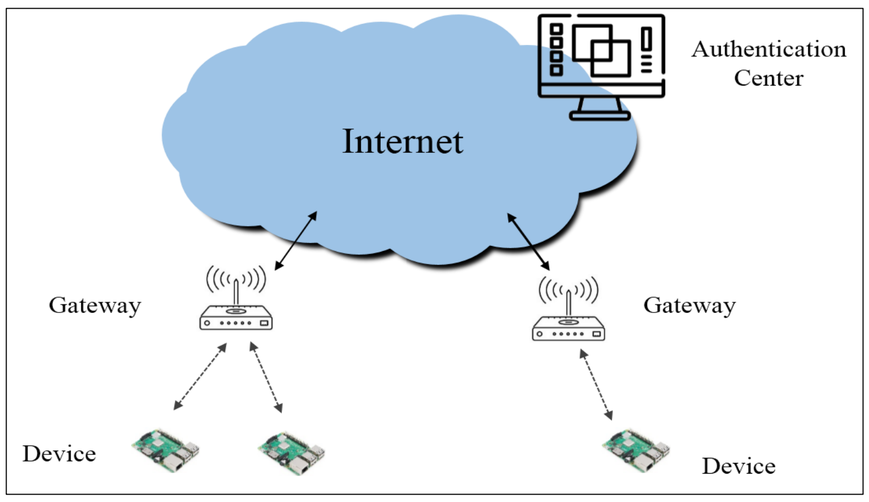

圖2、物聯網系統架構圖

```
---------Device Infomation--------
device_ID:
 nsda00008
PUF:
 OM0A7wh9Brln9cm2
--------------------------------

-------------Step 1-------------
Nonce_D:
 =y0fHar$&SA8907c
Check Code:
 69c2c412d034ad8aeacb338b88a0778e1ffb49ba6c3e20e7ebca97a56996d310
MAC:
 1d53be8978c080adef9922e6a8ac481f50ed6f4bc92be141618b73961d2ad79b
-------------Step 2-------------
Join message:
 b'authentication@nsda00008#47e4f8c4af275f76c64693b3d48f17e5563fc1b00ed33dd67c1d
b06323f9710f#1d53be8978c080adef9922e6a8ac481f50ed6f4bc92be141618b73961d2ad79b'
Message state:
```

圖3、物聯網設備發送加入請求

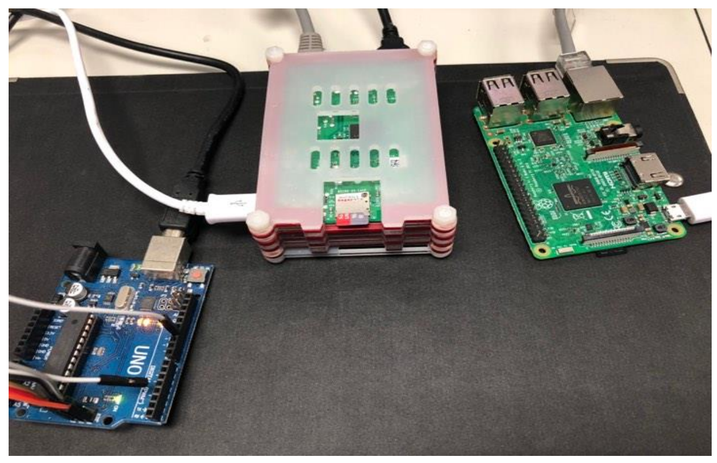

圖4、實作身份驗證機制於Raspberry Pi

結論

- 本計畫所提出的輕量化身分驗證機制，利用PUF作為設備身分和金鑰的來源，提供一個負擔低且安全的驗證機制。
- 圖1和圖3為本計畫身分驗證機制實作在設備上，實際的執行畫面。