Enhancement of Network Security in Open flow
Framework Using Software Defined Networking

P. Maragathavalli, Assistant Professor,
Department of Information Technology
Pondicherry Engineering College
Puducherry-605 014, India

S. Vanathi, M.tech[II Year]
Department of Information Technology
Pondicherry Engineering College
Puducherry-605 014, India

Abstract— Software defined networking is a computer networking by using a open flow protocol. To provide a security measure in a opensec in Software Defined Networking (SDN) environment for malicious node reacts to a opensec protocol. In this the communication between the switch and controller and requested node in a network. Main objective is to give priorities on the basis of trust level, then according to that it will handle the request. And to keep the control plane in running state efficiently even when suffering from data-to-control plane saturation by assigning less timeout value for the flow rule in peak time. The secondary objective is to differentiate between fake packet request from normal packet request and it handles the data-to-control plane saturation. The performance metric is evaluated by using the number of packet loss and its time taken for its transmission.

Keywords— Software defined network, openflow, security, attack detection, secured data.

I. INTRODUCTION

Thus they are various security issue has been occurred in the openflow in software defined network environment. In a flow table missive relocation in environment thus the data allocation between the controller ,switch and with the requested node to transfer the data. And it based on the functionality of an abstraction of lower –level in the environment. Since there is no extent to afford security in the openflow flowtable messages. Through abstraction of lower-level functionality. To improve a security issue first to process the bunching to the neighbor node and dissemination is performed. And it develops the computational of scalability and it stagnant in position. Thus it process a decoupling the node in a coordination that make to perform a verdict making that which node to proceed. And the data transfer in flowtable communications is between the control and the receiver as entreated node transfer. Thus the process involved with a open flow protocol for the purpose of isolated data communication and to select the path between the grids controls.

Thus the procedures of security disputes and the attacks present in software defined networks are as data outflow when more numbers of node entreated from the packet while transmitting data. It causes a denial of services, revised data while conveying the when attacker hack the data in a node. Attacks on evolving data plane embraces in DOS are control dos, complex dos, TCAM collapse, switch back hole. In existing work, they accomplish only in the site network environment by using a OpenSec in a software defined situation, where security charter is based on openflow. And security strategy is written in a human readable language which is instigated in a network security operator that allows a network security operator. The security measures are realistic to its field, using opensec such as attacks In this work the security policy will reacts to opensec if the malicious node traffic is found detected. And it passes a openflow message to opensec when a mischievous nodes is detected to the controller in a network. In a campus network they use a dataset to evaluate the security and the scalability issues by performing the testbed as GENI to detect the spasms and the malicious node present in the network in which it blocks inevitably as 95%of attacks and the 97% of source of malicious node in grounds network.

In a proposed work , the consumption of nodes are accomplished and the neighbor fragment acquaintance is performed. And the statistics announcement in flowtable missive is done between the amendment and resistor and with the entreated nodes. First it process done by bundling is done by using AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks) in this every single node will preserve the series number to track the node and it update the way value by RREQ and RREP for a path progressing in node . and it procedures a cloudwatcher procedure the perceive and wedge the attacks before it hacks the data while diffusing.attacks which include gray scale attacks and dos attacks in controller. Finally it spots the malicious nodes such as selfish node are perceived and it updates the secure data update in the reliable flow table broadcast.

II Related work

This section briefly review earlier works based on the security issue in openflow framewor. A number of approaches have been reported in the literature survey for security measure and block of attacks and the malicious nodes.
Adrian Lara and Byrav Ramamurthy in their work they propose a Network-aware controller handles the configuration of all network devices. Software applications running on top of the network controller provide an abstraction of the topology and facilitate the task of operating the network. We propose OpenSec, an OpenFlow-based security framework that allows a network security operator to create and implement security policies written in human-readable language. Using OpenSec, the user can describe a flow in terms of OpenFlow matching fields, define which security services must be applied to that flow (deep packet inspection, intrusion detection, spam detection, etc.) and specify security levels that define how OpenSec reacts if malicious traffic is detected. In this paper, we first provide a more detailed explanation of how OpenSec converts security policies into a series of OpenFlow messages needed to implement such a policy describe how the framework automatically reacts to security alerts as specified by the policies.

Jiaqiang Liu, Yong Lia, and Huandong Wang have addressed the problem in Network operators to employ a variety of security policies for protecting the data and services, deploying these policies in traditional network is complicated and security vulnerable due to the distributed network control and lack of standard control protocol. We introduce a safe way to update the configuration of these switch one by one for better load balance when traffic distribution changes. The update process as a path in a graph, in which each node represents a security policy satisfied configuration, and each edge represents a single safely update. Based on this model, we design a heuristic algorithm to find an optimal update path in real time. Simulations of the update scheme show that our proposed algorithm is effective and robust under an extensive range of conditions. The Dijkstra algorithm can be used to find the shortest path from the initial state to the destination state. A Security holes would be generated during updating the configuration of these switches. To avoid it, we propose a security guaranteed update scheme based on a graph model. Smaller size of flowtable and has lower overhead on the control plane. OpenSec can also achieve real-time blocking using a different policy that sends all traffic to the unit and then receives all traffic back and forwards it.

Bing Xiong, Kun Yang, Jinyuan Zhao, Wei Li, and Keqin Li in this work they discussed about the Performance evaluation security issues in OpenFlow-based software-defined networks based on queueing model in OpenFlow is one of the most famous protocols for controller-to-switch communications in software-defined networking (SDN), commonly seen as a promising way towards future Internet. Understanding the performance and limitation of OpenFlow-based SDN is a prerequisite of its deployments. To achieve this aim, this paper proposes a novel analytical performance model of OpenFlow networks based on queueing theory. After depicting a typical network scenario of OpenFlow deployments, we model the packet forwarding of its OpenFlow switches and the packet-in

International Journal of Computer Application (2250-1797) Volume 7– No.2, March - April 2017

message processing of its SDN controller respectively as the queueing systems $M X / M / 1$ and $M / G / 1$. Subsequently, we build a queueing model of OpenFlow networks in terms of packet forwarding performance, and solve its closed-form expression of average packet sojourn time and the corresponding probability density function. Finally, the numerical analysis is carried out to evaluate our proposed performance model with different parameter values. Furthermore, our controller model is contrasted with the classical one by utilizing the popular benchmark. It indicate that controller model provides a more accurate approximation of SDN controller performance.

Changhoon Yoona, Taegun Park, Seung soo Lee and Zonghua Zhang addressed the problem in Enabling security functions with SDN. In this paper, we verify whether SDN can enhance network security. Specifically, the idea of enabling security function with diverse SDN features is explored thoroughly. In order to elucidate the feasibility of SDN based security functions, such as in line mode security function as firewalls and IPS, passive mode security functions as IDS), network anomaly detection functions as scan and DDoS detector advanced security functions a stateful firewall and reflector networks. This paper are summarized as follows. To work is the first trial that examines real and practical is regarding the implementation of diverse network security functions with SDN. The main goal of this work is to investigate the possibility of designing practical security functions with SDN. OpenFlow enabled switch models from different vendors and compared the the focus on how different security applications affect the overall throughput and latency with different switches.

Wenjuan Li, Weizhi Meng and Lam For Kwok discussed Security challenges and countermeasures has been proposed as an emerging network architecture, which consists of decoupling the control planes and data planes of a network. Due to its openness and standardization, SDN enables researchers to design and implement new innovative network functions and protocol in a much easier and flexible way. In particular, OpenFlow is currently the most deployed SDN concept, which provides communication between the controller and the switches. However, the dynamism of programmable networks also brings potential new security challenges relating to various attacks such as scanning, spoofing attacks, denial-of-service (DoS) attacks and soon, where attackers may utilize to compromise the SDN. OpenFlow switch and flow table are likely to become a major target, since they contain information related to network management, routing and access control. More specifically, attackers can target the network elements within the network itself. An attacker can first attempt to gain unauthorized physical or virtual access to the network, or compromise a host that is already connected to the SDN, and the entry to perform attacks to destabilize the network elements.
Xiulei Wang, Ming Chen, and Changyou Xing has described about the Software-Defined Security Networking Mechanism to Defend against DDoS Attacks. The Distributed Denial of Service (DDoS) attack has seriously harmed network availability over decades and there is still no effective defense mechanism. The emerging software defined networking (SDN) gives a new way to rethink the defense of DDoS attacks. In this paper, we first modeled DDoS attacks from the perspective of network architecture. Then a software defined security networking mechanism was proposed to remove or restrict these necessary conditions which were summarized from the model. In this paper are summarized as follows. DDoS attacks from the perspective of network architecture and the necessary conditions of DDoS attacks were summarized from this model. A software defined security networking mechanism was proposed by removing or limiting these necessary conditions. A prototype was designed by OpenFlow and cloud computing technologies, which can be incrementally deployed in current IP network.

Saksit Jantila and Kornchawal Chaipah they discussed about A Security Analysis of a Hybrid Mechanism to Defend DDoS Attacks in SDN. In this paper, we propose adapting a hybrid mechanism against DDoS attacks from the traditional network for SDN. The mechanism relies on trust values and entropy based on clients’ access behaviors. We identify threats to this application and suggest use of existing SDN’s and our proposed mechanisms to prevent and mitigate the threats. Moreover, authentication, encryption, and the use of public/private keys play important roles in keeping entities in SDN safe from attackers. In the future, we plan to implement and simulate the proposed mechanism in a virtual SDN to assess the mechanism’s effectiveness and efficiency, and to identify any flaws we might have overlooked.

Javed Ashraf and Seemab Lati has come with system of handling the security measure in Intrusion and DDoS Attacks in Software Defined Networks Using Machine Learning Techniques This paper aims at studying SDN accompanied with OpenFlow protocol from the perspective of intrusion and Distributed Denial of Service (DDoS) attacks and suggest machine learning based techniques for mitigation of such attacks. The critical security threats of SDNs and in augmenting its security such as classifying applications and using rule prioritization, to ensure that rules generated by security applications will not be overwritten by lower priority applications. Other proposals try to go a step further by providing a framework for developing security-related applications in SDNs. The DDoS attack is an attempt with malicious intent to drain the resources of a computer or a network of computers by sending continuous and heavy traffic to them. Machine learning based techniques for handling DDoS attacks and intrusion has received much attention in the computational intelligence community handling conventional networks and as well as SDN, now. In this paper we have analyzed various machine learning techniques which can be used to handle the issues of intrusion and DDoS attacks to Software Defined Networks.

### III Proposed work

The proposed system has Main objective is to give priorities on the basis of trust level, then according to that it will handle the request. The prime objective is to keep the control plane in running state efficiently even when suffering from data-to-control plane saturation by assigning less timeout value for the flow rule in peak time. The secondary objective is to differentiate between fake packet request and normal packet request handles the data-to-control plane.

![System Architecture](image)

The Modules of the proposed systems are:

- Node deployment and neighbor phase coverage
• Routing and Data transmission
• Malicious host detection
• Block of attackers and Update Secured data

A. Node deployment and neighbor phase coverage
Node exploitation is the initial stage for the flow table message broadcast. In flow table there will be many attackers and the malicious node will be presented. For such purpose first the nodes must be deployed and the bunching process as it broadcast as neighbor phase coverage in software defined network environment. In the deployment process thus nodes as host moves frequently it act as an end point and forward packet routers in the transmission source range of multi hop environment. The topology of networks changes unpredictably. By organizing the node thus the materialization of new nodes might be transpired in the neighbor phase coverage.

- packet delivery ratio intensifications.
- Decrease in the average end -to-end delay Diffusions.
- Nonaggressive in Repeated link breakages and conduit failures leads to virtuous vast concert when the network is in high solidity.

B. Routing and Data Transmission
In a routing and data transmission it involves the clustering process it involves AOMDV algorithm .It maintain its own invariant sequence of its own destination numbers. In this Routing host will move from one packets to another across a networks. While transmitting it increases the Packet switching efficiency network, robustness. Thus the Packets of nodes has the header and payload. Each packet is then transmitted individually in same path or might be in different path to its destination. In a flowtable if all of the packets has reached at the destination, they automatically reassembled to recreate the original message.

An attacker in a malicious node to hack the data while transmitting the data in the flow table target system to prevent authentic access. Cloud watcher, which provides monitoring services for large and dynamic cloud networks. This framework automatically detours network packets to be inspected by pre-installed network security devices.

AOMDV/(On-demand Multipath Distance Vector Routing in Ad Hoc Networks(AOMDV) Routing Algorithm:
The node finds its own address among the addresses listed in the message and it updates the current status of the data transmission and the neighbor holding time in a controller. If the node does not find its own address among the addresses listed in the transmission message it broadcast again the another neighbor nodes in the host address. By using the clustering process it broadcast the messages.

C. Malicious host detection
In a malicious host detection it uses the cloudwatcher technique in the flow table transmission where the requested nodes is needed to transmit the message.by using the cloud watcher technique the attackers and the malicious node is detected.

Cloudwatcher technique
Cloud watcher technique is a technique is used to monitor the network security in the software defined network environment using openflow in opensec framework. it guarantee to the controllers of network flows to the security devices of all packets.

(ii) And it enhance the efficient policy scripting language to provide security and services easily.
(iii) In a flowtable the transmission between the controller and host the cloudwatcher can easily changes the path of routing network flows, and it makes the flows transmit through network nodes where security devices reside.

D. Block of attacks and update Secured data
In this process after detection and block of malicious host secured data update and the graphical results of the attacker has been blocked in a network. Since they exist a selfish node in a flow table in a software defined network environment and the gray scale attack has been detected while in the data transmission in the nodes. And it provides a Secure data protects the processing and storage of code using encryption, fault and manipulation detection, and secure code and data storage.

The open issue attacks are:
- Unauthorized Modification Using Identity Spoofing Attacks
- Flooding Attacks
- Man in middle attack
- Eavesdropping
- DDOS attack
- ARP spoofing
- Side-channel attacks

Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator and controller update the flow table against the attacker and provide a secured transmission.

IV Experimental Analysis
NS2 is an open-source simulation tool that turns on Linux. It is a discreet event simulator targeted at networking research and provides important support for replication of routing, multicast conventions and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless networks. It has many advantages that make it a useful tool, such as support for numerous protocols and the competence of explicitly detailing
link traffic. The nodes are free to move randomly and act as end points as well as routers to advancing packets in a multi-hop setting where all nodes may not be within the conduction range of the source.

By merging the analysis ratio and the connectivity issue, the rebroadcast probability occurs, which can be used to reduce the number of the RREQ packet, to improve the routing performance. Increase in packet delivery ratio. Decrease in the average end delay Transmissions. Attack has been detected and identify the malicious host and provides the security measure in it. And the controller updates the flowtable messages to the switch movement and provides the trusted data information to the demanded node.

V Result analysis

For assessing the performance of conforming technique and approaches, And the concert exploration is based on the packet loss, amount, and recognition of attacks with malicious nodes and without attacks based upon the throughput.

![Fig 1.2 Packet Loss](image)

Packet loss is calculated by

\[
\text{Packet loss} = \frac{\text{Total number of packet transmitted}}{\text{Total Number of packet received.}}
\]

Packet transmission time = total number of Packet size

\[
\text{Bit rate}
\]

And by using the cloudwatcher technique thus the attacks and the malicious nodes are identified and block the grayscale attacks in the requested node.

Throughput is calculated by

\[
\text{Throughput} = \frac{\text{file size}}{\text{transmission Time}}.
\]

![Fig 1.3 Throughput (Time vs Delay)](image)

Since the clustering process is performed and the cloud watcher technique is efficient to route and cluster the node deployment with the network formation. By data transmitting it uses the UMTS process for transmit and for routing process. And after the completion of process in routing and transmission it enables the attack detection technique and block of irrelevant data and the attacks present in the open flow. It process and update the secured data in the software defined network environment.

VI Conclusion

The project analyze the various security issue in a data transmission and data routing by using the broadcasting the neighbor nodes using controller, switches and host. In a OpenFlow-based framework that allows network operators to describe security policies controller and automatically converts security policies into a set of rules that are pushed into network devices. OpenSec also allows network operators to specify how to automatically react when malicious traffic is detected. It allows for automated reaction to security alerts based on pre-defined network policies. The analysis of traffic away from the controller and into the processing units makes our framework more scalable. An attack detection trigger method was for the first time presented to agenda the starting of attack revealing. An attack detection method was used to discover the attack. A system the trigger mechanism of the attack detection implemented on controller. In security entrenched routing, a routing protocol can act as a exporter that helps not only in guiding the traffic but also in protecting it. Security controls permit deny traffic based on network level information IP, port number or protocol.
VII References


