中華民國第三十五屆電力工程研討會
台灣　高雄市 2014 年 12 月 5-6 日

基於智慧電網通訊與資安標準之微電網故障偵測雛型系統實現與探討
The Prototype Implementation of the Fault Detection Algorithm for Microgrid: A Feasibility Study Based on IEC 61850 and IEC 62351 Standards

李定謙　　賴裕昆
Ding-Chian Li　　Yu-Kuen Lai

中原大學通訊碩士學位學程　　中原大學大學電機工程研究所
Master Program in Communication Engineering
Department of Electrical Engineering, Chung Yuan Christian University
{g10179011,ylai}@cycu.edu.tw

摘要

由於分散式能源的興起，為完善佈建一微電網系統，其保護機制的發展遂成為了微電網佈建的重要議題。本文基於 IEC 61850 變電站自動化標準中能即時傳遞電壓、電流、電力潮流走向等量測資訊之 Sampled Value 通訊協定，實現微電網故障偵測演算法，再根據 IEC 62351 安全標準中之建議，利用公開金鑰基礎建設，驗證資訊來源的正確性，不但可以提供系統快速找尋故障區域之能力，並且符合微電網所需的安全機制。本文搭配嵌入式系統與網路模擬器的使用，透過真實環境所獲得的量測數據，於系統中探討相關參數與行為改變時，對於演算法效能之影響。

關鍵詞：IEC 61850、IEC 62351、微電網保護機制、身分認證機制、嵌入式系統、故障偵測。

Abstract

The information and communication technologies are the key building blocks that provide the important infrastructure for system implementation of distributed energy resources. In this study, we build an embedded IED prototype for real-time fault detection in Microgrid systems. The system exchanges SMV (Sampled Measured Values) packets defined in IEC 61850 with neighborhood IEDs through Ethernet. The prototype is not only capable of locating the fault immediately but also capable of verifying the authenticity of the messages based on the requirement of IEC 62351 standards. We conduct simulations based on the EstiNet network simulator and verify the effectiveness of the proposed algorithm based on the transmission latency in real-world local area network environment.

Keywords: IEC 61850, IEC 62351, Fault Detection, Microgrid protection, Identity verification, Embedded system。

1.前言

隨著再生能源使用需求增加，微電網的發展亦趨熱絡，透過以再生能源為主之各式分散式能源的使用，將可改善較偏遠地區之用電問題，並實現節能減碳的目標，進而達成永續發展的宗旨。微電網在大量佈建前，必須具備安全功能，即辨別故障的能力，相關故障偵測演算法運行時需要有快速的通訊能力及安全的資料防護機制作為後盾，進而提高其效能及正確性，並確保免於非人為之天災或人為之攻擊行為影響。

2.相關背景介紹

2.1 微電網故障偵測

微電網是一個由分散式電源及負載所組成的系統，具備小型負載、分散式電源及儲能系統的高、低壓配電網路[1]，同時具備有：(1)分區架構，微電網區域內部為一分區運作結構；(2)微電網區域內之電力潮流分布常作大幅度的改變等兩大特性，根據其運轉的情形可分為市電併聯(Grid-connected)及孤島運轉(Islanded Model)兩種運轉模式[2]。

由於再生能源易受日照、風速等環境因素影響，在大量佈建前，適用於微電網的故障偵測及保護系統之發展為一重要議題，其中美國電力可靠度技術聯盟 CERTS (Consortium for Electric Reliability Technology Solutions) 所發展的微電網保護方法在現有文獻中最具代表性，但由於國內 380V 低壓微電網的運作特性，導致此方法並無法根據故障電流偵測故障位置，故此方法並不適用於國內 380V 低壓微電網多重接地系統上[3][4]。

微電網故障前後電壓及電力朝流具有以下幾種特徵：

1. 當微電網區域內發生故障時，其電壓值會迅速的降至零或接近零，同時，電流則會大幅度上升，如圖 1 與圖 2 所示，當故障於第 305 點發生在電源第一相時，其電壓驟降幅度相當大，而電流則大幅上升。

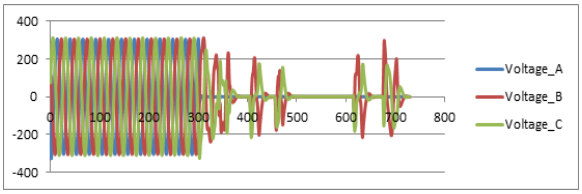

圖 1:故障前後之電壓值作圖

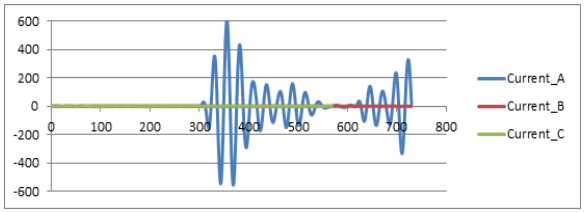

圖 2:故障前後之電流值作圖

2. 當故障發生時，電力潮流會根據各節點與故障點之相對位置進行改變，如圖 3 及圖 4 所示，

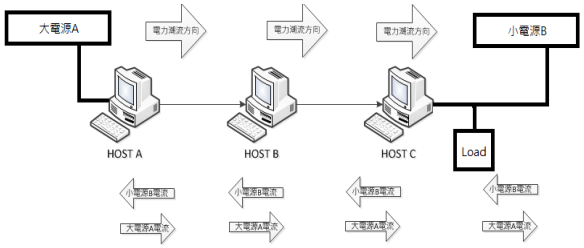

圖 3:故障發生前之電力潮流走向

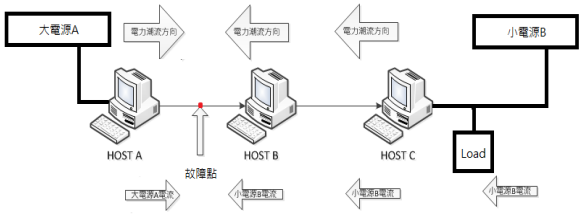

圖 4:故障發生後之電力潮流走向

2.2 IEC 61850 與 62351 國際標準

IEC 61850 標準以物件化為導向，透過映射(mapping)將所需的資料及服務對應於各種通訊協定當中。

表 1:IEC 61850 國際標準架構[5]

章節	標題
1	Introduction and Overview
2	Glossary of terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Functions and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	-Principles and Models
7.2	Abstract communication service interface (ACSI)
7.3	Common Data Classes
7.4	Compatible logical node classes and data classes
8	Specific communication service mapping (SCSM)
8.1	Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
9	Specific communication service mapping (SCSM)
9.1	Sampled values over serial unidirectional multidrop point to point link
9.2	Sampled values over ISO/IEC 8802-3
10	Conformance testing

表 1 為變電站自動化標準 IEC61850 之架構，在第三、四及五部份中定義了變電站所需的功能及需求；第六部分中，定義了以 XML 資料格式做為基礎的變電站配置語言(Substation Configuration Language, SCL)，藉由變電站配置語言的使用，各式與變電站自動化相關的設備；第七部份中，定義了與變電站及饋線設備相關的通訊架構；第八部分中定義了如何將各式資料、物件及服務映射於製造業訊息規範(Manufacturing Messaging Specification, MMS)；第九部分規範了與資料取樣(Sampled Value, SV)相關的映射作業；而第十部分則規範了相關的一致性測試作業。

IEC 61850 中對於傳輸時間敏感的(time-critical)通訊協定如圖 5 所示，常用於資料傳輸的則為 Sampled Value, SV 及 Generic Substation Event, GSE。

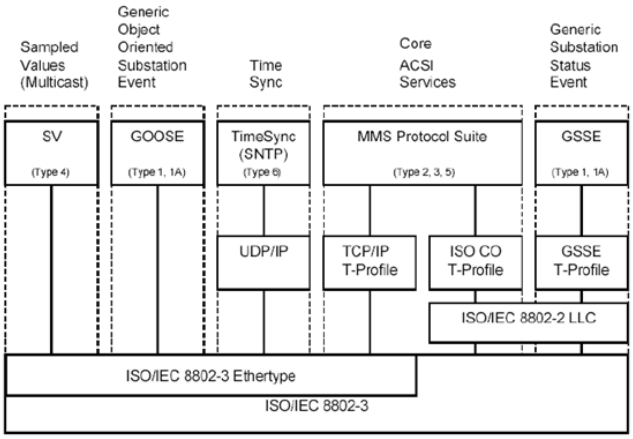

圖 5:IEC 61850 相關通訊協定[5]

表 2:IEC 62351 國際標準架構[6]

章節	標題
1	Introduction to the standard
2	Glossary of terms
3	Security for any profiles including TCP/IP.
4	Security for any profiles including MMS
5	Security for any profiles including IEC 60870-5
6	Security for IEC 61850 profiles
7	Security through network and system management
8	Role-based access control.
9	Key Management.
10	Security Architecture
11	Security for XML Files

IEC 62351 標準涵蓋了與 IEC 自身制定的相關通訊協定所需之資通安全規範，如表 2 所示，包含了 IEC 60870-6、IEC 61850、IEC 61970 及 IEC 61968 等標準。

在第一部分當中指出相關規範制定的歷史緣由及智慧電網各項安全問題，例如，智慧電網的環境中，由於通訊連線特性與傳統網路的差異，各設備必須要定期

的進行重新協商的動作，以處理五千個訊框/封包或十分鐘為一周期；第三部分以傳輸層為探討對象，使用身分驗證為主要的資安解決手法，以 TLS 協定提供所需之安全需求；第四部份則以 MMS 為主體，針對應用層，定義了 A-Profile 配置，實體層至傳輸層則定義了 T-Profile，保障 MMS 之安全；第五部分則與 IEC 60870-5 相關之訊息格式、操作流程、演算法與達成系統戶操作性的必要需求等規範有關；第六部分則與 IEC 61850 所定義之通訊協定有關，包含了 GOOSE、GSE、Sampled Value 等，為達到 3 毫秒響應時限，傳輸過程中並不使用資料加密相關手法；第七部分則針對網路及系統管理技術做詳細的規範；第八部分與以角色為基底之存取控制有關；第九部分則與系統所使用之金鑰的管理議題相關，包含完整金鑰的金鑰生命週期，包含金鑰產生、憑證使用、憑證撤銷清單維護至金鑰撤銷，涵蓋所有確保安全及正確的管理相關金鑰的程序與措施；第十部分及第十一部份則包含了安全的系統架構與 XML 相關的安全需求。

3. 智慧電網之網路與資訊安全

在智慧電網中，存在著許多試圖影響電網系統運作的電網駭客(Power hacker)[7]，其動機不乏出於恐怖主義、藉此敲詐勒索亦或者是透過攻擊重要基礎建設提升自身知名度，因此，一套完整且適用於智慧電網中的網路與資訊安全對策必須涵蓋了許多層面。

表 3:傳統電力系統與智慧電網之網路環境比較表

環境	特性
傳統電力網路	1.為一較為封閉之系統 2.以序列埠通訊模式為主要連線方式
智慧電網	1.為一較為開放之系統 2.大量使用以網際網路為基礎之通訊協定作為連線方式

表 4:智慧電網網路與電腦網路環境比較表

網路環境	特性
智慧電網網路	1.常有嚴格的響應時限 2.較為長的連線週期，常為一”永久性的”連線方式
電腦網路	相關的應用程式使用的連線周期較短

由表 3 及表 4 可知，智慧電網相較於傳統電網為一開放性系統，再加上，由於連線行為的不同，在智慧電網的環境中，連線時間較長，因此，重新協商(re-negotiation)為一重要的措施，透過週期性的確認相關連線的可信度確保資料的來源正確性，身分認證的機制將成為保護智慧電網的重要手段。

除了資料本身的安全之外，對於硬體設備的監控、各裝置的密碼管理、裝置內敏感的文件控管(如操作手冊、設備結構圖)、裝置的即時警報功能以及操作人員的安全訓練，皆需要有明確的規範[8]。

由於 Sampled Value 及 GOOSE 通訊協定必須滿足變電站自動化標準 IEC 61850-5 中傳輸時間的需求[9]，因此，資料加密的方式並不適用於需要即時交換訊息的使用環境中，在資通安全標準 IEC 62351 中提到[6]，身分認證機制為 Sampled value 及 GOOSE 等通訊協定可採用的安全措施。

3.1 公開金鑰基礎建設

公開金鑰基礎建設是由眾多服務及技術相輔相成[10][11]，可提供智慧電網一系統化的安全架構及身分驗證的機制並確保資訊內容完整性、資訊來源正確性、資訊內容時效性、資訊內容合法性等重要資訊安全要點。

公開金鑰基礎建設包含了憑證管理中心(Certificate authority ,CA)、註冊中心(Registration Authority ,RA)、生效 (validation) 、撤銷 (Revocation) 及認證發行方法 (Certificate publishing methods)，金鑰對包含可公開於網路環境中的公開金鑰以及由持有者所擁有的私密金鑰，兩者相互作用所形成的應用如表 5 所示。

表 5:金鑰使用方法、類型與時機[11]

金鑰功能	金鑰類型	金鑰持有人
為接收者加密資料	公開金鑰	接收者
簽章	私密金鑰	傳送者
解密密文	私密金鑰	接收者
簽章識別	公開金鑰	傳送者

4.系統架構

4.1 嵌入式系統設計架構

本論文使用含有雙核心 ARM Cortex A9 處理器與 512 MB DDR3 記憶體之 ZedBoard 開發版[14]作為嵌入式系統硬體平台，以基於嵌入式 Linux 作業系統的 BusyBox[15]相關工具，透過 Rapid61850 [16]以及 OpenSSL[17]函式庫實現 Sampled Value 訊框傳送、微電網故障偵測演算法及身分驗證機制，其完整系統架構圖如圖 6 所示。

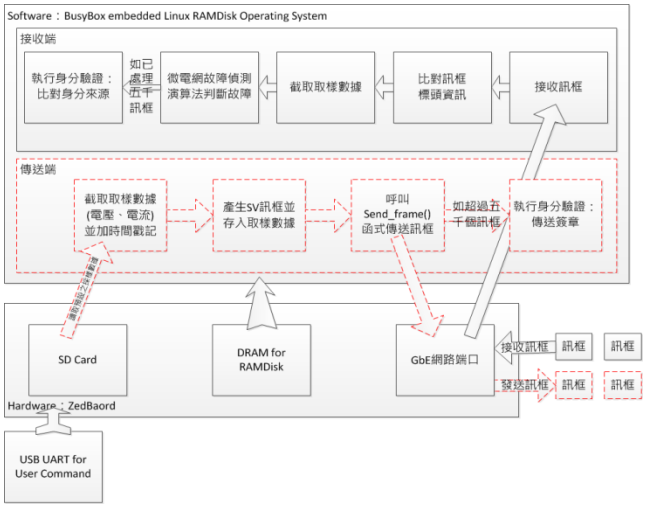

圖 6:嵌入式系統設計架構圖

根據前述之行為特徵，施柏安等人[4]發展出一適用於國內核研所微電網 380V 系統之***微電網故障偵測演算法***，此故障偵測流程共可分為故障發生時間點偵測、確定發生故障及檢出故障類型、故障區間偵測三部分，演算法流程如圖 7 所示，

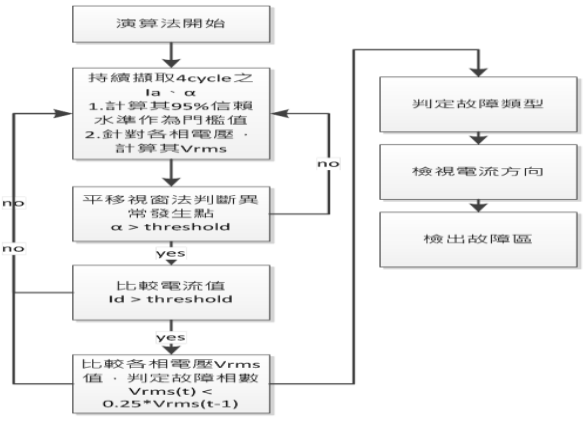

圖 7:微電網故障偵測演算法流程圖

其中 α 如方程式(1)所示，

$$\alpha = 2\cos(\omega\Delta T_1)*X_1 - X_0 - X_2 \quad (1)$$

電流判定方式如方程式(2)所示，

$$I_{d,fault} > I_{d,prefault,95\%} \quad (2)$$

電壓判定方式如方程式(3)所示，

$$V_{rms,fault} < 0.25 * V_{rms,prefault} \quad (3)$$

電流方向則透過相電壓與相電流零交越點兩者之間的取樣數差值來計算故障後兩者之間的角度，再比較相鄰電驛的功率因數角，藉此判斷故障電流是否反相。

5.實驗結果與討論

本論文實驗是將微電網之中實際的電壓及電流故障數據量測資料[4]，如圖 1 及圖 2 所示，置入系統記憶體中，取代擷取量測值的步驟，並透過直接指定電流方向取代計算零交越點的流程。

由圖 1 及圖 2 可知，此數據為一單相接地故障模擬數據，故障點發生於 A 相第 305 資料點上，流程圖與系統實驗拓樸如圖 8 及圖 9 所示，預設故障點將會發生於故障偵測系統 A 與控制器電腦之間，而預設電力潮流方向為系統拓樸之左手邊流至右手邊。

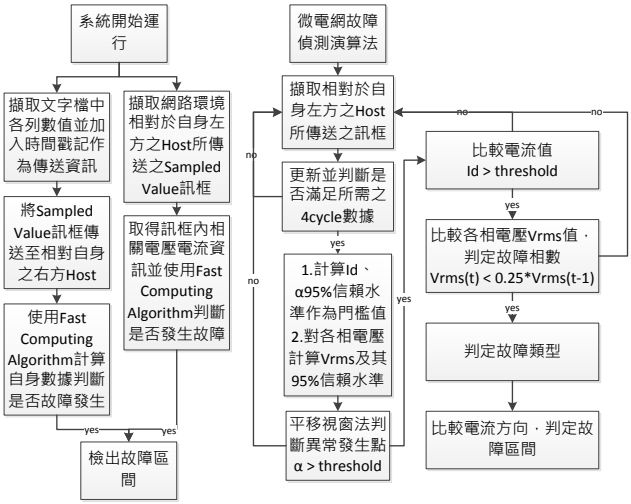

圖 8:Sampled Value 與故障偵測演算法運作流程

圖 9:含有一組控制器電腦和兩組具有故障偵測能力之智慧電子裝置(IED)雛型系統

5.1 微電網故障偵測演算法功能測試

微電網故障偵測演算法所訴求的為一快速的響應時間，必須要能夠在故障發生後 2cycle(共 48 取樣點，約 0.03312 秒)內判別故障區間，圖為控制器電腦所視之結果，由圖 10 可知，當第 307 訊框進入時，可透過比較電流方向判斷出故障區間。

```
this is 306 frame
in unormal case
rms_pre = 38.680145, rms_now = 24.415894
frame_up update
this is 307 frame
in unormal case
rms_pre = 24.415894, rms_now = 5.520730
direction changed, fault area is on left-hand side
phs1 fault
frame_up update
this is 308 frame
in unormal case
rms_pre = 7.520730, rms_now = 2.148645
phs1 fault
frame_up update
this is 309 frame
in unormal case
rms_pre = 2.148645, rms_now = 0.766103
phs1 fault
frame_up update
this is 310 frame
in unormal case
rms_pre = 0.766103, rms_now = 0.780831
```

圖 10:控制器電腦所顯示之結果

5.2 網路行為對於故障偵測演算法之影響

由於微電網故障偵測演算法對於傳輸及響應時間有著嚴格的需求，因此，本節透過此些篇幅探討網路行為對於微電網故障偵測演算法之影響。

網路行為內包含了許多影響訊息傳送之因素，與時間因素有關的為網路系統產生的相關延遲效應，包含了除佇列延遲(Queuing Delay)、傳播延遲(Propagation Delay)、傳輸延遲(Transmission Delay)、處理延遲(Processing Delay)，另一方面，與資料正確性相關之因素則包括了位元錯誤率(Bit Error Rate)、封包遺失率(Packet Lost Rate)以及封包序列錯誤(Out-of-order packet delivery)。

在延遲部分，影響最為顯著的為除佇列延遲，其餘延遲在正常情形下可視為一常數，本章節透過網路模擬器 NCTUns[19]模擬相關環境參數，包含頻寬、佇列大小、位元錯誤率以及吞吐量等，結果如表 6 所示，

表 6:NCTUns 模擬結果-1

傳送頻率(次/秒)	1440	1440	1440	1440
訊框大小(位元組)	144	144	144	144
吞吐量(Mbps/s)	1.66	1.66	1.66	1.66
頻寬(Mbps)	10	10	100	100
節點數	5	5	5	5
傳播延遲(us)	5	5	5	5
暫存器大小(個訊框)	50	500	50	500
位元錯誤率	10^{-6}	10^{-6}	10^{-6}	10^{-6}
最大延遲(ms)	16.898	17.55	0.846	1.765
最小延遲(ms)	0.33	0.336	0.061	0.042
平均延遲(ms)	8.142	8.5	0.456	0.835
訊框遺失率(%)	4.35	0.5	4.29	0.5

由表 6 可知，影響整體效能最主要的因素為可用頻寬，同時，增加暫存空間能有效的減少訊框遺失發生，但也連帶地影響了訊框傳輸的延遲時間，在 IEC 61850-6 中規範，Sampled Value 訊框傳輸延遲必需小於 3 毫秒[18]，而傳輸部分必須佔總體延遲時間 20 個百分點以下，即 0.6 毫秒以下，由表 6 的結果來看，僅在頻寬為 100Mbps 及暫存空間為 50 個訊框空間時能夠滿足標準之要求，3 毫秒同時也將考驗系統整體效能。

在微電網故障偵測演算法功能測試的實驗結果中顯示，微電網故障偵測演算法必須要在故障發生後取得 1~2 個訊框資訊進行分析才可正確判斷故障區間，在模擬結果中，訊框遺失的分布情形中包含了 2~3 個訊框連續遺失的情況，此現象將導致故障偵測演算法判斷出故障的時間向後推遲，判斷故障所需時間如公式(4)所示，

$$T=0.00069*(2+n)+T_{delay} \quad (4)$$

於公式(4)中，參數 n 為故障後至接收兩個有效訊框前所遺失的訊框數，T_{delay} 包含了傳送端傳至目的地端之間所有時間延遲。

表 7NCTUns 模擬結果-2

傳送頻率(次/秒)	1440	1440	1440	1440
訊框大小(位元組)	257	257	257	257
吞吐量(Mbps/s)	2.96	2.96	2.96	2.96
頻寬(Mbps)	10	10	100	100
節點數	5	5	5	5
傳播延遲(us)	5	5	5	5
暫存器大小(個訊框空間)	50	500	50	500
位元錯誤率	10^{-6}	10^{-6}	10^{-6}	10^{-6}
最大延遲(ms)	26.79	27.5	1.35	2.7
最小延遲(ms)	0.511	0.511	0.063	0.063
平均延遲(ms)	12.715	13.218	0.722	1.325
訊框遺失率(%)	4.56	0.76	4.58	0.78

為避免訊框遺失過多造成等待時間過長，可透過將多筆資料由同一訊框傳送的方法來改善，但資料量增加，將會影響系統負載流量，導致訊框傳輸的延遲增加，整體延遲時間與吞吐量大小為高度正相關關係，過多的資料將造成整體網路負載上升，進而影響系統效能。除了網路效能之外，大量的資料處理也將影響硬體計算效能，尤其在有限硬體資源之嵌入式系統上更為顯著。以下我們以夾帶一筆回復資料作為範例，探討增加資料量對於整體訊框延遲的影響，結果如表 7 所示，由表 7 可知，當資料量由一筆資料增加至兩筆資料時，對於整體傳輸延遲產生了相當大的影響，以下針對表 6 及表 7 中兩組最佳的結果進行比較，如表 8 所示，

表 8:資料量大小影響比較表

	一筆資料	兩筆資料	影響程度(%)
傳送頻率(次/秒)	1440	1440	X
訊框大小(位元組)	144	257	+78.31%
吞吐量(Mbps/s)	1.66	2.96	+78.31%
頻寬(Mbps)	100	100	X
節點數	5	5	X
傳播延遲(us)	5	5	X
暫存器大小(個訊框空間)	50	50	X
位元錯誤率	10^{-6}	10^{-6}	X
最大延遲(ms)	0.846	1.35	+59.57%
最小延遲(ms)	0.061	0.063	+3.28%
平均延遲(ms)	0.456	0.722	+58.33%
訊框遺失率(%)	4.29	4.58	+6.76%

由表 8 可知，當資料量增加了 78 個百分比，整體平均延遲將增加了 58 個百分比，資料量將對整體延遲有著嚴重的影響，此拓樸中，訊框遺失的比率低，並無大量訊框連續遺失的情形，因此，單一訊框夾帶一筆回復資料為此實驗環境最佳的回覆機制設定。

5.3 運算身分驗證機制所需時間

微電網故障偵測演算法具有嚴格的響應時間限制，各式複雜的資料加密演算法並不適用於故障偵測演算法所傳輸的每一筆訊框當中。因此，系統須透過身分認證達到安全的要求[20]，然而，認證牽涉到了龐大的計算，勢必會影響系統效能，本文基於公開金鑰演算法，使用 OpenSSL 函式庫，實現資訊摘要、驗證之相關流程，於 ZedBoard 開發板上之 ARM Cortex A9 處理器實際運行，來探討身分認證機制所需處理時間。

在實務上，為確保流通金鑰的正確性，常會透過公正的第三方單位傳遞金鑰，以此確保金鑰與金鑰持有人身分的配對關係，常見的身分認證流程如圖 11[21]所示，本小節利用圖 11 做為探討情境，排除網路傳輸所造成之延遲時間，僅考慮在傳送及接收端所處理的摘要及加解密的運算，實驗結果皆為運作十次所取得之平均運行時間，所使用之摘要原文為 64 個位元組大小；雜湊函數為 SHA1；金鑰選用長度為 1024 位元長度之 RSA 金鑰，其結果如表 9 所示。

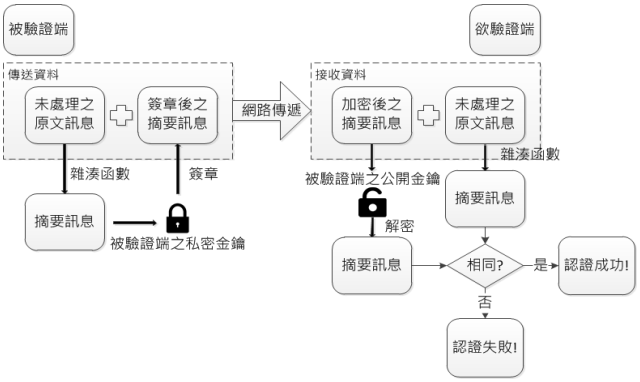

圖 11:公開金鑰基礎建設身分認證流程

表 9:傳送與接收端運算時間

	傳送端	接收端
摘要次數	1	1
簽章次數	1	0
解密次數	0	1
驗證次數	0	1
比對次數	0	1
平均時間(秒)	0.017	0.033

由表 9 結果顯示，當系統傳送頻率為 1440(訊框/秒)並以單線程(Single Thread)運作時，傳送端與接收端在身分驗證的階段中將會損失 25 個傳送及 48 個接收訊框，而微電網故障偵測演算法需要在 48 個訊框處理時間內判斷出故障位置，再加上網路環境所造成的封包延遲及遺失行為的發生，將有可能導致微電網故障偵測演算法無法在時限內判斷出故障點位置。

6. 結論與未來展望

本文基於 IEC61850 國際標準所規範的 Sampled Value 通訊協定，於嵌入式硬體平台上，實現了微電網故障偵測演算法系統，我們透過網路模擬器，調整網路頻寬、佇列大小、位元錯誤率以及吞吐量等相關的網路行為，藉此了解其對於演算法效能影響，更根據 IEC 62351 標準之規範，透過公開金鑰基礎建設以及身分驗證機制，藉由週期性的驗證模式，確保系統資料傳輸之資訊安全需求。

在未來，我們計畫優化系統的設計，再加入使用於微電網系統的相關通訊協定，並將實驗的測試平台和網路拓樸建置的更趨近於真實，來深入分析資訊安全規範以及網路行為對整體系統運行效能的影響。

誌謝

本文承蒙行政院國科會研究計畫補助，特此致謝。國科會編號:NSC 101-3113-P-033 -003。

參考文獻

[1] Sortomme, E. (2010), ”Microgrid Protection Using Communication-Assisted Digital Relays,” Power Delivery, IEEE Transaction on (Volume:25, Issue: 4), 2789-2796

[2] Qin Lei (2009), “Islanding Control of DG in Microgrids,” Power Electronics and Motion Control Conference, 450-455

[3] Nikkhajoei, H. (2007), “Microgrid Protection,” Power Engineering Society General Meeting, IEEE, 1-6

[4] 施柏安 (民國 102 年)，微電網保護電驛演算法之發展，碩士論文，中原大學電機工程研究所。

[5] IEC 61850 wiki, online available: http://en.wikipedia.org/wiki/IEC_61850

[6] IEC 62351, online available: http://en.wikipedia.org/wiki/IEC_62351

[7] 電網黑客 online avalible: http://www.twwiki.com/wiki/%E9%9B%BB%E7%B6%B2%E9%BB%91%E5%AE%A2#1

[8] IEEE 1686-2007, online available: http://standards.ieee.org/findstds/standard/1686-2007.html

[9] IEC 61850-5, online available: http://goo.gl/8w2uaC

[10] Jean Carlo Binder (2002),”Introduction to PKI – Public Key Infrastructure v1.1,” online available: http://www.k-binder.be/Papers/PKI_V11.pdf

[11] An Introduction to PKI (Public Key Infrastructure), online available: http://www.articsoft.com/public_key_infrastructure.htm

[12] Baumeister, T. (2011), “Adapting PKI for the smart grid,” Smart Grid Communications (SmartGridComm), IEEE International Conference on, 249-254.

[13] Perlman, R. (1999), “An overview of PKI trust models,” Network, IEEE (Volume:13, Issue: 6), 38-43.

[14] ZedBoard, online available: http://www.zedboard.org/product/zedboard.

[15] BusyBox, online available: http://en.wikipedia.org/wiki/BusyBox

[16] Rapid61850, online avalibale: https://github.com/stevenblair/rapid61850

[17] OpenSSl, online available: http://zh.wikipedia.org/zh-hant/OpenSSL

[18] IEC, “IEC/TS 61850-6 Communication networks and systems in substations – Part 6 Configuration description language for communication in electrical substations related to IEDs,” IEC technical committee 57, pages IEC 61850_6, March 2004.

[19] NCTUns, online available: http://nsl10.csie.nctu.edu.tw/

[20] IEC, "IEC/TS 62351-6 power systems management and associated information exchange -- data and communications security -- part 6: Security for IEC 61850 reference," IEC technical committee 57, pages IEC 62351_6, June 2007.

[21] "PKI(Public Key Infrastructure) 簡介 ", online available: http://goo.gl/oOLOJO