ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 66, No. 12, pp. 1913~1920, 2017
http://doi.org/10.5370/KIEE.2017.66.12.1913

DDoS 공격 완화를 위한 새로운 분산 SDN 프레임워크

New Distributed SDN Framework for Mitigating DDoS Attacks

Ahmed Alshehhi* · Chan Yeob Yeun† · Ernesto Damiani*

Abstract – Software Defined Networking creates totally new concept of networking and its applications which is based on separating the application and control layer from the networking infrastructure as a result it yields new opportunities in improving the network security and making it more automated in robust way, one of these applications is Denial of Service attack mitigation but due to the dynamic nature of Denial of Service attack it would require dynamic response which can mitigate the attack with the minimum false positive. In this paper we will propose a new mitigation Framework for DDoS attacks using Software Defined Networking technology to protect online services e.g. websites, DNS and email services against DoS and DDoS attacks.

Key Words : Information security, Denial of service attack, Software defined networking, Distributed SDN

1. Introduction

Today Information Security is gaining much more attention specially with the raise of technology and IP based consumer devices, and on the other side the risk and threats are raising in parallel, these threats are targeting the information confidentiality, integrity and as well the services availability.

However the researchers are addressing these issues and proposed innovated security solutions starting from IoT and ubiquity networks [1, 3] to smart grid and healthcare cloud security solutions [4, 5], beside that researchers did't ignore the lawful interception requirements in a balance to the users privacy requirements [6, 7, 8].

Considering that online services like web sites, email, ecommerce services is available online to the public and whoever has an access to the internet can reach these services would make it exposed to high risk and that would implies deploying sufficient security control to protect these online services, the security control would vary from a network access control solutions like Network Firewall to Advance Persistence Threat mitigation solutions, in despite of all these advance solutions still they fail to stand in front of aggressive types of attack like Denial of Service Attack although these attacks are not involving complex cyber techniques but it is simply exhaust the available resource allocated for the service being it the allocated network links in the Internet Service Provider, local enterprise or even the servers hosting the application logic or the database.

On the other side there is continues debate on who is responsibility to mitigate Denial of Service attack especially if it exceeds the capacity of the enterprise or end online service provider, is it the traffic carrier providers like the Internet Service Providers or it is the owner of the online service being it a website, email service, gaming service and etc. Eventually, the Internet Service Provider can't tell if traffic is a malicious or genuine beside that the Internet Service Provider doesn't know what the network capacity at the enterprise end is.

Therefore, the only feasible solution to resolve this problem is to establish cooperation mechanism between the Internet Service Provider and the enterprises or online service provider in a way that they keep sharing useful information to mitigate Denial of Service attack.

Our proposal is introducing new DoS/DDoS mitigation which is based on Local SDNs and Global SDNs architecture, the proposal called Distributed SDN Framework, we are aiming to take advantage of the collaborative mitigation and make use of the communication between the Local SDN setup and the Global one to eliminate false positive and having effective results.

The local SDN which is deployed in the enterprise side will pass mitigation information to the Global SDN setup at

† Corresponding Author : Dept. of ECE, Khalifa University of Science and Technology, Abu Dhabi, UAE.
E-mail: chan.yeun@kustar.ac.ae
* Dept. of ECE, Khalifa University of Science and Technology, Abu Dhabi, UAE.

Received : November 10, 2017; Accepted : November 26, 2017

the ISP level, this information will help the Global SDN setup to deploy focused monitoring on client traffic rather than monitoring everything also it will help it to define proper thresholds to trigger any mitigation action.

The research is structured in four sections, Section II will highlight previous related researches efforts, Section III will explain the proposed framework and discuss it is components. In the section IV, we will analyses the proposed framework in comparison to the other DoS mitigation frameworks or solutions, finally there is a conclusion in Section V.

2. Related work

2.1 Denial of Service (DoS)

Denial of Service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users; it could be temporary or indefinitely interrupt or suspend service of a host connected to the internet. Denial of Service Attack is offensive activity that can be caused by sending malicious traffic to block online service or cause an interrupt to the service which might accordingly degrade the quality of the online service, DoS is one of the most basic attack that can be carried by mid expert attacker but still on the other hand DoS considered one of the most sever attacks that can cause a serious damage to the IT infrastructure and online services, in case of multiple sources involved in DoS attack then it is called Distributed Denial of Service attack (DDoS), in some scenarios the address sources might be spoofed ones and not real.

DoS attacks can be divided into two types:

a) Network DoS attacks

Network DoS attacks exploit two layers in Open Systems Interconnection (OSI) model, Network Layer (L3) and Transport Layer (L4) and that could be by either by fully utilizing the allocated network bandwidth or exhausting the network and servers' resources (memory, firewall state table, CPU, ARP table and etc.).

b) Application DoS Attack

Application DoS attack targets mainly vulnerabilities in internet service applications e.g. web servers, mail, web content management and etc. Therefore, it is called also software vulnerability attack, the most common type of such attack are:

- Land attack
- Ping of death attack
- Teardrops attack

2.2 Software Defined Network

Software Defined Networking is emerging networking technology where the network can be programed according to predefined conditions or external application.

The SDN system architecture consists of three major components as show:

1. Application Layer: Example of applications in that layer, business, network management and security application which analyze network status and technology requirements and accordingly it submit an action to the SDN Controller for implementation.
2. Control Layer: SDN controller provides central network view, it maintains the network status and instructs the networks nodes (switches/routers) via one of an SDN protocols, an example of SDN Controller OpenDayLight, Floodlight and RYU.
3. Infrastructure Layer: consists of SDN compliant networks devices, many networking vendors provide support to SDN through multiple protocols like netconf, flowspec and openflow protocols Figure 1, illustrates the architecture of standard Software Defined Networking.

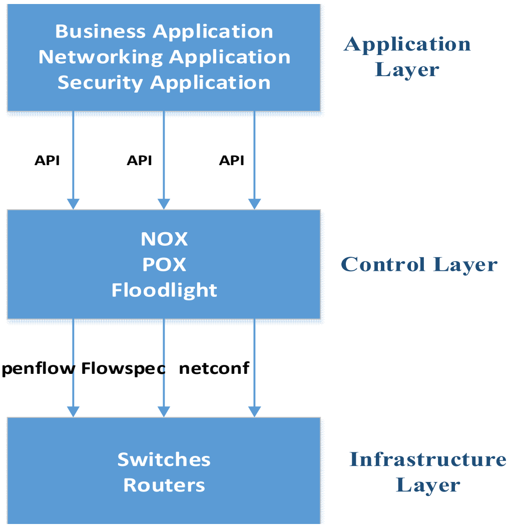


Fig. 1 Traditional SDN Architecture

As if today there are many DoS mitigation solutions available some of them are based on SDN technology, Table (1) shows some traditional DoS mitigation solutions:

For aggressive type of DDoS attack the preferred option is using Scrubbing Service, and that can be deployed in four stages:

- Stage One: Detecting the DoS attack using predefined thresholds.

Table 1 Mitigation Solution for DoS Attack

Attack type	Mitigation solution
Volumetric attack	• Scrubbing service • Blackholing • Rate limiting (BGP Flowspec)
TCP state-exhaustion attack	• Network firewall
Application layer attacks	• Intrusion prevention system • Application firewall

- Stage Two: Redirecting the attack flows (based on destination address) to a scrubbing center.
- Stage Three: Filtering the traffic based on deep inspection filter.
- Stage Four: Redirecting the clean traffic back to the normal route toward the destination address.

The next preferred option is rate limiting based on predefined threshold, nowadays the most effective protocol to implement such threshold is Flowspec over BGP, Flowspec normally is BGP update message which is instructing the router to limit the traffic to certain defined bandwidth.

The final resort to mitigate DDoS attack is lackholing based on destination address and that can be deployed by announcing a BGP update with special community code to tell the peers to drop or discard any packet or flow.

From the date of introducing Software Defined Networking technology there were some researches on how to make use this technology to improve the network security especially in detecting and mitigating DoS/DDoS type of attacks,

Mitigating Botnet-based DDoS flooding using SDN and sFlow was proposed using two-dimensions metric called Distribution-Collaboration Degree DCD to quantify the distribution/collaboration of the flow in one dimension and also measure the intensity of the flow in the other dimension [9], such approach is easy and effective in detecting anomalies within the flows.

Mitigation based on Shiryaev-Roberts Algorithm can be utilized to find the starting point of DoS attack, which can detect the anomalies correctly and timely and then redirected to filtering box (DDoS Filtering Algorithm) [10].

Fuzzy inference system was introduced also in such scope to provide a statistical analysis of real network traffic under normal and attack state in parallel with hard decision thresholds, there were six parameters considered in the analyzing phase:

- Distribution of flow quantity from single source.
- Distribution of Intra-Arrival Time.
- Distribution of packet quantity per flow.
- Flow quantity to a server.
- Number of source IP addresses to a server.
- Total traffic volume counted in bytes to a server.

In case the detection algorithm wasn't able to confirm whether the traffic is an attack or not they a fuzzy logic function is used [11]. FlowTrApp was introduces also which performs DDoS detection and mitigation using some bounds on two per flow based traffic parameters i.e. flow rate and flow duration of a flow, such techniques supposed to detect attacks from low rate to high rate and long duration attack to short duration attack. [12]

Another good approach for detecting DoS attack is through granular monitoring for the flow volume and flow rate to allocate potential victims and attackers, the proposed approach is divide to two models, sequential were victims are identified first then the next step is allocate the attackers anther model is concurrent model were both victims and attacker are identified in parallel, the first model is preferred to identify victims while the second model is preferred to identify victims and attacker.[13]

In another approach Time-based solution is considered for detection purposes, in that approach the SDN-Controller will receive any new flow and will redirect to a flow collector, in case there was high rate of flows within short time frame then the controller will deploy a rule in network devices to send any invalid packet directly to the flow collector. [14]

One of the most sever DDoS type is the amplified one e.g. using DNS server, in that scenario the attacker is flooding a DNS server with spoofed source IP (replace with victim IP), some researches has address such issue and proposed a solution based on authentication mechanism via an controller server so for any new DNS query the Controller server will send an authentication request to the requestor to make sure it is real and not faked request once it is authenticated the client or user traffic will be redirected to the DNS server.[15]

Similar architecture was considered in another but more general approach, where the controller is reviewing any new request and accordingly it inject a flow entry in the switch but if it noticed the flow rate became high then it will inject another flow entry to block such flow [16, 17].

A proposed concept of mitigation called DrawBridge which is consists of multiple controllers, if a hosted server was attacked then it can inform local controller to push filtering action, the local controller can push the filter to upstream ISPs if it is required[18].

Overall majority of the researches in this area are focusing on detecting DoS attack, our proposal is addressing both detection and mitigation in local and ISP level which can facilitate also detecting and mitigating DoS attack in the ISP level using the predefined thresholds and without waiting a notification from the end client in the downstream, moreover the proposed framework is trying to exploit the maximum benefits of the shared intelligence between the Local and Global SDN to have effective and accurate DoS mitigation.

3. The proposed framework

The proposed framework consists mainly of two parts, Local SDNs and Global SDN setup, as it shown in Figure (2) both setups will cooperate together to detect and mitigate DoS/DDoS attacks in automated fashion.

Local SDN setup provides Local detection and mitigation capabilities for the local customer network and beside that the Local SDN setup synchronize thresholds and information with the Global SDN setup, this information could be:

- Bandwidth Thresholds (Mbps)
- Number of Packets Per second Thresholds (PPS)
- Asset IPs to be protected (in CIDR format)
- Action (Rate limit, Block and etc.)

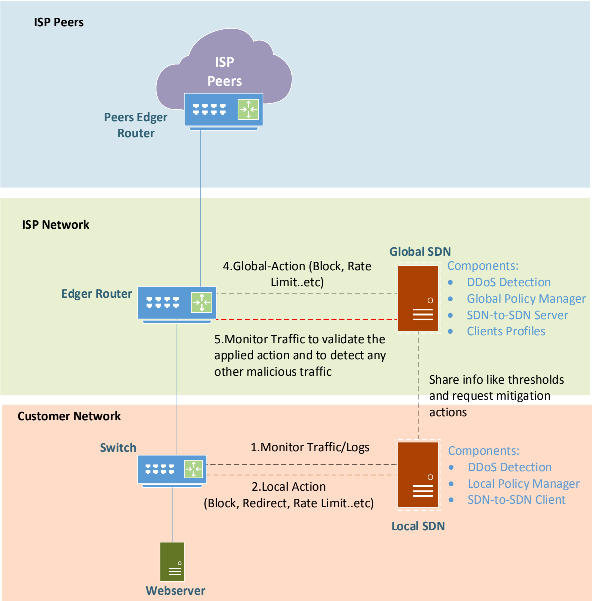


Fig. 2 Propesed Distributed SDN Framework Architecture

To support all above functions the Local SDN should have the following components:

- DoS detection Application: Using defined thresholds, networks statistics, end servers logs or other security monitoring solutions.
- Local Policy Manager to push the local networking rules whenever an attack is detected.
- SDN-To-SDN client or agent which will be responsible for all communication with the global SDN setup.

Global SDN setup provides detection and mitigation capabilities at the ISP Edge routers using thresholds and actions provided by the Local SDN setup.

To support all above functions the Local SDN should have the following components:

- DoS detection Application: Using defined thresholds, networks statistics or other security monitoring solutions.
- Global Policy Manager to push the networking rules whenever an attack is detected.
- SDN-To-SDN server which will be responsible for all communication with all other Local SDN setups.
- Clients Profiles with all thresholds, networks IP and available capacity within the client network.

The operation of the mentioned proposal involves three stages:

1) Synchronization Stage: in this stage the Local SDN share local enterprise parameters with the Global SDN setup that can help to have efficient detection and mitigation.
2) Monitoring Stage: in this stage the Local or Global SDN will monitor the traffic based on available parameters shared by Local SDN.
3) Mitigation Stage: at this stage Local or Global SDN setup will trigger a proper mitigation action which could be blocking attack source, redirecting to scrubbing center, rate-limiting and etc.

The mitigation action can be escalated to the Global SDN setup via three methods:

- Manual execution of action: in this case the customer will send an action directly to the Global SDN setup for execution.
- Auto signal for action: in this scenario once the network traffic exceeds any of the defined thresholds then it will send a signal to the Global SDN setup for mitigation action.

Auto Action in Global Setup: in this scenario, the Global SDN setup will have predefined thresholds for all Local SDN setups and in case any of them is exceed then an action will be triggered in the ISP level.

One major part of the proposed is the communication protocol between Local SDN setup and Global SDN setup, this protocol will facilitate exchanging information, status and action between local and global SDN setup, such protocol can be extended beyond the scope of Denial of Service Mitigation.

Table (2) shows the SDN to SDN messages types that can be exchanged between the Global SDN and Local SDN.

SDN to SDN communication protocol is core component in the proposed framework, Figure (3) illustrates the communication protocol between one Global SDN and multiple Local SDN and it is preferred to have separate line of communication between the local and global SDN, one of the proposed solution for such communication is data over 3G or LTE network.

The authentication process should be mutual between the Client and the Global SDN this to avoid any confidentiality or integrity security issues, in addition to that an Access Control mechanism can be deployed to grant privileges based on the authorization level, two privileges can be proposed in such context:

Read Access: This privilege will grant a read privilege so the client can read his related configuration and status on the Global SDN setup.

Read/Write Access: this will grant the client read and write privilege on his profile configuration on the Global SDN setup.

Table 2 SDN to SDN Messages type

Parameter	Description
Configuration	• Bandwidth Thresholds(Mbps) • Packets Per Second thresholds (PPS) • Asset IPs to be protected (in CIDR format) • Action (Rate limit, Block,etc)
Information/ Status	• SDN Status (Up/Down) • Configured Parameters • Attack alarms
Authentication	• Authentication Credentials to authenticate both parties to each other

Next scenario is an example for an implementation using the proposed solution, with Active Local SDN and Automatic Global Mitigation is ON.

Figures (4-6) demonstrate how the Local SDN is mitigating DDoS attack using Scrubbing Center, but still in case of massive DDoS attack which is might be greater than the local router or switch capability such protection will not be sufficient, therefore the client will need to prevent the attack in higher level (ISP level).

Figures (7-9) demonstrate how the Local SDN escalate DDoS with the help of Global SDN, in this stage the local client will signal the Global SDN server for the further protection, the Global SDN will send Flowspec message to

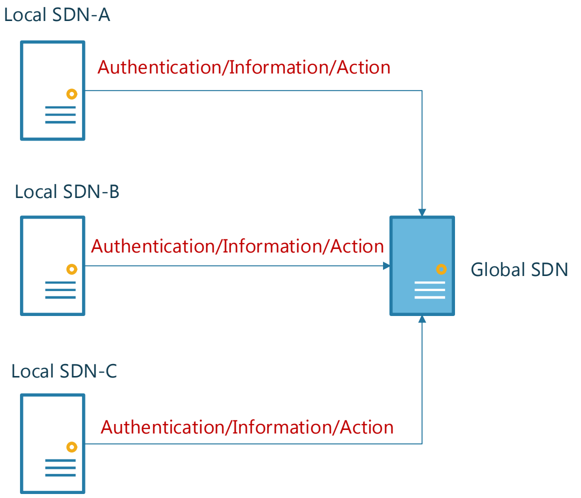

Local SDN-A
Authentication/Information/Action
Local SDN-B
Authentication/Information/Action
Global SDN
Local SDN-C
Authentication/Information/Action

Fig. 3 Communication between Local and Global SDNs

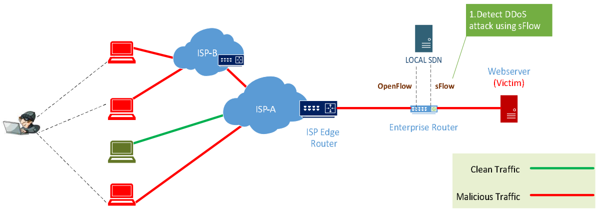


Fig. 4 Step (1) DDoS Detection

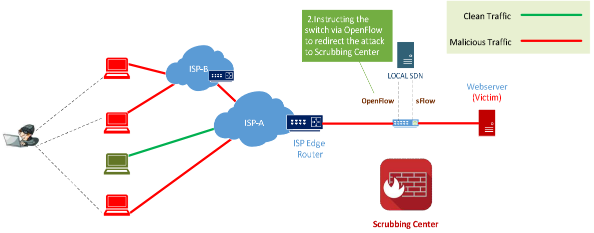


Fig. 5 Step (2) Deploy local redirection rule

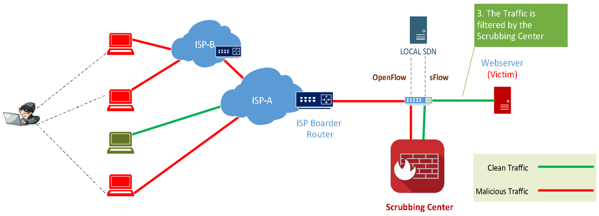


Fig. 6 Step (3) Filter the traffic using Scrubbing Center

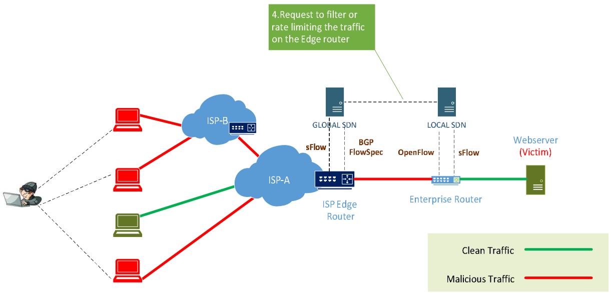


Fig. 7 Step (4) Send action signal to the Global SDN

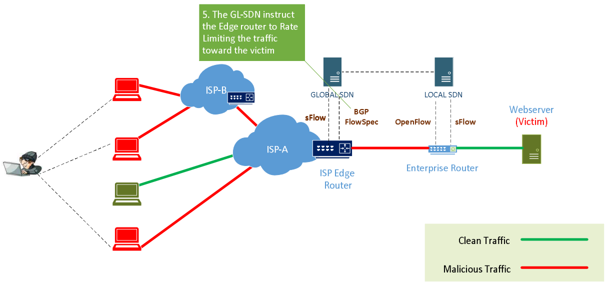


Fig. 8 Step (5) Send action to the Boarder Router

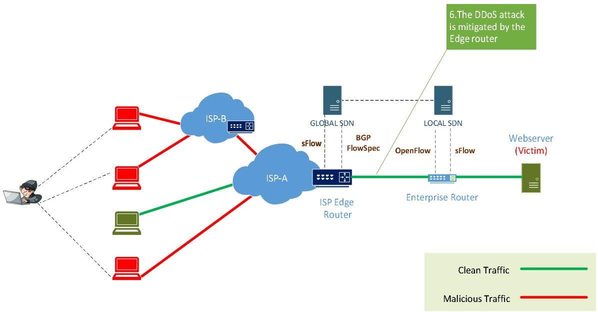


Fig. 9 Step (6) The DDoS attack is filtered bby the boarder router

the peered routers within the ISP to rate-limit the traffic toward the victim.

4. Framefork and security analysis

The effectivity of the proposed framework depends on the cooperation level between the Internet Service provider (ISP) and the enterprise entity, such cooperation will deliver many benefits, below are some of these benefits:

- Accurate detection with less false positive: Due to the data sharing concept between Local and Global SDN.
- Higher mitigation capacity: Considering that large scale attacks can be filtered in the ISP level.
- Global protection: using cyber intelligence based on Options reported attacks by the Locals Client this information can be used to provide proactive protection to other clients.
- Real Time Action Escalation: Due to the real-time synchronization an action can be deployed immediately in the ISP level.

Table (3) shows a comparison between the proposed framework and other traditional DoS mitigation solutions:

The Security of the proposed framework is major subject due to the fact that the Framework components have access to networking management components especially the Global SDN setup which has the global configuration and any security violation at that level might impact all ISP clients.

Below is a list of potential threats to the proposed framework:

- Unauthorized access
- Spoofing Local SDN identity
- Sniffing the communication between the Local and

Table 3 Comparison between DoS Mitigation

Solution	Deployment	Detection	Mitigation
ACL: Allow Specific IPs: Ports	- Easy in case of limited source and destination IPs/Ports - Manual Configuration	Required another solution for detection	- Effective but in case of large scale attack then it would - Require Manually deploying ACL on the ISP level
Source based Blackhole	- Easy in case of limited number of attacker IPs - Manual Configuration.	Required another solution for detection	- Effective in case of limited number of attack sources
Destination based Blackhole	- Easy - Manual Configuration.	- Required another solution for detection	- Effective but the access to the resource will be narrowed down
BGP Flowspec	- Easy but would require ISP to support Flowspec - Manual Configuration.	- Required another solution for detection	- Effective
The Proposed Framework	- Require deploying SDN setups in the customer and ISP network	- Effective - Real Time	- Effective - Real Time

Global SDN setup
- Man in the middle attack
- Denial of Service attack

In order to prevent spoofing SDN setup identity or unauthorized access to the setup identity whether it is targeting Local SDN setup or Global SDN setup a mutual authentication mechanism should be implemented. In order to protect the integrity and confidentiality of the proposed solution a strong encryption algorithm must be used this is will prevent any sniffing or Man in the Middle attacks.

Similar to the protected network the proposed setup is exposed to DoS attack in many scenarios, one potential scenarios e.g. flooding the SDN setup with spoofed requests, another scenario in case any of Local

SDN setup is exploited and managed by an attacker then it might be used to flood the Global SDN setup with actions or configurations updates.

In order to prevent these threats, it is recommended to have separate links with defined network Access List then it is recommended to have a validation mechanism in the Global SDN to filter unnormal requests and restrict the number of actions or configuration that can be pushed by any Local SDN in any interval of time.

One major component of the proposed framework is the communication protocol between the local and Global SDN setup which is used to exchange thresholds and actions between each SDN. As future work and continuation for this work, we will focus on this protocol from requirements and design perspective.

4. Conclusion

In this paper we have proposed a new Denial of Service detection and mitigation based on Distributed , the key element of the mentioned proposed framework is the collaborative feature between Local SDN and Global SDN which might be deployed in the ISP level, such cooperation and will facilitate efficient and focused monitoring in the ISP level which accordingly will reduce the false positive mitigation and will provide quick and effective jointly mitigation based on the severity and the size of DoS attack.

One major component of the proposed framework is the communication protocol between the local and Global SDN setup which is used to exchange thresholds and actions between each SDN in real time. As future work and continuation for this work, we will focus on this protocol from requirements and design perspective.

References

[1] Yeun, C.Y., Han, K., Vo, D.L., Kim, K., “Secure authenticated group key agreement protocol in the MANET environment,” information security technical report, Vol. 13, No. 3, pp. 158-164, 2008.

[2] Bariah, L., Shehada, D., Salahat, E., Yeun, C.Y., “Recent advances in VANET security: a survey,” In proceeding of the 82nd IEEE Vehicular Technology Conference, pp. 1-7, September 2015.

[3] Shehada, D., Yeun, C.Y., Zemerly, M.J., Al Qutayri, M., Al Hammadi, Y., Damiani, E., Hu, J., “BROSMAP: A Novel Broadcast Based Secure Mobile Agent Protocol for Distributed Service Applications,” Security and Communication Networks, Wiley, Vol. 2017, 3606424, 2017.

[4] Baek, J., Vu, Q.H., Jones, A., Al Mulla, S., Yeun, C.Y., “Smart-frame: A flexible, scalable, and secure information management framework for smart grids,” In proceeding of International Conference for Internet Technology And Secured Transactions, pp. 668-673, December 2012.

[5] Al Alkeem, E., Shehada, D., Yeun, C.Y., Zemerly, M.J., Hu, J., “New secure healthcare system using cloud of things,” Cluster Computing, Vol. 20, No. 3, Springer, pp. 2211-2219, 2017.

[6] Han, K., Yeun, C.Y., Shon, T., Park, J., Kim, K., “A scalable and 6.efficient key escrow model for lawful interception of IDBC based secure communication,” International Journal of Communication Systems, Vol. 24, No. 4, pp. 461-472, 2011.

[7] Gajparia, A.S., Mitchell, C.J. , Yeun, C.Y., “Supporting user privacy 7.in location based services,” IEICE transactions on communications, Vol. 88, No. 7, pp. 2837-2847, 2005.

[8] Konidala, D.M., Yeun, C.Y., Kim, K., “A secure and privacy enhanced protocol for location-based services in ubiquitous society,” In proceeding of IEEE Global Telecommunications Conference, GLOBECOM'04, Vol. 4, pp. 2164-2168, 2004

[9] Lu, Y., Wang, M.: An Easy Defense Mechanism Against Botnet-based DDoS Flooding Attack Originated in SDN Environment Using sFlow. In: ACM, New York (2016)

[10] Xiulei, W., Ming, C., Xianglin, W., Guomin, Z.: Defending DDoS attacks in software defined networking based on improved Shiryaev – Roberts detection algorithm. J. High. Speed. Networks. 22, 285-298, (2015)

[11] Trung, P.V, Huong, T.T, Tuyen, D.V, Duc, D.M, Thanh, N.H, Marshall, A.: A Multi-Criteria-based DDoS-Attack

Prevention Solution using Software Defined Networking. In: ATC, (2015)

[12] Buragohain, C., Medhi, N.: FlowTrApp: An SDN Based Architecture for DDoS Attack Detection and Mitigation in Data Centers. In: International Conference on Signal Processing and Integrated Networks, (2016)

[13] Xu, Y., Liu, Y.: DDoS Attack Detection under SDN Context. In: The 35th Annual IEEE International Conference on Computer Communications, (2016)

[14] Dharma, G., Muthohar, M.F, Prayuda, A.J.D., Priagung, K., Choi, D.: Time-based DDoS Detection and Mitigation for SDN Controller. In: APNOMS, (2015)

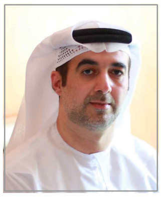
[15] SAHRI, N., OKAMURA, K.: Protecting DNS services from IP spoofing - SDN collaborative authentication approach. In: ACM, New York (2016)

[16] Lim, S., Ha, J., Kim, H., Kim, Y., Yang, S.: A SDN-Oriented DDoS Blocking Scheme for Botnet-Based Attacks. In: ICUFN, (2014)

[17] Dao, N., Park, J., Park, M., Cho, S.: A Feasible Method to combat against DDoS Attack in SDN Network. In: ICOIN, (2015)

[18] Li, J., Berg, S., Zhang, M., Reiher, P., Wei, T.: DrawBridge−Software-Defined DDoS-Resistant Traffic Engineering. In: ACM, 2014

저자소개

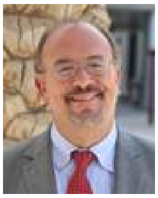


Ahmed Alshehhi

Received his M.Sc in Information Security from Khalifa University in Abu Dhabi, in 2016, he has more than 14 years' experience in Information Security, he had been working in Emirates Telecommunications Corporation for 10 years and he had become head of Security Planning, he has published many researches in Information Security and participated in many Security Projects.

Chan Yeob Yeun

Received his M.Sc. and Ph.D. in Information Security from Royal Holloway, University of London, in 1996 and in 2000, respectively. After that, he joined Toshiba TRL in Bristol. Then, he became a Vice President at LG Electronics, Mobile Handset R&D Center in 2005. He was responsible for developing the Mobile TV technologies and its security. He left LG Electronics in 2007 and joined at KAIST in Korea until August 2008 and moved to Khalifa University. He is currently serving as an Associate Professor of Electrical and Computer Department and an active member of Information Security Research Center. He currently enjoys lecturing M.Sc. in Information Security Courses at Khalifa University. He has published 28 journal papers, 71 conference papers, 2 book chapters and 10 international patent applications. He is also serving as several Editorial Board members of International Journals and a steering committee member of ICITST conference series and he is a senior member of the IEEE.



Ernesto Damiani

Joined KUSTAR as Chair of the Information Security Group and Program, and EBTIC as Research Professor. He is on extended leave from the Department of Computer Science, Università degli Studi di Milano, Italy, where he leads the SESAR research lab and is the Head of the Ph.D. Program in Computer Science. Ernesto's research interests include secure service-oriented architectures, privacy-preserving Big Data analytics and Cyber-Physical Systems security. Ernesto serves in the editorial board of several international journals; among others, he is the EIC of the International Journal on Big Data and of the International Journal of Knowledge and Learning. He is Associate Editor of IEEE Transactions on Service-oriented Computing and of the IEEE Transactions on Fuzzy Systems. Ernesto is a senior member of the IEEE and served as Vice-Chair of the IEEE Technical Committee on Industrial Informatics. In 2008, Ernesto was nominated ACM Distinguished Scientist and received the Chester Sall Award from the IEEE Industrial Electronics Society. Ernesto has co-authored over 350 scientific papers and many books.