Communications of the CCISA
Vol. 28 No. 1 Feb. 2022

於智慧製造環境中具通訊保護機制之設計

戴文諺[1]、董劭威[2]、黃政嘉[3,*]
國立台灣科技大學資訊管理系[1, 2, 3]
[1]nlycloudy112042@gmail.com、[2]leo012178@gmail.com、
[3]jhengjia.huang@mail.ntust.edu.tw

摘要

本研究提供一彈性的外掛模組，可以解決內部網路之間非經授權使用者可，藉由內部網路隨意存取網路上所提供的資源。並針對不具保密性的傳輸資料或不安全的通訊環境作加密處理。在傳輸過程中，許多物聯網的通訊協定，皆以傳統 IP 封包的技術傳輸。然而，傳送端發送 IP 封包時，預估該封包會經過那些路徑是一個難題，同時，在轉送過程中，雖然每一個路由器收到封包後，可以藉由封包上讀取該封包上所註明的目的位址，尋找可能到達的路徑再傳送出去。卻也暴露了，IP 封包內的訊息很容易被洩漏與偽造。因此，本篇模組為了滿足內部網路的安全需求。使用虛擬私有網路 (VPN) 等相關研究，採用 IPSec 協定傳輸的技術，不輕易與外界網路相連，使傳輸的資料較具機密性，且達到安全性的需求。另外，本模組會設計對稱式加密系統，讓本模組無論在任何通訊環境，可以保障設備之間溝通的安全性，進而避免封包上的資訊外洩，使其達成資訊安全的機密性。

關鍵詞：虛擬私有網路、IPSec、IoT 、資訊安全、對稱式加密

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 28 No. 1 Feb. 2022

The Module on Secure Communication Scheme in Smart Manufacturing Environment

Wen-Yan Dai[1], Shao-Wei Tung[2], Jheng-Jia Huang[3,*]
[1, 2, 3] Department of Information Management, National Taiwan University of Science and Technology
[1] onlycloudy112042@gmail.com, [2] leo012178@gmail.com,
[3]jhengjia.huang@mail.ntust.edu.tw

Abstract

This paper provides a flexible plug-in module, which can solve the management problem that the resources provided on the network can be freely accessed without authorization between the intranets. And for the transmission of data that is not confidential or does not guarantee safe arrival at the destination for encryption. Many IoT communication protocols are still transmitted in IP packets during the transmission process. However, when the transmitting end sends an IP packet, it cannot predict which paths the packet will go through. After each router receives the packets during the forwarding process, it reads the destination address indicated on the packets and searches for the destination address. The possible path to reach is then sent out. As a result, the information carried in the IP packet can be easily forged. Therefore, this module is designed to meet the security requirements of the internal network. Research on the use of the private network (VPN), using IPSec protocol transmission technology, is not easy to connect with the external network. The transmitted data is more confidential and meets the needs of security. And in the communication environment, the communication between the two parties will be symmetric encryption to avoid the leakage of information on the packet to achieve the confidentiality of information security.

Keywords: Virtual Private Network, IPSec, IoT, Information Security, Symmetric Encryption

壹、前言

網際網路的蛻變與創新，源源不絕的網路的技術脫穎而出，帶來各種新奇的網路應用，如物聯網、工業物聯網、智慧製造等變革，改變許多商業模式與生產模型，然而，在這看似美好的嶄新發展，卻暗藏了許多難以預估的威脅，其安全研究的課題也隨之表露在各行各業中，並帶給各個領域令人費解的全新難題，帶出以往不同的威脅與未知的攻擊機會。

在現今的物聯網應用中，物聯網除了推動前所未見的應用與創新，帶動許多商業發展，而在這些發展中，網路的部署、設備的保護等物聯網發展也產生許多問題，在現今的 M2M[1]的通訊環境中，傳統的 RS485 Modbus[2]協定、常見的 OPC UA 協定[3]、MQTT 協定[4]設計理念，都是針對點對點的通訊設計。然而，在不同設備間的通訊設計中，會因為不同的協定設計或是設計上的方便性，或是為了迅速帶來實際的收益，往往把安全性給降低，甚至繞過相關安全機制，進而產生許多淺在的安全威脅。

在複雜的協定環境中，許多企業為了滿足資訊安全的需求，會劃分內部網路與外部網路的區域，在這樣架構，內部網路的通訊安全往往藉由權限做控管，讓內網的使用者可以橫向提取資源，如最典型的 DMZ[5]網路架構，作為區分外網 (不信任的外部網路) 與內網 (可信任的內部網路) 的區分，並在這兩者之間建立防火牆或路由器等區隔內外網的網路裝置。然而，隨著網路攻擊型態的變化，愈來愈捉摸不定，許多研究也開始指出 DMZ[5]的不足，進而提出所謂的零信任網路架構 (zero trust network) [6]，零信任網路與傳統的安全模式相比，不是區分可信任與不可信任的網路區塊，而這個新概念的本質是已不再預設任何的信任，零信任網路指出在 DMZ[5]架構中，邊界防護的限制。而這樣的架構，又與許多環境的部署產生衝突，在一般的 M2M 的通訊環境中，如果雙方都是不信任，光是安全協議設計與通訊的方式就要重新設計，進而影響鉅額的成本。

因此，為了方便物聯網的環境部署，同時，可以做到在不影響網路架構下，讓內網的通訊還能做到安全防護，本研究實做出一具彈性化、輕量化的外掛加密模組，其目的在解決複雜的安全設計部署。本模組在物聯網環境中，減少使用者理解大量的安全協定外，對於內部的橫向存取做安全管理，本模組解決 DMZ[5]架構的痛點，讓使用者無需為耗費大量的成本去權限劃分或是去做環境控管。更可以輕易滿足若最新的零信任網路架構 (ZTA) [6]的理念。

本模組的設計理念，提供具有彈性的物聯網通訊的部署，為了在內部可信任網路下，做安全通道，本模組參照虛擬私人網路 (VPN) [7-9]，為溝通雙方建立一個私人的安全通道，並在虛擬私人網路的技術下，引用安全性較高的 IP 安全協定 (IP Security Protocol, IPSec) [7-9]，可以確保機台的訊息確認，保護機台的標頭訊息，可以避免封包的目的被暴露，同時，在雙方溝通上，為傳輸內容資被監聽，本模組針對資料做對稱式加密 (AES-256) [10]，並對加密的資料做輕量化的認證，可以輕易部署在傳統的網路環境與新的物聯網環境中。

貳、文獻探討

在設計此模組時，本研究參照資訊安全的技術與各種物聯網的應用，研究許多私有網路的架構，近幾年，許多私有網路已將應用系統轉移到 TCP/IP 協定上，開放網路與私有網路已使用同樣的通訊協定 (TCP/IP)，安全性較低的 TCP/IP 協定，在物聯網環境中，幾乎是不可行的。因此，本模組引用了以下文獻，作為本模組的設計，進而增加物聯網的安全與彈性化的部署。

2.1 虛擬私有網路 (Virtual Private Network, VPN) [7-9]

虛擬私有網路又稱作虛擬專用網絡，虛擬私有網路的技術主要是在描述使用公共網絡時建立受保護的安全網路通道，虛擬私有網路透過加密網路之間的封包並偽裝裝置的身份，這使第三方更難以追踪裝置在網路上的活動並竊取資料。虛擬私有網路 (VPN) 是網路上從設備到網絡的加密連接，使用加密連接方式有助於確保安全傳輸敏感資料，同時它可以防止未經授權的人竊聽流量，並允許用戶遠程進行工作，例如：虛擬私有網路技術廣泛用於企業環境中，透過虛擬私有網路可以將兩個不同地區的辦公室形成一個私人的內部網路，可以讓企業更快速的擴展以及方便使用各項網路設備。

在使用虛擬私有網路的時候會有以下幾種的特性，第一種是隱藏你在網路中的位置以及網路得行為，例如：網頁的瀏覽紀錄、下載的檔案以上行為都會被虛擬私有網路隱藏起來，因此使用虛擬私有網路的時候會具有匿名性的效果。第二個特性是在虛擬私有網路的網路環境中，傳輸過程的資料都是進行加密，這也使攻擊者更難以去更改或者竊取資料，這個特性在使用公開得網路中極其重要，因為傳輸過程的資料會包括一些個人隱私資料例如：帳號密碼，個人商業文件，所以透過虛擬私有網路可以有助於減少個人資料外洩的問題。

2.2 IP 安全協定 (IP Security Protocol, IPSec) [7-9]

IP 安全協定常常用於在設備之間建立加密連線，此協定有助於確保通過公開網絡發送的資料安全。 IP 安全協定廣泛用於設置虛擬私有網路 (VPN)，它通過加密 IP 封包以及驗證封包的來源來進行運作。網路封包通常缺乏有效的安全機制，在公共網絡上傳輸時可能會被偽造、竊取或篡改，為了解決上述問題，通信雙方建立 IP 安全協定通道 (IPsec tunnel)，通道之間透過加密網路封包，來確保了在不安全的網絡上的安全傳輸。

在 IP 安全協定底下主要會包含以下幾種特性，第一個特性是金鑰交換，金鑰在加密過程中是必要的元素，主要是透過金鑰加密或解密訊息，IP 安全協定通過連接設備之間密鑰交換來設定金鑰以方便在 IP 安全協定底下的裝置都可以解密其他設備加密過後得訊息。第二個特性是在網路當中傳送的資料會被切成一小塊的封包，在封包當中包含

了標頭 (header)、承載 (payload)，以及實際資料 (data) 的內容，所以當裝置接收到封包的時間下可以透過以上的內容做出相對應的回應，而在 IP 安全協定中會在封包的前面加入許多的標頭 (headers)，包括用來驗證及加密的標頭 (headers)，所以當另外一台裝置接收到這個封包即可透過這兩個標頭 (headers) 來進行驗證即解密。

2.3 認證標頭 (Authentication Header, AH) [11-14]

認證協議 (Authentication Protocol) 是一種可以提供資料的身分驗證，資料的完整性檢查以及防禦重送攻擊的一種協定，但是在此協定之下所有資料是透過明文傳送，並不會進行加密，因此在 IPsec 當中通常會跟另外一個封裝安全承載 (Encapsulating Security Payload) 搭配著使用來確保資料得安全。

在認證協議 (Authentication Protocol) 中是根據以下方法來進行運作，第一個使用 MD5 等類型的雜湊函數 (hash function) 產生的檢查碼 (checksum) 來確保資料的完整性，第二個為了能達到身分驗證，認證協議 (Authentication Protocol) 在演傳法當中加入了隨機亂數來驗證彼此的身分，最後一個是認證協議 (Authentication Protocol) 會在封包的標頭 (header) 加入序號 (sequence number) 來抵擋重送攻擊。簡單來說認證標頭 (Authentication Header) 會透過上面三種方式來保證資料到目的地之前沒有被經過竄改。

2.4 封裝安全承載 (Encapsulating Security Payload, ESP) [15-16]

封裝安全承載 (Encapsulating Security Payload) 是一種可以提供資料的機密性同時也提供資料得完整性檢查並且防禦重送攻擊的一個演算法，在 IPsec 當中就是透過此演算法來對資料做加密來確保資料的安全。如果同時要進行加密和身分驗證，則在過程中會先進行身分驗證，如果身分驗證成功才會進行解密，用上述方式可以減少 processing overhead 同時也可以降低阻斷服務 (denial-of-service) 的攻擊。

封裝安全承載 (Encapsulating Security Payload) 是透過對稱式加密來對資料進行處理，在通訊過程中使用雙方預先設定好的金鑰去做加密或解密的動作，而在虛擬私有網路 (VPN) 中常見的對稱式加密方法有 DES、3DES、AES 等來保護資料的安全。在 IPsec 當中如果選擇使用 AES 來對資料進行加密，那麼需要啟動擴展序號 (Extended Sequence Number)，透過 64-bit sequence numbers 可以預防序號 (Sequence Number) 很快的被用完同時也會減少裝置上的資源消耗。

封裝安全承載 (Encapsulating Security Payload) 同時也可以提供資料的完整性，透過常見的 HMAC-MD5, HMAC-SHA, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, and AES-XCBC-MAC 的演算法可以達到完整性得驗證。在上面幾個演算法當中都是透過輸入資料可以得到一個固定長度的輸出。如果兩個雜湊值 (hash value) 一致，就可以確定兩筆資料是一樣的資料。

2.5 虛擬區域網路 (Virtual Local Area Network, VLAN) [11-16]

虛擬區域網路 (VLAN) 是一個邏輯方法將設備設定在同一個廣播的網段當中。虛擬區域網路通常會在交換 (switch) 或者是路由 (router) 上設定，將要設定在一起的介面 (interface) 放入同一個虛擬區域網路當中，可以形成一個私人的虛擬區域網路。主要要使用虛擬區域網路的原因是因為透過虛擬區域網路可以將不同的阜 (port) 區隔開來，來避免攻擊者可以透過某些不安全的裝置入侵主要的設備或者隱私資料，也可以透過此方式讓傳送資料不會發生衝突。

在使用虛擬區域網路的時候會有以下幾個優勢，第一個是可以有效的區隔網段當沒辦法負擔多網段的管理以及價格時，使用虛擬區域網路可以有效的解決這個問題。第二個可以快速的管理以及擴充設備，不像傳統的交換 (switch) 要透過繁瑣的設定來達到區隔網段的效果，透過虛擬區域網路可以直接從交換 (switch) 控制介面進行管理的動作，讓開發以及管理更加安全快速。第三點是安全性，虛擬區域網路 (VLAN) 給予網路管理員權限將交換 (switch) 實體阜 (port) 劃分為不同的虛擬區域網路 (VLAN)，來限制只能從特定的介面 (interface) 來存取 (access) 特定裝置，因此可以一定程度上防禦不明裝置以及流量。

2.6 對稱式加密 (Symmetric Encryption) [17-19]

對稱式加密主要是透過同一把金鑰去做加密和解密，而通常對稱式加密會有以下幾種特點，第一對稱式金鑰的產生不會耗費太多資源，對稱式金鑰可以是亂數或者是很簡單的一個參數，因此對比非對稱式加密會節省許多資源。第二在對稱式加密演算法當中的運算成本往往會比非對稱式加密來的低，因此可以為硬體資源省下一些成本。第三在使用對稱式加密也提供了一定程度上得身分驗證，只有同一把得金鑰才能做出相對應的加密或解密，因此透過這方式可以保證是否是擁有此金鑰的裝置。

現在常見的對稱式加密主要有 RC4、AES、DES、3DES 等演算法，在對稱式加密的低運算成本特性來看，通常是應用於加密大量資料或者是應用在硬體資源比較不足的設備上面，因此很適合用在現在比較常見得 IoT 裝置上面，但此狀況底下由於金鑰都是同一把所以一旦金鑰遺失或被竊取，攻擊者就可以看到資料或者竄改資料，在對稱式加密中要做好金鑰管理。

參、方法

在基本的物聯網環境中，必須先滿足機密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability) 作為基本的資料處理的方式。在機密性中，如何確保資料傳遞與儲

存的過程中，能保證其私密性，避免遭受到相關攻擊或其他因素，造成資料不小心被揭露。

為了保護在通訊過程中，避免遭受惡意更改資訊，在傳送指令或是儲存資料中，其過程必須不斷的證明其內容並未遭更動，以確保其完整性。同時，為了保證在公開分享資料的過程中，確保資料能隨時保持可用的情形，本研究提供一外接模組，使用虛擬私人網路的技術，配合認證標頭 (Authentication Header) 與封裝安全承載 (ESP) 的應用，完成模組如圖 1 所示，本研究使用 Raspberry Pi 來開發此模組，在機器溝通的環境中，每次使用時為二個一組一起使用。此模組採用參照認證標頭 (Authentication Header) 的身份驗證機制，其機制採用的方式為兩方協議。而在此機制中，認證標頭 (Authentication Header) 允許認證雙方 (例如 client 端連接到 server 端) 傳輸的內容所需資訊的類型來對雙方進行身份驗證。

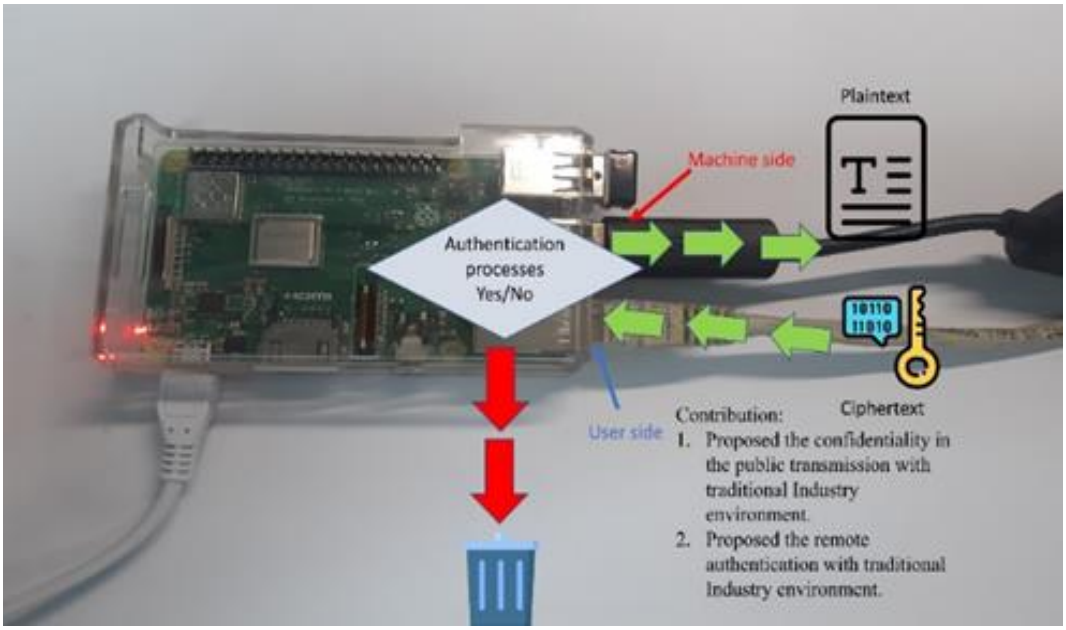

圖 1：具擴充性認證授權外接模組

本模組的協議設計考量兩個階段，如圖 2，其一為註冊階段，其目的為參與的兩方共享一些秘密。其二為身份認證階段，在此階段雙方相互進行身份認證，以便檢查對方是否是共享秘密的一方。欲保護通訊的資訊，本模組在通訊通道上，參照相關訊息確認的訊息傳輸技術，使用封裝安全承載 (ESP)，保障雙方的資訊，並確保共享的秘密鑰匙來確認傳送者的身份。

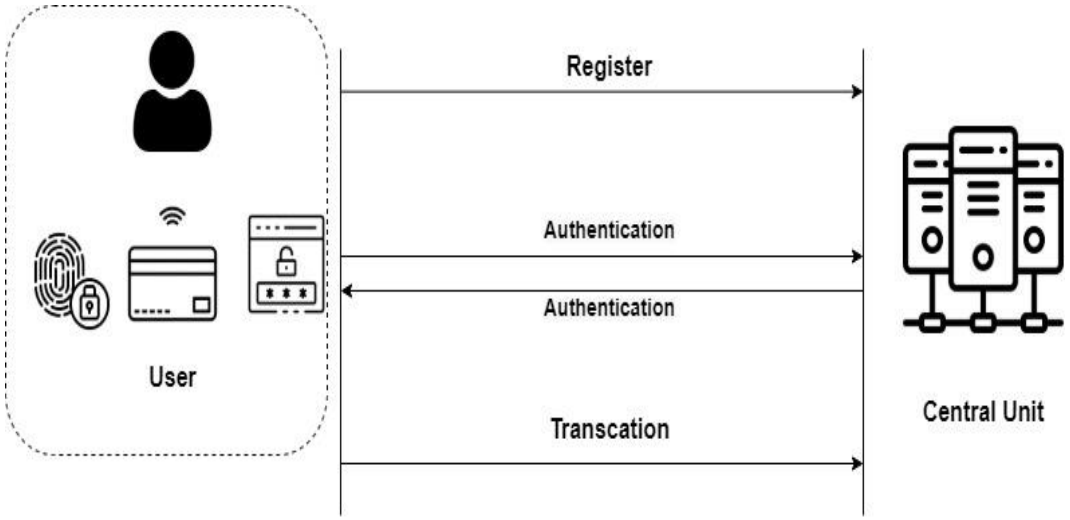

圖 2：系統流程圖

本模組具有彈性的資訊安全設計，不影響物聯網通訊的部署，可以確保機台之間的溝通，並做到雙方的訊息確認，確認對方是否是傳送資訊的來源方。如圖 3 之 Plug-in 所示。此模組先用認證標頭 (Authentication Header) 完成身份驗證，在使用封裝安全承載 (ESP) 來保護傳輸資料，最後，針對傳輸的資料做快速的加密 (AES-256)，並對加密的資料做輕量化的認證 (long-term secret key 及 timestamp)。如有駭客擷取加密後的封包甚至修改封包，此模組的認證機制會先經由安全承載 (ESP) 來確認資料完整性，若發生竄改等攻擊行為，立即將該封包丟棄以保護各種終端設備或。而封包需經由使用正確的秘密金鑰 (secret key) 方能解密，再傳送至通訊環境中之控制器或裝置，整體運作如圖 3 所示。

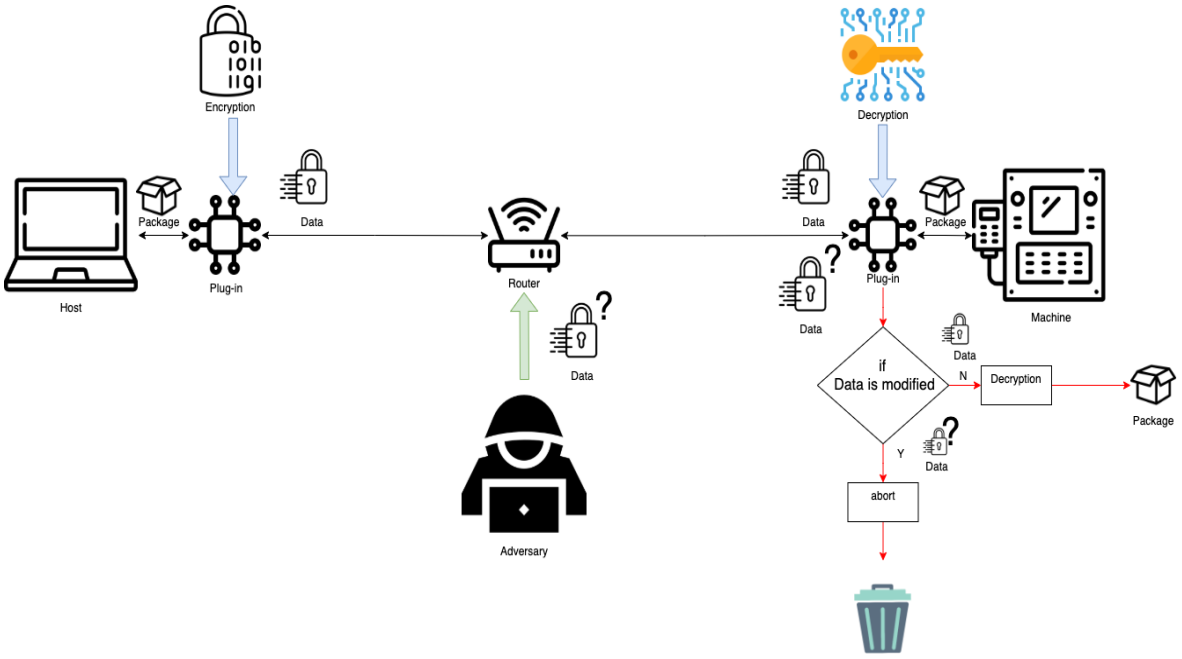

圖 3：外接式認證機制模組之運作模式

肆、安全分析

針對本研究的協定設計，本模組滿足於可信任的網路溝通，可以輕量化的部署在物聯網環境中，在技術上使用 IPSec 最基本的安全協定，針對封包標頭做安全認證，在安全分析上，具有無連接式通訊、資料來源認證、以及抵抗重送攻擊等保護服務。以下為本模組的完整安全分析。

4.1 抵擋重送攻擊 (Replay Attack)

在本研究的機制當中是使用的是 IPsec 通訊協定，因此在每一個網路封包當中都會加入序號 (sequence numbers)，序號 (sequence numbers) 為 32 位元的無號整數值，32 位元的無號整數值，是一個計數器的數值，利用滑動視窗 (Sliding Window) 防止重播攻擊 (Replay Attack)。由於序號 (sequence numbers) 計數器都必須清除為 0 開始，傳送方每發送一封包出去便將序號 (sequence numbers) 加一；接收者再利用滑動視窗法檢視封包是否接收過。當重送攻擊的發生時，接收端將檢測封包序號 (sequence numbers) 是否小於後端指標所指引的數值，如果較小的話，表示該封包已回應過，可不予理會，如此便能避免重播攻擊。透因此，過序號 (sequence numbers) 可以檢查說是否為同樣的訊息進一步來預防攻擊者送出同樣的封包來 access 到機密的設備或者拿到重要得資料。

4.2 資料的機密性 (Confidentiality)

本模組有參照 ESP 協定，將原來封包的資料經過加密處理之後，再重新封裝一個新的 ESP 封包才傳送給接收端；接收端拆解 ESP 封包後，先將資料解密，再組合回原封包格式，對傳輸的資料可進行加密，以達到隱密性功能。同時，在本研究的機制當中使用 pre-share long term secret key 的對稱式加密演算法，來對每一次傳送得訊息做加密的保護，因此就算攻擊者從中間攔截資料也無法做出任何行為，因為只有擁有那把金鑰的人才能解密那包資料，所以攻擊者不能做到竄改資料或者竊聽資料的惡意行為，本機制透過這個方法，保證了資料的隱密性、資料來源認證、與有限度的流量機密性等功能。

4.3 相互認證 (Mutual Authentication)

在本研究的機制當中使用了認證標頭 (Authentication Header) 來做雙方的認證以及完整性的保護，由於認證標頭 (Authentication Header) 對封包提供認證，可以確保遭受竄改的封包可以被偵測出來。首先會在一開始溝通的時候加入雙方的挑戰和回應來驗證彼此身分，並加上訊息認證碼 (MAC) 來認證封包。在本模組中，傳送端將在每一個封包前面認證標頭 (Authentication Header) 裡面會包括雜湊值 (hash value)，並經過雜湊演

算法得到一個訊息摘要 (Message Digest, MD)，再利用秘密金鑰加密此訊息摘要，會得到一個 MAC 碼，最後將此 MAC 碼與封包一併傳送給接收端；接收端收到此封包後，以同樣的演算法與秘密金鑰產生另一個 MAC 碼。如果兩者 MAC 碼相同的話，表示封包未遭受竄改或偽造；透過此方式可以來驗證傳送的封包有無被竄改過，因此本篇的機制可以達到互相認證的特性以及完整性的保護。

伍、結論

隨著科技的進步，新軟體的推陳出新，也產生不同的資訊安全設計。然而，客製化的軟體設計所付出的成本往往過高，本研究提出一彈性化的模組，可以解決在 M2M 環境中具遠端存取控制的設備，並建穩健的資訊交換，無論新設備與舊設備的溝通衝突，皆可以使用本模組解決，讓任何使用者皆可以輕易部署通訊環境。傳統機器之間的溝通上，對於通訊間的安全加密較不嚴謹，本機制滿足輕量化的加密設計，可以主動去保護終端設備的異常。再配合系統的時間戳記管理，既可以追蹤問題的時間與地點，也能輕易地保護設備被惡意攻擊。在未來，彈性化的模組設計、輕量化的資訊安全技術與保護機台安全溝通，是極其重要的。

參考文獻

[1] F. Hussain, L. Ferdouse, A. Anpalagan, L. Karim, and I. Woungang, “Security threats in m2m networks: A survey with case study,” COMPUTER SYSTEMS SCIENCE AND ENGINEERING, vol. 32, no. 2, pp. 117–135, 2017.

[2] Specification and Implementation Guide for MODBUS over serial line (2002/12/02)

[3] OPC Unified Architecture (opcfoundation.org) (2020/07/21)

[4] MQTT Version 5.0 (oasis-open.org) (2019/03/07)

[5] A. Chowdhary, V. H. Dixit, N. Tiwari, S. Kyung, D. Huang and G. Ahn, "Science DMZ: SDN based secured cloud testbed," 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) , 2017, pp. 1-2, doi: 10.1109/NFV-SDN.2017.8169868.”

[6] S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry and S. McSweeney, "Performance Analysis of Zero-Trust multi-cloud," 2021 IEEE 14th International Conference on Cloud Computing (CLOUD) , 2021, pp. 730-732, doi: 10.1109/CLOUD53861.2021.00097.

[7] Ferguson, Niels, and Bruce Schneier. "A cryptographic evaluation of IPsec." (1999) :

28.
https://www.schneier.com/academic/archives/2003/12/a_cryptographic_eval.html

[8] Doraswamy, Naganand, and Dan Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003. https://www.oreilly.com/library/view/ipsec-the-new/013046189X/

[9] Hamed, Hazem, Ehab Al-Shaer, and Will Marrero. "Modeling and verification of IPSec and VPN security policies." 13th IEEE International Conference on Network Protocols (ICNP'05) . IEEE, 2005. https://ieeexplore.ieee.org/abstract/document/1544626/

[10] R. Jain, R. Jejurkar, S. Chopade, S. Vaidya, and M. Sanap, “AES Algorithm Using 512 Bit Key Implementation for secure Communication,” Int. J. Innov. Res. Comput. Commun. Eng., vol. 2, no. 3, pp. 3516–3522, 2014. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1068.8767&rep=rep1&type=pdf

[11] Atkinson, Randall, and S. Kent. IP authentication header. RfC 1826, August, 1995. https://www.hjp.at/doc/rfc/rfc4835.html

[12] Elkeelany, Omar, et al. "Performance analysis of IPSec protocol: encryption and authentication." 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333) . Vol. 2. IEEE, 2002. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=997033

[13] Metzger, Perry, and William Simpson. IP authentication using keyed MD5. RFC 1828, August, 1995. https://www.hjp.at/doc/rfc/rfc1828.html

[14] Kent, Stephen, and Randall Atkinson. "IP authentication header." (1998) . https://www.hjp.at/doc/rfc/rfc4302.html

[15] https://www.tutorialspoint.com/what-is-encapsulating-security-payload-esp (2021/9/3)

[16] https://www.techopedia.com/definition/1504/encapsulating-security-payload-esp (2022/3/24)

[17] A. Murtaza, S. J. Hussain Pirzada and L. Jianwei, "A New Symmetric Key Encryption Algorithm With Higher Performance," 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) , 2019, pp.17,doi:10.1109/ICOMET.2019.8673469. https://ieeexplore-ieee-org.ezproxy.lib.ntust.edu.tw/document/8673469

[18] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," 2021 2nd International Conference on Computing and Data Science (CDS) , 2021, pp. 616-622, doi:

10.1109/CDS52072.2021.00111.
https://ieeexplore-ieee-org.ezproxy.lib.ntust.edu.tw/document/9463286

[19] James T.Harmening, Chapter 58 - Virtual Private Networks, Computer and Information Security Handbook (Third Edition) , Morgan Kaufmann Publishers, 2017https://www.sciencedirect.com/science/article/pii/B9780128038437000582