IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 91-94
www.iosrjournals.org

Detection of Smurf Attack in SDN with Multiple Controllers

N.Priyanka[1], V.Vetriselvi[2]
[1,2]*Department of Computer Science and Engineering, College of Engineering, Guindy, India*

Abstract : *Traditional networking structure is gradually replaced by Software Defined Networking (SDN). It is the new approach in design, build and manage networks. SDN is a promising technique which enables network administrators to program dynamically. Although it is more flexible to manage, one must be aware of security threats in its deployment. In this paper, we analyzed SDN network from the perspective of Distributed Denial of Service attacks (DDOS). DDOS attacks in SDN are very difficult to identify as it have similar characteristics of normal packets. We outline our ideas based on the analysis of network and detection of DDOS attacks using multiple controllers in this environment.*

Keywords: *DDOS, Multiple Controllers, Packets, Software Defined Network*

I. INTRODUCTION

Software Defined Network (SDN)has acquired a lot of assiduity in recent years, because it is different from ordinary network in terms of lack of programmability and enables easy and fast network innovation. SDN separates data plane and control plane unlike traditional networking where it is embedded itself in network devices. The expectation for cheaper hardware which is controlled by software application is fulfilled by software defined network which has standard interface. New features can also be added depending on the needs through dynamic programming facility. In software defined network the control and data planes are separated from each other, enabling the control of network programmable which enables easy network administration.

The power of SDN has been being proven day by day worldwide from enterprises to big organizations. The SDN had already proved its success in providing reliability, effectiveness, simplicity, flexibility at lower cost.SDN faces loads of challenges which must be resolved especially in security issues. Because of the predefined feature of centralized controller, it became a potential target for attackers to exploit the network. Whenever a new packet arrives in SDN network, and if the switch could not find any matched flow entry, then the packets will be forwarded to the controller to ask about method to handle. It is a great chance for an attacker to deplete the resources of network and threaten from availability.

Recently, many solutions have been proposed by various authors to decrease the impact of the security problems. Some ideas try to setup specific policies and/or classify the security requirement separating normal data and from vulnerable data in a separate process. Some of which is to customize the SDN framework to make all components work independently and securely.

However, none of them focuses on defense against DDOS attack. The paradigm of software defined networking (SDN) induced a more centralized approach of network control, where the network is controlled and managed by the controller in a global perspective.SDN is simplified in network management which is facilitated through dynamic programming instead of low- level device configurations. However, SDN is facing great challenge in network security because of centralized control plane.

Peng Li et al[1].,proposed a secure SDN architecture, in which one switch is controlled by many controllers using Byzantine mechanism and controller assignment problem to minimize the number of employed controllers while the security requirements are satisfied for each individual switch, in terms of the required number of associated controllers and the maximum latency among them. Heuristic algorithm is proposed to solve this issue. Curtis et al [2]., proposed DevoFlow, a modification of the OpenFlow model in which he tried to broke the coupling between central control and visibility, without imposing high costs. Kim et al [3]., described CORONET, a SDN fault-tolerant system that can be recoverable from multiple link failures in the data plane. Onix [4]. a platform for control plane on top that is implemented as a distributed system. Control planes which are written within Onix are operated on a global view of the network. The FatTire [5]. a language for writing network programs which is fault-tolerant. FatTire, provided algorithms for compiling programs to Open Flow switch configurations.

DDos attack is the great threat to any network and SDN is not exceptional. It has the capability to destroy the entire network resources and bandwidth. We focused mainly in detection of one of the DDos attack called smurf attack.

Our paper is structured as follows: First we gave brief introduction about Software define network and the threat faced by network in terms of security. After that various literature surveys about the security issues in

Software defined networking is defined and analyzed. Then we discussed about the overall concept about DDOS attack and each detection method is clearly explained in detail along with its output obtained.

II. SDN ORCHESTRATION USING MULTIPLE CONTROLLERS

Proposed Design of SDN Networkwith Multiple Controllers

The main contribution is to show the way in which DDOS attack can bind controller resources while processing malicious packets while processing in SDN. The following figure specifies the detection of DDOS attack called smurf attack. Multiple controllers in SDN are established as master-slave method in which one controller act as master and others act as slave. Connections are established between those controllers and the master controller allows flow of packets inside the network as per queuing algorithm. Oncethe packets flows inside the network architecture the controller will check for its flow table entries. Master controller check its flow table updates with other controllers and check its flow table entries. If the entries are different with other controller's flow table entries and identify the vulnerable controller and the master controller does not allow flow of packets inside the network.

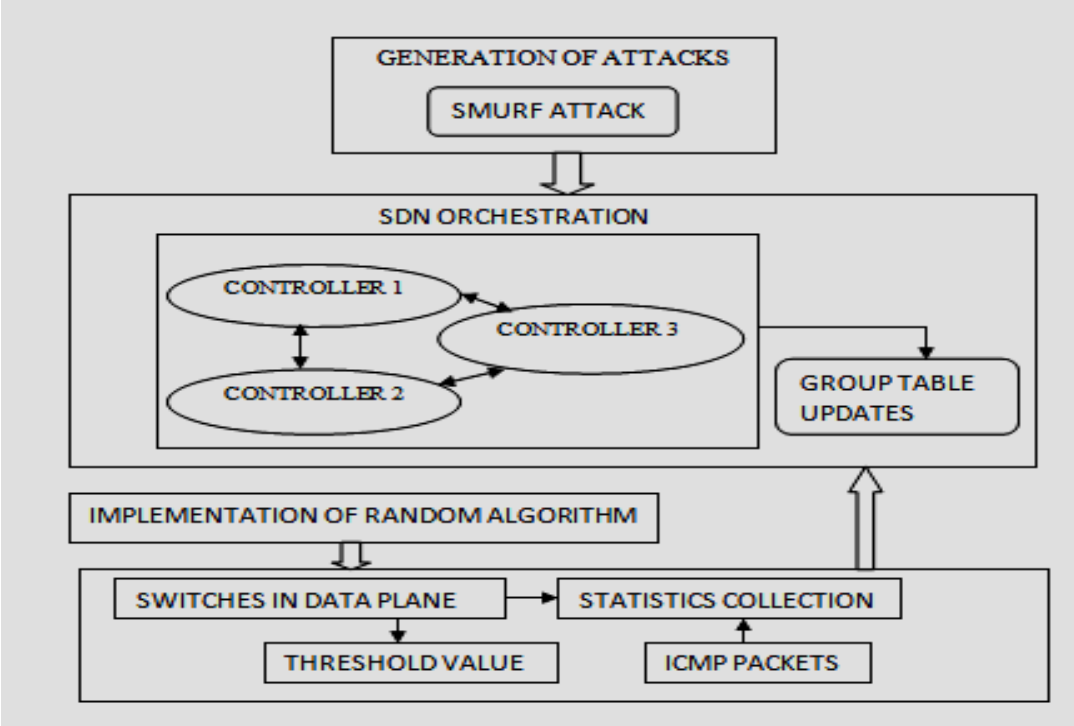

Fig 1: SDN Orchestration

Deployment ofAlgorithm In SDN Orchestration

The job scheduling policies in Software Defined Networks were carefully selected for evaluation namely Random algorithm. This algorithm is considered the most common and frequently used algorithm for job scheduling in SDN. The idea of random algorithm is to send the packets randomly to the SDN network switches. The algorithm does not analyze the status of the network which might be either being under heavy or low load. It will just forward the packets to the assigned switches by the controllers. The job is to allocate service to the queued switches which is connected with controllers. Hence, this may result in the selection of switches under heavy load and service is provided.

Statistics Collections during DDOS Attack

A distributed Denial-of-Service (DDOS) attack imposes major threat to SDN for the availability of the resources to global internet infrastructure. Here DDOS attacks are detected using statistics about the hosts in the network. During smurf attack, a huge amount of icmp packets are broadcasted by the attacker to all the subnet of hosts in SDN network. The ip address of particular host is spoofed to become a victim to attack. In our network, the compromised controller will spoof the particular host and flood the flow rules to particular switch in the network. This will affect the network traffic in terms of resource. A threshold value is set for every available

switch in the network. The value is set based on icmp packets. If that value exceeds during the attack and it is detected as attack. The window size should be set to be very small or equal to the number of switches in order to provide accurate calculations. The total packet size is divided intoset of icmp packets. It is possible to see its value during detection when a large number of packets are attacking one host or a subnet of hosts.

III. ALGORITHMSFOR SOFTWARE DEFINED NETWORKS

Monte Carlo Random Algorithm (MCRA):

A random algorithm that may produce incorrect results, but with bounded error probability

Las Vegas Random Algorithm (LVRA):

A random algorithm that always produces correct results, the only variation from one run to another is the running time.

- Consider random unreliability Δ and a bounding set B
- **Δ** is a (real or complex) random vector (parametric unreliability) or matrix (nonparametric unreliability)
- Consider a performance function
  J (**Δ**): $R^{n, m} \rightarrow R$ and level$\gamma > 0$.
- Define worst case and average performance
  J_{max} = max J (Δ) ,$\Delta \in B$
  J_{ave} = E Δ(J (Δ))
- H_∞ performance of responsive function
  S(s, Δ) = 1/ (1 + P(s, Δ) C(s))
  J (Δ) = || S(s, Δ) $||_\infty$
- Objective: Check if
  $J_{max} \leq \gamma$ and $J_{ave} \leq \gamma$
- These are unreliability decision problem

Random algorithm

Input: List of available switches
Output: Map each host to switches
Steps

```
Nocl ← switchlist.size ();
NoVM← VML.size ();
index←0;
   For j← 0 to Nocl do
        Cl ← switchlist.get (j);
        index ← random () x (NoVM-1);
        V← VML.get (index);
        stageIn ← TransferTime (cl, v, in);
        stageOut ← TransferTime (cl, v, out);
        Execute← ExecuteTime (cl, v);
if (stageIn+Execute+stageOut+ Cl.AT +V.RT≤Cl.DL) then
        SendJob (Cl, V)
        update (v);
        else
        Drop (cl);
                Failedjobs;
end if
```

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

The packets entering during DDOS attack is given based on time interval. The simulation is done using emulator called mininet. During DDOS attack there will be huge amount of icmp packets entering the network. This packet has characteristics of normal packets. This abundant packet is the vulnerabilities which attack the network.Vulnerabilities are icmp packets entering the network. The packets flowing through the network is the icmp packets of smurf attack. The packet size is almost detected which is shown in Fig 2. Nearly sixty percent of incoming vulnerable packets are detected.

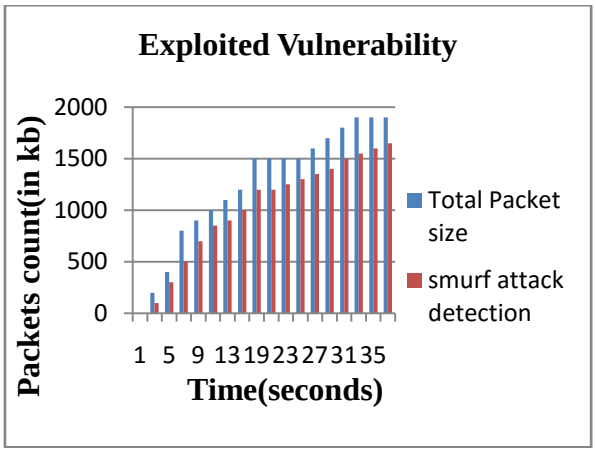

Fig 2: Exploited Vulnerability

There is a sharp detection in attack which is specified in Fig 3 when large number of packets flows to the same subnet, the confidence interval of 73% rate attack is found on a single host.

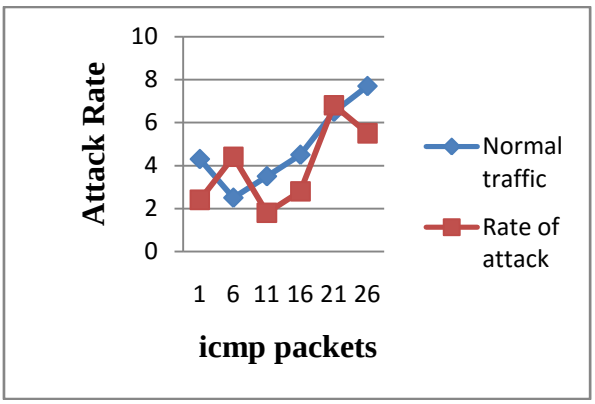

Fig 3: Statistics Collections

V. CONCLUSION

In this paper, a different approach is proposed to detect the DDOS attacks in multiple controllers using a special technique called statistics collection. A special algorithm named random algorithm is implemented in SDN network to provide service efficiently to the hosts which using this network and the smurf attack is detected. The future work is to minimize the attacks using suitable algorithms.

REFERENCES

[1]. Amiya Nayak, Li, Peng Li and Song Guo (2014), "Byzantine-Resilient secure software defined networks with multiple controllers in cloud", IEEE TRANSACTION,Volume:2, issue:4, pp. 436-447.

[2]. A.R.Curtis,J.Tourrilhes,J.C.Mogul, P.Yalagandula, P.Sharma and S.Banerjee (2011), "DevoFlow: SCALING FLOW MANAGEMENT FOR HIGH PERFORMANCE NETWORKS, ACM SIGCOMM Conference, pp.254-265.

[3]. H.Kim,J.Santos, J.Tourrilhes, M.Schlansker, N.Feamster and Y.Turner (2012), "Coronet: Fault tolerance for Software Defined Networks ",IEEE ,Network protocols (ICNP), pp. 1–2.

[4]. H.Inoue,J.Stribling,L.Poutievski,M.Casado, M.Zhu,N.Gude, R.Ramanathan, S.Shenker, T.koponen, T. Hema, and Y. Iwata, "ONIX: *A Distributed Control Platform for Large Scale Production Networks*", in Proceedings of the 9th USENIX Conference: OPERATING SYSTEMS DESIGN AND IMPLEMENTATION, CA, ser. OSDI'10. Berkeley, USA: USENIX Association, 2010,pp.1–6.

[5]. A.Guha, M.Reitblatt, M.Canini and N.Foster (2013), "Fattire: Declarative Fault Tolerance for Software Defined Networks",ACM SIGCOMM,Workshop on SDN, ser. HotSDN '13. New York, NY,pp.109–114.