國科會資訊安全技術研發專案計畫
『系統測試報告書』

System Testing Document

經由網路之時脈偏移快速測量技術研究
A Quick Approach for Clock Skew Measurement over Network
MOST104-2221-E-011-070

鄧惟中

國立台灣科技大學 資訊工程系

Department of Engineering and Applied Science

National Science Council, Taiwan

2016/06/14

目錄

文件版本修正履歷表

版次	變更項目	變更日期
1.0	初版	2016.06.10
1.1	修訂版	2016.06.14

1 簡介 (Introduction)

經由網路之時脈偏移快速測量技術研究 (A Quick Approach for Clock Skew Measurement over Network, CSMN 1.0.0)的具體目的在於設計一個能在短時間內求得穩定估計值的時脈偏移測量方法。並針對無線通訊時離群值可能出現在底部的情形，改良目前的霍氏轉換為基礎的離群值過濾方法，不再用捨入做為選擇高密度區域的方式，而透過滑動視窗等手法尋找固定寬度的最佳解區域，以提高過濾精確度，同時降低計算量。由於任何有電子鐘以及通訊能力的裝置都可測量出時脈偏移，本計畫之成果將有機會擴大時脈偏移的應用價值。

1.1 測試目的 (Scope of Testing)

這份文件提供基於時脈偏移的裝置識別技術於雲端服務之系統的測試計劃。以確認本系統所有的設計元件均可正確的輸出，在此我們著重於接受度測試(Acceptance Test)。

本文件內容將依據系統需求規格書，描述關於接受度測試的相關計畫與內容。並希望透過此文件之描述與實踐，達到順利進行測試工作之目的。

1.2 接受準則 (Acceptance Criteria)

本測試計劃需要滿足下列的測試接受準則：

- 本系統需要對所有列為必要(Critical、Important、Desirable)之需求作完整測試。
- 測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需 要能符合預期測試結果方能接受。
- 以測試案例為單位，當測試未通過時，需要進行該單元的測試，其 接受的準則與前一項規定相同。

2 測試環境 (Testing Environment)

2.1 硬體規格 (Hardware Specification)

- 桌上型電腦
  - CPU：Intel® Core™2 CPU 6420 @ 2.13GHz
  - RAM：4GB
  - 硬碟：160GB HDD
  - 作業系統：Windows 7(64 bit)
- 筆記型電腦
  - 型號：ASUS A46C
  - CPU：Intel® Core™ CPU I5-3317U
  - RAM：4GB
  - 硬碟：500GB HDD
  - 作業系統：Windows 8.1

2.2 軟體規格 (Software Specification)

- 作業系統：Windows 7(64 bit)、Windows 8.1

2.3 測試資料來源 (Test Data Source)

- 關於測試期間所需的測試資料來源及數量，說明如下：
  - ◆ 桌上型電腦 一台
  - ◆ 筆記型電腦 一台

3 測試時程、程序與責任

(Testing Schedule, Procedure, and Responsibility)

3.1 測試時程 (Testing Schedule)

- 時程
  - ◆ 系統接受測試：105/6/6~105/6/10
- 查核點
  - ◆ 系統接受測試：105/6/10

3.2 測試程序 (Testing Procedure)

- 接受測試 (Acceptance Testing)

需求編號	優先順序	需求描述
CSMN-F-001	1	客戶端傳送時間戳記到伺服器端
CSMN-F-002	1	伺服器端紀錄客戶及伺服端資料並輸出成檔案
CSMN-F-003	1	計算量測時間
CSMN-F-004	1	顯示數據分布圖及量測結果
CSMN-F-005	1	量測時間在 1 分鐘以內
CSMN-F-006	1	能處理高於主群體之離群值
CSMN-F-007	1	能處理低於主群體之離群值
CSMN-F-008	1	分段數據誤差低於 1 ppm
CSMN-F-009	1	累計數據誤差低於 1 ppm

針對測試報告之需求，本系統設計時期之使用案例(UseCase)如下圖所示，本系統須達成使用案例所列之所有功能。

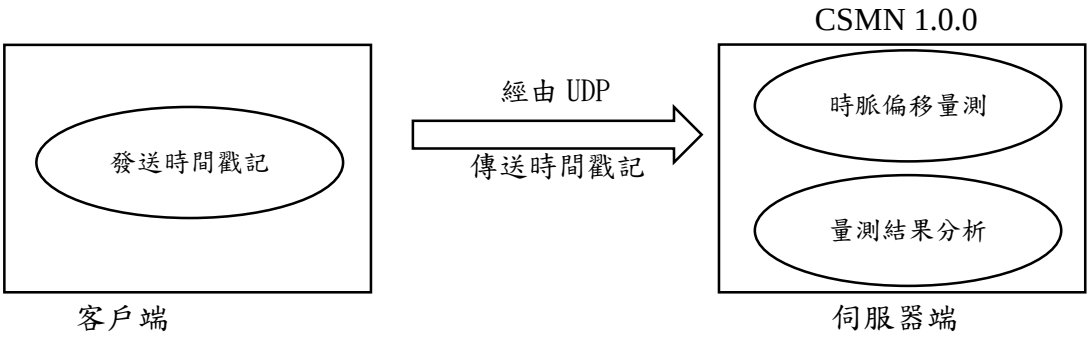

圖3-2-1 CSMN使用案例

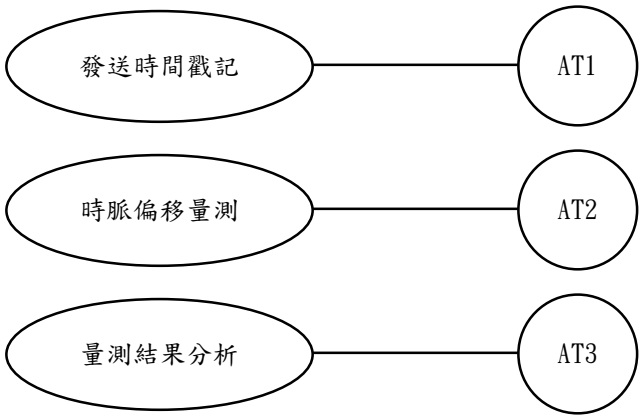

圖 3-2-2 接受度測試圖

3.3 人員職責分配 (Personnel Responsibilities Assignment)

本系統之測試人員姓名及職責如下列所示。

成員名單與縮寫對照表	
縮寫	姓名
OS	Komang Oka Saputra
CF	江奇峰
YY	蘇育毅

Testing Activities	**Personal**
AT1	OS、CF、YY
AT2	OS、CF、YY
AT3	OS、CF、YY

4 測試案例 (Test Case)

4.1 接受測試案例 (Acceptance Testing Cases)

4.1.1 AT1 Test Case

4.1.1.1 目的

- 客戶端傳送時間戳記到伺服器端
- 伺服器端紀錄客戶及伺服端資料並輸出成檔案

4.1.1.2 輸入與輸出

- 客戶端輸入發送間隔，單位為毫秒
- 系統以輸入之發送間隔連續輸出客戶端之時間戳記

4.1.1.3 操作說明

Identification	AT1	
Name	發送時間戳記	
Tested Target	[CSMN 1.0.0]	
Reference	CSMN-F-001、CSMN-F-002	
Severity	1(Critical)	
Instructions	Actor Actions	System Responses
	1.客戶端輸入發送間隔	
	2.客戶端程式發送時間戳記	
		3.伺服器端每接收一次客戶端時間戳記便同時記錄自己的時間戳記
		4.伺服器端將 3.之資訊輸出至檔案中
Expected Result	客戶端系統成功發送使用者定義發送間隔之時間戳記至伺服器端，伺服器端接收並輸出成檔案。	
Cleanup	無	

4.1.2 AT2 Test Case

4.1.2.1 目的

- 計算量測時間
- 顯示數據分布圖及量測結果
- 量測時間在 1 分鐘以內

4.1.2.2 輸入與輸出

- 輸入客戶端/伺服器端之時間戳記組合
- 輸出數據分布圖、量測結果及量測時間

4.1.2.3 操作說明

Identification	AT2	
Name	時脈偏移量測	
Tested Target	[CSMN 1.0.0]	
Reference	CSMN-F-003、CSMN-F-004、CSMN-F-005	
Severity	1(Critical)	
Instructions	Actor Actions	System Responses
		1.系統套用基於霍氏轉換之時脈偏移量測法量測 AT1 產生之檔案
		2.系統顯示數據分布圖、時脈偏移量及量測時間
Expected Result	系統能針對接收之檔案套用基於霍氏轉換之時脈偏移量測法量測並輸出需求之結果。	
Cleanup	無	

4.1.3 AT3 Test Case

4.1.3.1 目的

- 能處理高於主群體之離群值
- 能處理低於主群體之離群值
- 分段數據誤差低於 1 ppm
- 累計數據誤差低於 1 ppm

4.1.3.2 輸入與輸出

- 輸入數據分布圖、量測結果
- 輸出是否符合目的之要求

4.1.3.3 操作說明

Identification	AT3	
Name	量測結果分析	
Tested Target	[CSMN 1.0.0]	
Reference	CSMN-F-006、CSMN-F-007、 CSMN-F-008、CSMN-F-009	
Severity	1(Critical)	
Instructions	Actor Actions	System Responses
		1.系統藉由預設之門檻值鑑定是否能處理高/低於主群體之離群值
		2.系統鑑定分段/累計誤差是否低於 1 ppm
		3.系統回傳鑑定結果
Expected Result	系統正確鑑定基於霍氏轉換之時脈偏移量測法是否符合目的之要求。	
Cleanup	無	

5 測試結果與分析 (Test Result and Analysis)

5.1 接受測試案例 (Acceptance Testing Cases)

在 AT2 測試中套用了本研究提出之改良的基於霍氏轉換之時脈偏移量測法，於門檻值設定為±1 ppm 之下我們採用 FRR(系統辨識合法使用者之誤判率)來進行統計，重複施行 50 次量測後我們發現與改良前結果相比，FRR 值有顯著的改善。儘管伺服器端接收到客戶端發送之時間戳記之過程中傳輸穩定度受到影響會出現高/低於主群體之離群值，本研究之改良法能有效抑制離群值之干擾亦能大幅縮短量測時間至 1 分鐘以內，測試結果符合預設之期望。

表 5-1-1 為接受測試案例的測試結果表。

Test Case#	Results(PASS/FAIL)	Comment
AT1	PASS	
AT2	PASS	
AT3	PASS	

表 5-1-1 接受測試結果

Appendix A：Traceability

- Requirements vs. Test Cases

Test Case / Requirement	AT1	AT2	AT3
CSMN-F-001	V		
CSMN-F-002	V		
CSMN-F-003		V	
CSMN-F-004		V	
CSMN-F-005		V	
CSMN-F-006			V
CSMN-F-007			V
CSMN-F-008			V
CSMN-F-009			V

Appendix B：Glossary

Clock Skew：時鐘偏移，指在雲端伺服器與客戶端裝置連接時，主動要求客戶端的裝置發送封包回伺服器，並收集該封包上的收集時間戳記，用以計算相對於雲端伺服器的偏移值。

Appendix C：References

[1] Tadayoshi Kohno, Andre Broido, and Kc Claffy, “Remote Physical Device Fingerprinting,” IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 2, pp. 93-108, 2005.

[2] Steven J. Murdoch, “Hot or not: Revealing Hidden Services by Their Clock Skew,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 27-36, 2006.

[3] Sebastian Zander and Steven J. Murdoch, “An Improved Clock-skew Measurement Technique for Revealing Hidden Services,” in Proceedings of the 17th conference on Security symposium, pp. 211-225, 2008.

[4] Ding-Jie Huang, Wei-Chung Teng, Chih-Yuan Wang, Hsuan-Yu Huang, and Joseph M. Hellerstein, “Clock Skew Based Node Identification in Wireless Sensor Networks,” IEEE Global Communications Conference (GLOBECOM 2008), pp. 1-5, 2008.

[5] Suman Jana and Sneha Kumar Kasera, “On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews,” in Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, pp. 104-115, 2008.

[6] Chrisil Arackaparambil, Sergey Bratus, Anna Shubina, and David Kotz “On the Reliability of Wireless Fingerprinting Using Clock Skews.” in Proceedings of the third ACM conference on Wireless network security (WiSec 2010), pp. 169-174, 2010

[7] Ding-Jie Huang, Kai-Ting Yang, Chien-Chun Ni, Wei-Chung Teng, Tien-Ruey Hsiang, and Yuh-Jye Lee, “Clock Skew Based Client Device Identification in Cloud Environments,” The 26th IEEE International Conference on Advanced Information Networking and Applications (IEEE AINA 2012) , pp. 526-533, 2012.

[8] 鄭理介(2013)，《基於時脈偏移的可攜式裝置識別技術》，國立臺灣科技大學碩士論文。

[9] Ding-Jie Huang and Wei-Chung Teng, “A defense against clock skew replication attacks in wireless sensor networks,” Journal of Network and Computer Applications, Elsevier, vol. 39, pp. 26-37, 2013.

[10] Marius Cristea and Bogdan Groza, “Fingerprinting Smartphones Remotely via ICMP Timestamps,” IEEE Communications Letters, vol. 17, no. 6, pp. 1081-1083, 2013.

[11] Swati Sharma, Alefiya Hussain, and Huzur Saran, “Experience with Heterogenous Clock-

skew Based Device Fingerprinting," in Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results (LASER 2012), pp. 9-18, 2012.

[12] Xiaowei Mei, Donggang Liu, Kun Sun, and Dingbang Xu, "On Feasibility of Fingerprinting Wireless Sensor Nodes Using Physical Properties," IEEE 27th International Symposium on Parallel & Distributed Processing (IPDPS 2013), pp. 1112-1121, 2013.

[13] Md. Borhan Uddin and Claude Castelluccia, "Toward Clock Skew Based Wireless Sensor Node Services," in The 5th Annual ICST Wireless Internet Conference, pp. 1-9, 2010.

[14] Makoto Aoki, Eiji Oki, and Roberto Rojas-Cessa, "Measurement Scheme for One-Way Delay Variation with Detection and Removal of Clock Skew," ETRI journal, vol. 32, no. 6, pp. 854-862, 2010.

[15] Vern Paxson, "On Calibrating Measurements of Packet Transit Times," ACM SIGMETRICS joint international conference on Measurement and modeling of computer systems (SIGMETRICS 1998/PERFORMANCE 1998), vol. 26, no. 1, pp. 11-21, 1998.

[16] Sue B. Moon, Paul Skell, and Don Towsley, "Estimation and Removal of Clock Skew from Network Delay Measurements," IEEE INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings vol. 1, pp. 227-234, 1999.

[17] Komang Oka Saputra, Wei-Chung Teng and Tsung-Han Chen, "Hough Transform Based Clock Skew Measurement Over Network," IEEE Transactions on Instrumentation and Measurement, in press, doi: 10.1109/TIM.2015.2450293.

[18] Paul V. C. Hough, "Method and Means for Recognizing Complex Patterns," U.S. Patent 3,069,654, 1962.

[19] Richard O. Duda and Peter E. Hart, "Use of the Hough Transformation to Detect Lines and Curves in Pictures," Communications of the ACM, vol. 15, no. 1, pp. 11-15, 1972

[20] Peter E. Hart, "How the Hough Transform Was Invented," IEEE Signal Processing Magazine, vol. 26, no. 6, pp. 18-22, 2009.