Regular Paper

Communications of the CCISA
Vol. 30 No. 1 Feb. 2024

時間敏感工業控制系統的入侵偵測系統

周耘廣 [1*]、鄭伯炤 [2]
[1] 國立中正大學通訊工程學系、[2] 國立中正大學電機工程學系
[1]609430045@alum.ccu.edu.tw、[2]bcheng@ccu.edu.tw

摘要

工業控制系統(Industrial Control System, ICS)用於各種工業製程的專用控制系統，如監視、管理和控制實體設備和製程，在提升其產業的營運自動化和優化具有關鍵性作用。ICS 在智慧製造和工業 4.0 行業中發揮了極重要的功能及作用，因為它可以透過網路接收遠端感測器資訊，並對控制站發出指令並履行管理職責，以提高生產效率並有效管理工廠的所有生產設備。然而，隨著越來越多的設備連接到網際網路時，網路攻擊的可能性也在增加。另一方面，傳統乙太網路(Ethernet)沒有考慮到需要保證工業控制系統中特定封包的傳輸在時限內(deadline)完成。如果數據不能在期限內送達目的地，將造成不可挽回的後果。時間敏感網路(Time Sensitive Network, TSN)可確保重要流量(flow)確定性的低延遲傳輸特性，使工業控制系統的重要流量能即時到達控制端。因此，TSN 受到了廣泛的關注並迅速應用在工業控制系統中。入侵偵測系統(Intrusion Detection System, IDS)可以有效偵測 ICS 系統中關鍵設施的運作是否有問題或遭受到網路攻擊。然而，在 ICS 和 TSN 網路的結合環境下，目前的入侵偵測系統已無法完美勝任工作，因此，我們提出了一個基於封包大小和週期概念的入侵偵測系統，命名為 Packet size & Period Intrusion Detection System (PsPIDS)，可適應在 TSN 網路環境中 ICS 的 IDS。透過分析，我們發現封包大小和封包週期之解決方案是能夠偵測加密環境中的惡意攻擊。實驗結果也證明了所提出的 IDS 的性能和能力，毫無疑問地為工業應用提供卓越的安全性。

關鍵詞：時間敏感性網路、入侵檢測系統、工業控制系統

* 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol. 30 No. 1 Feb. 2024

Intrusion Detection for Time-Sensitive Industrial Control Systems

Yun-Kuang Chou [1*], Bo-Chao Cheng[2]
[1]Department of Communications Engineering, National Chung Cheng University
[2] Department of Eletrical Engineering, National Chung Cheng University
[1]609430045@alum.ccu.edu.tw, [2]bcheng@ccu.edu.tw

Abstract

Industrial control system (ICS) is specialized control systems used in various industrial processes, such as monitoring, managing, and controlling physical equipment and processes, which is critical for boosting automation and optimizing industry processes. ICS plays a very important function and role in smart manufacturing and Industry 4.0 industries because it can receive remote sensor information through the network, issue instructions to the control station and perform management responsibilities to improve production efficiency and effectively manage all production devices within a factory. However, as more and more devices are connected to the Internet, the potential for cyberattacks increases. On the other hand, traditional Ethernet does not take into account the need to ensure that the transmission of specific data flow is completed within the time constraint in industrial control systems. Industrial control systems will have irreversible consequences if the data cannot be delivered within the deadline. In order for vital traffic from industrial control systems to reach the control end station on time, time-sensitive networks (TSNs) can guarantee that important traffic satisfies predefined low-latency transmission characteristics. As a result, TSN has drawn a lot of interest and been quickly used in industrial control systems. Intrusion Detection System (Intrusion Detection System) is able to identify network attacks with the functioning of important ICS facilities. The existing intrusion detection technology is no longer able to identify attacks in the environment where the networks of ICS and TSN are integrated. Thus, in order to design and implement an IDS appropriate for ICS in a TSN network environment, we proposed an intrusion detection system based on the concept of packet size and period, named Packet size & Period Intrusion Detection System (PsPIDS). Through our analysis, we find that the packet size and packet period scheme is capable of detecting malicious attacks in encrypted environments. The experiment results demonstrate the ability and capability of the proposed IDS, which unquestionably delivers superior security for industrial applications.

Keywords: Time-Sensitive Network, Intrusion Detection System, Industrial Control System

壹、前言

數位化轉型意旨利用資通訊(Information Communication Technology, ICT)技術將傳統產業的產品與產線上，導致其流程、設計或管理上發生重大轉變，進而改變企業營運方式及增加市場競爭力。在企業營運中，工業控制系統(Industrial Control System, ICS) 佔有舉足親輕重的地位，並已佈署於多數企業公司之數位轉型的生產線上或智慧工廠場景中(如發電廠、變電所、油田管路或是其他重點設施等等)，它不只監控主要設施並即時傳輸，確保生產過程中的安全[1]。在過去，工業網路是和企業網路或是網際網路之間是相互單獨存在的，均有其獨立的偵測及保護機制[2]。為了支援各種設備和系統之間的資料交換，多種類型的網路將以互連型態出現，其中時間敏感網路(Time-Sensitive Networking, TSN)能滿足工業網路中即時通訊(real-time communication)的要求，在工業4.0 中更發揮至關重要的作用。TSN 是一組 IEEE 通訊標準，旨在透過標準乙太網路實現確定性(deterministic)和低延遲(low-latency)的通訊特性，因此，可確保資料傳輸之可預測性，有助於在設備之間實現可靠及即時的資料交換[3]。

IEEE 802.1 工作組制定了一系列的標準,稱為時間敏感性網路(Time-Sensitive Networking, TSN)。這些標準與先前的乙太網路保持向上的相容性,最特別特的是超低延遲的傳輸，這對數位轉型的智慧製造至關重要，因為它們必須要在低延遲下完成傳輸任務,否則會導致災難性的後果。TSN 能夠滿足許多典型 Ultra-Low Latency (ULL)應用對端到端的延遲和抖動(Jitter)之要求(如工業自動化之延遲要求為 0.2μs~0.5ms with 1Gbit/s link speeds)[4]。透過結合時間觸發(Time-Trigger flow)的流量和盡力而為(Best-Effort flow)的流量，TSN 可以節省工業網路的成本，提供高互通性及可靠性的 ULL 應用網路環境[5]。

前述 TSN 流 (flow)可在於為該流量所屬的流量類別定義的 QoS 屬性(頻寬或延遲)來定義。 特別是，TSN 流(flow)由乙太網路標頭中 802.1QVLAN 標記內的優先權代碼點 (Priority Code Point, PCP) 欄位和 VLAN ID (VID)所定義。在 TSN 的所有設備配置的 flow 都被門控制表(Gate Control List, GCL)指定，成為一個調度排程表(schedule)其任務是對佇列(Queue)出口的開關時間控制，所有在 TSN 的設備要依據流量類型妥善分配到準確的時間點上。當設備和流量複雜度到一定程度時，需要使用集中式網路配置(Centralized Network Configuration, CNC)，在其區域的數據面上擁有全區視角，透過遠端管理協定對 TSN 交換機(TSN switch) 進行配置與設定。另一方面，設備端節點(node)可透過標準應用程式介面 (Application Programming Interface, API)與集中用戶配置(Centralized User Configuration, CUC)進行通信溝通，這可用於發現設備端 node、檢索 node 功能和用戶需求，並通知 CNC 進行延遲優化的 TSN 配置功能，進行 TSN switch 的配置設定工作，最後將配置的結果回傳給 CUC [6]。

為了將 TSN 技術應用於 ICS，需要對工廠流量進行分類，以便 ICS 應用環境能夠依照 TSN 協定執行[7]。由於 ICS 系統的時間限制性(time constraint)，TSN 能夠透過

802.1Qav、802.1Qbu、802.1Qbv 等等的概念來實現低延遲的綁定，使訊息的端到端的延遲(end-to-end delay)能夠在確定性時間內完成。TSN 交換器中有 8 個佇列(Queue)，優先權範圍從 7 到 0 到最低。這可運用於時間觸發流量(TT flow)，讓它成為所有流中優先順序最高的流量類型，因此當需要傳輸 TT flow 時，會搶佔其他類型資料的傳輸，以便 TT flow 能夠在規定的時間內完成傳輸；由於 TT flow 具有高優先權傳輸，因此其傳輸順序和路由是固定的，與普通乙太網路相比，只要經過 CNC 計算過延遲優化的配置方案，再配置成功，TSN 便能保證傳輸的封包能夠在要求的時間內按順序傳輸完成。透過 TSN 的特性，我們可以利用封包的傳輸週期和封包序列的方法來檢測流量(flow)是否有異常。

工業控制系統 (ICS)可利用時間敏感網路 (TSN)建立一個可靠即時通訊系統，用來傳輸控制指令或是資料。時間敏感網路 (TSN)在 ICS 中採用率正在增加，促使 IT 和 OT 結合並實現工業物聯網 (Industrial IoT) 之虛實跨界整合[8]。ICS 儼然成為工廠控制的組成核心部分，然而，當 ICS 與外部網路連接後，會有被網路攻擊的風險，常見的網路攻擊有:阻斷服務攻擊(DoS attack)、延時攻擊(Time delay attack)、回放攻擊(Replay attack)等等[9][10]。

入侵檢測系統(Intrusion Detection System)能夠有效的檢測 ICS 系統中是否有入侵的行為或攻擊問題，但在 ICS 與 TSN 網路整合之下，網路流量特性是有別於傳統的乙太網路(Ethernet)的特徵，以致目前入侵偵測系統是無法有效地應用到 ICS 環境中。再者，如果系統應用屬於多個組織，則網路中會對送出的封包進行加密保護，其檢測技術要考慮不需透過檢查封包內容就能進行檢測的技術問題;另外入侵檢測機制需要考慮關鍵性 ICS 應用程序必須有確定性的端到端的延遲(end-to-end delay)。因此，在本研究中，我們利用時間敏感網路(Time-Sensitive Network, TSN)保證重要流量能夠滿足確定性的低延遲傳輸特性，使工業控制系統的重要流量能夠在一定時間內達到控制端，再利用流量的週期、封包順序的特性來設計一套新穎入侵檢測系統，名字為 Packet size & Frequency Intrusion Detection System (PsPIDS)來檢測 ICS 環境下的惡意攻擊，透過簡單的分析封包規律，而不需要對加密的封包進行解密後進行檢測，也能檢測出網路中的惡意攻擊。

接下來，本文的結構介紹如下。第 2 章將討論相關入侵偵測系統方法的研究。第三章介紹了本文所提出的 PsPIDS 系統演算法。 第四章介紹實驗場域及探討實驗結果，第五章是本文研究的總結。

貳、相關文獻

入侵檢測系統的種類很多應用的場景也不盡相同，本章節將介紹入侵檢測系統的相關技術。這些方法分別主要以封包的週期、順序和大小的分佈進行入侵檢測，均可有效地檢測出惡意的攻擊類型。Du 等人[2]提出了一種使用 Packet Size Entropy 的技術，是將

不同封包類型的封包大小算出其熵來判斷是否有攻擊存在。文中介紹當一個封包被 DoS 攻擊的時候，其封包的熵會有很大的變化，透過(1)計算出熵的大小，把有問題的封包標記出來得到有問題的封包，檢測出攻擊。

$$H(t) = -\sum_{l}\left(\frac{\eta_l}{S}\right) log\left(\frac{\eta_l}{S}\right) \quad (1)$$

η_l 是封包大小為 l 的出現次數，S 是滑動觀察窗口的大小，觀察窗口大小根據攻擊持續的時間做調整。他的優點在於利用封包的熵去檢測攻擊時不需要檢查封包的內容，並且能夠檢測長期和短期的攻擊，並隨著攻擊率越高期檢測能力就越高，但是當網路的封包的週期產生變化，或是攻擊率太低，檢測能力會大幅降低甚至無法檢測出攻擊，還有一個問題是隨著檢測能力越高，花費的時間越多。

由 Song 等人[11]提出的我們提出了一種基於控制器區域網路(Controller Area Network, CAN) 訊息時間的間隔分析的發展一套輕量級車載網路(Intra-Vehicle Network, IVN)入侵偵測演算法。其概念是將每個 CAN ID 都有唯一的時間間隔，因為每個連接到 CAN bus 的電子控制單元(Electronic Control Unit, ECU)都會定期發送訊息，因此，根據訊息時間間隔的分析來設計 IDS。這篇論文所提出的方法能夠根據時間的推移有效地找出流量的異常點，再對異常的區域進行比對確認找出攻擊，然而，對於封包到達的順序遭到改變時，無法檢測出異，且在這篇論文中這方法只能透過封包擷取期間 (time window)的方式進行檢測，使這個方法無法實用在 TSN 裡工業控制系統環境中。

由 Udd 等人[3]所提出的一種使用 Bro 平台(現在平台稱為 The Zeek Network Security Monitor)在數據採集系統(Supervisory Control and Data Acquisition, SCADA)建立的入侵檢測系統，其方法是利用兩套機制，一開始將資料收集後自動建立白名單，當沒有在白名單的封包出現時會送出警告，接下來將封包的到達時間進行比較，是將學習階段所記錄的統計信息去計算出參數 D，封包到達時間超過參數 D 時會送出警告給用戶知道。透過白名單和分析封包到達的時間能夠有效的進行檢測，但所提出的方法對於現今通訊都會對封包進行加密導致無法分辨白名單的封包，使其方法無法用在加密的場景，還有時間誤差的計算是由統計所得知的，無法精準的推測到達時間，可能會造成誤報率上升或是沒檢測出攻擊。

由 Aiello 等人[12]提出的利用一個線上入侵檢測方法去辨識低速率的 DoS 攻擊。利用快速傅立葉轉換(Fast Fourier Transform, FFT)和綜合隨著時間演變的流量來檢測出來低速率的 DoS 攻擊。藉由定義出兩個觀察範圍的參數(Observation Horizons, OHs)做為檢測機制，分別是目前的觀察範圍(current OH)和上一個觀察範圍(previous OH)，即為兩個時間段內監控所選的特徵，選取完成後如果在時間範圍內發生攻擊，經過快速傅立葉轉換後的頻譜可以清楚的觀察到隱藏在正常流量內的攻擊訊號，其優點是不需要透過檢查封包內容，且能有效率的檢測攻擊，但是這篇沒有可慮到封包大小的變化帶來的影響，如果封包大小發生變化沒有辦法檢測出來。

Singh 等人[13]介紹了兩個基於異常的入侵檢測系統 (Anomaly-based Intrusion Detection Systems, AbIDS) 在檢測對SCADA控制系統的網絡攻擊中的應用: Snort和Bro兩種不同的入侵檢測系統工具，其目的是在擾動期間執行糾正措施以保持電力系統的穩定性和可靠性。兩個入侵檢測系統的工具的檢測過程以及涉及的主要組件，檢測的步驟主要分為五個步驟，分別是網絡的封包監聽、協定封包過濾、學習階段、規則定義階段、實時檢測。第一階段監聽所有來自電力系統的控制器傳送到執行器的信號，接下來根據IP 地址和端口號(Port Number)，過濾一般的 DNP3(Distributed Network Protocol 3)封包，第三階段學習 DNP3 封包的功能碼，直到控制器在特殊場合送出關鍵指令，例如發生故障或有意外事件，此種類的指令有一定的時間限制，作者攻擊發生後能發現到與正常操作相比，DNP3 封包之中有大量的寫入與操作的情況，因此，透過出挑選 TCP 上的 DNP3 應用層中的寫入/操作條件功能代碼進行統計，經過定義的規則後找出攻擊。在該篇論文中，檢測方法是針對 DNP3 協定開發的，但是，也可以應用於其他基於 SCADA 的協定，將已經應用 IDS 工具在 SCADA 環境中開發實時入侵檢測引擎，但是其缺點也是如果將封包進行加密，其檢測模式也無法應用，也需要再透過將封包解密才能進行檢測。

第工業 4.0 過程中由自動化金字塔影響工業網絡的設計，尤其是現在保留在機器上的處理組件可能會位於工廠 IT 很遠的地方，為了滿足工業自動化過程的要求，特別是網絡非常重要，尤其是交換機和路由器等基礎設施設備，必須通過賦予實時能力的新技術來增強。網絡也必須滿足工業 4.0 對安全性以及自動配置或無縫重新配置等更高靈活性的要求。在這種情況下，控制應用程序對通信具有特定的服務質量要求，可以通過更改網絡的拓樸來滿足這些要求。Kobzan 等人[14]提出了一種為遠端過程控制和監控建立安全且時間敏感的通訊的解決方案及初步實施步驟。此概念和實現乃是時間敏感網路和軟體定義網路(Software-Defined Networking, SDN)的結合。所提出之方案可為時間敏感的工業網路的配置提供了靈活性，並增加了保護它們的可能性。

參、PsPIDS 解決方法

本文提出的基於封包大小和週期的入侵檢測方法，主要是針對於工業控制系統中的入侵檢測系統做改良，且考慮到在 ICS 傳送訊息時需要對封包進行加密，在傳送過程中不容易被竊聽，但是大部分的入侵檢測系統都無法在加密的封包中進行檢測，於是我們找出利用週期(頻率)、封包熵(Entropy)分布、時間間隔的方式進行改良應用到 TSN 的環境中。在 ICS 中大部分為工廠設備中發送檢索數據的流量，通常是來自現場的感測器(Sensor)或是驅動器(Actuator)檢索數據的輪詢(Polling)的機制，因此流量中會帶有強烈的週期特性，又因為 CNC 產生的是流量調度(schedule)使得流量順序、流量端到端延遲時間限制和封包傳遞位置路徑皆具有確定性(deterministic)，並利用流量中的週期性流量加上時間觸發流量(Time-Trigger flow)支持低延遲和抖動(Jitter)的應用特性，以期限時間

(deadline)和流量周期的順序檢測方法應用在 PsPIDS 入侵檢測系統。

802.1Qdj 標準為 CUC 和 CNC 的職責的附加定義,在各種應用實例中添加有關 CUC 分配功能的廣泛可用性的主題，例如根據談話者(Talker)和聽眾(Listener)的流(flow)配置請求與網路流量狀況,計算並配置生成,並使用 CUC 接口分發給發送端和接收端。Chang 等人[6]詳細敘述計算過程及 CNC 如何產生的時間表(Schedule)，並實驗證明在此產生的時間表(Schedule)控制之下，是可確保每個 TT flow 可以符合各個的端對端的延遲要求。CNC 分配的功能應是可供各種 CUC 使用，例如可以應用到 TSN 與 Open Platform Communications - Unified Architecture (OPC UA)的結合應用，CNC 其中的職責為探索實體網路拓樸，並且負責配置與控制轉發層面，換言之，透過 CNC 發送指令給相關的 TSN switch 進行 flow table 之修改,並透過 VLAN 的方法來進行劃分使其能夠進行通訊。CUC 在收到 CNC 之設定成功訊息後，它便會將 schedule 資訊(如表 1 所示)傳送給 PsPIDS 作為辨識基準，並依照 stream ID 的順序以及發送端以及接收端的時間來判斷封包順序及封包週期，其中週期、封包大小等條件皆要與 schedule 相符才會認定為正常封包。

表一：CNC 產生的流量資訊範例表格

Stream ID	Destination MAC	週期(ms)	VLAN	截止時間 (ms)	封包大小 (bytes)
Flow 1	00:00:00:00:00:12	10	1	10	200
Flow 2	00:00:00:00:00:14	25	1	25	400
Flow 3	00:00:00:00:00:16	30	1	30	600

因此，PsPIDS 主要使用週期、封包大小等條件來捕獲網路流資料中訊息相關性和資訊差別的複雜性,進而提高入侵偵測機制的有效性。其中 PsPIDS 利用封包的週期性、封包傳輸的順序以及封包的大小分佈做結合，將三者功能合併改善 IDS 的檢查機制。再者，本篇論文利用 TSN 的工業控制系統中的環境中解決三種流量(TT flow、Audio Video Bridging (AVB) stream 和 Best-Effort (BE))的異常行為檢測，並且可以在封包加密且不須檢查封包內容完成檢測。其原創性歸納如下：

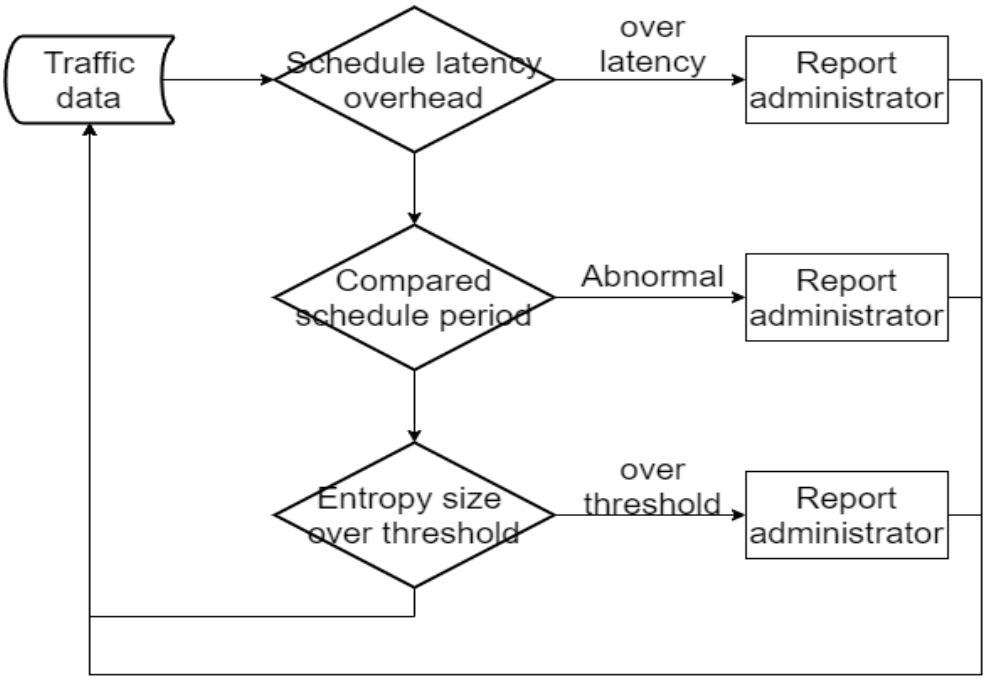
- No deep packet inspection: 指的是其入侵檢測系統是否有能夠僅能根據流量所提供的內容資訊來做入侵檢測基準，這點只有利用白名單在 Bro 平台上的入侵檢測系統無法達成，其方法是判斷封包類型作為白名單，需要查看封包內容獲得，因此封包加密時無法判斷封包種類。然而，PsPIDS 是不需要費時費力檢查封包內容。
- Packet size distribution: 利用攻擊封包大小分佈情況會和正常流量的分佈有所不同，透過計算公式可以確定是否有攻擊的發生。
- Packet period: 在 ICS 網路中，由於流量類型比起一般網際網路相比，在工廠中主要都是感測器或是驅動器，其流量類型和網際網路中相比，相對單一且是

有週期性的，對於檢查封包的頻率或週期能夠確保其沒有因為被入侵而被更動。這點是有別於一般網路，ICS 有獨特對時間的相關要求，包括非常高的一致性、規律性和同步性。

- Packet sequence: 也就是說在 TSN 網路中其流量是透過集中用戶配置產生出的排程表，其網路流量順序是已經決定的，如果檢查道經過設備的流量順序不同，代表有攻擊的發生。

綜合上述，PsPIDS 的檢測方法，目的是在不需要解密封包內容找出惡意攻擊即入侵行為，使整體的使用 TSN 的 ICS 環境服務品質及安全性提高，降低了被攻擊的可能性，和其他的 IDS 不同，在考慮封包到達時間外，還以封包的順序和大小做比較已檢測惡意攻擊及入侵企圖，透過流量獲取的資訊，配合 schedule 提供的參數資訊，能夠快速檢測出異常。

入侵檢測流程分為三個流程階段(如圖一所示)，在第一個過程中，將時間表(schedule)的封包資訊作為白名單對流量進行辨別，在此階段流量將會對時間表(schedule)的以下幾個內容進行確認，截取時間表(schedule)傳輸的封包進行分析，首先會確認時間性的封包是否在時間表(schedule)的延遲容忍的範圍之內，當有時間性的封包超出時間表(schedule)所規定的延遲時間則會回報給使用者。在第二個階段會比對時間性的封包的週期是否出現變化，傳送期間如果時間性的封包出現週期變得過短或是變得過長得狀況，代表網路中有異常並回報給使用者。最後階段，是利用 Du 等人[2]提出的方法，使用(1)計算出封包熵(Entropy)的分布數值，檢查分布數值是否有超出範圍。

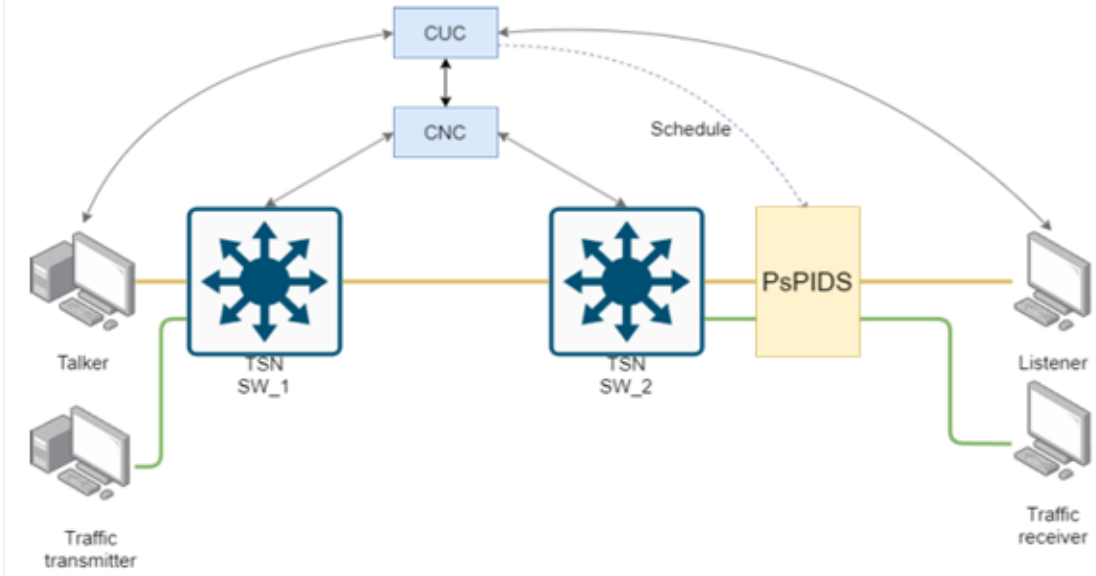


圖一：PsPIDS 內部流程圖

肆、實驗結果與分析

本實驗主要目的為證明本篇方法 PsPIDS 的成效，透過 TSN 交換機模擬真實的工業控制系統環境，能夠有效地保證儘管在高負載流量的情況也能有確定性的傳輸，經過入侵檢測系統的條件過濾，篩選出有異常的時間延遲、封包週期以及封包分布的網路流量，提升對於異常流量檢測為異常的檢測率，提升原有的 ICS 的安全，本章節的實驗使用真實的 TSN 交換器進行實驗，來證明方法的可行性。

為了實現研究論文的運行環境，參考思科文件建議[15]，採用兩台思科(Cisco)的 TSN 交換器:工業乙太網路交換器 4000 系列(Cisco IE 4000 Series Switches)，其型號為 IE-4000-4TC4G-E。對兩台 TSN 交換器進行鏈路連接，模擬出工業控制系統環境，假設 TSN 交換器 1 (TSN SW_1) 與傳送訊號的設備相連接，TSN 交換器 2 (TSN SW_2) 與接收訊號的設備連接，TSN SW_1 與 TSN SW_2 互相連接，形成一個簡易的 TSN 的工業控制系統網路，如圖二所示。本研究將把入侵檢測系統設定在接收端設備前，利用 CUC 轉傳過來的 CNC 計算安排的調度時間表(Schedule)及 flow 的週期訊息，PsPIDS 藉由這些訊息與封包熵(Entropy)分布的計算，檢測環境中的異常行為。其中談話者(Talker)和聽眾(Listener)分別為模擬工業控制系通設備中的發送端與接收端，所發出的訊號具有時間性以及固定的週期性，下方的流量發送器的作用為模擬當有來自其他單位的網路傳輸時共同使用同一條路徑是否會影響到重點設備的封包資料傳輸，兩個 TSN 交換器之間所連接的頻寬為 1Gb/s，綠色線傳輸的流量從 Traffic transmitter 傳送到 Traffic receiver 送出不同傳輸量的 UDP 封包，實驗的傳輸量由 100Mb/s 到 1Gb/s，因此連接兩個 TSN 交換器的傳輸線將會被不同傳輸量的 UDP 封包所干擾佔據，產生 UDP 封包的流量則是使用 Solarwinds 公司所開發的網路壓力測試軟體工具 WAN Killer 產生不同的流量，來實驗是否會影響 TSN 流量的傳輸並且產生巨大的端到端延遲。



圖二：實驗環境架構

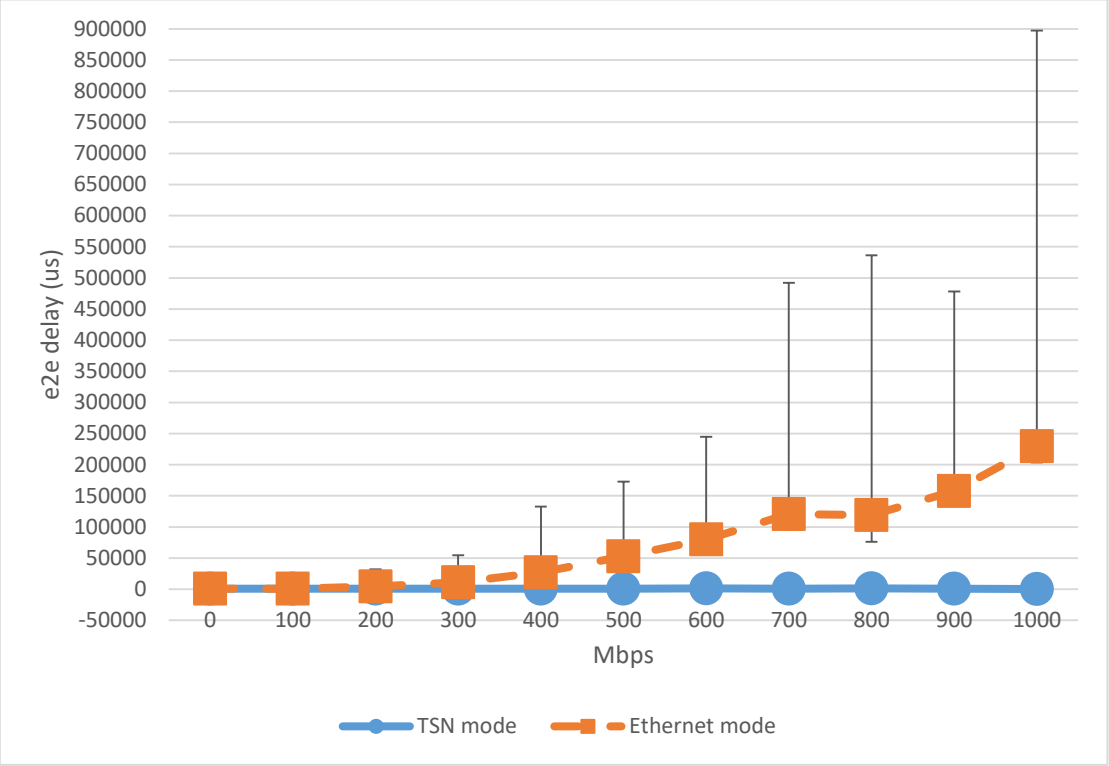
對 PsPIDS 進行驗證，我們參考過去在工業網絡系統中可能看到的一般攻擊類別:

- 延時攻擊(Time delay attack)：攻擊者在系統的測量和控制值中注入額外的時間延遲，這可能會擾亂系統的穩定性並導致設備崩潰，時序偏差可能是會導致硬件故障的間接結果。攻擊者可能會暫時堵塞通信通道，以延遲傳輸的信號流，同時保持數據包中包含的信息不變。儘管此攻擊手法不會阻止正確信息的傳遞，但它可能會通過妨礙不同的系統組件之間的正確同步，進而破壞系統操作和性能。我們利用 Colasoft 公司所開發的 Colasoft Packet Builder 對封包進行編輯分別將封包延遲增加 100ms、200ms 以及 300ms，檢測的判定範圍由從和傳輸間隔時間相同到傳輸間隔時間的 2.25 倍，以找出最佳檢測大小。
- 拒絕服務 (DoS) 攻擊: 這種攻擊目的在於拒絕合法用戶對某些資源的可用性，例如拒絕用戶的網絡、系統設備或任何其他計算資源的可用性。而分佈式拒絕服務攻擊 (DDoS) 利用多個受感染的系統，將這些感染了惡意軟件的系統來攻擊拒絕服務的目標，這類的攻擊例如 Mirai 殭屍網絡，是目前為止所見到的一些最大的 DDoS 攻擊類別，也有類似於 Mirai 的新型殭屍網絡正在出現，展示了物聯網設備設置的方法存在著危險。我們使用 solarwinds 公司所開發的 UDP 發送工具 WAN killler 來發送固定的攻擊速率，攻擊時間固定持續在一分鐘，對於攻擊速率的變化，從每秒 10 個封包至每秒 70 個封包不等。

在實驗當中，分別探討了不同的面相，分別有在網路使用率愈高時，TSN 與傳統的乙太網路的端到端之間的延遲變化，以及拒絕服務 (DoS) 攻擊和延時攻擊(Time delay attack)的比較，前者主要是證明 TSN 交換器在 TSN 模式下的延遲保證是有用且有效的，在高度使用的線路中能夠保證流量在時間內送達，不會因為高度密集的流量而影響 TSN 所保證延遲的流量，後兩者則是針對環境所常見的攻擊模式，藉由發起攻擊來驗證檢測工具的效能。

4.1 TSN mode vs. Ethernet mode

如圖三所示，可以看到 TSN 方法與傳統的乙太網路相互比較，並且模擬傳送資料的流量對於 TSN 模式與 Ethernet 模式之間的差異，UDP 干擾流量的發送量由 100Mbps 逐漸提升到 1Gbps，端到端之間的延遲單位為微秒(μs)，每一個點都由上下限的數值，代表在當下的傳輸量之中的最大值與最小值，每一個點代表的則是當下的傳輸量之中的平均值，可以發現 UDP 的傳輸量到達 400Mbps 時，乙太網路的端到端延遲就已經逐漸提升，端到端的最大值與最小值已經變得非常不穩定，到達 1000Mbps 時，也就是 UDP 傳輸量到達 1Gbps 時，端到端延遲的最大值已經到達 9 秒，平均值則超過 2 秒，可以見乙太網路的不可靠性，反之在 TSN 模式時，不管網路的傳輸量的變化，其端到端的延遲接保持穩定，以證明 TSN 對於流量的穩定性與可靠度。

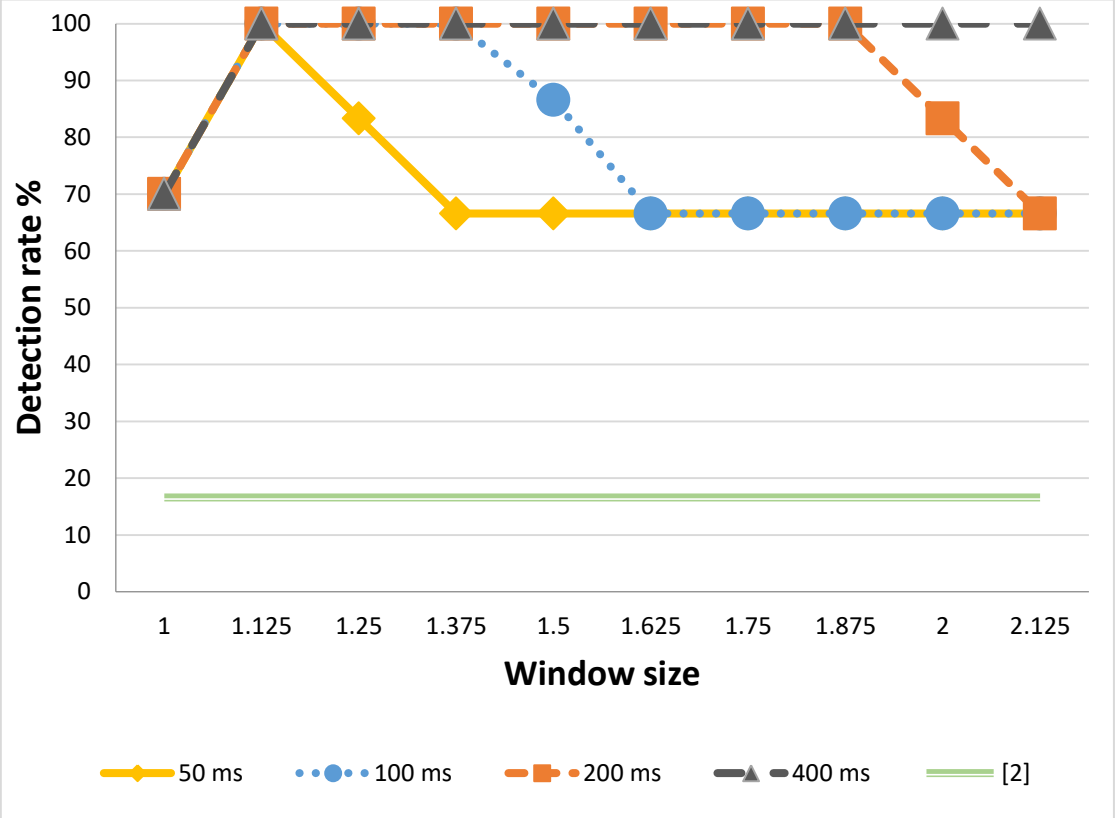


圖三：TSN 模式與乙太網路模式之端對端延遲(end-to-end delay)

4.2 延時攻擊(Time delay attack)

延遲工業控制系統中控制資料包的傳輸，換言之，延時攻擊是將封包在時間 t 的傳輸被惡意延遲 n 個時間間隙，因此，在第(t+n)個時間間隙過後才會到達接收端。延時攻擊可以通過受感染的路由器或使用工業物聯網的殭屍網絡病毒藉由干擾通信通道來發動攻擊。本小節展示了 PsPIDS 的檢測方法對於延時攻擊的場景的檢測結果比較，如圖四所示。實驗展示了延時攻擊的檢測率的影響，X 軸以週期為基準等比例放大檢測範圍，分別有 100ms 和 200ms 兩個周期，Y 軸是檢測率如公式(2)所示，變化的延遲時間則是以 50ms、100ms、200ms 以及 400ms 進行變化，由於 window size 的大小會影響其中的流量有部分的正常流量可能會被判定異常，導致檢測結果不佳，例如在 window size 完全等於封包週期會有部分流量到達時間會有傳輸上的誤差，使封包出現週期有微秒的差距，以至於檢測率低，經過實驗觀察過後，發現在 window size 等於週期的 1.125 被為最佳檢測率，由於 Window Size 的逐漸變寬，實驗中所注入的延遲時間攻擊封包皆包含在觀察範圍之中，因為正常的數據比例佔多數，當所有攻擊封包無法被檢測到時，其檢測率為百分之 66.66%。

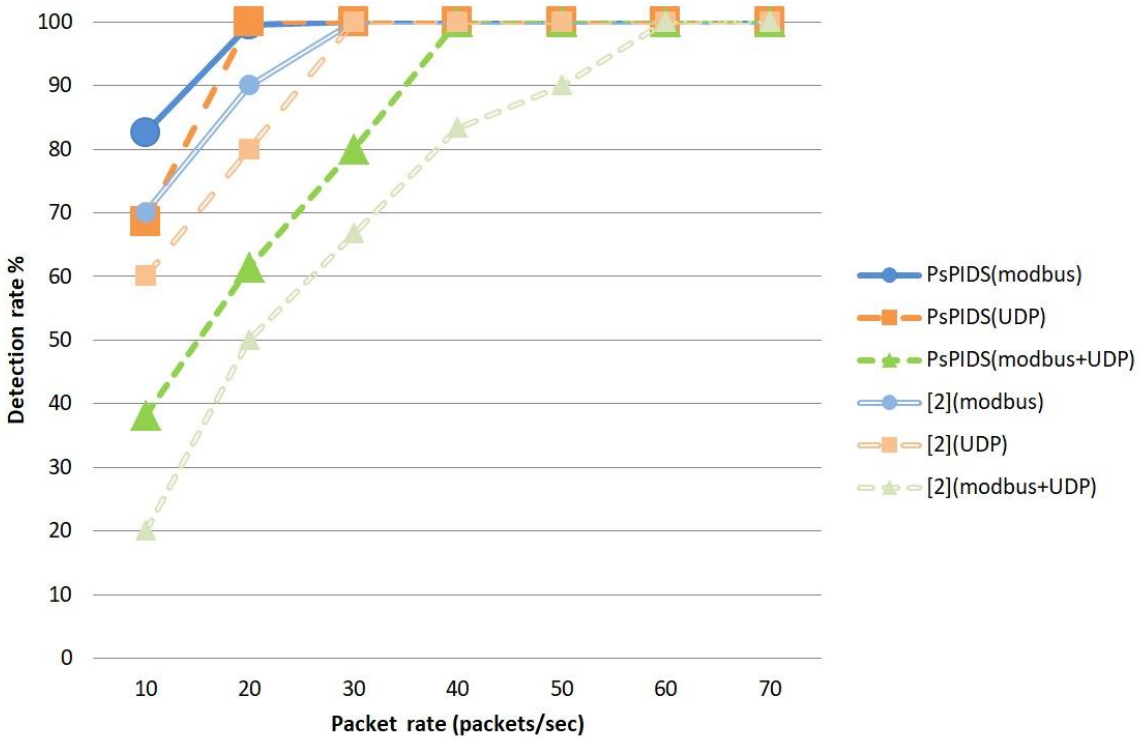
$$\text{Detection Rate} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (2)$$



圖四：延時攻擊的檢測結果

4.3 拒絕服務 (Denial of Service, DoS) 攻擊

拒絕服務(DoS)攻擊是一種旨在癱瘓設備或網絡，使其目標用戶無法對設備或是網路進行操作，攻擊的受害者通常以銀行、商業和工廠設備控制或政府的服務器為目標，儘管 DoS 攻擊通常不會導致重要信息或其他資產的盜竊或丟失，但它們可能會對受害者需要大量時間解決和損失許多成本來處理。另一種 DoS 攻擊是分佈式拒絕服務(Distributed Denial of Service, DDoS) 攻擊，攻擊不是來自相同一個位置發動攻擊，其幫助攻擊者增加了更多的優勢，例如利用更大量的機器來執行造成更加嚴重的破壞性攻擊、由於隨機分佈的攻擊系統導致攻擊位置難以指認、因為發動攻擊的是被控制的主機，真正的攻擊者則隱藏在系統後面，所以難以識別真正的攻擊來源等等的優勢。本小節展示了 PsPIDS 對於拒絕服務(DoS)攻擊的場景的檢測結果比較，如圖五所示。實驗展示了 DoS 攻擊的檢測率的影響，封包每秒的傳送數量分別從每秒 10 個封包至 70，Y 軸是檢測率如公式(2)所示。



圖五：拒絕服務的檢測結果

進行 DoS 攻擊的類型分別有 Modbus、UDP 以及兩者混和(Modbus+UDP)來實驗，混和攻擊的比率為 1:1，實驗前先將計算出正常的環境中 Modbus 封包在正常傳送時的封包熵(Entropy)分布的數值範圍，在判斷時除了要符合封包的週期與延遲，計算出封包熵(Entropy)分布的數值如果超出正常傳送的數值範圍則判定流量中存在異常，反之則為正常，接下來開始在環境中注入 DoS 攻擊的封包到正常的流量當中，實驗發現本文所提出的方法最晚在每秒 30 個封包的情況下達到 100%的準確率，在混和的攻擊中，正常流量中的封包協定為 Modbus，混和的攻擊流量各別封包上升為其他兩者的一半，因此封包熵(Entropy)大小分布與正常的流量較為相近，導致在混和攻擊的起始檢測率較低相較於其他兩者攻擊。

伍、結論

本篇提出的 PsPIDS 檢測工具適用於在 TSN 標準下的工業控制系統的環境中，基於 TSN flow 傳輸的確定性，PsPIDS 能夠根據訊框(frame)抵達的延遲時間以 flow 的週期檢查流量中是否有惡意攻擊，將檢測到的異常工之系統或是管理者以對攻擊做出及時的反應，對於工業控制系統所需要嚴格的時間確定性的需求而言是至關重要，再利用封包熵(Entropy)大小分布，進一步提升檢測率，因此和一般的 IDS 相比，PsPIDS 能夠擁有快

速的檢查速度的前提下，進一步提升對於加密流量的檢測效率。

在未來的研究當中，能夠擴展更大的拓樸，利用乙太網路常見到的環形、網狀、樹狀或是星狀拓樸等等增加網路之間的複雜度。我們也可以增加更多技術的整合，例如利用 OPC UA 用於實現現場層子系統與上層實體之間的橫向和縱向通信，實現更大的應用領域。或是可以使 IT 與 OT 之間的資訊進行整合，如果 OT 方面的感測器數據和 IT 資訊對齊，就能使異常檢測有更好的檢測效率，也能使檢測更精準更容易成功，可以根據更多元的數據進行參數調整，根據不同的單位的數據進行調整，而不會因為環境差異導致影響檢測準確度測試。

參考文獻

[1] T. Ainsworth, J. Brake, P. Gonzalez, D. Toma, and A. F. Browne, “A Comprehensive Survey of Industry 4.0, IIoT and Areas of Implementation,” SoutheastCon 2021, Mar. 2021, doi: 10.1109/southeastcon45413.2021.9401860.

[2] P. Du and S. Abe, “Detecting DoS attacks using packet size distribution,” Proceedings of the 2nd International Conference on Bio-Inspired Models of Network Information and Computing Systems, 2007, doi: 10.4108/icst.bionetics2007.2406.

[3] F. Zezulka, P. Marcon, Z. Bradac, J. Arm, and T. Benesl, “Time-Sensitive Networking as the Communication Future of Industry 4.0,” IFAC-PapersOnLine, vol. 52, no. 27, pp. 133–138, 2019, doi: 10.1016/j.ifacol.2019.12.745.

[4] IEEE 802.1 Working Group. “IEC/IEEE 60802 TSN profile for industrial automation,” 2021

[5] A. Nasrallah et al., “Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research,” IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 88–145, 2019, doi: 10.1109/comst.2018.2869350.

[6] S.-H. Chang, H. Chen, and B.-C. Cheng, “Time-predictable routing algorithm for Time-Sensitive Networking: Schedulable guarantee of Time-Triggered streams,” Computer Communications, vol. 172, pp. 183–195, Apr. 2021, doi: 10.1016/j.comcom.2021.03.019.

[7] C.-C. Chuang, T.-H. Yu, C.-W. Lin, A.-C. Pang, and T.-J. Hsieh, “Online Stream-Aware Routing for TSN-Based Industrial Control Systems,” 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sep. 2020, doi: 10.1109/etfa46521.2020.9211969.

[8] K. Nikhileswar, K. Prabhu, D. Cavalcanti, and A. Regev, “Time-Sensitive Networking Over 5G for Industrial Control Systems,” 2022 IEEE 27th International Conference on

Emerging Technologies and Factory Automation (ETFA), Sep. 2022, doi: 10.1109/etfa52439.2022.9921680.

[9] S. McLaughlin et al., “The Cybersecurity Landscape in Industrial Control Systems,” Proceedings of the IEEE, vol. 104, no. 5, pp. 1039–1057, May 2016, doi: 10.1109/jproc.2015.2512235.

[10] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” Computers & Security, vol. 89, p. 101677, Feb. 2020, doi: 10.1016/j.cose.2019.101677.

[11] H. M. Song, H. R. Kim, and H. K. Kim, “Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network,” 2016 International Conference on Information Networking (ICOIN), Jan. 2016, doi: 10.1109/icoin.2016.7427089.

[12] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, and M. Ekstedt, “Exploiting Bro for Intrusion Detection in a SCADA System,” Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, May 2016, doi: 10.1145/2899015.2899028.

[13] V. K. Singh, H. Ebrahem, and M. Govindarasu, “Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment,” 2018 North American Power Symposium (NAPS), Sep. 2018, doi: 10.1109/naps.2018.8600548.

[14] T. Kobzan, S. Schriegel, S. Althoff, A. Boschmann, J. Otto, and J. Jasperneite, “Secure and Time-sensitive Communication for Remote Process Control and Monitoring,” 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Sep. 2018, doi: 10.1109/etfa.2018.8502539.

[15] Cisco, “Time-Sensitive Networking: A Technical Introduction,” 2017. available at https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/white-paper-c11-738950.pdf

[作者簡介]

周耘廣，從明志科技大學電子工程系畢業後，因為對網路世界的好奇心，考取國立中正大學通訊工程研究所通訊網路組，加入資訊網路安全暨確保實驗室(Information Networking Security and Assurance Lab, INSA)，就讀期間主要研究物聯網、機器學習等相關網路安全議題，目標是希望將來能夠進入世界一流的公司進行軟體開發。

鄭伯炤，1996 年獲得新澤西理工學院 CIS 博士學位。現為國立中正大學通訊工程系教授。畢業後，他也曾在 Transtech Network (2000-2002)、Bellcore (1998-2000)和 Racal DataCom (1996-1998) 工作。他的廣泛興趣包括網路安全、網路管理和即時嵌入式系統設計。