HEURISTIC APPROACH OFADAPTIVE POLICY BASED SECURITY USING SDN

[1]Abhijit Jamble
Computer Network department
G.H. Raisoni College of Engineering and Management
Wagholi, Pune, India

[2]Geeta Atkar
Computer Network department
G.H. Raisoni College of Engineering and Management
Wagholi, Pune, India

Abstract—Hardware based routers have limited constraints of routing knowledge as they do have lesser processing capacity. Now a days as the field of distributed system, cloud computing system and internet grows computer industry is in huge demand of intelligent routing devices. But the fact is that due to limited hardware in the physical router they are unable to take the run time decisions about routing. So Software Defined networks(SDN) plays vital role in defining the routing protocol in run time according to the raising situation. This paper proposes a heuristic approach of routing the incoming data to a SDN Server based on the adoptive policies. These policies are defined based on the data distribution factor which is measured using Shannon information gain on clusters created by the Fuzzy C means clustering. Then an enhanced Decision tree technique is used to take the finite decision of routing for different purposes.

Keywords—Policy making, Fuzzy C-meansClustering,information gain , Decision Trees, Software define network.

I. INTRODUCTION

Software Define Network (SDN) is a latest kind of networking technology, in which the network is as agile, and flexible as the virtualized server. In this technology the control of network is distributed from its origin and then rerouting by programming. It provides open interfaces which, allows network engineers to programmatically initialize, change, respond quickly according to changing business demands and manage network behavior dynamically. In a SDN, a network engineer can control traffic flow through a control console without any need to manipulate switches and assign services to the required network. It is a simple, new technique of handle networks that separates network control from the network plane. SDN also simplifies the devices used in network, due to which there is no need to handle and used many protocol standards, but only follow instructions from the SDN controllers. It also supports a set of APIs, due to which it is possible to implement common network services.

In SDN the network is handled by differentiating the control logics to centralize the network protocols to work efficiently. SDN handle the entire network through intelligently organized and provisioning systems, it has some version of an SDN controller, as well as southbound APIs, and northbound APIs. SDN controller is the main part of the network, it enable network engineers to define switches and routers how to handle network traffic. SDN uses both APIs to relay information to switches and routers to interfere with the needed requirements based on the protocols. Theses help network engineers to programmatically handle traffic and deploy services.

Decision tree is a very important tool used for decision making in the field of machine learning, decision analysis and operational research. It is a tree like diagram or graph to identify every possibility and results of the decision. The internal node of decision tree represents a test (attribute), branches represent the results of the test, and leaf node represents the final decision after calculating all the attributes. The overall path from root to leaf is defined as classification rules. It is very effective in taking complex decision in the field of operational research, data mining, operation management etc. The structure of decision tree makes people to analyze multiple solution of a problem, the risk and rewards linked with every decision and find the best decision from all possible outcomes. The decision tree is drawn from left to right as long or as short depends upon the proper outcome. Normally, the decision tree is drawn using flowchart symbols to make it easy to understand. Some of the advantages of decision tree are, it is easy to understand, calculate all the outcomes of decision either it is worst, good or as expected, allow to add new scenarios at any point etc.

Short for Denial of Service Attack (DOS), where attacker attempt to prevent users to access network service temporarily or permanently by causing disturbance of a network connected server. The attacker deliver flood of message to the host to make systems overload with an invalid return address. Incorrect return addresses make the server unable to get authentication approval, due to which server wait for sometime before closing the connection. The attacker sends more authentication message with wrong return address after server closing the connection this makes the server busy continuously. The attacker prevents users to access email, online accounts, or the sites user looking for by targeting its computer or network connection. The most frequent type of DOS attack happen when the attacker floods the network with information, due to which user cannot access the site when sending the request because server of that site is overloads with invalid information of attackers. An attacker also make your email account affected by DOS attack by using spam email message. The slow internet performances, incapability to approach any website, increase in spam message are some of the symptoms of DOS attacks.

Internet uses for commercial purpose by the organizations raises the demand of technology that provides them fruitful products to increase their business opportunities without compromising with their security. The open internal network connection with public and weekly controlled network raises lots of security threat to these organizations. Theses security threat raises the technology of Deep Packet Inspection (DPI) or Complete Packet Inspection (CPI) that allow devices like firewall or IPS to inspect packet data contents deeply, including all the seven layers of OSI (Open Systems Interconnection) model.

Analysis of packets using DPI, includes searching for virus, intrusions, spam, protocol, etc., and after proper analysis to decide whether the packet forward or reroute to different destinations. DPI technology makes the service personnel to allocate serviceable resources to make highly efficient and effective traffic flow. For example, high priority tag message routed ahead than a low priority message to its destination. Span Port or Pot mirroring is the common way to obtain packets for DPI (Deep Packet Inspection). DPI enables the proper maintenance of network management, network security, overhearing, internet censorship and data mining of the internet. DPI technology is used in many government organizations, telecommunication services, large institution, etc.

In this paper, section 2 is dedicated for related work of past works. Section 3 describes the proposed methodology and Section 4 discusses the results and evaluation of the proposed technique.

Finally Section 5 concludes this paper with future extension possibilities.

II. RELATED WORK

Guest Tutorial presented by **[1]** introduces software defined networking concept. With enormous infrastructure in IT ecosystem is challenging task to handle. Numerous components have achieved limitation thrashing progress of IT industry. Development of cloud and IOT based System have uplifted computing power with serious issue of security. Current security mechanism are hardware based, costing largely with major limitations.

To overcome this new software based security system approach is been required. This Approach is been introduced in software defined networking. Major limitations exists in implementation of software defined networks but advantages are decoupling of network service with security implementation. software defined environment brings jointly software defined compute, networking, and storage, and unifies the control planes from individual software defined components. Unified control planes provide rich resource abstractions to enable assembling purpose fit systems, and provide programmable infrastructures to enable dynamic optimization in response to changing business requirements.

Future Scope of work is development of software defined environment.

Experimental implementation of **[2]** present challenges that in real time network debug and security implementation is challenge. As such self contained network management system OSN development is essential. In this scenario as single laptop machine would assist in run time Prototype implementation. Prototype implementation is been presented .this system would require in more development. The prototype presented is simpler laptop based design which could be modified developed and enhanced

Scope of work is better mininet based software defined network system.

Paper focuses on PBM Address struggle determination in PBM, an indispensable perspective while handling with a structure using strategies in OSN. The paper focuses on quality of services. Presenting at least minimum scalability level to be achieved. Survey presents the contention determination issue in implementing OSN and Software defined environment. In goal to achieve dynamic security prototyping. Opensec guarantee this implementations bringing together better network handling ability.

Research outcomes of work in **[4]** illustrate that opensec system scale well on grounds of dynamic network management. Newly defined protocols are been implemented with sampled modifications. Demonstration illustrate advanced security mechanism are been implemented with minimal hardware requirement. The time and cost required in network management is minimized. As such OPENSEC Methodology is up and above existing approaches and superior in all parameters of comparison.

Article post on **[5]** signifies the importance of SDN in network management. SDN are popular approach in network design and management. Harder implementation of network is been simplified with SDN . Complete network control remains at one level. Putting up network to work with manual queries is shifted with automated approach. Fully dynamic policies are been generated at run time. With new rules network security is been implemented.

Breakdown of network control flow from data plane is done with SDN implementation. Overall data handling is been done logically designed controller. Complex work flow is been implemented in simple flow plan of SDN. This methodology shift of control is done from central to logical SDN controllers. OPENFLOW rule has built standardization. This model gives complete network data flow view in single mapped way.

OPEFLOW help regulator to modify delete or add new policies of. System could switch in one layer to another using OPEN FLOW protocol **[5].** As such OPENFLOW builds a complete security framework. Numerous operators exist in implementing desirable security policies. In real time implementation . System are been switched from one layer to other with OPENSEC for all data packets. This protocol with assist system to switch from layer to layer for incoming packets. OPENFLOW and OPENSEC build a better framework assisting network admins to implement new desired security system . This scenario admin mirror traffic data and performs check for spam files. SDN hope to bring high level policies for dynamic policy implementation.

This is where SDN are scope of work ,where admin is not been required to classify and route desired traffic to server. Manual blocking of users.

While OPENSEC is overview of network machinists would give attention to stipulating easy human understandable policies for security. OPENSEC contains of a software layer seriatim on first of network controller also multiple exterior plans that achieve security facilities like IDS(intrusion detection system), system firewall, DPI(deep Packet inspection, spam detection while others recently been reported to controller. OPENSEC objective is to allow network operator to provide advanced security policies {in the event of| case there is the case of specific flow.

Author **[6]**address battle assurance in PBM, a basic perspective while managing a system using techniques. Certainly, as the makers point out, when a couple of methodologies exist together it is most likely going to encounter that no less than two game plans give a substitute yield for a comparative data. This audit addresses the issue of dispute assurance while using ways to deal with give Nature of Administration (QoS). OpenSec resembles these strategies in that it proposes a united structure prepared for getting game plans as information and examining them, checking for conflicts and executing them.

A great deal of work has focused on procedure specific , game plan refinement and approach examination in frameworks. Procedure based organization (PBM) has in like manner been associated with arrange organization [and security **[7].** Agrawal et al. give a graph of how course of action based organization can be associated with sorted out systems. In particular, they illuminate how Strategy Administration for Autonomic Figuring (PMAC) can be associated with organize organization. Pretty much, PMAC is a nonexclusive procedure middleware that sponsorships wide and versatile approach lingos.

In like manner, a Strategy Definition Device (PDT) should be given to allow customers to make and change approaches. Finally, an automated boss is accountable for social affair courses of action and executing them.

Extent of work lies in outline arrangement usage in understanding to human configuration. Furthermore information identified with organize movement should deal with through handling units. As controller is been troubled with many-sided quality and little jug necks of preparing. Existing works concentrate on outlining system that execute and make human great strategies**[9,10].**

Author **[11]**Extent of work lies in outline arrangement usage in understanding to human configuration. Furthermore information identified with organize movement should deal with through handling units. As controller is been troubled with many-sided quality and little jug necks of preparing. Existing works concentrate on outlining system that execute and make human great strategies

III PROPOSED METHODOLOGY

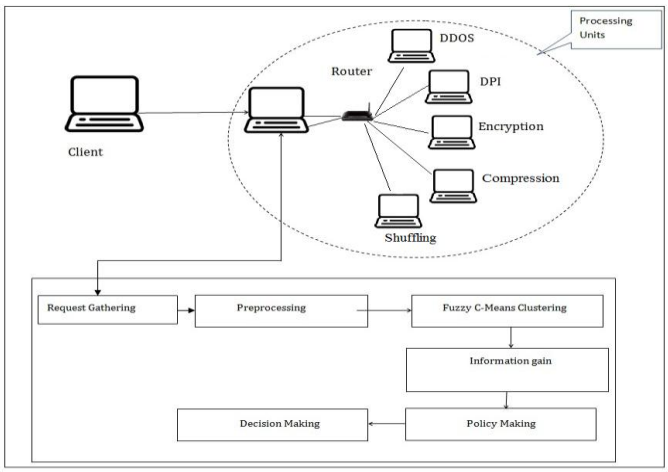

Figure 1: Proposed Sytem Overview

Software defined methodology for adaptive secuirty policies is been detailed asbelow . thi ha s been show in figure 1 . process envolved in development life cycle is as below .

Step 1:Initialization of process -This is ths intial venture of the framework where customers are sending differnet sorts of demand from various systems for various assignments, These undertakings and solicitations are been gathered in a vector for additionally prepare.

Step 2: Request Collection - Here in this progression every one of the solicitations that are gathered in a vector are put to preprocess, where fundamental required characteristics are chosen and put away in another vector to yield preprocessed vector.

Step 3: Here preprocessed information vector is utilized to make diverse groups in view of the demand data. This bunching should be done in view of the sensible perspective as these groups are in fact assumes imperative part in arrangement making.

Advanced Fuzzy Means clustering process is used for this process that can be depicted in algorithm 1.

ALGORITHM 1: FCM

Let P = {p_1, p_2, p_3 ..., p_n} be set of data points and
c = {c_1, c_2, c_3 ..., c_c} be the set of centers.
Step 0: Start
Step 1: Randomly select *'c'* centers.
Step 3: Calculate fuzzy membership $'\mu_{ij}'$ using:
$\mu_{ij}=1/\sum_{k=1}^{c}(c_{ij}/c_{ik})^{(2/m-1)}$
Step 4: Compute fuzzy centers $'v_j'$ using:
$V_j= (\sum_{i=1}^{n}(\mu_{ij})^m X_i) / (\sum_{i=1}^{n}(\mu_{ij})^m)$,
for all j=1,2,…c
Step 5: Repeat step 2) and 3) until minimum *'J'* value is achieved or $||U^{(k+1)} - U^{(k)}|| < \beta$.
where, *'k'* is iteration step.
'β' termination criterion between [0, 1].
'U = $(\mu_{ij})_{n*c}$' is the fuzzy membership matrix.
'J' is the objective function.
Step 6: Stop

---

*Step 4:*With a specific end goal to choose the best trait for production of arrangement framework utilizes data put on theory.Here Weight based selction handle is done in view of the shannon data pick up hypothesis, Which is said in condition 1.

IGR(C) = -Σ (| C_i | / | C |) log (| C_i | / | C |) --------(1)

Here
$C_{i=}$ repetataion of Cluster C.

Step 5: Once the Important solicitations are been distinguished then approaches are been characterized utilizing choice tree strategy by ecaluating the required entropy of the diverse perforamance servers. By doing this system properly prepares routing policy based on algorithm 2.

ALGORITHM 2: POLICY MAKING

// Input – Data Vector D
// Output -Policy P
Step 0: Start
Step 1: FOR i=0 to size of D
Step 2: each Data vector element Di
Step 3: verify Data Extension E
Step 4: Get Protocol List L
Step 5: If E belongs L
Step 6: Decision making M
Step 7: M belongs to Set S { Ds,Dpi,Rcc,Dc,Ds}
Step 8: Update Policy Database
Step 9: End IF
Step 10: End For
Step 11: Stop

Where Ds : DOS attack Evaluation Policy
Dpi : Deep packet Intrusion Policy
Rcc : Reverse Circle Cipher Encryption Policy
Dc : Data Compression
Ds: Data Shuffling

IV RESULTS AND DISCUSSIONS

4.1 Experimental Setup

The proposed system's implementation is carried out by using 6 machines of pentium i3 processor which are having minimum primary memory of 2Gb. Each of the machines are windows based java machines, Netbeans is used as IDE for the development process. And System uses all format of file system for policy making process.

Proposed system is incorporated for 5 different tasks that are carried out due to the decision making capability of our system in the live network.

The tasks are like DOS attack, Performing Deep packet intrusion on Data(DPI) , Encrypting the data using Improved Reverse circle cipher Encryption Algorithm, Compressing the data for storage using tree based compression technique and Data shuffling using random shuffling technique.

4.2 Evaluation

To evaluate the process of policy making by our methodology of decision making through clustering proposed model subject the system to measure time taken for policy making. When our proposed system is measured for time taken to create proper policy and the obtained results are tabluted as shown in the below table1.

Policy No	Open Sec (In milliseconds)	Entropy Based (In milliseconds)
1	2.5	2.8
2	3	2.7
3	3.4	2.9
4	2.9	2
5	2.4	2.2

Table 1: Time taken for policy making

Above table 1 shows the values of time taken for policy making by our system and the system that ismentioned in [12]. The method mentioned in [12] works on the policy making process for SDN

using opensec technique.The graph for the table 1 can be depicted in figure 2.

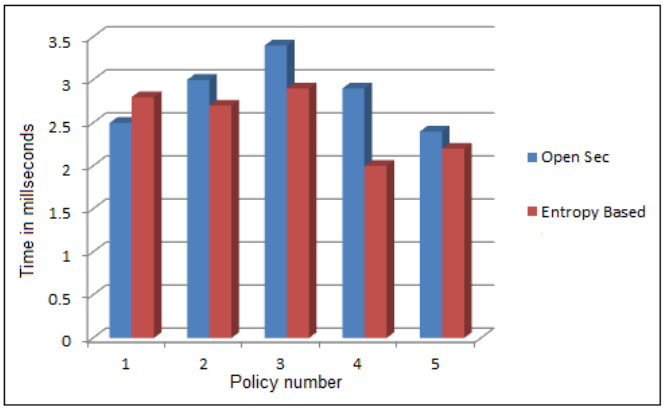

Figure 2: Performcane comparision for Policy making for SDN between Open sec V/s Entopy based technique.

Above figure2 indicates that proposed methodology of entropy based technique for policy making achieves good timings then that of Open sec method of policy making used in [12].

V. CONCLUSION AND FUTUREWORK

This paper deals with the adaptive policy making using software defined network for different tasks that are generally performed by the different performer servers in the distributed network. Proposed system uses the Software defined network for routing the data based on adaptive decision making for different performer servers. These server perform some actions like Idenfiying DOS attack, Performing Deep packet intrusion on Data(DPI) , Encrypting the data using Improved Reverse circle cipher Encryption Algorithm, Compressing the data for storage using tree based compression technique and Data shuffling using random shuffling technique.

Proposed system can be enhance to take multiple actions based on the user defined protocols in quick time using distributed decision making system.

REFERENCES

[1] Li, Chung-Sheng, and Wanjiun Liao. "Software defined networks." IEEE Communications Magazine 51.2 (2013): 113-113.

[2] Lantz, Bob, Brandon Heller, and Nick McKeown. "A network in a laptop: rapid prototyping for software-defined networks." Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. ACM, 2010.

[3] H. Kim and N. Feamster, “Improving network management with softwaredefined networking,” IEEE Communications Magazine, vol. 51,no. 2, pp. 114–119, February 2013.

[4] Tootoonchian and Y. Ganjali, “HyperFlow: A Distributed Control Plane for OpenFlow,” in Internet Network Management Conference onResearch on Enterprise Networking, San Jose, CA, April 2010.

[5] http://www.webopedia.com/TERM/S/software_defined_networking.html[online].

[6] H. Kim and N. Feamster, “Improving network management with softwaredefined networking,” IEEE Communications Magazine, vol. 51,no. 2, pp. 114–119, February 2013.

[7] N. Foster, R. Harrison, M. J. Freedman, C. Monsanto, J.Rexford,A. Story, and D. Walker, “Frenetic: a network programming language,”in ACM SIGPLAN International Conference on Functional Programming,Tokyo, Japan, September 2011.

[8] A. Voellmy, H. Kim, and N. Feamster, “Procera: a language for highlevel reactive network control,” in Workshop on Hot Topics in Software Defined Networks (HotSDN), Helsinki, Finland, August 2012.

[9] Lara and B. Ramamurthy, “OpenSec: a framework for implementingsecurity policies using OpenFlow,” in IEEE Globecom Conference,Austin, Texas, USA, December 2014

[10] F. Yonghong, B. Jun, W. Jianping, C. Ze, W. Ke, and L. Min, “A dormantmulti-controller model for software defined networking,” Communications,China, vol. 11, no. 3, pp. 45–55, March 2014.

[11] S. Lange, S. Gebert, T. Zinner, P. Tran-Gia et al., “Heuristic approachesto the controller placement problem in large scale SDN networks, Network and Service Management, IEEE Transactions on, vol. 12, no. 1,pp. 4–17, March 2015.

[12] Adrian Lara and Byrav Ramamurthy ,"OpenSec: Policy-based Security Using Software-defined Networking",IEEE GLOBECOM 2014.