JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 09, 2020

Cloud-to-Edge Internet of Things and 5G Network Security via Software-Defined Networking

Kajal Aggarwal,
Asst. Professor, SOC (School of computing),
GEHU-Dehradun Campus
DOI: 10.48047/jcr.07.09.586

Abstract: SDN has introduced a new networking paradigm, and its programmability enables the effective deployment of new services for today's networks, which have constantly changing needs. Through its decoupled control plane and programmable forwarding devices, SDN has addressed critical issues of administration and scalability. The NFV paradigm uses hypervisors for computational functions to virtualize networking functions, and it uses VMs to deliver a whole set of networking services. In addition to facilitating dynamic administration of software-based network activities, SDN also offers more flexibility in directing packet flows. Applications of these enabling technologies range from managing the direction packets go via a device or a chain of network function services to shaping traffic in a network to specify pathways programmatically. Proactive Intrusion-Prevention filters at strategic nodes are possible because to the network's software-defined nature, which also allows for effective traffic-dynamics management and response to cyber-attacks in today's virtualized datacenters. Despite the many advantages of SDN, its design introduces new vulnerabilities due to the proliferation of attack vectors made possible by its central characteristics (such as the separation of the control and data planes). Moreover, the existing separation of an intelligent control plane and an excessively simplistic, stateless data plane prevents full utilisation of a network's software-based adaptability.

Keywords: Software-Defined-Networking, Network Function Virtualization (NFV), Virtual Machines

Introduction

The Internet's massive size is mind-boggling. By providing flexibility, simplicity in deployment, hosting, and maintenance of corporate applications, cloud computing has impacted all enterprises' IT operations and ICT organisations. It drastically reduced expenses related to setting up shop, growing the business, running the business, etc. End consumers experienced more delay for time-sensitive services as a result of network congestion, over-provisioning, and routeing complexity brought about by the expansion of digital services. Cloud service providers fall short in areas like customer satisfaction, responsiveness, mobility, and location/context awareness. Managing and implementing traditional networks' infrastructure and services is an iterative process that often necessitates the use of proprietary interfaces to alter the settings of different network defaults. Complex and widely dispersed protocols like OSPF[1], BGP, and EGP [2] control packet forwarding. Enforcing complicated rules in traditional IP networking infrastructures is challenging due to a lack of standardised descriptions of global network status and a lack of adequate network abstractions. Because

the network is planned rather than coded, rolling out new services is laborious and time consuming [3][4]. By decoupling control data from forwarding devices like switches and routers, "Software-Defined Networking (SDN)" introduces a new design paradigm and blank slate in networking [5][6]. By separating the control function from the forwarding devices (such as switches and routers), SDN has revolutionised the administration of large-scale networks. Before the advent of software-defined networking (SDN), every switch used to run its own control plane software from the manufacturer. The spanning tree protocol [7] is one example of a distributed algorithm that was conducted by this programme to establish network topology and forwarding rules. The problems with this strategy were numerous: To begin with, the distributed control plane was more complicated and had compatibility issues amongst manufacturers. Second, it severely limited network administrators' ability to customise and innovate by forcing them to use just the capabilities explicitly listed as "supported" by the manufacturer. Third, a tight integration between all components necessitated a close partnership with a single supplier. This meant that in addition to the high total cost of ownership, network managers faced additional expenses for training and certification. Many of the difficulties in multi-tenant data centres, as well as those with dataplane forwarding devices, have been greatly alleviated because to SDN's flexibility, programmability, dynamic policies, upgrading, and innovation. As a result of the reduced obstacles to entry, the market saw the introduction of new suppliers. With SDN enabled, the manual and resource-intensive process of deploying network services and enforcing rules on the fly is transformed into a controllable (programmable) autonomic activity. SDN has been widely adopted in both the business and academic worlds, and it has been effectively implemented in both data centres and wide area networks [8][9]. SDN is now being examined by businesses and operators and is the subject of much academic study. SDN-based WAN is being used by major content and IT distributors like Google Inc. to link their many datacenters located all over the world. As a result, network performance was greatly enhanced, and link utilisation rose from 30–40% to over 100% [9]. SDN's enhanced control of transmission and programming of network flows is largely responsible for this remarkable success. Increasing backing from major networking suppliers including Cisco [10], Huawei [11], Juniper [12], and Hewlett Packard [13] suggests that SDN's expansion will continue into the foreseeable future. SDN is expected to be the central enabling technology for the 5G networking applications [15], and it is already being used in current virtualized datacenters and IoT based smart infrastructures [14]. The drastically new method of SDN network administration and configuration has major effects on network safety. New networking paradigm presents threats to security, administration, and resilience of its deployed environment despite its many benefits and complexity.

"Security of SDN" refers to measures taken to ensure the safety of the software-defined network infrastructure itself. The central control plane in an SDN architecture is a potential design flaw that might lead to a single point of failure. Researchers in both the academic and business sectors have bolstered the argument for SDN by studying the prevalence of vulnerabilities and attack vectors in live settings. In addition, "Security via SDN" refers to how SDN's centralised perspective and programmability facilitate the deployment and enforcement of security rules across a whole network. We provide novel approaches to

ISSN- 2394-5125 VOL 07, ISSUE 09, 2020

bolstering front-line network security using SDN, which gives network operators centralised control over their infrastructure. We get there by first reevaluating the use of SDN in business settings. We then extend cloud capabilities and SDN into the manufacturing setting. Our study demonstrates how SDN-based security solutions may be adapted to address deployment hurdles by taking into account the specific features and constraints of each network. This thesis solves issues with today's front-line networks that would go unresolved without our SDN approaches. We begin by discussing how current issues with scalability and lack of context might be overcome by rethinking SDN adoption in the workplace. Due to network complexity, scalability and situational awareness become challenging. Because of this intricacy, there are sometimes times when network operators cannot see traffic on their networks. If network operators had a more complete picture of network activity from end-systems, they would be better able to prevent threats like the propagation of malware from a compromised machine. Since hosts often forwards intra-subnet communication directly without going via security enforcement and monitoring devices, conventional methods typically leave network operators in the dark about intra-subnet traffic. To stop the spread of malware, containment methods include temporarily or permanently disabling critical network services or even the whole network. Because of this holistic perspective, DDoS assaults may be thwarted in their early phases under the SDN paradigm.

By taking use of the increased computing capabilities available in the control plane, SDN architecture is preferable to implementing NIDS in the traditional network model for addressing network intrusion and identifying complex assaults. In an SDN-enabled data centre, packet streams are seen as flows since there is an innate relationship between all of the packets in a given flow, and the switches provide the controller with information about the flows. Applications may use the data center's centralised controller to enforce restrictions on these flows and do ML-based analytics on the flow data by accessing the controller's interface (through "northbound API"). In order to identify network breaches and foresee future assaults, ML-based techniques may mine a massive amount of time series data and derive knowledge. The advent of many-core co-processors (such as graphics processing unit (GPU) and Tensor units) and multi-core CPUs (such as scalable Intel Xeon and Phi) made it possible to run ML-based analytics and deep computational networks. The effectiveness and practicality of any ML-based NIDS are determined by the dataset and training the machine using labelled data, etc. The SDN architecture naturally gathers network-wide statistics and runtime data in a centralised location. Therefore, the controller-based system provides a strategic location for ML-based IDS/IDA tools. In addition, SDN provides the programmable model through API, based on both historical and real-time data analytics, to automate the provisioning, services chaining, dynamic security choices, and traffic rules at run time. We found that current ML based classifiers enhance IDS accuracy, but at the expense of increased processing power and memory need, making them unfeasible for real-time solutions. Thus, we were able to solve some of the most pressing problems with NIDS in SDN-enabled installations via our investigation.

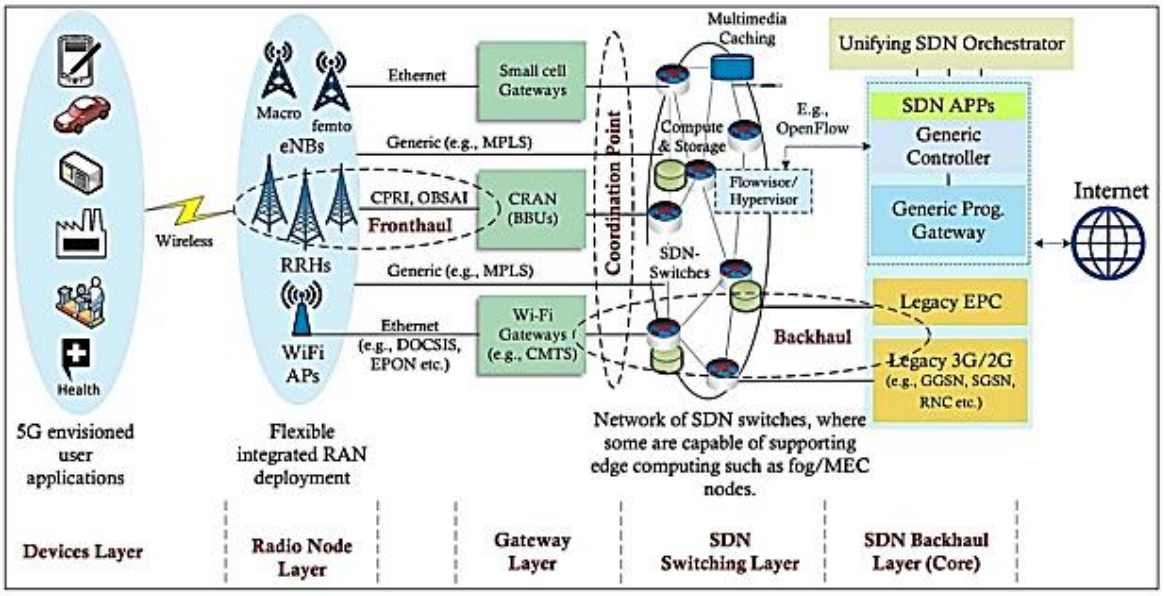

Figure 1. Conceptual Model of SDN/NFV Architecture for Modern Networks

Literature Review

Sharifah H. S. Ariffin et.al.,(2020) Most people's everyday lives and businesses today span international, geographical, and political borders. The low-powered devices used in the IoT system make it difficult to ensure the system's security, which in turn decreases the system's dependability. Policy enforcement and dynamic network reconfiguration are two areas that Software Defined Networking (SDN) hopes to improve considerably. In order to increase network and system safety, this article discusses several designs for integrating IoT with SDN.

Dongdong Ma et.al (2019) New lightweight encryption techniques are tested and evaluated in this work from a number of perspectives. Experiments have shown that the lightweight encryption technique presented in this research may successfully transmit data in a software-defined industrial Internet of Things (IoT) edge network.

Pranav Godway et.al (2019) Congestion is alleviated by using a new networking paradigm called software-defined networks (SDN), which is additionally known as Network Automation and Network Programmability. In this paper, we use a real-world model for traffic management taken from the Indian state of Orissa and its capital city of Bhubaneshwar. The SDIoT (Software Defined Internet of Things) framework was used in the development of this app. Our results emphasise the importance of SDN in IoT.

Industrial Efforts in SDN and NFV

The development of SDN and NFV architectures is being considered by several efforts, ONF among them. "Open Network Foundation(ONF)", one of the most active groups in this network softwarization sector, finds new ways to further the use of software-defined networking (SDN) and network function virtualization (NFV), which together turn networks into high-performance platforms. The "Next Generation SDN (NG-SDN)" effort, headed by

the ONF, is an expansion on the work done with SDN thus far. Traditional network designs have been increasingly supplanted with SDN-enabled ones in campus networks, wide area networks, and datacenters since the release of the OpenFlow protocol in 2008. Open source ecosystems for SDN and NFV technologies have advanced rapidly in recent years, thanks to the efforts of institutions and standards organisations like the European Telecommunications Standards Institute (ETSI), the open source management and orchestration group (OSM), the OpenStack cloud platform, CORD, and OPNFV. The ETSI focuses on four main areas of inquiry—structural design; NF performance; NF management; and NF placement—among many others. By offering excellent reference designs and blueprints, ONF creates and promotes the integrated SDN/NFV project efforts. Through OpenStack integration and attempts to optimise SFC through OpenDaylight SDN controller initiatives, the OPNFV community has been a champion of the advancements of NFV platforms in Cloud infrastructure. The Open Network Operating System (ONOS) [199] is a popular choice for controller software due to its compatibility with and contributions to OpenStack.

Implementation

We implemented a security and threat detection package into SDN and OpenStack. The OvS dataplane switches will keep a watchful eye on the network as a whole, analyzing traffic to identify potential threats. The data plane is protected because the switches conduct mitigation network functions and maintain consistent communication. statistics to the OpenDaylight (ODL) controller for the SDN. OpenStack supports installing the OpenDaylight controller package, which has been verified by the open source community. APIs are plentiful on the north-bound interface. Integration with cloud infrastructures like OpenStack is the primary goal of REST APIs. The "SAL (Service Abstraction Layer)" maps the various network hardware (switch/NIC) with a common access mechanism, and is therefore the most crucial architectural layer. Neutron's version of ODL (OpenDaylight) communicates with the Open vSwitch Database Management Protocol (OVSDB) through the ML2 (Modular Layer 2) plugin, which in turn communicates with the OVS stack/OVSDB via the OpenFlow protocol in the integrated architecture. The plugin handles all networking tasks, including the setup and teardown of virtual networks and the establishment of connections among virtual machines (VMs), the Cloud Controller, and the public internet. Each plugin communicates with the compute node's virtual switch (OVS vSwitch) through an agent module. Procedures in Neutron are as follows:

i) A command is sent to the Neutron server using its API

ii) A database entry is inserted through the neutron server, which then calls the relevant plugin's REST API. After the plugin has received this request, it will invoke the southbound protocols to establish communication with the appropriate network nodes.

OpenStack's networking functions are optimized and protected by the SDN techniques. We built the OpenStack testbed on our lab server, which includes Nova, Neutron, and Keystone, three of the most fundamental components of the OpenStack cloud operating system. OpenStack Pike release was deployed using the matching version of devstack [628] to

streamline the installation process and to acquire an OpenStack deployment profile for further usage of our solution in various scenarios. As data plane switches, we opted for Open vSwitch with Data Plane Development Kit (OVS- DPDK). To accomplish running the OVS br-int bridges in DPDK mode (user-space), we compiled Open vSwitch 2.9.2 with DPDK 17.11.2 on each Compute node. Virtual machines (VMs) running individual components (such an application or virtual network function, or NFV) on a single server or distributed across numerous NFV-based systems coordinate their activities via communications. Mininet was used to simulate a leaf-spine network (Figure 2) with 4 spine switches (OVS), 8 leaf switches (each with 2 hosts), and an OVS serving as an intermediary. In order to reduce the complexity of the network, we assumed that each leaf switch was a Top-of-Rack (ToR) switch, and that each host's MAC address was immediately mapped to its IP address.

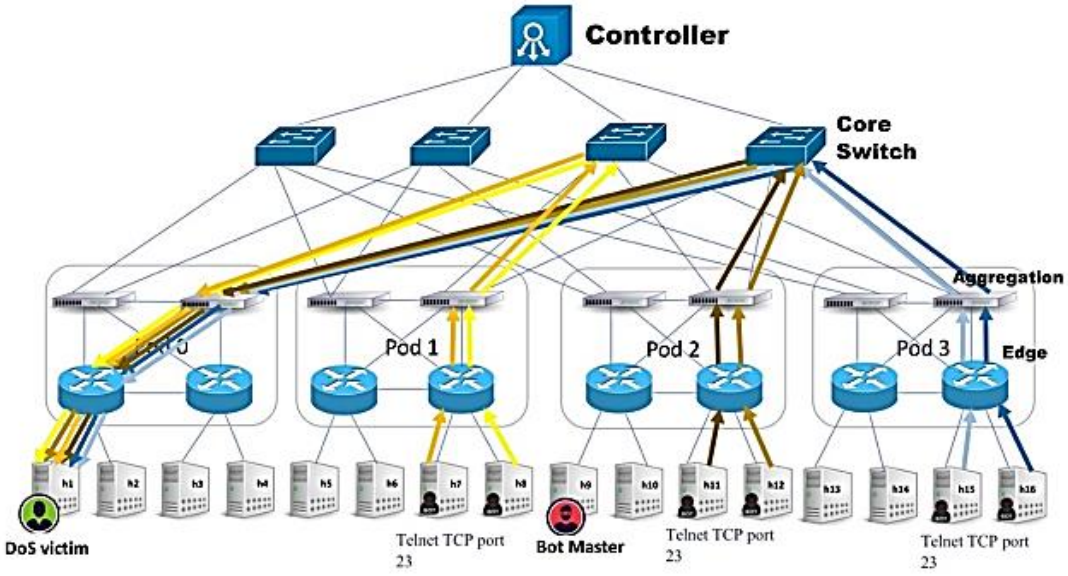

Figure 2. Large Software-Defined Data center network setup

Comparison of Linux Bridge/Classic OpenStack/CloudSDN

We tested how well several key performance indicators (KPIs) performed under varying network and CPU loads. We configured each computing node with enough memory and processing power to support five virtual machine instances. Our "30 tests of netperf TCP STREAM. per node" were carried out using a single Virtual Machine (VM) as the server and several clients.

Figure 3 displays the CPU and memory use of the three techniques (old LB, native OvS, and CloudSDN). TCP Throughput, Latency: When the number of clients per node is changed and external clients flood a single server, the OvS-based firewall shows better sustained TCP throughput than the Linux Bridge solution. This demonstrates that OvS is the best choice for OpenStack Cloud software. Over time, the sum of all TCP flows approaches the theoretical maximum throughput of the network interface. Figure 3 shows over 8.4 Gbps of total TCP throughput as four clients submit data to a single server. When there are more users, the overall aggregated flows use up all available bandwidth.

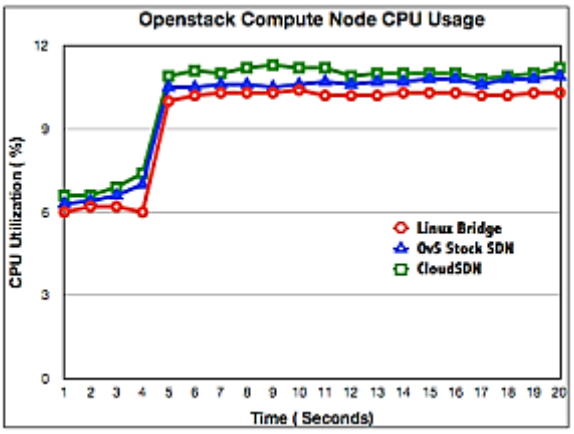

Figure 3 CPU usage in node

Conclusion

In this study, we suggested a CloudSDN security architecture for SDN-managed OpenStack Cloud environments. The proposed framework streamlines the process of monitoring inter-VM communication at the packet level and offers users with centralised control over security policies and access permissions. The distributed virtualized edge network enforces safety policies and access control specifications as OpenFlow standard rules. It is preferable in cloud settings to monitor worldwide security events and react rapidly to any dangers or assaults. If this feature could also be programmed and scaled to larger, geographically dispersed cloud networks, it would be much more desired. We managed to realise this goal via diligent investigation. We have combined SDN with the use of cloud computing and dealt with several DDoS/botnet attack situations. Through a massively scalable application for cloud-computing, our proposed SDNFV-based security framework integrates multi-plane security monitoring, threat analytics, and attack detection/prevention. Our findings suggest that SDN may one day be able to realise one of its fundamental visions—namely, the provision of a programmable capacity for an international perspective of the security events and quick response—even in massive, geographically scattered Cloud networks.

References

1. S. H. S. Ariffin, "Securing Internet of Things System using Software Defined Network based Architecture," *2020 IEEE International RF and Microwave Conference (RFM)*, Kuala Lumpur, Malaysia, 2020, pp. 1-5, doi: 10.1109/RFM50841.2020.9344768.
2. D. Ma and Y. Shi, "A Lightweight Encryption Algorithm for Edge Networks in Software-Defined Industrial Internet of Things," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1489-1493, doi: 10.1109/ICCC47050.2019.9064352.
3. P. Godway et al., "Smart Traffic Management System Based on Software Defined Internet of Things Architecture," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 2019, pp. 1-5, doi: 10.1109/ANTS47819.2019.9118094.

4. K. Jayavel, V. Nagarajan, K. Sornalakshmi and K. Navin, "Migration techniques of data centric networks to internet of things with control plane based virtual sensor layer," *2017 International Conference on IoT and Application (ICIOT)*, Nagapattinam, India, 2017, pp. 1-8, doi: 10.1109/ICIOTA.2017.8073633.
5. T. Theodorou and L. Mamatas, "CORAL-SDN: A software-defined networking solution for the Internet of Things," *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, Berlin, Germany, 2017, pp. 1-2, doi: 10.1109/NFV-SDN.2017.8169870.
6. T. H. Szymanski, "Security and Privacy for a Green Internet of Things," in *IT Professional*, vol. 19, no. 5, pp. 34-41, 2017, doi: 10.1109/MITP.2017.3680952.
7. M. B. Yassein, Q. Abuein and S. A. Alasal, "Combining software-defined networking with Internet of Things: Survey on security and performance aspects," 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, 2017, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273027.
8. K. Jaswal, T. Choudhury, R. L. Chhokar and S. R. Singh, "Securing the Internet of Things: A proposed framework," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 1277-1281, doi: 10.1109/CCAA.2017.8230015.
9. T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh and H. -C. Chao, "Defending Against New-Flow Attack in SDN-Based Internet of Things," in IEEE Access, vol. 5, pp. 3431-3443, 2017, doi: 10.1109/ACCESS.2017.2666270.
10. M. M. Mazhar, M. A. Jamil, A. Mazhar, A. Ellahi, M. S. Jamil and T. Mahmood, "Conceptualization of Software Defined Network layers over internet of things for future smart cities applications," 2015 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Orlando, FL, USA, 2015, pp. 1-4, doi: 10.1109/WiSEE.2015.7393104.
11. H. Li, M. Dong and K. Ota, "Radio Access Network Virtualization for the Social Internet of Things," in IEEE Cloud Computing, vol. 2, no. 6, pp. 42-50, Nov.-Dec. 2015, doi: 10.1109/MCC.2015.114.
12. M. A. Salahuddin, A. Al-Fuqaha and M. Guizani, "Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles," in IEEE Internet of Things Journal, vol. 2, no. 2, pp. 133-144, April 2015, doi: 10.1109/JIOT.2014.2368356.
13. O. Flauzac, C. González, A. Hachani and F. Nolot, "SDN Based Architecture for IoT and Improvement of the Security," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangju, Korea (South), 2015, pp. 688-693, doi: 10.1109/WAINA.2015.110.
14. Y. H. Lin, Q. Wang, J. S. Wang, L. Shao and J. Tang, "Wireless IoT Platform Based on SDR Technology," *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, Beijing, China, 2013, pp. 2245-2246, doi: 10.1109/GreenCom-iThings-CPSCom.2013.426.
15. E. Patouni, A. Merentitis, P. Panagiotopoulos, A. Glentis and N. Alonistioti, "Network Virtualisation Trends: Virtually Anything Is Possible by Connecting the

Unconnected," *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Trento, Italy, 2013, pp. 1-7, doi: 10.1109/SDN4FNS.2013.6702545.

16. G. Savarese, M. Vaser and M. Ruggieri, "A Software Defined Networking-based context-aware framework combining 4G cellular networks with M2M," *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Atlantic City, NJ, USA, 2013, pp. 1-6.
17. L. Velasco *et al.*, "Cross-stratum orchestration and flexgrid optical networks for data center federations," in *IEEE Network*, vol. 27, no. 6, pp. 23-30, November-December 2013, doi: 10.1109/MNET.2013.6678923.