Intelligent Automation And Soft Computing, 2019
Copyright © 2019, TSI® Press
Vol.25,no.1, 217–228

# Active Detecting DDoS Attack Approach Based on Entropy Measurement for the Next Generation Instant Messaging App on Smartphones

**Hsing-Chung Chen[1,2], Shyi-Shiun Kuo[1,3]**

[1] Department of Computer Science and Information Engineering, Asia University, No. 500, Lioufeng Rd., Wufeng Dist., Taichung City, Taiwan
[2] Dept. of Medical Research, China Medical University Hospital, China Medical University, Taichung City, Taiwan
[3] Dept. of Multimedia Animation and Application, Nan Kai University of Technology, No. 568, Zhongzheng Rd., Caotun Township, Nantou County, Taiwan

**ABSTRACT**
Nowadays, more and more smartphones communicate to each other's by using some popular Next Generation Instant Messaging (NGIM) applications (Apps) which are based on the blockchain (BC) technologies, such as XChat, via IPv4/IPv6 dual stack network environments. Owing to XChat addresses are soon to be implemented as stealth addresses, any DoS attack activated form malicious XChat node will be treated as a kind of DDoS attack. Therefore, the huge NGIM usages with stealth addresses in IPv4/IPv6 dual stack mobile networks, mobile devices will suffer the Distributed Denial of Service (DDoS) attack from Internet. The probing method is deployed in this paper by using the active ICMP (Internet Control Message Protocol) protocol. Thus, the aim of this paper is to provide the active approach based on the integrated entropy calculations for the NGIM traffics, the numbers of IPv4 and IPv6 addresses of the abnormal events found and counted after active inquiring ICMP procedure. However, many DDoS attacks in Internet were found to paralyze NGIM Apps on smartphones. It is a lightweight approach could be applied in mobile device.

**KEY WORDS**: Blockchain, DDoS Attack, Entropy, Instant Messaging, XChat.

## 1 INTRODUCTION

NOWADAYS, popular smartphones increasingly communication by using Next Generation Instant Messaging (NGIM) applications (Apps) via IPv4/IPv6 dual stack network environments. In fact, the simpler network architecture for native IPv6 traffic in mobile networks translates into better performance (Chen, 2016; Chen el al., 2016; Zhangsk, 2012). More and more mobile networks around the world switch to this IPv6-only deployment model plus using DNS64 (IPv6 to IPv4 Domain Name System) plus NAT64 (IPv6 to IPv4 Network Address Translation) for access to legacy IPv4-only content. With an IPv6-only deployment model, only requests to IPv4-only content need to go through NAT64 servers while access to dual-stacked content could proceed directly to the Internet without any need for address translation.

In IPv6-only mobile networks, IPv6 traffic has direct access to the Internet while IPv4 traffic has its access mediated through a NAT (Network Address Translation). These NATs add latency and can be bottlenecks as they could be expensive for Internet Service Providers (ISPs) to deploy enough capacity to keep up with demand (Bass et al., 1998). At present, one of the top usages applications (Apps) is Instant Messaging Chat (IMC) App, such as WeChat, WhatsApp, LINE, and Facebook Messenger, etc. (Statista, 2016; Chen et al., 2016; Li et al., 2017; Lim, 2016; Wang et al., 2017). It has become one of life's necessary communication services for smartphones' users. There's a new decentralized chat App that uses Bitcoin's blockchain (BC) technology, e.g. XChat (Coinbuzz, 2017). It's labeled as a "next generation instant messaging App" with industry-leading privacy and security features. XChat is part of the XCurrency platform, which is founded on the Xnode communication protocol (Coinbuzz, 2017). In the further IPv4/IPv6 dual stack mobile networks based on the blockchain technologies, each mobile device, e.g. smartphone, assigned a public address could

CONTACT Hsing-Chung Chen ✉ shin8409@ms6.hinet.net, cdma2000@asia.edu.tw

communicate to each other's by using some popular Next Generation Instant Messaging (NGIM) applications (Apps), e.g. XChat. Owing to XChat addresses are soon to be implemented as "stealth addresses", any DoS attack activated form malicious XChat node will be treated as a kind of DDoS attack. Additionally, the huge NGIM usages with stealth addresses for the XChat nodes which each node will be assigned a public address in IPv4/IPv6 dual stack mobile networks, mobile devices will suffer the DDoS attacks from Internet or become a node in botnet.

R. Wang, et al. (2015) proposed an entropy-based distributed DDoS detection mechanism in software-defined networking (SDN). X. T. Wang, et al. (2015) proposed a DDoS attack detection algorithm based on an IP entropy model. Their scheme proposed a DDoS attack detection algorithm based on an IP entropy model through the establishment of a destination IP entropy model, setting the flow and entropy threshold with membership function, and checking the progressive conditions of DDoS attacks. Niyaz, et al. (2016) also proposed a deep learning based DDoS detection system in SDN. In addition, Han, et al. (2016) proposed a response to DDoS architecture within a smartphone environment in 2016.

These proposed entropy-based distributed DDoS detection mechanisms (Han et al., 2016; Niyaz et al., 2016; R. Wang et al., 2015; X. T. Wang et al., 2015) mentioned above provide only the passive approaches in order to detecting malicious traffics for server-based applications. However, they did not propose any active detection approach for abnormal traffics, which the approach can detect the abnormal traffics via analyzing the RTT and RTO results inquiring their IP addresses from abnormal traffics by using ICMP (Internet Control Message Protocol) command(s) based on IPv4/IPv6 dual stack. Therefore, the method of inquiring and analyzing the traffics of RTT and RTO to active detect DDoS traffics is adopted in this study. The inquiring results of finding the abnormal RTT and RTO events are counted as the numbers of IPv4 and IPv6 addresses in the abnormal traffics, individually. Because of this study focus on Instant messaging App on smartphones, the active detecting DDoS attack approach based on entropy measurement for the instant messaging App on smartphones is proposed in this article. It is based on the entropy measurement in order to detect the DDoS attacks on smartphones. Both parameters RTT and RTO in the ICMP protocol are employed in this paper. It could instantly react whether traffics were attacked or not. Through entropy computing, the cost value defined in this paper could be immediately obtained.

The remainder of this paper is organized as follows: Section 2 describes NGIM App, RTT, RTO and entropy operation in related works. Section 3 presents the preliminary definitions of entropy operations for the packet traffics measured from these NGIM chat Apps. In Section 4, the new active approach for detecting a DDoS attack based on the integrated entropy calculations of the NGIM in smartphones, and describe how to calculate the evaluated value of risk information of the NGIM in smartphones. Two cases and discussions are given In Section 5. Finally, our conclusions are drawn in Section 5.

## 2 RELATED WORKS

IN this section, the next generation instant messaging (NGIM) App is addressed in Subsection 2.1. The basic measurement definitions for Round Trip Time (RTT) and Retransmission Timeout (RTO) are illustrated in Subsection 2.2. Finally, the entropy operations is described in Subsection 2.3.

### *2.1 NGIM Apps*

IMC App becomes very important that online chat and instant messages delivering. It is quite different from other traditional technologies, such as email, on the perceived synchrony of the communication actions by the users. There's a new decentralized chat application that uses Bitcoin's blockchain technology, e.g. XChat (Coinbuzz, 2017). It's labeled as a "next generation instant messaging App" with industry-leading privacy and security features. XChat is part of the XCurrency (XC) platform, which is founded on the Xnode communication protocol. The entirely peer-to-peer messaging application relies on no centralized servers whatever and offers end-to-end AES-256 encryption. Therefore, it is nearly impossible to decipher the delivered messages. XChat communication is encrypted from end to end with AES-256 so that no third party could decipher the transmitted message. XChat makes it computationally infeasible for anyone to snoop on messages, in this way privacy is assured (Coinbuzz, 2017).

Moreover, for anyone who does not want to reveal their location, XChat could be executed from the XC TOR Stick. It could incorporate a TOR node that obfuscates your IP address. In addition, the TOR Stick performs inside the TOR network so that it does not use exit nodes. This implies that packet sniffer tools are useless against XChat App as there are no incoming and outgoing packets to be matched. Even if a message is sent to a recipient outside TOR, the message originates inside the network and so there is only an outgoing packet, again flouting packet sniffers. By this way, XChat avoids common vulnerabilities of TOR. If this is not enough, soon XC will add yet another layer of privacy. XChat addresses are soon to be implemented as "stealth addresses". Someone could send a payment to an XC address, but it will be received on a different address that not even the sender knows. As such, one can publicly display XChat address as a kind of cryptographic "business card" for both payments and messages, without any link to its existing on the blockchain (Coinbuzz, 2017). Thus, owing to XChat addresses are soon to be implemented as “stealth addresses”, any DoS attack to smartphone will be treat as a kind of DDoS attack.

### 2.2 RTT and RTO

In this subsection, the RTT and RTO will be described as below. RTT is the time required for an IPv4 or IPv6 packet to travel from a specific source IPv4 or IPv6 address to a specific destination IPv4 or IPv6 address and back again (Zhangsk, 2012). Typically, RTT is divided into three parts: propagation delay, processing delay and queuing delay (Bass, 1998). The first parts of the values for a Transmission Control Protocol (TCP) connection is the fixed opposite. The router cache queues and the processing time for the entire IPv4 or IPv6 address network congestion is dependent the amount of congestion events. Therefore, the RTT will change in a degree as it reacts to the IPv4 and IPv6 network congestions, individually. RTT measurements can be used in two ways: TCP Timestamp option and the retransmission queue control block TCP data packets. The recorded timestamp is the packet flow when sending out of time. It can easily get a measurement of the RTT. To recognize the received current time and sent times, it can be easily used to get a measurement value of the RTT. In the TCP retransmission, the queue saves the sent data packets, but unacknowledged data. In general, the TCP will use Karn’s algorithm (Zhangsk, 2012) for taking the RTT samples. That is, the RTT samples must not be made using segments that were retransmitted, and thus, for which it is ambiguous, whether the reply was for the first instance of the IPv4 or IPv6 packet or a later instance. The only case is when the TCP is able to safely take the RTT samples from retransmitted segments while the TCP timestamp option is employed, since the timestamp option removes the ambiguity regarding which instance of the data segment triggered the acknowledgement. The TCP of retransmission and timeout are very important for obtaining the connected RTT measurements. Because the IPv4 or IPv6 network traffic is changing, the retransmission time for IPv4 or IPv6 packets will also change. The TCP needs to follow these changes and dynamically adjust the timeout of the timed RTO. The RTO is described in RFC2988, the TCP uses a retransmission timer to ensure data delivery and in the absence of any feedback from the remote data receiver, the duration of this timer is referred to as the RTO.

### 2.3 Entropy Operation

Entropy is the method which could be used to measure the uncertainty or randomness for a random variable. The entropy operation (Astronomy, 2012) could explicitly be written as the equation (1).

$$H(X) = \sum_i P(x_i) I(x_i) = -\sum_i P(x_i) \log_b P(x_i) \quad (1)$$

where $b \in \{2, e, 10\}$ is the base of the logarithm used.

## 3 PRELIMINARY

IN this paper, once the situation is satisfy for huge traffic on the NGIM are detected in smartphones, the entropy measurement method is activated to measure the traffics behavior of the RTT and RTO by adopting the ICMP commend as 'ping -4 –t –l $n_4$ ' and 'ping -6 –t –l $n_6$ ' with large size packets, where $0 \le n_4 \le 65500$ and $0 \le n_6 \le 65500$ . Therefore, the preliminary definitions of entropy operations will be described in this subsection for the IPv4 and IPv6 messages flows’ traffics measured from these NGIM chat Apps, e.g. XChat, together with the numbers of IPv4 and IPv6 addresses which the abnormal events of the RTT and RTO are found and counted after active inquiring ICMP commands with appropriate and flexible packet-sizes.

Assume that denote $S_i = \{S_{n_{NGIM},y}, S_{n_{a\_RTT},y}, S_{n_{a\_RTO},y}\}$ $= \{S_1, S_2, S_3\}$ as the set of the observed traffics, where $S_1$, $S_2$ and $S_3$ represents NGIM traffics, the numbers of IPv4 and IPv6 addresses counted by the abnormal events of RTT and RTO during a time period, individually. Each observed traffic $S_i = \{S_{n_{NGIM},y}, S_{n_{a\_RTT},y}, S_{n_{a\_RTO},y}\}$ $= \{S_1, S_2, S_3\}$ will be monitored in a smartphone, respectively. The count number of the traffics or the numbers of IPv4 and IPv6 addresses of $S_i$ is observed and represented during the time interval t as follows.

$$N_i(t), \ i=1, 2, 3.$$

Furthermore, $f_i(\Delta t)$ is denoted as the differential value for the observed traffics or the numbers of IPv4 and IPv6 addresses $S_i$ in a measuring time interval $\Delta t$ , that is,

$$f_i(\Delta t) = \left| N_i(t) - N_i(t + \Delta t) \right|, \ i=1, 2, 3.$$

The probability of the differential value of the observed traffics or the numbers of IPv4 and IPv6 addresses $S_i$ could be defined as the equation (2).

$$p_i(\Delta t) = \frac{f_i(\Delta t)}{\sum_i f_i(\Delta t)}, \ i=1, 2, 3. \quad (2)$$

Let $Z$ be the random variable of the number of the observed traffic or the numbers of IPv4 and IPv6 addresses $S_i$ in the smartphone. Therefore, the entropy of the differential value of the observed traffics or the numbers of IPv4 and IPv6 addresses for the smartphone could be defined as the equation (3).

$$H(Z) = -\sum_i p_i(\Delta t)\log p_i(\Delta t) \qquad (3)$$

## 4 ACTIVE CALCULATION ENTROPY PREVENTION AGAINST DDOS ATTACK FOR NGIM ON SMARTPHONE

IN this section, the approach of providing active calculation entropy prevention against DDoS attack for NGIM on smartphone which is deployed and emphasize under the active ICMP (Internet Control Message Protocol) protocol. Therefore, using the proposed approach in this section, the entropy measurement method is used to measure the behavior of the NGIM traffics and the numbers of IPv4 and IPv6 addresses in which the abnormal events of the RTT and RTO are found and counted after active inquiring ICMP procedure with appropriate and flexible packet-sizes after detecting huge NGIM traffics in smartphones. Therefore, the entropy operations for the NGIM traffics and the numbers of IPv4 and IPv6 addresses are described in this section.

At first, assume that a user communicates to each other via an NGIM App activated in his smartphone. At the same time, a traffic monitoring procedure is also activated in his smartphone. Once some abnormal also burst packets are detected by his smartphone. Subsequently, the smartphone then activates and measures an active ICMP procedure, and then calculates the entropy values for the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses via the entropy calculation operations. Finally, the entropy values are computed by using the measured the NGIM traffics and the numbers of IPv4 and IPv6 addresses in which the abnormal events of the RTT and RTO are found and counted after active inquiring ICMP procedure with appropriate and flexible packet-sizes. The system flowchart is given, please see the Figure 1, in order to easily read as well as understand.

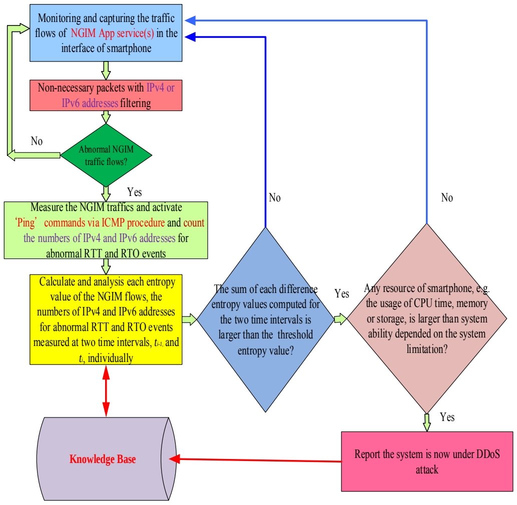

Monitoring and capturing the traffic flows of NGIM App service(s) in the interface of smartphone
Non-necessary packets with IPv4 or IPv6 addresses filtering
Abnormal NGIM traffic flows?
No
Yes
Measure the NGIM traffics and activate 'Ping' commands via ICMP procedure and count the numbers of IPv4 and IPv6 addresses for abnormal RTT and RTO events
Calculate and analysis each entropy value of the NGIM flows, the numbers of IPv4 and IPv6 addresses for abnormal RTT and RTO events measured at two time intervals, $t_{i-1}$ and $t_i$ individually
The sum of each difference entropy values computed for the two time intervals is larger than the threshold entropy value?
No
Yes
Any resource of smartphone, e.g. the usage of CPU time, memory or storage, is larger than system ability depended on the system limitation?
No
Yes
Report the system is now under DDoS attack
Knowledge Base

**Figure 1.** **The system flowchart.**

According to the collected traffics consisting of the huge NGIM traffics, the numbers of IPv4 and IPv6 addresses counted by the abnormal events of the RTT and RTO during an active inquiring ICMP procedure with appropriate and flexible packet-sizes in the smartphone, it could be evaluated whether the smartphone is under a DDoS attack or not. The method of evaluation could use the DDoS detection algorithm in *Algorithm 1*. In addition, *Case 1* and *Case 2* in Section 5 are the two examples which are given and described how to detect a DDoS attack by applying *Algorithm 1* in a smartphone.

***Algorithm 1. DDoS detection algorithm.***

*INPUT: The numbers of the observed traffics* $\{S_{x,y}\}$, *where* $x \in \{n_{NGIM}, n_{a\_RTT}, n_{a\_RTO}\} = \{1,2,3\}$, $y \in \{t_i, t_{i+1}, t_{i+2,}\ldots\} = \{0,1,2,3,4,\ldots\}$, *the initial values* $\{S_{1,0}, S_{2,0}, S_{3,0}\}$, *the system resource usage* $R_y$, *where* $y \in \{t_i, t_{i+1}, t_{i+2,}\ldots\} = \{0,1,2,3,4,\ldots\}$, *and the last updated averaged Entropy* $\bar{H}^{nor}_{y,y+1}(p \cdot \log(p))$;

*OUTPUT: The result of the decision together with their corresponding* $R_y$ *and their corresponding differential values between* $H_{y,y+1}(p_{y,y+1} \cdot \log(p_{y,y+1}))$ *and* $\bar{H}^{nor}_{y,y+1}(p \cdot \log(p))$;

*Step 1: If the usage of the system resources is larger than 0.8 which is according to the limitation of the system, then go to Step 2; otherwise, back to Step 1 in order to continue the usage monitoring of the system resources.*

*Step 2: The differential values among the numbers of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses* $\{S_{x,y}\}$, *where* $x \in \{n_{NGIM}, n_{a\_RTT}, n_{a\_RTO}\} = \{1,2,3\}$, $y \in \{t_i, t_{i+1}, t_{i+2,}\ldots\} = \{0,1,2,3,4,\ldots\}$ *are calculated by the equation* $|S_{x,y} - S_{x,y+1}|$;

*Step 3: The total differential values for each interval* $t_y$ *are computed by* $\sum_{x=1}^{3} |S_{x,y} - S_{x,y+1}|$, $y \in \{t_i, t_{i+1}, t_{i+2,}\ldots\} = \{0,1,2,3,4,\ldots\}$;

*Step 4: The probability values are given as*

$$p_{y,y+1} = \frac{|S_{x,y} - S_{x,y+1}|}{\sum_{x=1}^{3} |S_{x,y} - S_{x,y+1}|},\ y \in \{t_i, t_{i+1}, t_{i+2,}\ldots\} = \{0,1,2,3,4,\ldots\};$$

*Step 5: The entropy* $H_{y,y+1}(p_{y,y+1} \cdot \log(p_{y,y+1}))$ *according to the equations(2) and (3) for the two sets of the differences of the numbers of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses counted by the abnormal events* *between two time intervals, $y$ and $y+1$, where $y \in \{t_i, t_{i+1}, t_{i+2,} ...\} = \{0,1,2,3,4,...\}$;*

Step 6: *The average Entropy $\bar{H}^{nor}_{y,y+1}(p \cdot \log(p))$ according to the equations(2) and (3) for the number of the observed normal NGIM traffics traffic, the numbers of IPv4 and IPv6 addresses counted by the abnormal events determined and updated by the experiences of system;*

Step 7: *Calculate the differential values between $H_{y,y+1}(p_{y,y+1} \cdot \log(p_{y,y+1}))$ and $\bar{H}^{nor}_{y,y+1}(p \cdot \log(p))$;*

Step 8: *Perform the decision procedures below. If any the differential value $\left| H_{y,y+1}(p_{y,y+1} \cdot \log(p_{y,y+1})) - \bar{H}^{nor}_{y,y+1}(p \cdot \log(p)) \right|$, where $y \in \{t_i, t_{i+1}, t_{i+2,} ...\} = \{0,1,2,3,4,...\}$, is larger than the threshold value determined and updated by system and the usage of the system resources, e.g. CPU time plus memory or storages, is larger than the limitation of the system. The result of the decision procedure will be outputted as 'Under DDoS attack', otherwise 'Under normal status' will be outputted;*

Step 9: *Output the result of the decision together with their corresponding differential values between $H_{y,y+1}(p_{y,y+1} \cdot \log(p_{y,y+1}))$ and $\bar{H}^{nor}_{y,y+1}(p \cdot \log(p))$.*

□

In general, a DDoS attack usually lasts at least several hours. The active calculation entropy prevention against DDoS attack for NGIM on smartphone could be divided into three phases: *Attack launch*, *Attack in progress*, and *Attack Determination*. These three phases will be discussed as follows.

Phase 1 - *Attack launch.*

At first, the burst and large number of NGIM traffics will be monitored in real time in order to determine whether it is possible under DDoS attack or not. Since DDoS attacks usually go on in continuing, the smartphone should monitor continuously the usage of its resources and the results of the outputted differential entropy values according to *Algorithm 1* in every two subsequent time intervals. If a possible DDoS attack still exists after detecting in the next succeeding time interval, then DDoS attacks are identified. Otherwise, the burst and large number of NGIM traffics detected in previous time interval could be regarded as the NGIM traffics are rising in temporal at that time interval.

Phase 2 - *Attack in progress.*

Because of the DDoS attack is continuous, the number of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses counted by the abnormal events in the subsequent time intervals will be remained highly. According to *Algorithm 1*, when the difference of the differential entropy value set for the two sets of the observed NGIM traffics plus the numbers of IPv4 and IPv6 addresses measured at the two consecutive time intervals is not large as well as the difference between the differential entropy value sets and the average of the differential entropy values may be lower than threshold, this case will be determined as 'non under DDoS attack'. Therefore, after the first DDoS attack being detected, the number of requested services in NGIM and the usage of system resources should be checked continuously. Once the NGIM App under DDoS attack is identified, the corresponding defense scheme will then start up to prevent the DDoS attack.

Phase 3 - *Attack Determination.*

The number of the observed NGIM traffics as well as the numbers of IPv4 and IPv6 addresses counted by the abnormal events will be abruptly reduced when the attack is no longer persisted. However, the difference between the measured differential entropy values and the average of differential entropy values according to *Algorithm 1* will be also more than the system threshold, which it will still raise a DDoS attack alarm. But the usage of system resources does not exceed the limitation of the system, and the number of the observed NGIM traffics as well as the numbers of IPv4 and IPv6 addresses counted by the abnormal events are similar to normal case. In this case, the further checking on the usage of system resources and the number of the observed traffics for NGIM should be carried out to exclude the wrong DDoS attack alarm.

□

Furthermore, the average of differential entropy values of the system is measured under non-attack status for a long time. The average value could be obtained by using some machine learning algorithms, such as genetic algorithms, neural networks, and even deep learning algorithms, *etc*.

## 5 DISCUSSIONS

THE two cases are represented in Subsection 5.1 shown that it is a lightweight approach could be applied in low-battery mobile devices, e.g. smartphone. Moreover, in Subsection 5.2, our scheme is compared to the past schemes (Chen et al., 2015; Devi and Yogesh, 2012; Han et al., 2016; Kambourakis et al., 2007; Kitana et al., 2016; Liu and Chang, 2011; Ranjan et al., 2009; Rahul et al., 2012; Srivatsa et al., 2008; Walfish et al., 2010; Wang et al., 2010; R. Wang et al., 2015; X. T. Wang, et al., 2015; Yu et al., 2007; Yu et al., 2009; Yu et al., 2011; Xie and Yu, 2009) and it could be applied to detect the DDoS attack on NGIM Apps, e.g. XChat installed in smartphone.

### 5.1 Two Cases

In this subsection, two cases are shown in *Case 1* and *Case 2*. Once the situation is satisfy for huge traffic on the NGIM are detected in smartphones, the entropy measurement method is activated to measure the traffic behaviors of the RTT and RTO by adopting some ICMP commend as 'ping -4 –t –l $n_4$' and 'ping -6 –t –l $n_6$' with large size packets, where $0 \le n_4 \le 65500$ and $0 \le n_6 \le 65500$. Therefore, the entropy operations for both the numbers of IPv4 and IPv6 addresses measured and counted by the abnormal events of the RTT and RTO during an active inquiring ICMP procedure with appropriate and flexible packet-sizes the packet traffics $S_{n_{a\_RTT},y} = \sum_{k \in \{v_4, v_6\}} S_{n_{a\_RTT_k},y}$ and $S_{n_{a\_RTO},y} = \sum_{k \in \{v_4, v_6\}} S_{n_{a\_RTO_k},y}$, where $y \in \{t_i, t_{i+1}, t_{i+2}, t_{i+3}, ...\}$ measured from these NGIM chat Apps and the inquiring traffics from the RTT and RTO will be described in this subsection. Moreover, *Algorithm 1* proposed in Section 4 has been proven according to the two cases which it could be used to detect traffic on smartphones whether they are under DDoS attack or not under DDoS attack.

***<u>Case 1</u>***. Assumed that the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses counted by the abnormal events are given as a set $\left\{S_{n_{NGIM},y}, S_{n_{a\_RTT},y}, S_{n_{a\_RTO},y}\right\} = \left\{S_{1,y}, S_{2,y}, S_{3,y}\right\} = \{\{39783,53,45\},\{25829,35,10\},\{30725,40,25\},\{250672,71,20\},\{30328,20,36\}\}$, $y = \{0,1,2,...,4\}$. Then, the details of detecting DoS attack could be presented and shown in Table 1 according to the system flow chart in Figure 1 and DoS detection algorithm in *Algorithm 1*.

***<u>Case 2</u>***. Assumed the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses counted by the abnormal events are given as a set $\left\{S_{1,y}, S_{2,y}, S_{3,y}\right\} = \left\{S_{n_{NGIM},y}, S_{n_{a\_RTT},y}, S_{n_{a\_RTO},y}\right\} = \{\{25829,35,10\},\{30725,40,25\},\{250672,270,80\},\{260282,250,15\}\{30238,20,36\}\}$, $y = \{0,1,2,...,4\}$. Next, the details of the operations for *Case 2* could be presented and shown in Table 2 according to the system flow chart in Figure 1 and DDoS detection algorithm in *Algorithm 1*.

### 5.2 Discussions and Comparisons

The proposed scheme considers the differential entropy values for the set of the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses counted by the abnormal events $\left\{S_{n_{NGIM},y}, S_{n_{a\_RTT},y}, S_{n_{a\_RTO},y}\right\}$, and further takes into account the usage of the overall resources such as the CPU time and memory of the system. The system resources will be monitored and analyzed whether or not the usage of resources in CPU time and memory in smartphone has been exhausted. Each set of the differential entropy value for the two sets of the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses counted by the abnormal events $\left\{S_{n_{NGIM},y}, S_{n_{a\_RTT},y}, S_{n_{a\_RTO},y}\right\}$ and $\left\{S_{n_{NGIM},y+1}, S_{n_{a\_RTT},y+1}, S_{n_{a\_RTO},y+1}\right\}$, $y \in \{t_0, t_1, t_2, ...\} = \{0,1,2,3,...\}$ will be calculated, which are measured at two adjacent time intervals. Once the usage of the system resource in the smartphone has been exhausted together with one of the analyzed value which is more than the threshold, defined by the system expert, from these sets of the differential entropy value in the smartphone, the 'under DDoS attacks' will be outputted, immediately. Moreover, the system expert could be learned and trained by using the machine learning algorithms, such as genetic algorithms, neural networks, and even deep learning algorithms, *etc*. All the training data could be stored into knowledge base (KB) in Figure 1. In addition, the average of the differential entropy values in the system is continuous measured and updated under the status in non-attack for a long time.

In *Case 1*, the results of the differential entropy values {0.00296, 0.00234, 0.0141, 0.01355} computed by $H_{y,y+1}(p \cdot \log(p))$ and $\overline{H}^{nor}_{y,y+1}(p \cdot \log(p))$ according to *Algorithm 1* at the time intervals { $t_1$ , $t_2$ , $t_3$ , $t_4$ }, individually. The value {0.0141} calculated at the time interval $t_3$ compared to the value {0.00234} computed at the time interval $t_2$ is suddenly increased. Therefore, the status of 'under DDoS attack' will be then determined and outputted according to *Phase 1 - Attack* launch at the time interval $t_3$.

The number of the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses counted by the abnormal events for each time interval in Table 1 is depicted in Figure 2. It is obvious to see that the number of packets bursts out at time interval $t_3$ for the observed NGIM traffics and the numbers of IPv4 and IPv6 addresses counted by the abnormal events, and the differential entropy value also rises up abruptly, there is an attack occurred at $t_3$.

In *Case 2*, the results of the differential entropy values calculated by $H_{y,y+1}(p \cdot \log(p))$ and $\overline{H}^{nor}_{y,y+1}(p \cdot \log(p))$ according to Algorithm 1at the time intervals { $t_0$ , $t_1$ , $t_2$ , $t_3$ , $t_4$ }, separately, are {'0.00296', '0.00234', '0.0141', '0.00903' , '0.01368'}. The value {0.0141} calculated at the time interval $t_2$ compared to the value {0.00234} computed at the time interval $t_1$ is suddenly increased. Therefore, the status of 'under the DDoS attack' is determined and outputted according to *Phase 1 - Attack launch* during the second time interval $t_2$ . The value {0.00903} calculated at the time interval $t_3$ compared to the value {0.0141} computed at the time interval $t_2$ is suddenly decreased. It means that the difference values for $\left|H_{y,y+1}\left(p_{y,y+1}\cdot\log(p_{y,y+1})\right)-\overline{H}^{nor}_{y,y+1}\left(p\cdot\log(p)\right)\right|$ are similar at two intervals $t_2$ and $t_3$ . However, according to *Phase 2 - Attack* in progress, the DDoS attack is continuous during the third time interval $t_3$ . In the other words, the set of {'0.00234', '0.0141', '0.00903', '0.01368'} means that the smartphone is 'under the continuous DDoS attack' according to *Phase 2 - Attack in progress*. For the fourth time interval $t_4$ , the number of NGIM traffics {30238} compared to the third time interval $t_3$ is not large. Thus, the difference value for $\left|H_{y,y+1}\left(p_{y,y+1}\cdot\log(p_{y,y+1})\right)-\overline{H}^{nor}_{y,y+1}\left(p\cdot\log(p)\right)\right|$ is lower than the threshold, which this status will be determined

**Table 1.** **The details of calculations and the operations for *Case 1* by using *Algorithm 1*.**

| Time intervals | $t_0$ (Initial interval) | | | $t_1$ | | | $t_2$ | | | $t_3$ | | | $t_4$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| System resource usage $R_y$ | 0.4 | | | 0.3 | | | 0.37 | | | 0.9 | | | 0.35 | | |
| The observed traffics | $S_{1,0}$ | $S_{2,0}$ | $S_{3,0}$ | $S_{1,1}$ | $S_{2,1}$ | $S_{3,1}$ | $S_{1,2}$ | $S_{2,2}$ | $S_{3,2}$ | $S_{1,3}$ | $S_{2,3}$ | $S_{3,3}$ | $S_{1,4}$ | $S_{2,4}$ | $S_{3,4}$ |
| S1: No. of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses | 39783 | 53 | 45 | 25829 | 35 | 10 | 30725 | 40 | 25 | 250672 | 71 | 20 | 30238 | 20 | 36 |
| S2: The differential value $\left\|S_{x,y}-S_{x,y+1}\right\|$ , where $x\in\{1,2,3\},y\in\{1,2,....\}$ | - | - | - | 13954 | 18 | 35 | 4896 | 5 | 15 | 219947 | 31 | 5 | 220434 | 51 | 16 |
| S3: The total differential value $\sum_{x=1}^{3}\left\|S_{x,y}-S_{x,y+1}\right\|$, $y\in\{1,2,....\}$ | | | | 14007 | | | 4916 | | | 219983 | | | 220501 | | |
| S4: Probability $p$ | - | - | - | 0.996 | 0.001 | 0.002 | 0.996 | 0.001 | 0.003 | 0.9998 | 0.0001 | 2.27e-5 | 0.9997 | 0.0002 | 7.26e-5 |
| $\log(p)$ | - | - | - | -0.002 | -2.891 | -2.602 | -0.002 | -2.993 | -2.516 | -7.1e-5 | -3.851 | -4.643 | -1.3e-4 | -3.636 | -4.139 |
| $p\cdot\log(p)$ | - | - | - | 1.64e-3 | 3.72e-3 | 6.5e-3 | 1.76e-3 | 3.04e-3 | 7.67e-3 | -7.1e-5 | 5.43e-4 | 1.06e-4 | 1.32e-4 | 8.41e-4 | 3e-4 |
| S5: The entropy $H_{y,y+1}\left(p_{y,y+1}\cdot\log(p_{y,y+1})\right)$ for two sets of the differential entropy values among no. of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses in two intervals $y$ and $y+1$ , where $y\in\{0,1,2,...\}$ | - | | | 0.01186 | | | 0.01248 | | | 0.00072 | | | 0.0013 | | |
| S6: The average entropy $\overline{H}^{nor}_{y,y+1}\left(p\cdot\log(p)\right)$ for the No. of the observed normal NGIM traffics traffic, the numbers of IPv4 and IPv6 addresses determined by the experiences of system | - | | | 0.01482 | | | 0.01482 | | | 0.01482 | | | 0.01482 | | |
| S7: The differential values between $H_{y,y+1}\left(p_{y,y+1}\cdot\log(p_{y,y+1})\right)$ and $\overline{H}^{nor}_{y,y+1}\left(p\cdot\log(p)\right)$ | - | | | 0.00296 | | | 0.00234 | | | 0.0141 | | | 0.01355 | | |
| S8 and S9: Final decision | - | | | - | | | - | | | Under DDoS attack | | | - | | |

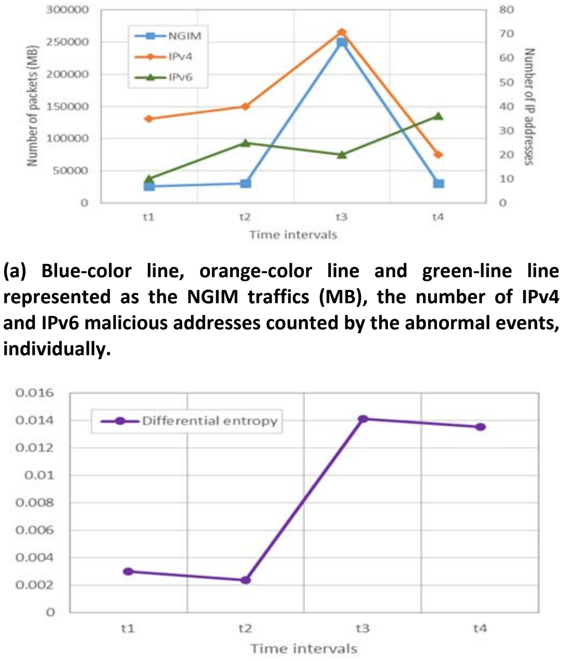
according to *Phase 3 - Attack Determination* as 'non under DDoS attack' in Table 2.

The number of the observed traffics measured in number of packets for each time interval in Table 2 is depicted in Figure 3. The NGIM traffic and the differential entropy values have been normalized in the chart. The number of packets for instant messaging is abruptly raised at time interval $t_2$ , and the differential entropy is also raised, so there is an attack launching at $t_2$ . At time interval $t_3$ , the differential entropy value is reduced, but the traffic of instant messaging is still high, that is, the attack is in progress. After time interval $t_3$ , the traffic of instant messaging drops down, but the differential entropy value rises again, which means the attack is terminated.

**Table 2. The details of the calculations and operations for *Case 2* by using *Algorithm 1*.**

| Time intervals | $t_0$<br>(Initial interval) | | | $t_1$ | | | $t_2$ | | | $t_3$ | | | $t_4$ | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| System resource usage $R_y$ | 0.3 | | | 0.37 | | | 0.9 | | | 0.86 | | | 0.35 | | |
| The observed traffics | $S_{1,0}$ | $S_{2,0}$ | $S_{3,0}$ | $S_{1,1}$ | $S_{2,1}$ | $S_{3,1}$ | $S_{1,2}$ | $S_{2,2}$ | $S_{3,2}$ | $S_{1,3}$ | $S_{2,3}$ | $S_{3,3}$ | $S_{1,4}$ | $S_{2,4}$ | $S_{3,4}$ |
| S1: No. of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses | 25829 | 35 | 10 | 30725 | 40 | 25 | 250672 | 71 | 20 | 260286 | 60 | 15 | 30238 | 20 | 36 |
| S2: The differential value $\lvert S_{x,y} - S_{x,y+1} \rvert$ , where $x \in \{1,2,3\}, y \in \{1,2,....\}$ | 13954 | 18 | 35 | 4896 | 5 | 15 | 219847 | 31 | 5 | 9614 | 11 | 5 | 230048 | 40 | 21 |
| S3: The total differential value $\sum_{x=1}^{3} \lvert S_{x,y} - S_{x,y+1} \rvert$, $y \in \{1,2,.... \}$ | 14007 | | | 4916 | | | 219883 | | | 9630 | | | 230109 | | |
| S4: Probability $p$ | 0.996 | 0.001 | 0.002 | 0.996 | 0.001 | 0.003 | 0.999 | 1.4e-4 | 2.27e-5 | 0.998 | 1.14e-3 | 5.19e-4 | 0.999 | 1.74e-4 | 9.13e-5 |
| $\log( p )$ | -0.002 | -2.891 | -2.602 | -0.002 | -2.993 | -2.516 | -7.1e-5 | -3.851 | -4.643 | -7.2e-4 | -2.942 | -3.285 | -1.2e-4 | -3.76 | -4.04 |
| $p \cdot \log( p )$ | 1.64e-3 | 3.72e-3 | 6.5e-3 | 1.76e-3 | 3.04e-3 | 7.68e-3 | 7.11e-5 | 5.43e-4 | 1.06e-4 | 7.21e-4 | 3.36e-3 | 1.7e-3 | 1.15e-4 | 6.54e-4 | 3.69e-4 |
| S5: The entropy $H_{y,y+1}$ $(p_{y,y+1} \cdot \log( p_{y,y+1}))$ for two sets of the differential entropy values among No. of the observed NGIM traffics, the numbers of IPv4 and IPv6 addresses in two intervals $y$ and $y+1$ , where $y \in \{0,1,2,...\}$ | 0.01186 | | | 0.01248 | | | 0.00072 | | | 0.00579 | | | 0.00114 | | |
| S6: The average entropy $\overline{H}^{nor}_{y,y+1}(p \cdot \log( p))$ for the No. of the observed normal NGIM traffics traffic, the numbers of IPv4 and IPv6 addresses determined by the experiences of system | 0.01482 | | | 0.01482 | | | 0.01482 | | | 0.01482 | | | 0.01482 | | |
| S7: The differential values between $H_{y,y+1}$ $(p_{y,y+1} \cdot \log( p_{y,y+1}))$ and $\overline{H}^{nor}_{y,y+1}(p \cdot \log( p))$ | 0.00296 | | | 0.00234 | | | 0.0141 | | | 0.00903 | | | 0.01368 | | |
| S8 and S9: Final decision | - | | | - | | | Under DDoS attack | | | Under DDoS attack | | | - | | |

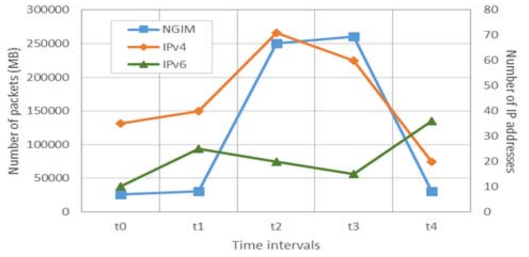
Finally, this two cases shown that *Algorithm 1* could return the final decision for supporting the NGIM in a smartphone whether under DDoS attacks or not. Also, the results are shown what the proposed approach is useful by activating an active ICMP procedure, and then measuring, entropy calculating plus analyzing whether smartphone is under DDoS attack or not. Due to the lower computation operations in applied system mentioned above, it is a lightweight approach could be applied in low-battery mobile devices, e.g. smartphone. Finally, the comparison among the proposed schemes (Chen et al., 2015; Devi and Yogesh, 2012; Han et al., 2016; Kambourakis et al., 2007; Kitana et al., 2016; Liu and Chang, 2011; Ranjan et al., 2009; Rahul et al., 2012; Srivatsa et al., 2008; Walfish et al., 2010; Wang et al., 2010; R. Wang et al., 2015; X. T. Wang, et al., 2015; Yu et al., 2007; Yu et al., 2009; Yu et al., 2011; Xie and Yu, 2009) and our scheme is listed as Table 3.



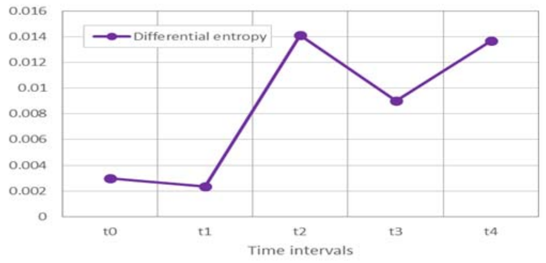
**(a) Blue-color line, orange-color line and green-line line represented as the NGIM traffics (MB), the number of IPv4 and IPv6 malicious addresses counted by the abnormal events, individually.**

**(b) Purple-color line represented as the differential entropy values of** $\left|H_{y,y+1}\left(p_{y,y+1}\cdot\log(p_{y,y+1})\right)-\overline{H}^{nor}_{y,y+1}\left(p\cdot\log(p)\right)\right|$.

**Figure 2. The observed data in each time interval for Case 1. (a) The number of packets and the number of malicious IPv4/v6 addresses. (b) The differential entropy values.**



**(a) Blue-color line, orange-color line and green-color line represented as the NGIM traffics (MB), the number of IPv4 and IPv6 malicious addresses counted by the abnormal events, individually.**



**(b) Purple-color line represented as the differential entropy values of** $\left|H_{y,y+1}\left(p_{y,y+1}\cdot\log(p_{y,y+1})\right)-\overline{H}^{nor}_{y,y+1}\left(p\cdot\log(p)\right)\right|$.

**Figure 3. The observed data in each time interval for Case 2. (a) The number of NGIM packets and the number of malicious IPv4/v6 addresses. (b) The differential entropy values.**

## 6 CONCLUSIONS

NEWLY, XChat becomes a NGIM App based on the BC technology could be assigned both the IPv4 and IPv6 addresses which they could be worked as stealth addresses. Thus, any DoS attack activated form the malicious XChat node will be treated as a kind of DDoS attack. Therefore, the huge NGIM usages with stealth addresses for mobile devices will suffer the Distributed Denial of Service (DDoS) attack from Internet. In this paper, we proposed a new scheme based on an integrated entropy measurement approach in order to detect DDoS attacks in NGIM Apps in smartphones. The approach provides the approach based on the integrated entropy calculations for the NGIM traffics, the numbers of IPv4 and IPv6 addresses in which the abnormal events of the RTT (round-trip time) and RTO (retransmission timeout) are found and counted after active inquiring ICMP commands with appropriate and flexible packet-sizes. It could return the final decision for supporting the NGIM in a smartphone whether it is under DDoS attack or not. Two cases are given and proved that could be applied in smartphone. Due to the lower computation operations in applied system mentioned above, it is a lightweight approach could be applied in low-battery mobile devices. Finally, it is a more quick and efficient approach in analyzing the current status of the traffics of NGIM APPs in smartphones, and then determining whether the NGIM App is under DDoS attack or not.

## 7 ACKNOWLEDGEMENTS

THIS work was supported by the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under Grant MOST 106-2632-E-468-003.

**Table 3. Functionality comparison among the schemes.**

| Compared Items<br>Proposed Schemes | Application level | Smartphone -based DDoS detection approach | Entropy-based detection mathematic method | Adopting ICMP to inquiring the no. of abnormal IPv4 and IPv6 traffics | Supporting Detecting DDoS for NGIM traffics |
|---|---|---|---|---|---|
| Our Scheme | Yes | Yes | Yes | Yes | Yes |
| Chen, et al. (2015) | Yes | None | Yes | None | None |
| Wang, R. et al. (2015) | None | None | Yes | None | None |
| Wang, X. T. et al. (2015) | None | None | Yes | None | None |
| Han, et al. (2016) | Yes | Yes | None | None | None |
| Kambourakis, et al. (2007) | Yes | None | None | None | None |
| Rahul, et al. (2012) | Yes | None | None | None | None |
| Ranjan, et al. (2009) | Yes | None | Yes | None | None |
| Xie and Yu (2009) | Yes | None | Yes | None | None |
| Liu and Chang (2011) | Yes | None | None | None | None |
| Walfish, et al. (2010) | Yes | None | None | None | None |
| Yu, et al. (2007) | Yes | None | None | None | None |
| Srivatsa, et al. (2008) | Yes | None | None | None | None |
| Yu, et al. (2009) | Yes | None | None | None | None |
| Devi and Yogesh (2012) | Yes | None | Yes | None | None |
| Yu, et al. (2011) | Yes | None | Yes | None | None |
| Wang, et al. (2010) | Yes | None | Yes | None | None |
| Kitana, et al. (2016) | None | Yes | None | None | None |

## 8 REFERENCES

Absolute Astronomy, (2012). Information Entropy. Available from: [On-Line] http://www.absoluteastronomy.com/topics/Information_entropy.

T. Bass., A. Freyre, D. Gruber, and G. Watt, (1998). Email Bombs and Countermeasure: Cyber Attack on Availability and Brand Integrity, *IEEE Network*. 12(2), 10-17.

H. C. Chen, (2016). A trusted user-to-role and role-to-key access control scheme, *Soft Computing*. 20(5), 1721-1733.

H. C. Chen, C. H. Mao, and S. S. Tseng, (2015). An Approach for Detecting a Flooding Attack Based on Entropy Measurement of Multiple E-Mail Protocols, *Journal of Applied Science and Engineering*. 18(6), 79-88.

H. C. Chen, C. H. Mao, Y. T. Lin, T. L. Kung, and C. E. Weng, (2016). A secure group-based mobile chat protocol, *Journal of Ambient Intelligence and Humanized Computing*. 7(5), 696-703.

H. C. Chen, I. You, C. E. Weng, C. H. Cheng, and Y. F. Huang, (2016). A security gateway application for End-to-End M2M communications, *Computer Standards & Interfaces*. 44, 85-93.

Coinbuzz, (2017). New secure chat client, XChat, is based on Bitcoin blockchain technology. Available from: [On-Line] https://99bitcoins.com/new-secure-chat-client-based-bitcoin-blockchain-xchat/.

S. R. Devi and P. Yogesh, (2012). A hybrid approach to counter application layer DDoS attacks, *International Journal on Cryptography and Information Security*. 2(2), 45-52.

M. R. Han, Y. C. Oh, and J. B. Kim, (2016). A study on responding to DDoS architecture in smart phone environment, *International Journal of Security and Its Applications*. 10(6), 87-98.

G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, (2007). Detecting DNS amplification attacks, *Lecture Notes in Computer Science*. 5141, 185-196.

A. Kitana, I. Traore, and I. Woungang, (2016). Impact study of a mobile botnet over LTE networks, *Journal of Internet Services and Information Security*. 6(2), 1-22.

G. Li, H. Zhou, G. Li, and B. Feng, (2017). Application-aware and dynamic security function chaining for mobile networks, *Journal of Internet Services and Information Security*. 7(4), 21-34.

K. Lim, Y. Jeong, S. Cho, M. Park, and S. Han, (2016). An Android application protection scheme against dynamic reverse engineering attacks, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. 7(3), 40-52.

H. I. Liu and K. C Chang. (2011). Defending systems against tilt DDoS attacks, *Proceedings of 6th International Conference on Telecommunication Systems, Services, and Applications.* 22-27.

Q. Niyaz, W. Sun, and A. Y. Javaid, (2016). A deep learning based DDoS detection system in software-defined networking (SDN). arXiv preprint arXiv:1611.07400.

E. Nygren, (2016). Preparing for IPv6-only mobile networks: Why and How. Available from: [On-Line] https://blogs.akamai.com/2016/06/preparing-for-ipv6-only-mobile-networks-why-and-how.html.

A. Rahul, S. K. Prashanth, B. Sureshkumar, and G. Arun, (2012). Detection of intruders and flooding in VoIP using IDS, Jacobson fast and Hellinger distance algorithms, *IOSR Journal of Computer Engineering*. 2(2), 30-36.

S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly, (2009). DDoS-shield: DDoS-resilient scheduling to counter application layer attacks, *IEEE/ACM Transactions on Networking*. 17(1), 26-39.

Statista, (2016). Number of monthly active LINE users worldwide as of 3rd quarter 2016 (in millions). Available from: [On-Line] https://www.statista.com/statistics/327292/number-of-monthly-active-line-app-users/.

M. Srivatsa, A. Iyengar, J. Yin, and L. Liu, (2008). Mitigating application-level denial of service attacks on web servers: A client-transparent approach, *ACM Transactions on the Web*. 2(3), 15.

M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, (2010). DDoS defense by offense, *ACM Transactions on Computer Systems*. 28(1), 3.

J. Wang, X. Yang, and K. Long, (2010). A new relative entropy based app-DDoS detection method, *Proceedings of 2010 IEEE Symposium on Computers and Communications*. 966-968.

R. Wang, Z. Jia, and L. Ju, (2015). An entropy-based distributed DDoS detection mechanism in software-defined networking, *IEEE Trustcom/BigDataSE/ISPA*.

X. T. Wang, G. Q. Liu, J. G. Yang, and J. Z. Ran (2015). DDoS attack detection algorithm based on IP entropy mode, *Proceedings of the 2015 International Industrial Informatics and Computer Engineering Conference*.

Y. Wang, S. Song, F. Zhou, and X. Zheng, (2017). Chinese WeChat and blog hot words detection method based on Chinese semantic clustering, *Journal of Intelligent Automation & Soft Computing*. 23(4), 613-618.

Y. Xie and S. Z. Yu, (2009). A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors, *IEEE/ACM Transactions on Networking*. 17(1), 54-65.

J. Yu, C. Fang, L. Lu, and Z. Li, (2009). A lightweight mechanism to mitigate application layer DDoS attacks, *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*. 18, 175-191.

J. Yu, Z. Li, H. Chen, and X. Chen, (2007). A detection and offense mechanism to defend against application layer DDoS attacks, *Proceedings of Third International Conference on Networking and Services*. 54-59.

S. Yu, W. Zhou, R. Doss, and W. Jia, (2011). Traceback of DDoS attacks using entropy variations, *IEEE Transactions on Parallel and Distributed Systems*. 22(3), 412-425.

Zhangsk, (2012). RTT of Measure and RTO of Calculations in TCP. Available from: [On-Line] http://blog.csdn.net/zhangskd/article/details/7196707.

## 9 NOTES OF CONTRIBUTORS

**Hsing-Chung Chen (Jack Chen)** received the B.S. degree in Electronic Engineering from National Taiwan University of Science and Technology, Taiwan, in 1994, and the M.S. degree in Industrial Education from National Normal University, Taiwan, in 1996, respectively. In addition, he received the Ph.D. degree in Electronic Engineering from National Chung Cheng University, Taiwan, in 2007. During 1991-2007, he served as a Mobile Communication System Engineer for Mobile Business Group, Chunghwa Telecom Co., Ltd. in Taiwan. From 2008 to 2013, he was the Assistant Professor of the Department of Computer Science and Information Engineering at Asia University, Taiwan. He is employed as an Associate Professor at Department of Computer Science and Information Engineering, Asia University, Taiwan. He is also the Research Consultant of Department of Medical Research at China Medical University Hospital, China Medical University, Taichung City, Taiwan. He is also the member of CCISA, ICCIT, IET and IEEE. His research interests are in Information Security, Cryptography, Role-based Access Control, Computer Networks, Internet of Things, Mobile and Wireless Communications. He was the General Co-Chair of international conference MobiSec2017, and the Program Co-Chair of numerous international conferences, e.g. MobiSec2016, IMIS2015, CISIS2013, IMIS2013 and EMC2012. In addition, he was the Editor-in-Chief of *Newsletter of TWCERT/CC* from July 2012 to June 2013. Currently, He is the Guest Editor of Special Issue “Recent Advances on Radio Access and Security Methods in 5G Networks” in IEEE *ACCESS*, Dec. 1 2017.

**Shyi-Shiun Kuo** received the B.S. and M.S. degrees in computer science and information engineering from Feng-Chia University, Taiwan, R.O.C., in 1989 and 1991. He currently works toward a doctoral degree in computer science and information engineering at Asian University, Taichung city, Taiwan. He also works as assistant professor of Department of Multimedia Animation and Application at Nan Kai University of Technology, Nantou county, Taiwan. His research interests are network security and image processing.