Ph.D. Research Proposal

Doctoral Program in “Department Name”

Four Tiered Intrusion Detection and Prevention Model for SDN/NFV Assisted Ecosystem in 5G Communications

by

<Name of the Candidate>

<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>

I. INTRODUCTION / BACKGROUND

Intrusion Detection and Prevention System (IDPS) is an emerging security solution in almost all wireless networks. In particular, 5G is one of that, which faces severe security issues. For instance, SDN controller and switches are suffered by various kinds of attackers as DDoS, DoS, Man-in-the-Middle, and so on. In SDN, software based centralized controller is deployed in the control plane, whereas the data plane consists of huge network switches that frontward data packet. On the other hand, SDN controller has ability control/manage the behavior of the network devices and forward control commands and rules for large user flows. NFV is the way to virtualize network functionality and provide services. Particularly, network management is encouraged via specific Network Virtual Function (NFVs) [1], [2]. SDN/NFV is the most beneficial that mutually support 5G networks. There are six main challenges of SDN/NFV in 5G as follows:

- Performance monitoring
- Scalability
- Orchestration and Management
- Security
- Probability
- Heterogeneous Network

NFV enables key types such as service function chaining (SFC) and service personalization. In SDN, the centralized controller provides benefit to network management, but it causes serious security threats. In control plane, the controller will be affected DDoS attackers. Initiation of DDoS attacks in OpneFlow switches enabled controller will lead to huge amount of traffic by attackers in short duration [4].

TABLE.1. INTRUSIONS LIST

S.No	Security Attacks	Description
1	DDoS	Switches and controller resources could be target by the intruder. For example, intruder can bottleneck a controller-switch resource, which causes flow table overloading attack)
2	IP Spoofing	Impostors can study the particulars (IP address) of mobile users for retrieving applications from SDN controller. This type of impostors can create fake IP packets with spoofed IP address.
3	Flow Table Overloading	Attackers set goal for specific switch to overload the size of flow table, which lead to switch failures.
4	Control Plane Saturation	This type of intruders consume large amount of resources by sending packets concurrently
5	Host Location Hijacking	By details of host in controller, intruders can get the host current location.
6	Bandwidth Spoofing	Network flooding by intruders, which affects the legitimate user flows
7	Fraggle	This type of intruders send spoofed UDP packet to broadcast in the network.

8	SYN flood	In this type of attack, intruder can transmit SYN packets which tend to make the system busy and the particular service is absent for legitimate users.

On the other hand, large number of unmatched flows sent to the controller, processing legitimate flow request is not possible. Lightweight DDoS attack solution is required to be designed for multi-controller scenario [14]. The host location hijacking attack occurs which is controlled by SDN controller that evaluates the host location by examine the packet-in messages. SDN/NFV technology, controller can easily process VNFs traffic flows (how requests/traffic flows are routed?). The VNF characteristic functions are deep packet inspection and load balancing [11]. SDN/NFV enabled 5G network applied to IaaS cloud (Infrastructure-as-a-Service) and the function of NFV orchestrator can manage thousands of devices.

Artificial Intelligence plays significant role in Intrusion Detection and Prevention System, which covers machine learning and deep learning [5]. Considering network security have received particular attention where malicious attacks classified using machine learning algorithms such as neural network, support vector machine, adaboost, k-means++, and so on. Today, it will face with different challenges while detecting security attacks. Advantage from the combined SDN/NFV in 5G, it delivers security functionalities and also AI based security protection mechanisms are proposed to detect unknown security attacks from large volume of data. According to flow requests from users, outbreaks detected in SDN/NFV of 5G networks.

1.1 Research Outline & Scope

SDN/NFV has paying great attention in current insecure world. Especially, 5G environs consist of huge mobile users, devices and their communication is frequent. Research in this large integration is very few in terms of security and privacy. Further, those works are poor in terms of detection rate, false alarm rate and also energy consumption of 5G access points.

1.2 Research Objectives

The main objective of this research is to bring novel IDPS for wide range of attacks detection and mitigation over SDN/NFV with Cloud of 5G environment by means of Machine Learning and Deep Learning approaches.

1.3 Applications / Use cases

Several applications have need of IDPS. For instance, when sensitive request forward from the source to destination, it requires security. Such applications are follows,

- Web application logged in for organization
- Password application design
- Video conferencing by organization
- And also many more

II. RESEARCH GAPS

Most of the works limit their research in prevention. Due to lack of this, more overhead faces during intrusion detection. Still some intrusions are difficult to detect it that is follows.

- **DDoS / DoS:** Here, resources absent to illegal users which means it saves network busy with meaningless traffic. The amount of DDoS threats increased when large volume of requests contributing in Internet.
- **Malwares / Viruses:** Intruder code is executed to affect switches and controllers and such code will be possible to be used to read sensitive information or receive unauthorized access to the devices. Intruder can also control the devices after malware execution and it can utilizes those devices to launch attacks
- **Stealing/Theft Data:** Some devices are poorly endangered and confirmed by third-party. In such cases intruder can easily steal crucial and confidential information. Phishing or spoofing can be used to retrieve such sensitive information.

2.1 Common Problem Statement

It is very perplexing to make IDPS in SDN/NFV assisted cloud of 5G networks with use of AI. Now security provisioning is the major requirements recently have significant interest among researchers. Both internal and external attackers have exploited more security threats and issues for forwarding devices and their users. Many defense mechanisms based on SDN concentrated very few key concepts for attack detection and mitigation. IDPS based on SDN/NFV, cloud and 5G using ML or DL produces many advantages including security enforcement, quality of service (QoS) and virtual management.

2.2 Problem Definition

In [3] authors have focused on the mixture of SDN, NFV, cloud in 5G networks for user privacy. Initially, authentication is provided for users at access points using highly secured authentication and handover mechanism (HS-AOHM) for reducing the handover latency and thus user privacy is protected. Then authorized user packets are processed at dispatcher in which tree based switch assignment algorithm is presented to choose under-loaded switch. Entropy function is invoked at controller to mitigate DDoS attack. Arrived packets are further classified in controller using hybrid ANN with fuzzy logic.

Problems

- Secret key is generated using ECC which is fast algorithm, but produces small key size and hence attacker can easily guess secret user key
- For user password and secret key, G-OTP is created and watermarked. This process takes large time for authentication.
- Binary tree is proposed to assign packets. Herein searching for packets assignment requires $O(\log n)$ per individual search. It is relatively large for single packets assignment. However searching requires constant time i.e. $O(1)$.

Proposed Solutions

- Four Q Curve with QUARK is proposed which is combination of asymmetric and hashing for strong authentication

- Pseudoidentity is proposed which purpose is to reduce the timing in authentication

Authors in [4] have proposed machine learning algorithm for IDS using 5G - SDN. This machine learning based model pools security function in SDN- 5G. Hybrid Adaboost and K-means++ algorithm is combined for IDS. Source IP address (srcip), Destination IP address (dstip), Destination Port Address (dstport), Source Port Address (srcport), Duration and Protocol are used for packets classification.

Problems

- For given data Adaboosting algorithm is sufficient to obtain very high detection rate and also it is proved. Though, Adaboost algorithm has some difficulties are as follows. (a). Very difficult to implement in real-time, (b). Detection complexity increases for detection, and (c). Computation and time is expensive.
- Hybrid Adaboost and K-means++ algorithm is not the best combination algorithm for IDS since K-means++ has taken large computational time for intrusion detection.

Proposed Solutions

- SOM is unsupervised which classifies packets for intrusion detection. It does not difficult and it finds multiple stages
- In real-time and massive amount of input packets, it is very simple

Authors in [5] have proposed hybrid model using fuzzy logic and self-organizing maps (FSOMDM) in SDN Cloud. The proposed FSOMDM is an enhanced version of neural network that changes the neurons of the conventional Kohonen Neural Network via Modified Fuzzy-IF-THEN rules. From rules, normal and abnormal malicious packets are splits into two classes.

Problems

- The problems of this approach are limited control of classes and identities, and classes do not necessarily match information categories of classes and identifies.

Proposed Solutions

- For unknown packets, it can classify and environment learned in a random timer.

Authors [6] have focused on four dissimilar security attacks including network scanning, openflow flooding attack, switch compromised attack and ARP attack. These attacks will be mitigated on both data plane and control plane. To detect such attacks based on packet features, multiple-observations Hidden Markov Model (HMM) is proposed. Furthermore, Viterbi algorithm is used to find the network status and Baum-Welch algorithm is used to train the model.

Problems

- The drawback of this work is it only a first process towards security situation awareness in SDN and it is not adaptable for real time application scenario.

Proposed Solutions

- Any kind of complicated real-time application scenario, the proposed work will be suited.

Authors in [7] talked about the flow table of DDoS attack mitigation using queuing theory for DDoS attacks mitigation on SDN enabled cloud environment. The flow table overloading DDoS attack is mitigated. However, attackers can be exploited all the switches flow table space and thus forwards huge number of spoofed flow requests. For this reason, legitimate user requests become waiting stage or stops serving at switches. M/M/S/C Queuing model is presented wherein Poisson distribution is followed for arrival of new requests.

Problems

- This DDoS attack mitigation model consume lot of resources at both switch and the controller with the superabundant communication between the switch and the controller and also this leads to new big security threats in SDN including controller resource consumption attack and link saturation attack.
- M/M/S/C Queuing model may be hard to implement for large arrival user requests. This type of queuing model is time consuming and it does not provide quicker results.

- Nowadays lightweight DDoS attack solution is required in multi-controller scenario and also detection of DDoS attack under multi-controller scenario become complex

Proposed Solutions

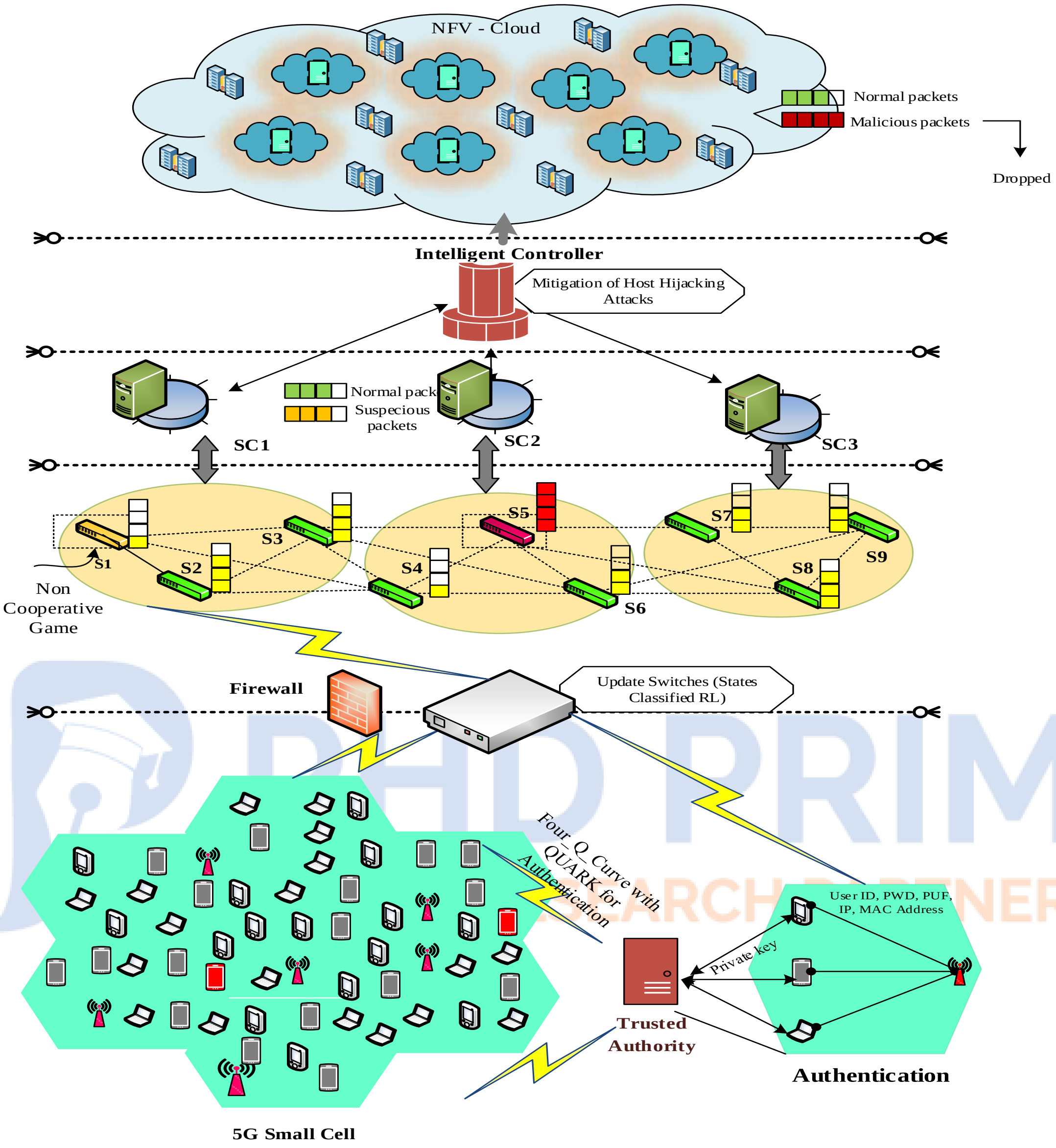
- The proposed proposes fast way to reduce the overhead in DDoS attack detection
- Multi-controller environment is tested for multi attacks detection.

III. RESEARCH CONTRIBUTIONS

To resolve the glitches stated in Section II, this research designed a novel four tiered IDPS in SDN/NFV assisted 5G network. The proposed network environs consists of two types of controllers (Intelligent Controller and Sub Controllers), Switches, NFV, Trusted Authority (TTP), 5G Base Stations (BS), Mobile Users / Devices and IDP Agents. There are four tiered IDPS in SDN/NFV assisted 5G network that are following:

- Tier 1 - Mobile Users
- Tier 2 – Data Plane
- Tier 3 – Control Plane
- Tier 4 – Virtualization

The proposed work detects intrusions in all tiers. Fig 1 shows the proposed system architecture.



Overall the proposed work detects and mitigates many security attacks as follows,

1. IP spoofing attack
2. Man in the middle attack
3. Flow table overloading attack
4. DDoS attack
5. Control plane saturation attack
6. Host location hijacking attack

Tier 1: Mobile Users

In this tier, mobile user authentication is performed using **Four-Q-Curve with Quark Algorithm**. When user enters into network, then user is registered their credentials to trusted authority. Here, user registered with ID, Pwd, MAC address and IP address. If user information is TRUE, trusted authority generates secret key, which is created using **Four-Q-Curve** algorithm. User generated secret keys are provided to BS by trusted authority. To mitigate IP spoofing attack, registration to trusted authority considers IP address of device. In 5G, IP address will be change. Further, QUARK algorithm used to hash all credentials in authentication. To mitigate IP spoofing 5G BS generate PseudoIdentity for user registration. User must retrieve the PseudoIdentity from 5G BS through user secret key.

Tier 2 – Data Plane

In this tier, flow table overloading attack is mitigated, which is employed in IDP agent. In game theory, IDP agent detects optimal switch for each flow processing. IDP agent is introduced to completely avoid flow table overloading attack with use of **States Classified Reinforcement Learning**. This IDP agent classifies switches into three states as under loaded, overloaded and idle. This is classified by five features as

- Packet Drop Rate
- Packet Forward Rate
- Duplicate Packet Rate
- Packet Received Rate
- Packets Time Interval

Based on the usage of flow table, underloaded switch will be selected for sharing over loaded flows. IDP agent tackles the network from flow table overloading attack.

Tier 3 – Control Plane

An intelligent controller (IC) and subcontrollers (SCs) are deployed in this plane. In ICs, packets are handled and categorized based on packet features. In SC, packets are further classified into two types: normal packets and suspicious packets using **Deng Entropy function.** Then normal packets are forwarded to cloud via IC. In IC, host hijacking attack is alleviated by verification of MU MAC, IP Address, and Location Path ID (MU connected switch).

Feature Name	**Explanation**
Service Type	Requested service of network over destination e.g. http
Duration	Switch alive time (Nanoseconds)
Flags	It states the connection status (normal/error) If normal flag, then it is 0 If error flag, then it is 1
TTL	Time to live
Packet Count	Volume of bytes in each flow
Trx_Pkts	Volume of packets transmitted from Port No
Byte Count	Volume of bytes in each flow
RRT	It is reply time for given response
Nrx_Pkts	Volume of packets received from Port No
Tx Bytes	Volume of bytes transmitted from Port No
Rx Bytes	Volume of bytes received from Port No
Packet Header Length	Packet header data size
Epoch Time	Time duration required for 1 Epoch completion
Port No	It is the port number for switch
Protocol Used	Type of protocol used e.g. TCP or UDP

Tier 4 – Virtualization

In this tier, suspicious packets are forwarded to NFV for further classification into Normal Packets and Malicious Packets using **Fast Self Organizing Map with Multi Operations (FSOM-MO)**. The proposed **FSOM-MO** discovers DoS/DDoS attack.

Performance Evaluation

Finally, the proposed work shows better performance in following performance metrics,

- **Holding Time**
  - Number of mobile users
  - Number of malicious users
- **Switch failure Rate**
  - Number of mobile users
  - Number of malicious users
- **Detection Rate**
  - Number of mobile users
  - Number of malicious users
- **Packet Loss Rate**
  - Number of mobile users
  - Number of malicious users
- **Delay**
  - Number of mobile users
  - Number of malicious users
- **False Alarm Rate**
  - Number of mobile users
  - Number of malicious users

IV. RESEARCH NOVELTIES

IDP agent is one of the best solutions to address flow table overloading attack. And each tier detects and mitigates most severe attacks. The following research questions (RQ) are addressed in this work.

RQ1: How to defend against attackers in SDN/NFV 5G environment?

RQ2: Where & How high detection rate reached and how attacks detected while large numbers of flow requests are transmitting to IC and SCs?

RQ3: How can reduce the usage of CPU of SDN controller since it cause single point of failure?

V. PREVIOUS WORKS & LIMITATIONS

In this section, what are the works have been previously released in the field of IDPS for SDN/NFV enabled cloud of 5G networks.

PAPER 1

Title – EASM: Efficiency-aware Switch Migration for Balancing Controller Loads in Software-Defined Networking

Concept –

In this paper, EASM (Efficiency-aware Switch Migration) is proposed to balance the load of each controller and improve migration efficiency. EASM considers the migration cost and load balancing rate to migrate switches in optimal way. It minimizes controller response time up to 21.9% and increases controller throughput by 30.4% with large volume of traffic.

Limitations

- Security is not considered while migrating switches to another controller
- EASM is difficult in large scale environment

PAPER 2

Title – CIPA: A Collaborative Intrusion Prevention Architecture for Programmable Network and SDN

Concept –

In this paper, DDoS attack detected using worm spreading and scanning method called CIPA for various network sizes. The proposed CIPA method works well in both real world and simulation environment. It achieve high detection rate, which increases the efficiency of CIPA method. On the other hand, the false positive rate of CIPA is less than 4% and also computation and communication overhead of CIPA method become low.

Limitations

- CIPA works well, but it is only scalable in a small real-world environment

PAPER 3

Title – A DDoS Attack Detection Method based on SVM in Software Defined Network

Concept –

This paper concentrated on the detection of DDoS attack in SDN. The proposed attack detection method addressed challenges on existing solutions such as deep learning algorithm, neural network model, etc. In this DDoS attack is detected using SVM classification algorithm and attack classified by 6-tuple characteristic values of the flow table in switch.

Limitations

- Attack detection rate is high but low false alarm rate is large for normal data flow

PAPER 4

Title – Duo: Software Defined Intrusion Tolerant System using Dual Cluster

Concept –

In this paper, a new intrusion tolerant system (ITS) is proposed i.e. Duo. There are two types of servers are created in Duo: Servers with short exposure time (Gray server) and servers with long exposure time (White server). SDN/NFV technology will be adopted into these two different servers where traffic is classified into suspicious and benign according to packet features. The proposed Duo method addressed two major issues such as packet classification (benign/suspicious/malicious) and proper resource utilization even the volume of each type of traffic can be changed.

Limitations

- In SDN/NFV based ITS, user privacy will need to be considered

PAPER 5

Title – Data Driven Intrusion Detection System for Software Defined Networking Enabled Industrial Internet of Things

Concept –

In this paper, intrusion detection system is presented for SDN in IIoT (Industrial Internet of Things) environment. The proposed method has two phases: training phase and testing phase. In training phase, normal data is fed into network and network connected with devices. Then payload extract is promoted for critical components. Finally specific flow rules created and deployed in controller. In testing phase, incoming data forward to switch, where in rules are matched. It finds the data flow is benign or malignant based on features.

Limitations

- Flow rules are generated by human, which increases human effort
- Intrusion detection process does not considered more critical factors of data flow
- It is only suitable for industrial automation application.

PAPER 6

Title – Early Detection of DDoS Attacks Against Software Defined Network Controllers

Concept –

This paper addressed the major problem of SDN i.e. Single Point of Failure/Centralized Controller Control and Management. This paper designed with two security goals includes (1) lightweight DDoS attack detection solution, which consume small amount of resources and (2). Controller has global view to monitor and control the network and prevent from DDoS attackers. DDoS attack detection is implemented by entropy function.

Limitations

- Entropy value may not be change over time so that the whole network cannot prevent from DDoS attacks
- The proposed solution consumes less amount of resources, but the proposed approach is based on the centralized controller solution
- The proposed approach does not mitigate attacks since it only detect attack.

PAPER 7

Title – Effective Software-Defined Networking Controller Scheduling Method to Mitigate DDoS Attacks

Concept –

In this paper, controller scheduling method is introduced in which multi-queue is deployed. The proposed scheme has many advantages due to time slice allocation scheme in controller for scheduling flow requests at multi-queue. Controller will schedule several flow requests from each switch. Other than controller, SDN switches suffered by large volume of traffic load which reflects controller failure.

Limitations

- One major disadvantage is the Security. We have all the flow requests control and management in centralized controller. If the controller compromised, the whole network can be easily controller by attackers.

PAPER 8

Title – LineSwitch: Tackling Control Plane Saturation Attacks in Software-Defined Networking

Concept –

In this paper a new solution called LineSwitch is proposed to tackle a type of denial-of-service attack also referred as control plane saturation attack. A new solution is concentrated in data plane to mitigate control plane saturation attack and also it tackles SDN from new security threat called buffer saturation attack. Experimental results show that the LineSwitch scheme reduced 30% of time overhead than other approaches

Limitations

- Single point of failure due to centralized remote controller in control plane

PAPER 9

Title – Mitigation of Flooding and Slow DDoS Attacks in a Software-Defined Network

Concept –

This paper mitigates DDoS attacks (slow and flooding) in a SDN. Initially, the attack is observed and then attack is classified to determine the matching using defense scheme. Thirdly, attackers identified and blocked from the network to mitigate such flooding and slow DDoS attack.

Paper 10

Title – SecSDN-Cloud: Defeating Vulnerable Attacks through Secure Software-Defined Networks

Concept –

In this paper, authors designed secure cloud architecture in SDN that consists of the following process: user authentication, routing, third-party monitoring and attack resistance. The aim of this paper is to make the secure SDN architecture that resolve harmful security attacks such as Byzantine attack, Control Plane Saturation attack and Flow Table Overloading attack. User authentication is performed using digital signature algorithm called chaotic secure hashing. Then routing is implemented based on modified version of particle swarm optimization algorithm (PSO), which is presented to improve the QoS. SDN controllers are allocated to switches by integrating an enhanced genetic algorithm with modified cuckoo search algorithm.

Limitations

- The first flow request of a packet will lead to a larger latency since controller determines the shortest path among switches and deploys the rule for given flow request

PAPER 11

Title – A DDoS Attack Detection and Mitigation with Software-Defined Internet-of-Things Framework

Concept –

In this paper, DDoS attack is detected and mitigated in combined SDN enabled IoT networks. The proposed approach includes pool of SDN controllers, switches combined with a gateway and number of devices. To detect and mitigate DDoS attack in SDN-IoT, the cosine similarity is computed for every packet-in message. The proposed approach will be easily adaptable for heterogeneous IoT devices.

Limitations

- DDoS Attack detection and mitigation is not effective since it is only used cosine similarity, which is not sufficient for attack detection.

PAPER 12

Title – HYPER: A Hybrid High-Performance Framework for Network Function Virtualization

Concept – NFV provides the potential for improving both service delivery flexibility and reduction of costs using VNFs. The HYPER is proposed to obtain the best performance and flexibility for supporting VNFs. On the one hand, SLA aware service chaining algorithm is proposed to produce the large functional and performance requirements for service subscribers. This performance aware VNF placement algorithm is used to optimize efficiency of resource utilization while placing VNFs.

PAPER 13

Title – Towards Bayesian-based Trust Management for Insider Attacks in Healthcare Software-Defined Networks

Concept – In this paper, authors have focused on the determination of insider attackers in SDN for healthcare application networks. To find insider attackers, trust is computed and managed using Bayesian inference, wherein unauthorized devices are identified and excluded in SDN. In this work authors surveyed and obtained health records in 12 healthcare hospitals in China, Hong Kong and Singapore. The proposed trust-based approach is robust against malicious devices and also it does not provide service request response for any malicious device.

Limitations

- The proposed approach require further improvement to attack detection rate and it does not support for large environment

BIBLIOGRAPHY

Cabaj, K., Gregorczyk, M., Mazurczyk, W., Nowakowski, P., & Żórawski, P. (2019). Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System. Security and Communication Networks, 2019, 1–22.

Zhang, H., Cai, Z., Liu, Q., Xiao, Q., Li, Y., & Cheang, C. F. (2018). A Survey on Security-Aware Measurement in SDN. Security and Communication Networks, 2018, 1–14

Abdulqadder, I., Zou, D., Aziz, I., Yuan, B., & Dai, W. (2018). Deployment Of Robust Security Scheme In SDN Based 5G Network Over NFV Enabled Cloud Environment. IEEE Transactions on Emerging Topics in Computing, 1–1.

Li, J., Zhao, Z., & Li, R. (2018). Machine learning-based IDS for software-defined 5G network . IET Networks, 7(2), 53–60.

Pillutla, H., & Arjunan, A. (2018). Fuzzy self-organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing. Journal of Ambient Intelligence and Humanized Computing.

Fan, Z., Xiao, Y., Nayak, A., & Tan, C. (2017). An improved network security situation assessment approach in software defined networks. Peer-to-Peer Networking and Applications.

Bhushan, K., & Gupta, B. B. (2018). Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. Journal of Ambient Intelligence and Humanized Computing.

Hu, T., Lan, J., Zhang, J., & Zhao, W. (2018). EASM: Efficiency-aware switch migration for balancing controller loads in software-defined networking. Peer-to-Peer Networking and Applications.

Chen, X.-F., & Yu, S.-Z. (2016). CIPA: A collaborative intrusion prevention architecture for programmable network and SDN. Computers & Security, 58, 1–19.

Ye, J., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). A DDoS Attack Detection Method Based on SVM in Software Defined Network. Security and Communication Networks, 2018, 1–8.

Lee, Y., Lee, S., Seo, H., Yoon, C., Shin, S., & Yoon, H. (2018). Duo: Software Defined Intrusion Tolerant System Using Dual Cluster. Security and Communication Networks, 2018, 1–13.

Madhawa, S., Balakrishnan, P., & Arumugam, U. (2018). Data driven intrusion detection system for software defined networking enabled industrial internet of things. Journal of Intelligent & Fuzzy Systems, 34(3), 1289–1300.

Mousavi, S. M., & St-Hilaire, M. (2017). Early Detection of DDoS Attacks Against Software Defined Network Controllers. Journal of Network and Systems Management, 26(3), 573–591.

Yan, Q., Gong, Q., & Yu, F. R. (2017). Effective software-defined networking controller scheduling method to mitigate DDoS attacks. Electronics Letters, 53(7), 469–471.

Ambrosin, M., Conti, M., De Gaspari, F., & Poovendran, R. (2017). LineSwitch: Tackling Control Plane Saturation Attacks in Software-Defined Networking. IEEE/ACM Transactions on Networking, 25(2), 1206–1219.

Thomas Lukaseder, Shreya Ghosh, Frank Kargl (2018), Mitigation of Flooding and Slow DDoS Attacks in a Software-Defined Network, Cryptography and Security

Abdulqadder, I. H., Zou, D., Aziz, I. T., Yuan, B., & Li, W. (2018). SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks. IEEE Access, 6, 8292–8301.

Yin, D., Zhang, L., & Yang, K. (2018). A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework. IEEE Access, 6, 24694–24705.

Sun, C., Bi, J., Zheng, Z., & Hu, H. (2017). HYPER: A Hybrid High-Performance Framework for Network Function Virtualization. IEEE Journal on Selected Areas in Communications, 35(11), 2490–2500.

Meng, W., Choo, K.-K. R., Furnell, S., Vasilakos, A. V., & Probst, C. W. (2018). Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks. IEEE Transactions on Network and Service Management, 15(2), 761–773.