2015 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology

6–9 December 2015, Singapore
Preface to WI-IAT 2015 Workshops and Demo/Posters .......................................................... xi
Message from WI-IAT 2015 Workshop Chairs ................................................................... xii
Message from WI-IAT 2015 Demo/Poster Chairs ............................................................. xiv
WI-IAT 2015 Advisory/Steering Committees ................................................................. xv
DOCMAS/WEIN Program Committee ............................................................................. xvi
CMDWM Program Committee ......................................................................................... xviii
WPRSM Program Committee ......................................................................................... xix
KMWSM Program Committee ....................................................................................... xx
EGOVEM Program Committee ..................................................................................... xxi
NLPOE Program Committee ......................................................................................... xxii
EADA Program Committee ........................................................................................... xxiii

The Third International Workshop on Data Oriented Constructive Mining and the Seventh International Workshop on Emergent Intelligence
Networked Agents (DOCMAS/WEIN)

Analysis of User Behavior on Private Chat System .......................................................... 1
  Fujio Toriumi, Takafumi Nakanishi, Mitsuteru Tashiro, and Kiyotaka Eguchi

Machine-Learned Ranking Based Non-Task-Oriented Dialogue Agent Using Twitter Data .......................................................... 5
  Makoto Koshinda, Michimasa Inaba, and Kenichi Takahashi

Mining Opinion Words and Targets from Online Reviews in a Hybrid Framework ............ 9
  Hui Zhang, Qiyun Zhao, Hao Wang, Chen Zhang, and Fanjiang Xu

GenderPredictor: A Method to Predict Gender of Customers from E-commerce Website .......................................................... 13
  Siyu Lu, Meng Zhao, Hui Zhang, Chen Zhang, Wei Wang, and Hao Wang
Mining User Experience through Crowdsourcing: A Property Search Behavior Corpus Derived from Microblogging Timelines ......................................................................................................................... 17

Yoji Kiyota, Yasuyuki Nirei, Kosuke Shinoda, Satoshi Kurihara, and Hirohiko Suwa

Roadmap for Multiagent Social Simulation on HPC ............................................................................................................................... 22

Itsuki Noda, Nobayasu Ito, Kiyoshi Izumi, Tomohisa Yamashita, Hideki Mizuta, Tomio Kamada, Yohsuke Murase, Sachiko Yoshihama, and Hiromitsu Hattori

Indoor/Outdoor Mobile Navigation via Knowledge-Based POI Discovery in Augmented Reality ................................................................. 26

Michele Ruta, Floriano Scioscia, Saverio Ieva, Danilo De Filippis, and Eugenio Di Sciascio

How Do Newcomers Blend into a Group?: Study on a Social Network Game .................................................................................................. 31

Masanori Takano, Kazuya Wada, and Ichiro Fukuda

International Workshop on Complex Methods for Data and Web Mining (CMDWM)

A Multi-regional CGE Model and Its Application in Low Carbon Policy Simulation in China ................................................................. 36

Yongna Yuan, Li Na, and Minjun Shi

Smoothing Trust Region for Digital Image Restoration ............................................................................................................................... 40

Ruizhi Zhou, Lingfeng Niu, and Zhiquan Qi

Prediction of Sequential Static Input-Output Table ................................................................................................................................. 44

Wen Long and Huiwen Wang

An Approach to Identify SPAM Tweets Based on Metadata .................................................................................................................... 48

Martin Häeusl, Johannes Forster, and Daniel Kailer

Analysis on Marketing Ability and Financial Performance in Internet Company ........................................................................................ 52

Zhuofan Yang and Yong Shi

Linear Twin SVM for Learning from Label Proportions ............................................................................................................................ 56

Bo Wang, Zhensong Chen, and Zhiquan Qi

f-Fractional Bit Minwise Hashing for Large-Scale Learning ................................................................................................................... 60

Jingjing Tang and Yingjie Tian

Blog, Forum or Newspaper? Web Genre Detection Using SVMs .................................................................................................................. 64

Philipp Berger, Patrick Hennig, Martin Schoenberg, and Christoph Meinel

WOC: A New Weighted Ordinal Classification ........................................................................................................................................ 69

Markus Zeindl and Christian Facchi

A Content-Based Knowledge and Data Intensive System for Archaeological Motif Recognition ................................................................. 76

Lin Shu-Yu, Man-Fong Cheng, Ray-I Chang, Chao-Lung Ting, Yu-Chun Wang, and Jan-Ming Ho

The Fourth International Workshop on Web Personalization, Recommender Systems and Social Media (WPRSM)

Spoilers Ahead — Personalized Web Filtering ................................................................................................................................................. 80

Pascal Bissig, Philipp Brandes, Roger Wattenhofer, and Roman Willi

Unifying Geographical Influence in Recommender Systems via Matrix Factorization .................................................................................. 84

Ce Cheng, Jiajin Huang, and Ning Zhong
A Study of Drug Interaction for Personalised Decision Support in Dental Clinics ................................................................. 88
WeePheng Goh, Xiaohui Tao, Ji Zhang, and Jianming Yong

Data-Driven Semantic Concept Analysis for User Profile Learning in 3G Recommender Systems ................................................................. 92
Vladimir Gorodetsky and Olga Tushkanova

Effective 20 Newsgroups Dataset Cleaning ......................................................................................................................... 98
Khaled Albishre, Mubarak Albathan, and Yuefeng Li

An Intelligent Recommender System Based on Short-Term Risk Prediction for Heart Disease Patients .......................................................... 102
Raid Lafta, Ji Zhang, Xiaohui Tao, Yan Li, and Vincent S. Tseng

Contextually Intelligent Recommendation of Documents from User-Subscribed Channels .............................................................. 106
Ishan Verma and Lipika Dey

The International Workshop on Knowledge Management of Web Social Media (KMWSM)

Effects of Audience Characteristics and Sources of Information on Perceived Credibility of Web Information ................................................................. 110
Ching-Pi Chuang

Mining Topical Relevant Patterns for Multi-document Summarization ................................................................................................. 114
Yutong Wu, Yang Gao, Yuefeng Li, Yue Xu, and Meihua Chen

Explore the Development of WeChat Payment from User Behavior ................................................................................................. 118
Wei Huang and Jialian Tang

Using Event Identification Algorithm (EIA) to Improve Microblog Retrieval Effectiveness ................................................................. 122
Sukjin You, Wei Huang, and Xiangming Mu

It Does Matter Who I sell to and Whom I Buy From: Weighted Bilateral VCG ................................................................................................. 126
Esther David and Rina Azoulay

Handling Inconsistent Closed Predicates: A Paraconsistent Approach ................................................................................................. 130
Badrinath Jayakumar and Rajshekhar Sunderraman

Leveraging Zero Tail in Neighbourhood for Link Prediction ..................................................................................................................... 135
Andrea Chiancone, Valentina Franzoni, Yuanxi Li, Krassimir Markov, and Alfredo Milani

The Sixth International Workshop on Intelligent E-government and Emergency Management (EGOVEM)

Survey of Application and Research on Government Cloud Computing In China ................................................................................................. 140
Wang Ning, Xie Xiaoshan, Li Hui, Wang Xuehua, and Qin Xuechi

Research on Scenario Deduction of Unconventional Emergency Based on Knowledge-Unit ................................................................................................. 144
Yanzhang Wang and Lei Zhang

Research of Resources Allocation Model in Emergency Decision of Incidents ................................................................................................. 148
Huaiming Li and WenHui Chai

A Knowledge Element Based Model Integration Method for Emergency Management ................................................................................................. 152
Xuelong Chen and Yali Wang
Multidimensional Intelligence Presentation Based on Knowledge Element Fusion ..........................................................156

Lin Sun and Yanzhang Wang

Study on the Collaborative Pattern among Agents of Emergency DSS for the Response of Unconventional Emergency in China ..................................................................................................................160

Xin Ye, Yanxin Cui, Sihao Liu, and Wenyuan Zhou

Orders Flows Forecasting by Intermediary Service Provider .........................................................................................164

Anton Ivaschenko and Ilya Syusin

The Eighth International Workshop on Natural Language Processing on Ontology Engineering (NLPOE)

The Construction of a Kind of Chat Corpus in Chinese Word Segmentation .................................................................168

Xia Yang, Peng Jin, and Xingyuan Chen

Chinese Spelling Errors Detection Based on CSLM ........................................................................................................173

Zhaoyi Guo, Xingyuan Chen, Peng Jin, and Si-Yuan Jing

Quantitative Study of Preposition Based on Large-Scale Corpus ..................................................................................177

Zhimin Wang, Wei He, and Pierangelo Lacasella

Towards a Word Similarity Analysis of Chinese Noun Compounds ...............................................................................181

Lulu Wang, Meng Wang, and Na Tian

A Psycho-Lexical Approach to the Assessment of Information Quality on Wikipedia ......................................................184

Qi Su and Pengyu Liu

Comparing Argument Structure in Chinese Verb Taxonomy and Chinese Propbank .........................................................188

Xiaopeng Bai and Bin Li

Extracting Food Names from Food Reviews ..................................................................................................................191

Ge Xu and Likun Qiu

Semantic Structures of Chinese Disyllable New Words ..................................................................................................195

Xiaodie Zhang, Shiyong Kang, and Baorong He

Subject-Keyphrase Extraction Based on Definition-Use Chain .....................................................................................199

Hung-Min Hsu, Ray-I Chang, Yu-Jung Chang, Shu-Yu Lin, You-Jyun Wang, and Jan-Ming Ho

The International Workshop on Ensemble of Anomaly Detection Algorithms (EADA)

Video Anomaly Detection using Selective Spatio-Temporal Interest Points and Convolutional Sparse Coding ..................203

Rudy Cahyadi HP and Junaidillah Fadil

Anomaly Detection Ensembles: In Defense of the Average ..............................................................................................207

Alvin Chiang and Yi-Ren Yeh

A Clock Skew Replication Attack Detection Approach Utilizing the Resolution of System Time ....................................211

Komang Oka Saputra, Wei-Chung Teng, and Yi-Hao Chu

On Contextual Binding and Its Application in Cyber Deception Detection ........................................................................215

Jim Q. Chen
A Fraud Detection Model Based on Feature Selection and Undersampling Applied to Web Payment Systems .................................................................219
    Rafael Franca Lima and Adriano Cesar Machado Pereira

**WI-IAT 2015 Poster Papers**

Modelling Composite Emotions in Affective Agents .............................................223
    Xinjia Yu, Chunyan Miao, Cyril Leung, and Charles Thomas Salmon
Towards Integrating Ontologies in Multi-agent Programming Platforms ...................225
    Artur Freitas, Rafael H. Bordini, Felipe Meneguzzi, and Renata Vieira
Cooperative Network of Mobile Agents to Remotely Process User Information Requests .................................................................227
    Roberto Yus and Eduardo Mena
Organic vs. Sponsored Content: From Ads to Native Ads ........................................229
    Soumyava Das, Akshay Soni, Ashok Venkatesan, and Debora Donato
E-BACH: Entropy-Based Clustering Hierarchy for Wireless Sensor Networks ................231
    Petr Musilek, Pavel Krömer, and Tomáš Bartoš
Interactive Dynamic Influence Diagrams for Relational Agents ..................................233
    Yinghui Pan, Yingke Chen, Jing Tang, and Yifeng Zeng

**WI-IAT 2015 Demo Papers**

An Agent-Based Game Platform for Exercising People’s Prospective Memory ...............235
    Han Lin, Jinghua Hou, Han Yu, Zhiqi Shen, and Chunyan Miao
Agent Augmented Inter-Generational Crowdsourcing .............................................237
    Zhengxiang Pan, Chunyan Miao, Benny Toh Hsiang Tan, Han Yu, and Cyril Leung
Contextual Topic Model Based Image Recommendation System ...............................239
    Lei Liu
Silver Assistants for Aging-in-Place .................................................................241
    Di Wang, Budhitama Subagdja, Yilin Kang, and Ah-Hwee Tan
MyLife: An Online Personal Memory Album .........................................................243
    Di Wang and Ah-Hwee Tan
Classify: Classification of Experts by Their Expertise on the Fly ..............................245
    Gan Keng Hoon, Gan Kian Min, Oscar Wong, Ooi Bong Pin, and Chan Ying Sheng
MYSTREAM: An in Browser Personalization Service to Follow Events from Twitter ..........247
    Antoine Boutet, Frederique Laforest, Stephane Frenot, and Damien Reimert
Alignment of Configuration and Documentation for Highly Engineered Complex Product Configuration Systems: A Demonstration from a Case Study .................................................................249
    Sara Shafiee, Katrin Kristjansdottir, and Lars Hvam
NewsOpinionSummarizer: A Visualization and Predictive System for Opinion Pieces in Online News ........................................................................251
    M. Atif Qureshi, Arjumand Younus, Josephine Griffith, Colm O’Riordan, Gabriella Pasi,
    and Youssef Meguebi
A Clock Skew Replication Attack Detection Approach Utilizing the Resolution of System Time

Komang Oka Saputra*, Wei-Chung Teng†, and Yi-Hao Chu*

*Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology, Taipei 106, Taiwan
†Department of Electrical and Computer Engineering, Udayana University, Bali 80361, Indonesia
Email: okasaputra@ee.unud.ac.id, weichung@csie.ntust.edu.tw, M10215046@mail.ntust.edu.tw

Abstract—The clock skew, or the physical ticking rate difference between two digital clocks, has been revealed to have potential on serving as the device fingerprint for identification/authentication purpose. However, it remains as an open issue to detect clock skew replication behavior, which is realized by sending altered timestamps. In this study, it is confirmed that an attacker may fake any target skew with the error being no more than 1ppm in local network environments. Besides, it is also observed that the value of fake timestamps are affected by the time resolution of the attacker’s system clock. When the resolution is 1 ms or lower, a relatively large jump between consecutive offsets happens regularly, and the scale of each jump is theoretically the very time resolution of the attacker’s system clock. This characteristic is thus adopted to develop a filtering method such that the receiver is able to detect fake timestamps. When the periodical jumps are detected, the filter module abandons these jumps to recover the original clock skew. Experimental results on 15.6 ms and 1 ms time resolutions show that the developed method is effective to detect skew replication attacks, and the errors of the recovered clock skews are no more than 1ppm from the real skews of the attackers.

Index Terms—clock skew; replication attack; time resolution

I. INTRODUCTION

One of the essential supporting technologies for the upcoming Internet of Things era is identifying connected devices for services with security concerns. Apart from the cryptographic means, identifiable information like IP address, MAC address, and cookies are vulnerable to replication attack. Alternatively, a physical amount called clock skew is revealed to be unique to each device in parts per million (ppm) or higher precision and is thus appropriate to be used in device fingerprinting [1]–[3]. The skew of a digital clock is the frequency difference between the clock and true time, and the clock skew of a device to the measurer is the relative clock skew of the device. In this paper, only relative clock skew is discussed.

Although it is hard to alter the ticking rate of a digital clock, it is intuitive to fake a clock skew by slightly adjusting each timestamp such that the monotone-increasing time sequence proceeds in a stable yet different speed. Huang and Teng proposed a method to detect fake timestamps by asking the sender to change the sending period frequently [4]. However, their approach is limited to one-hop communications in wireless sensor networks (WSN) where the transmission delay variation is usually negligible. In a general, multi-hop network, the packet delay variation makes it much harder to determine if the received timestamps are origin ones or not.

In this research, a method is developed to help distinguish the fake clock skews from the real ones. This method utilizes the restriction that the timestamps have to proceed in unit of the system time resolution. According to this restriction, there exists error between the forged time and the target to fake in each timestamp, and the error accumulate as time passes. The sender, or the attacker, has to compensate the errors when the accumulated values become greater than the time resolution, and this behavior causes a periodical jump between consecutive timestamps. Since the scales of the jumps are theoretically the resolution of the attacker’s system clock, we can use this characteristic to develop a filtering method for the measurer to detect the fake timestamps.

In the following sections, we first demonstrate how an attacker can forge any clock skew by manipulating their timestamps to match the target skew. It is than explained in detail how to detect altered timestamps by detecting regular jumps when the system time resolution of the attacker be 1 ms or lower. Finally, experiments are conducted to verify that the proposed method is effective. The results also show that the recovered clock skews from the faked timestamps are very close (no more than ±1 ppm error) to the attacker’s origin clock skews.

II. HOW TO FAKE A CLOCK SKEW

To measure the relative clock skew of a device over network, the measurer M at first collects the timestamps from the target device T. For each received timestamp, an offset is calculated by subtracting the receiving time from the sending time of the packet. Fig. 1 shows the offsets collected in one measurement where the x-axis is the measurer’s elapsed time after receiving the first packet, and the y-axis is offset in unit of microsecond. Each blue circle represents one offset, and consecutive offsets are connected by blue lines. It is obvious that the lower bound of the offset set shapes in a strict line, and the slope of this line is the clock skew of the device. There are many sophisticated approaches [5]–[7] to derive the slope besides linear regression.
A. Timestamps and the Sending Interval

Now assume that the attacker $A$ knows the clock skew of $T$ to $A$: $s_{TA}$, and $A$ wants to replicate the clock skew of $T$ to cheat $M$. Every time one second passed in $A$, $1 + s_{AM}$ second passed in $M$. To make $M$ get $1 + s_{TM}$ instead of $1 + s_{AM}$, $A$ has to multiply the rate $r$ to the timestamps where

$$r = \frac{1 + s_{TM}}{1 + s_{AM}}$$

Let $t_1$ stands for the first timestamp, or the sending time of the first packet, then the $i$th altered timestamp $t'_i$ should be

$$t'_i = t_1 + r(t_i - t_1).$$

If $A$ does not know the value of $s_{AM}$, $A$ can approximate it by the following equation:

$$1 + s_{TM} = (1 + s_{TA})(1 + s_{AM}) \approx 1 + s_{TA} + s_{AM},$$

or $s_{AM} \approx s_{TM} - s_{TA}$. Since the absolute values of the clock skews rarely exceed 200 ppm [7], the productions of two clock skews are negligible here.

The weakness of this approach is that $M$ can easily defend from this attack by asking a fixed sending period $\Delta t$. Since the difference between two consecutive timestamps $t_i$ and $t_{i+1}$ has to be $\Delta t$, $A$ cannot modify the value of $t_{i+1}$ without being detected anymore. The alternative way to fake the clock skew is to change the sending period to $r^{-1}\Delta t$.

For example, assume the attacker $A$ knows that $s_{TM}$ is 20 ppm and $s_{AM}$ is 200 ppm, and the measurer $M$ asks for 1 second sending period. It is clear that $A$’s clock ticks faster than $T$’s clock, which is still slightly faster than $M$’s clock. To fake $s_{TM}$, $A$ sends out timestamps but keep the difference between any two consecutive values 1 second. However, the real sending interval in $A$’s time axis is $1 \cdot (1 + 200 \cdot 10^{-6})/(1 + 20 \cdot 10^{-6}) \approx 1.00018$ seconds.

B. The System Time Resolution Limitation

Due to the computer system design, the above mentioned sending interval has to be in unit of system time resolution. This resolution is determined by the type of operating systems. For instance, it is 1 µs in Linux and Android systems, and the default time resolution in recent Microsoft Windows systems is 15.6 ms. However, users of Windows systems may change the time resolution to up to 1 ms via system calls.

Let $k$ denotes the system time resolution of $A$. If a process is programed to sleep for $\Delta t$ seconds to get the next timestamp, the real sleeping time will be $\left[\frac{\Delta t}{k}\right] \cdot k$ seconds. For the sake of simplicity, we assume that $k$ divides $\Delta t$. Similarly, when $A$ set the sending period to $r^{-1}\Delta t$ seconds, the real sending period becomes $\left[\frac{r^{-1}\Delta t}{k}\right] \cdot k$ second, though the fake timestamp only increase $\Delta t$ seconds each time. The error $e = r^{-1}\Delta t \mod k$ might be tiny, but it accumulates and will eventually affect the estimated clock skew. To compensate this issue, $A$ needs to decrease one tick for every $\left[\frac{1}{e}\right]$ rounds.

The following formula summarizes the real sending interval and the fake timestamps of $A$:

$$t_{i+1} = \begin{cases} 
  t_i + \left[\frac{r^{-1}\Delta t}{k}\right] \cdot k & \text{if } \left[\frac{1}{e}\right] \cdot i \\
  t_i + \left[\frac{r^{-1}\Delta t}{k}\right] \cdot k & \text{otherwise}
\end{cases} \quad (1)

$$

$$t'_{i+1} = t'_i + \Delta t \quad (2)$$

III. PROPOSED METHOD TO DETECTING CLOCK SKEW REPLICATION ATTACK

According to (1) and (2), there exists a pattern on the timestamps collection at $M$ due to the one tick difference of scale $k$. Since the offsets on the scatter diagram represent "$M$’s timestamp - $A$’s timestamp", the lessened tick with magnitude of $k$ on $A$’s timestamp will cause the offset jump up or down $k$. Catching a glimpse on the scatter diagram, the effect by $k$ is not obvious there are also similar jumps that are caused by transmission delay. However, since $A$ has to reduce tick into the timestamps on a fixed interval to make a stable skew, $M$ can spot regular jumps which are totally different comparing with random outliers.

By detecting the time $A$ having attack that is indicated by the occurrence of jumps on the scatter diagram, $M$ can separate $A$’s real timestamps from the timestamps that is addressed for replicating $T$’s skew. Hence, $M$ can recover $A$’s clock skew, and therefore, $M$ can thwart $A$’s attack to keep the system save. The detail of the clock skew replication attack filter can be found in Algorithm 1. Some parameters used in this algorithm are: $O$ is set of all offsets between $A$ and $M$; $m$ is the threshold set for the maximum offset, or the clock resolution used; LargerDelay is used to store index of the offset-set that is higher than $m$; JumpPoint is used to store index of the offset-set that is categorized as the position the attack occurs; meanwhile $idx$ is index for the LargerDelay and JumpPoint. From lines 3 to 6, Algorithm 1 records into LargerDelay matrix the position in which $A$ is indicated to do attack. Since LargerDelay can be full filed by the position of $A$’s attack and also outliers, Algorithm 1 then separating the
Algorithm 1 Clock skew replication attack filter

Require: \( O, m \)

1: LargerDelay = null
2: JumpPoint = null
3: for \( i = 1; i \leq O\.length; i + + \) do
4:  if \( \text{The Absolute value of} \ (O_{i+1} - O_i) \geq m \) then
5:     Recording \((i + 1)\) to LargerDelay
6:  end if
7: end for
8: for all idx ∈ LargerDelay do
9:     Finding each continuous \( idx \) and then grouping them as \([\text{first idx}, \text{last idx}]\)
10:    if \( \text{first idx} == \text{last idx} \) then
11:       Recording \( idx \) to JumpPoint
12:    end if
13: end for
14: for all idx ∈ JumpPoint do
15:     \( O_{\text{temp}} = O_{idx} - O_{idx-1} \)
16:     for \( j = idx; j \leq \text{JumpPoint\.length}; j + + \) do
17:       \( O_j = O_j - O_{\text{temp}} \)
18:     end for
19: end for

The position of A’s attack indicated by a non-consecutive index in LargerDelay, in which the result is stored to JumpPoint matrix (Lines 8 to 13). Finally, code from line 14 to 19 rebuilds \( O \) by removing the effect of A’s attack. Since now \( O \) no longer contains the timestamps manipulation effect by A, when we estimating the clock skew of \( O \), the result will be just the clock skew of A to M. Therefore, M can identify that A trying to obtain an illegal access to M.

IV. Evaluation Results

Two kinds of experiments are conducted to evaluated the proposed method. A notebook with dual operating systems, Ubuntu 14.04 and Windows 7, was used as A; And a PC with Ubuntu 14.04 operating system plays the role of M.

A. Experiments of Clock Skew Replication

At first, we evaluated the clock skew replication attack method on the 15.6 ms clock resolution. We set the attacker in Windows operating system with default 15.6 ms clock resolution. As the based of the evaluation, Fig. 1 shows the scatter diagram of offsets with the original clock skew \( s_{\text{AM}} \). The red line in Fig. 1 is obtained by running the linear programming algorithm [5]. The slope of this line, or the clock skew, is -15.5 ppm.

Three skew values: -215.5 ppm, -35.5 ppm, and -18.5 ppm are the target to be replicated. To reach these targets, on each attack, the attacker has to increase its speed in the amount of 200 ppm, 20 ppm, and 3 ppm respectively. As an example, Fig. 2 shows the scatter diagram offsets that are obtained when the attacker tried to fake the -215.5 ppm skew target. The measured clock skew in this attack is -215.79 ppm.

From Fig. 2 we can also observe that the densest part of the offsets on the scatter diagram is broken up due to the presence of jump points. Furthermore, we found that the magnitude of each jump is nearly 15.6 ms, or it is close to the value of the clock resolution used by the attacker.

Similarly, we repeated experiments in 1 ms time resolution. Fig. 3 shows the result when A tries to imitate the -215.5 ppm skew. An accurate replication attack is observed with only 0.67 ppm error.

Table I details the results of all the above experiments. Some notations used here are: W for Windows, L for Ubuntu 14.04, 15m for the 15 ms time resolution used by the attacker, 1m for the 1 ms, \( 1\mu \) for the 1 \( \mu\)s, 200p for the condition when attacker trying to add 200 ppm in its original skew, 20p when the attacker trying to add 20 ppm, and 3p when the attacker
trying to add 3 ppm. It is obvious from Table I that even when the notebook attacker using Windows (1 ms resolution) or Linux (1 µs resolution), its replication attacks are finish with accurate results (all the errors are lower than 1 ppm).

The period the jump point occurs on 15.6 ms and 1 ms resolutions are different. By observing Figs. 4 and 5 more detail, we can find that the jump point occurs every 78 seconds and 5 seconds for the 15.6 ms and 1 ms resolutions respectively. The longer the measurement the more the jump point will occur. Hence, to obtain information about the relation between the number of jump point with the skew to be faked, we tried to arrange the length of the measurement, from 30 seconds into maximum 1000 seconds, and to try any possible skew values to be imitated.

### B. Experiments of Filtering the Replication Attack

As the jump point phenomenon only occurs on Windows with millisecond clock resolutions, we evaluated the proposed clock skew replication filter only for the 15.6 ms and 1 ms clock resolutions. With similar notations as used in Table I, Table II summarizes all the filtering results. On all the experiment combinations, the clock skew replication filter only for the 15.6 ms and 1 ms resolutions, we evaluated the proposed method. Although the proposed method may become ineffective to devices with 1 µs or higher resolutions, it provides a hint on designing clock skew measuring scheme.

### ACKNOWLEDGMENT

This work was supported by the Ministry of Science and Technology under Grant MOST 104–2923–E-011-005-MY3 and MOST 104–2221–E-011-070.

### REFERENCES


