International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol.10, No.1, 2023, pp.14-19.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Enhancing Network Security by using SDN Algorithm in Cloud Computing

R. Balaji [a], A. Deepakkumar [b], G. Prabhu [c], P. Thinakaran [d], S. Gowtham [e]

[a] *Final Year of B.Tech. – Information Technology, K.S.R. College of Engineering (Autonomous), Tiruchengode, Tamil Nadu, India.*

[b] *Final Year of B.Tech. – Information Technology, K.S.R. College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India.*

[c] *Final Year of B.Tech. – Information Technology, K.S.R. College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India.*

[d] *Final Year of B.Tech. – Information Technology, K.S.R. College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India.*

[e] *Assistant Professor, Department of Information Technology, K.S.R. College of Engineering (Autonomous) Tiruchengode, Tamil Nadu, India. Email: gowthams@ksrce.ac.in*

Abstract

Software Defined Networking (SDN) gives controllers and their applications the unmatched capacity to have thorough association detectable quality and versatile association programmability, thus enabling new developments in network shows and applications. One of the key benefits of SDN is its consistently assembled control plane, which provides the entire association with recognisable quality and is what different SDN applications rely on. We provide additional attack routes that are novel for the composition and unique to SDN, which seriously undermine this basis. Our new assaults are essentially the same as parodying attacks in legacy associations (such as an ARP hurting attack), but with significant differences in how current SDN operates significantly differently from legacy associations. The association geology data, a key building component for focus SDN sections and topography cautious SDN applications, can be successfully damaged by the productive attacks. The upper-layer OpenFlow controller organisations and applications may be completely duped by the harmed organisation detectable quality, leading to authorised taking, organisation rejection, or man-in-the-middle assaults. Our analysis demonstrates that every major SDN controller in use today—including Floodlight, Open Daylight, Beacon, and POX—is vulnerable because they depend on Network Topology Poisoning Attacks.

Keywords: Network Security, SDN (Software-Defined Networking), Cloud Computing, Virtualization, Firewall, Network Monitoring.

DOI: 10.71086/IAJSE/V10I1/IAJSE1003
Received: 14 December 2022/Revised: 13 January 2023/Accepted: 17 February 2023/Published: 30 March 2023

Introduction

Software Defined Networks

Software Defined Networking (SDN) has evolved as another organization viewpoint to advance the hardened organization foundation by separating the control plane from the information plane (e.g., switches), exactly as delivering comprehensive organization perceivability and adaptable programmability. As the organization's brain, an SDN regulator gives clients an exceptional tool to organise and manage the business using their own apps on the regulator's centre services. * The first two creators contribute equally to the project. SDN, specifically its well-known recognition OpenFlow1, has been increasingly used in academic settings as well as in accredited creative organisations.

From that point on, several application scenarios—from ground network expansion to cloud network virtualization and data center network improvement—were taken into consideration and delivered. Since the regulator is at the core of SDN engineering, if the OpenFlow regulator exhibits any real flaws in its strategy or execution, the entire organisation might be completely overthrown by aggressors. We examine network geography administrations/applications of the common OpenFlow regulators and identify a few new vulnerabilities that an attacker may try to exploit to damage the organisational geography data in OpenFlow organisations.

One of the main benefits of SDN over traditional organising techniques is the perceivability throughout the whole organisation. The geographical data is accepted to most regulation centre administrations and upper-layer applications, such as those identified with bundle directing, portability following, and organisation virtualization and improvement, as it serves as an essential building block for network administrators. However, if such fundamental organisational geography data is compromised, all the critical organisational services would be adversely affected right once, leading to catastrophic problems. For instance, it is possible to manipulate the guiding administrations and programmes inside the OpenFlow regulator to implement a dark opening path or man-in-the-middle attack.

Shortest Path on SDN Environment

Private broadband usage is growing significantly, widening the gap between costs and revenues for Internet specialist cooperatives (ISPs). In the meanwhile, the proliferation of Internet-enabled devices is impeding access to organisations, distorting end-user experiences, and affecting content providers' adaption. In this study, we offer a different architecture in which the content provider, using open APIs supported by software defined networking (SDN), explicitly signals rapid and moderate route requirements to the ISP on a per-stream basis. Our initial goal is to create an architecture that supports this theory, arguing that it benefits consumers (better customer experience), ISPs (two-sided money), and content providers (fine-grained control over peering plan). Our next commitment is to test our theory using a real sample of more than 10 million streams to demonstrate that the use of dynamic fast tracks can almost completely eliminate the degradation of video stream quality and that the use of moderate paths for large-scale exchanges can significantly reduce the time it takes for a page to load. In order to demonstrate the viability and performance benefits of our technique, we will construct a fully functional model of our framework using open-source SDN components (Open stream switches and POX regulator modules) and instrumented video/document move workers. Our proposal is a first step towards the long-term goal of recognising quality network administration that is valuable to customers, ISPs, and content providers on an equal footing.

FIXED-LINE Internet Service Providers (ISPs) are increasingly dealing with a commercial dilemma as private information usage continues to grow at a rate of 40% per year, driving up the cost of the infrastructure to provide the growing traffic volume. But despite this, income growth is just at 4% annually, mostly because to "level rate" evaluating. In an effort to close this growing gap between cost and revenue, ISPs have tried limiting some services (like distribution), which sparked backlash and led to the passage of "internet fairness" legislation. They now routinely impose use restrictions, which can stifle the delivery of creative content and services. It is becoming increasingly apparent that changing the course of action that allows ISPs to exploit the assistance quality measurement (along with data transfer capacity and download quantity) to separate their contributions and take advantage of new revenue opportunities is necessary to ensure the practical development of the Internet biological system.

Objectives

The main goals of the tasks will be discussed next.

Then, we look at the defences against Network Topology Poisoning Attacks and introduce Topo Guard, a new security feature for SDN controllers that provides continuous and scheduled location of Network Topology Poisoning Attacks.

Our analysis of a Topo Guard model execution in the Floodlight regulator demonstrates that the safeguard arrangement may successfully secure organisation geography while having a little impact on regular OpenFlow regulator operations.

Related Work

A discussion regarding who can manage the Internet traffic that enters our houses has been secured by policy makers, ISPs, and substance providers in this administrative work [1] by Yiannis Yiakoumis. In this essay, we argue that the client, not the ISP or the drug provider, should decide how traffic to and from the house is prioritised. Home clients focus on their preferences the most, and if they can effectively convey these preferences to the ISP, both parties will be in a good position. To put the theory to the test, we created a model that enables customers to convey high-level preferences that are intended to be utilised as organisational controls. Home businesses are an essential component of the modern household, and as the number of connected devices and programmes grows, so do our sensitivity to the nature of our home Internet connection. We predict that the network will be responsive, speedy, reliable, and always on. Simply said, we don't need the company to slow down traffic on the home-use applications. With video real-time, video chat, VoIP, gaming, and cloud-based reinforcement now being commonplace, we put increasing demands on our home organisation. The amount of traffic on home organisations has increased by 50% in the last year (from 7 GB per month to 10 GB). Our apps frequently cause snarls and poor customer experiences as they compete with one another for last-mile connections. Although Internet service providers (ISPs, delivering link or DSL) have made great strides in the transfer speed delivered to the house, they still struggle with how to split the available bandwidth among clients' applications. Recently, several ISPs have introduced dubious information cap designs and blocked traffic-critical applications, ignited controversy and igniting fears that ISPs may try to coerce the applications we use. Yiannis Yiakoumis has suggested a solution in this administrative job [2]. Home organisations are well-known, although they struggle with a number of fundamental problems: Broadband services are expensive to deliver, and it is unclear how the cost can be split among a few professional co-ops; (ii) home services are more difficult to manage as we connect more devices, use new applications, and rely on them for entertainment, correspondence, and work; (iii) it is common for home services to be improperly managed, unreliable, or outright broken; and (iv) it is unclear how home services will consistently improve. In this essay, we suggest eliminating home organisations as a strategy for resolving these problems. Cutting serves as a component that enables diverse specialised co-ops to share a common framework and supports multiple cost-sharing strategies and plans of action. We suggest four requirements for cutting home organisations: the ability to adjust and improve a cut's behaviour, the ability to change and improve transfer speed and tra_c disconnection between cuts. We look into how these requirements enable cost-sharing, the outsourcing of the board of home organisations, and the ability to adjust a cut to provide better support. Finally, we show an early version that we are distributing to families. A cutting-edge family must have access to broadband and be organised inside the home. Numerous household appliances are connected to the Internet, and high-bandwidth Internet services like real-time video and audio, professional video conferencing, file sharing, and reinforcement are now commonplace. However, despite the widespread interest in broadband and the long history of use of home WiFi, home businesses still encounter a number of fundamental issues.

Jon Matias has offered a solution in this desk work [3][8][9]. The sharing of access framework at a later stage in the creation of access networks creates an environment that fosters healthy competition among specialised organisations. Such a situation is currently being advanced by administrative viewpoints or CAPEX reserve money. The positive input circle includes clients, expert co-ops, and organisation administrators by adding absence of prejudice. Another layer 2 approach for Neutral Access Networks is used by the NANDO project. This NAN proposal includes a prefix-based transmitting mechanism (Ethernet-PF), a secured launch of services, and a component for organisation administrator choice. For its configuration, the Open Flow innovation was used. The stream table of a switch, which controls the sending cycle, can be handled or modified by an external substance (regulator) using the Open Flow protocol. The primary focus of this work is on illuminating the NANDO scenario and the key Open Flow execution nuances. The constructed regulator and its operational model, which includes various agent models, are also presented in detail. In a circumstance when several administrators share a comparable real framework for administration conveyance, the beneficial attainability of NANDO is finally authorised [10][11].

Alok Kumar has advocated that WAN transmission bandwidth remain a required asset that is financially unfeasible to significantly overprovision in this administrative task [4]. As a result, it is crucial to distribute the cap in accordance with administrative requirements and in light of the progressive estimation of further designation. For instance, there may be a high demand for one service to get 1 Gb/s of transfer speed, but after this distribution has been reached, the demand may gradually decline significantly in favour of other administrations. We propose the design and implementation of Bandwidth Enforcer (BwE), a global, multi-leveled data transmission portion foundation,

motivated by the belief that individual streams with ûxed requirement may not be the best justification for data transfer capacity allocation. BwE supports A global perspective on transmission capacity and disappointment conditions is represented by the following: I) administration level transfer speed portion following focused on transmission capacity capacities where a help can address a discretionary assortment of streams, II) autonomous distribution and assignment approaches as per client-characterized chain of command, III) multi-way sending typical in rush hour gridlock designed organisations, and IV) a focal managerial highlight. BwE has long advocated for more efficient use of transmission capacity and simpler administration.

Carlee Joe-Wong, in this desk work [5], has offered Customers spread out their use of transmission capacity across time when different prices for Internet access are charged at various times. The questions are: Is it feasible and how much benefit might it provide? Using both a static meeting level model and a unique meeting model with stochastic appearances, we provide an effective method to calculate the expenditure limiting time-subordinate expenses for an Internet specialist co-op (ISP). A significant advancement is choosing the improvement issue's representation such that the ensuing details are computationally doable for large-scale problems [6]. Next, we give reproductions that depict the limitations and uses of time-subordinate valuation. These results show that ideal charges, which "reward" customers for agreeing to meetings, typically correlate with requests over time, and that fluctuating fees based on ongoing traffic assessments may significantly reduce ISP costs [7]. The amount of traffic that is even out over time depends on the meetings' capacity to alter time, the ISP's cost structure, and the amount of traffic that is not subject to time-related expenses. Finally, we demonstrate the implementation of our framework, known as TUBE, and the experimentation with concept verification.

Proposed Methodology

We investigate potential protective strategies for Topo Guard (Topology Guard) to mitigate such assaults. We point out that it is challenging to simply use static setup to address the issue (such as using static ARP section for has or the port security feature for changes to address ARP harming assaults), as it requires time-consuming and error-prone manual labour and isn't appropriate for managing organisational elements, which is a significant development of SDN. We suggest Topo Guard, additional security addition to the present Open Flow regulators to provide programmed and continuous location of organisation geography misuse, in order to more easily change the security and usability in this work. Topo Guard analyses precondition and postcondition utilising SDN-explicit highlighting to validate the validity of host movement and alter port property to thwart the Host Location Hijacking Attack and the Link Fabrication Attack.

Allocation of Traffic Across Multiple Routing Paths

As lossy organisation stream enhancement problem, this module is used to allocating traffic across several directing methods while keeping position in mind. Using portfolio determination hypothesis, which enables each organisation hubs to locally depict the position effect and aggregate this data for the source hubs, we map the improvement problem to that of resource allocation. The SDN/Open Flow Topology Management Service is where we do the majority of our security research. We have specifically discovered new vulnerabilities in eight of the current standard SDN/Open Flow regulators' Device Tracking Service and Link Discovery Service.

Characterizing the Impact of Poisioning

For a source hub to include these assessments into its traffic designation, the organisation hubs in this module will assess and represent the impact of position. It is important to evaluate the effect of position on transmissions across each link before a source hub joins the position sway in the rush hour jam distribution issue. However, the adjacent gauges need to be continuously updated in order to pick up the mobility of the jammer and the distinctive effects of the location attack. We suggest Network Topology Poisoning Attacks to take advantage of the flaws we have identified. We demonstrate the viability of those assaults using an SDN testbed and a Net Beans-like environment.

Effect of Jammer Mobility on Network

The maximum connection number using min-max planning that can send absurd connections is shown in this module's limit. When a source is creating information with a high bundle convey rate, the information should be conveyed as soon as possible. If the source hub becomes aware of this effect, the amount of traffic may be altered to reduce the delivery proportion on each route, which will lead to route recovery.

Estimating End-to-End Packet Success Rates

The bundle accomplishment rate acts as a guiding indicator for the connections; therefore, in order to determine the best traffic allocation, the source must evaluate the feasible start to finish parcel achievement rate. When compared to the update hand-off duration, estimating the total time required to send bundles from all sources to the related target is unimportant. We investigate the defence area and provide programmed moderation techniques against Network Topology Poisoning Attacks, along with a prototype defence system, Topo Guard, currently implemented in Floodlight but easily transferable to other regulators. According to our analysis, the Topo Guard just adds unnecessary execution overhead. The trusted expert in a PKI allocates various benefits to business clients on behalf of the business owner. Not with standing, the organization proprietor may, for different reasons, imitate network clients to spread information things.

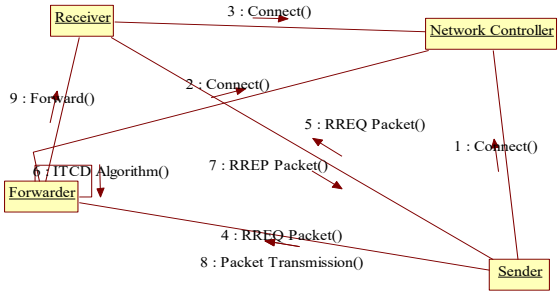


Fig. 1: Overall Architectural Diagram

Experimental Setup

The execution seasons of a few important Topo guard SDN operations are shown in the table. For instance, on a 1.8-GHz laptop computer, the execution timings for the framework instatement stage and marking a random 20-byte message (i.e., the yield of proposed computation) are, respectively, 1.608 and 0.6348 ms.

Table 1: Performance Calculation

Time	System Initialization	IP-Link Fabrication Attacks	The certificate generation (i.e., signing a 20 byte message)
Time (CPU = 1.8 GHz) (µs)	1608.0	1576.31	634.8
Time (CPU = 2.6 GHz (µs)	1111.3	1092.12	435.4
Time (CPU = 3.1 GHz) (µs)	931.1	915.18	372.3

Table: Running Time for each Topo Guard SDN Basic Protocol Phase, Except the Phase for Sensor Node Verification

Consequently, whenever proposed Topo guard SDN is utilized, producing a client endorsement or marking a message takes 0.6348 ms on a 1.8-GHz Laptop PC.

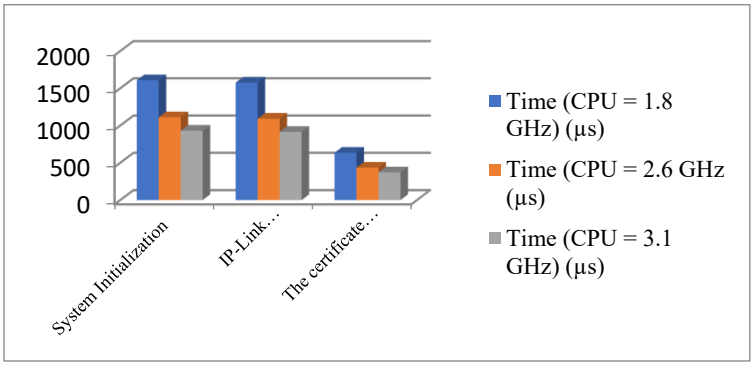


Fig. 2: Graphical Representation Performance Calculation

Conclusion

The steering of the Poisoning Network has been designed in a very organised manner, which is reducing the traffic's

potential for subsequent incidents. The code is done better since it is more logical and adaptable. By using a traffic allocation plan that is poison-aware, it is possible to evaluate the effects of shifting organisational and convention borders in order to observe presentation patterns. We are particularly interested in how the update transfer period and the greatest number of directing routes will affect how the flow allotment is shown.

References

Frink, D. D., & Klimoski, R. J. (1998). Toward a theory of accountability in organizations and human resources management. In G. R. Ferris (Ed.), *Research in personnel and human resources management (Vol. 16, pp. 1–51).* JAI Press.

Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103(1),* 14–76.

Matías, J., Jacob, E., Toledo, N., & Astorga, J. (2011). Towards neutrality in access networks: A NANDO deployment with OpenFlow. *In Proceedings of the 17th European Conference on Networks and Optical Communications (NOC 2011)* (pp. 7–12). IEEE. https://doi.org/10.1109/NOC.2011.5970502

Kumar, A., Amarandei-Stavila, M., Robin, M., Siganporia, A., Stuart, S., Vahdat, A., Jain, S., Naik, U., Raghuraman, A., Kasinadhuni, N., Zermeno, E., Gunn, C., Ai, J., & Carlin, B. (2015). BwE: Flexible, hierarchical bandwidth allocation for WAN distributed computing. *ACM SIGCOMM Computer Communication Review, 45(4),* 1–14. https://doi.org/10.1145/2829988.2787478

Joe-Wong, C., Ha, S., & Chiang, M. (2011). Time-dependent broadband pricing: Feasibility and benefits. 2011 31st *International Conference on Distributed Computing Systems*, 288–298. https://doi.org/10.1109/ICDCS.2011.81

Danphitsanuphan, P. (2011). Dynamic bandwidth shaping algorithm for Internet traffic sharing environments. *Lecture Notes in Engineering and Computer Science, 2190,* 1386–1391.

Laoutaris, N., Sirivianos, M., Yang, X., & Rodriguez, P. (2011). Inter-datacenter bulk transfers with NetStitcher. *In Proceedings of the ACM SIGCOMM 2011 Conference* (pp. 74–85). Association for Computing Machinery. https://doi.org/10.1145/2018436.2018446

Keerthika, S., Aarthi, P., Cibi, T. S., & Shankar, G. M. (2022). Tenant-led ciphertext information flow control for cloud virtual machines. *International Research Journal of Modernization in Engineering Technology and Science, 4(5)*, 1522–1527.

Seufert, M., Egger-Lampl, S., Slanina, M., Zinner, T., Hossfeld, T., & Tran-Gia, P. (2015). A survey on quality of experience of HTTP adaptive streaming. *IEEE Communications Surveys & Tutorials, 17(1),* 469–492. https://doi.org/10.1109/COMST.2014.2360940

Habibi Gharakheili, H., Vishwanath, A., & Sivaraman, V. (2015). Pricing user-sanctioned dynamic fast-lanes driven by content providers. *In Proceedings of the IEEE INFOCOM 2015 Workshops* (pp. 660–665). IEEE. https://doi.org/10.1109/INFCOMW.2015.7179439