ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

Survey on Interference Disclosure System by Using Machine Learning in Software Defined Network

Elumalai J[1], Bhuvaneshwari D[2], Malathi R[3]

Asst. Professor, Dept. of IT, Jeppiaar Maamallan Engineering College, Tamil Nadu, India[1]

Student, Dept. of IT, Jeppiaar Maamallan Engineering College, Tamil Nadu, India[2–3]

ABSTRACT: Software-Defined Networks (SDN) is an emerging area that promises to change the way we design, build, and operate network architecture. It tends to shift from traditional network architecture of proprietary based to open and programmable network architecture. Security is one of the major issue in SDN. Wse propose a system that send data in alternate path if traffic occurs or connection closed in the current path.Machine learning algorithm can predict the hindrance in the path and sends alert message to the client, then the client can change the route of the data in other shortest path. The data travelled path is stored in the MAC table for further references. The OTP message will send to the user mail id whenever they login to prevent the intruder. Here the intruder cannot steal the data because the data is in encrypted format, the only thing the intruder can do is either crash the data or change the data path. The advantage of the system is security and accuracy improved by using software defined network machine learning methodologies.

KEYWORDS : Software-defined Network; Intrusion Detection System; Machine Learning;

I.INTRODUCTION

SOFTWARE defined networking (SDN) has become one of the most important network architectures for simplifying network management and enabling innovation in communication networks. SDN decouples the network control from the data forwarding plane. The control plane is logically centralized and the forwarding plane is rendered simple to act on decisions from the control plane[2]. In SDN, new control functions can be implemented by writing software-based logic in the control plane which deploys the decision logic in the forwarding plane through standard interfaces. A network operating system (NOS) in the control planemaps the entire network to different services and applications that are implemented on top of the control plane. OpenFlow [3] is the most accepted and widely used implementation architecture of SDN.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

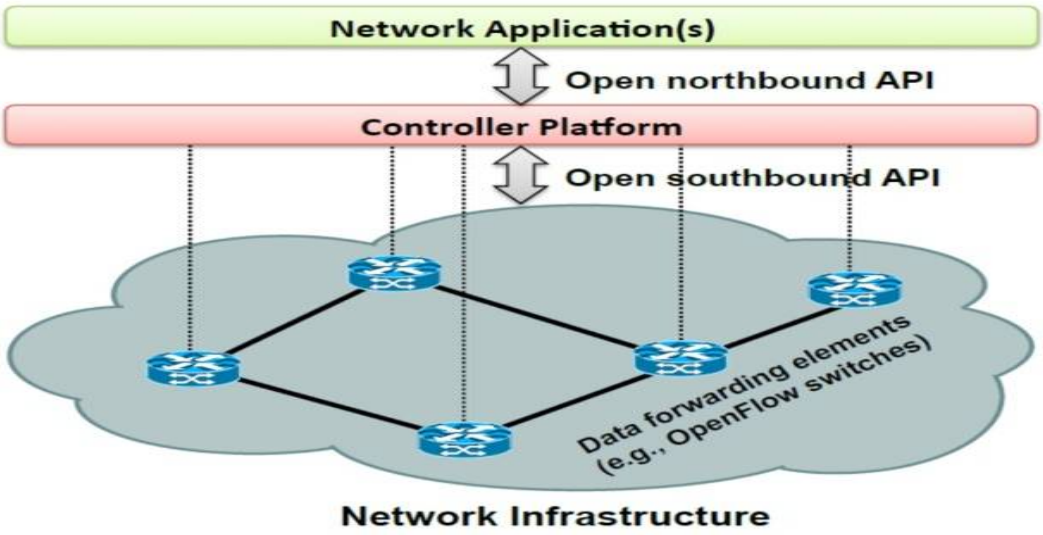

Figure 1:Software Defined Networking

Furthermore, current network architecture has many limitations, which were resolved with the emergence of new SDN architecture. These include but are not limited to: inability to optimize network for WAN and Data Centre to generate more revenue and reduce expenses. With SDN more revenue can be generated by monitoring network devices and optimizing device utilization with a dynamic feature of SDN. The increase in capital and operational cost with SDN automation reduces human involvement in managing resources to a minimum which significantly reduces the cost.
The SDN comprise three-tiered architecture that is designed to simplify network management[5]:

- The Application layer: contains application that delivers services.
- The SDN Controller: them a indecision-making component separated originally from data plane which facilitates automated network management.
- The Infrastructure layer: a hardware layer that requires command line interface (CLI), but it does not need programming language, unlike otherlayers.

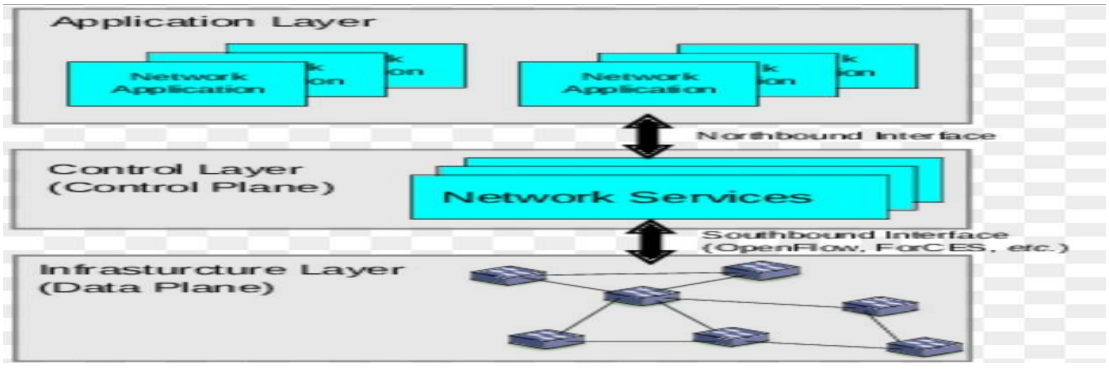

Figure 2: The SDN System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

II.BACK END PROCESS AND RELATED WORK

The main advantage of SDN is flexibility, efficiency and cost management. SDN is a highly configurable network. Traditional network have some restrictions in accessing some data's. Automation can done by using machine learning technology.Despite the security consideration in designing SDN architecture, the SDN environment still has security issues that need to be addressed [1]. An intrusion detection system (IDS) is a device or software application that monitors a network and/or information system for malicious activities or policy violations and responds to that suspicious activity by warning the system administrator, displaying an alert, and logging the event [12]. Machine learning mechanism which we use here is the algorithm that makes the system to think of its own and without the knowledge of humans. It is one of the applications of artificial intelligence. The machine learning algorithm works at the server side which can be decide the path of the nodes to travel in the network. IDS can be fixed in the network to avoid the intruder to access or stole the sensitive data that can be sending.

The earliest single-path routing protocols applied Dijkstra's algorithm for route selection.When it comes to any path routing, for example, appeared as a coordination mechanism between forwarders; broke such coordination where all the forwarders worked according to their workload. Besides, MORE introduced network coding into any path routing. On that basis, proposed the shortest any path first algorithm to determine the forwarders priorities, and proved its optimality; incorporated rate control and used a notion called credit to realize flow control; enabled concurrent transmissions of a window of segment it considered the problem of path divergence and rate limitation to efficiently support multiple flows; Source Sync synchronized senders to achieve combined signals which lowers the packet error rate. Besides, developed an optimization framework to exploit communication opportunities arising by chance; proposed based on a per-packet feedback mechanism. In addition, different from works such which should to some degree rely on synchronization between nodes, the throughput improvements of our algorithms in this work do not need MAC-Table coordination.Some existing cross-layer approaches jointly consider routing and link scheduling is formulated joint routing and scheduling into an optimization problem, and solved the problem with a column generation method. It dealt with the joint problem in cognitive radio networks considering the vacancy of licensed bands. It implemented k-tuple network coding and proved throughput optimality of their policy. Although these works can provide good performance theoretically, they need centralized control to realize MAC-Table scheduling, and to eliminate transmission contention. The algorithms proposed in this work do not require any scheduling, and the algorithms can be implemented in a distributed manner. Its aimed to work at exploiting spatial readability. Specifically, the authors in considered the trade-off between spatial reuse and data rate, and proposed a decentralized power and rate control algorithm for higher network capacity. It investigated the optimum carrier sensing range for throughput maximization. However, none of these works deal with the problem of route selection.

III.EXISTING SYSTEM

In the existing system, there is no option to send the in alternate path if traffic occurs in current path or connectivity lost in the data path. And the router has only limited amount of capacity to send. If the intruder enter in the system they can easily access and steal the data because of less security features.

The security threat has become so frequent from within, the effect of these attacks ranges from mild to critical.The credibility, integrity, or availability of hardware, software or an information resource usually alters the security breach. The attack on these components can bring considerable damage to the organization. The damages can be a loss in monetary or reputation which may lead to the total or partial collapse of the organization. Therefore, an effective measure must be put in place to avoid the damage [1].

The SDN architecture has some security issue in the network management. The security threat of the SDN architecture arises in three layers namely application layer, control layer and infrastructure layer. If someone who is unauthorized can enter the system, then the alert message is send to the client by the machine learning at the server side. Many

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

attacks becomes possible in the SDN by the centralized control access. The most common attack in the network is DOS which can denied theservices.

IV.PROPOSED SYSTEM

Our system send data in alternate path if traffic occurs or connectivity lost during data transmission. Machine learning algorithm can predict the hindrance in the path and sends alert message to the client and then the client change the data in other shortest path. By using OTP it become complicated to anyone other than user to login the system. Difficult to intruder to steal the data.

We propose a system that sending data in alternate path if traffic occurs or connection closed in the current path. Machine learning algorithm can predict the hindrance in the path and sends alert message to the client, then the client can change the route of the data in other shortest path. The data travelled path is stored in the MAC table for further references. The OTP message will send to the user mail id whenever they login to prevent the intruder. Here the intruder cannot steal the data because the data is in encrypted format, the only thing the intruder can do is either crash the data or change the data path. The advantage of the system is security and accuracy improved by using SDN machine learning methodologies.

A.ARCHITECTURE DIAGRAM

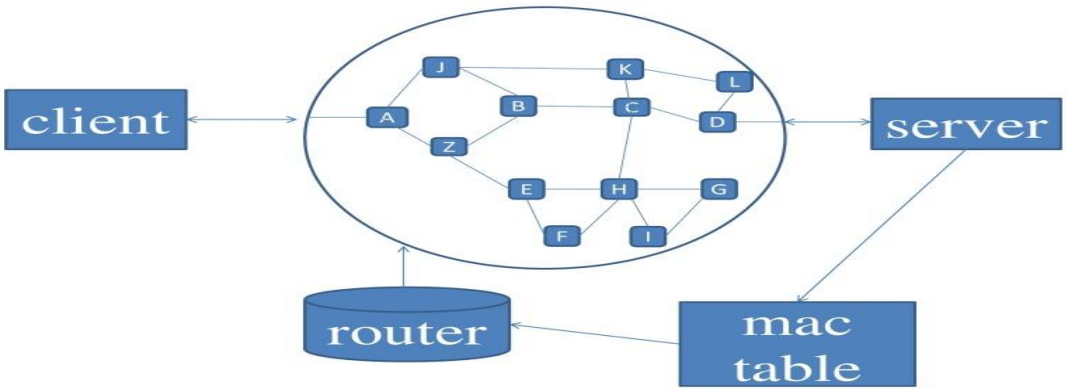

Figure 3: Overall Architecture

Client, server, router, MAC table are connected in the software defined network. At first client send the data to the server via software defined network. The network consist of n number of nodes, all nodes are connected with each other. Machine learning algorithm works on the server side to decide the path of the data and change it in alternate path if traffic occurs. MAC table stores all the information about the data transmission path and it is interconnected with the router. The performance of the router is mainly based on the algorithm which we use in the system. Intrusion detection system mainly focuses to prevent the data from the intruder and IDS process between the client and server.This device monitoring the incoming and outgoing packet within the system or network and notifies the user or administrator if the system is under any potential or actual attack or any unusual activities detected. Normally it operates by taking the snapshot of the existing files and compares it with the previous snapshot of system file, with this the unauthorized activities can be identified.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

B.ARCHITECTURE DESCRIPTION

The user first have to login to the system and the OTP was send to the user's mail id. After that the user have to verify the OTP then only they are permitted to access the system. This is because of preventing the system from intruders and the robots. Then after entering the OTP the user send the data to the server via software defined network. If they want to access the resource directly in SDN, they need not to worry about the user name and password. But in our proposed architecture the intruder cannot steal the data here also because the data is encrypted here. The only thing they can do is either crash the data and destroy the nodes.Machine learning algorithm can predict the hindrance in the path and sends alert message to the client, then the client can change the route of the data in other shortest path. The data travelled path is stored in the MAC table for further references. The OTP message will send to the user mail id whenever they login to prevent the intruder. Here the intruder cannot steal the data because the data is in encrypted format, the only thing the intruder can do is either crash the data or change the data path. The advantage of the system is security and accuracy improved by using SDN.

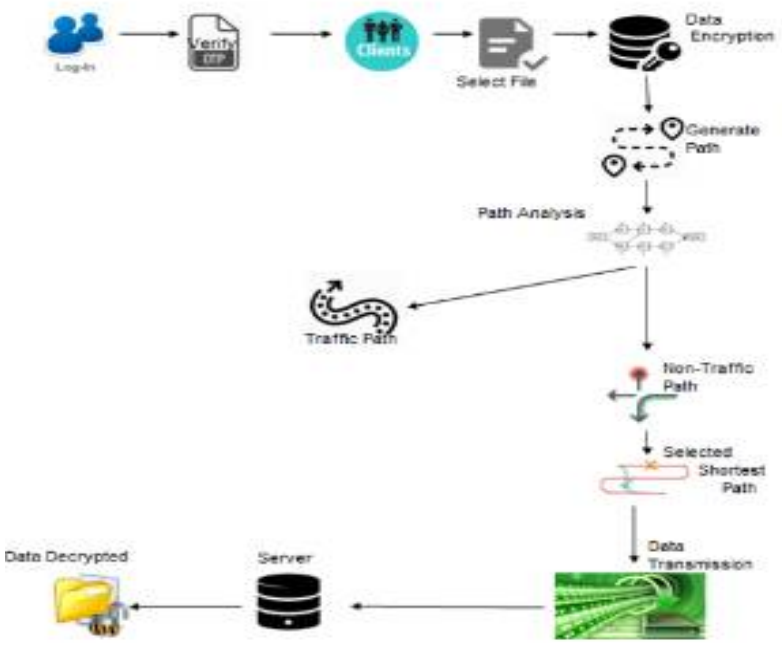

Figure 4: Flow of Architecture

V. NETWORK IMPLEMENTATION

Statistical machine learning has been widely used and has become an important tool in various applications for detecting and preventing malicious activity. Moreover, big data in the presence of redundant records makes intrusion detection a complicated task. Most IDS try to perform their task in real time but their performance suffers. The purpose of this research is to propose an efficient technique for intrusion detection that takes two ways into consideration. First,efficient use of data mining techniques to extract and filter out a suitable subset of data, for which we opt to use

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

raw data. Secondly,applying efficient machine learning techniques for extracting patterns for intrusion detection in real time, as machine learning approaches provide an opportunity to improve the quality and to facilitate easy administration of IDS [12].

Traditional packet networks lend themselves to scalable solutions because they do not require extensive state to be held between system units. Each network node is autonomous, requiring only limited knowledge of its neighbour. 2Routing protocols have been designed to control traffic with this in mind. In order to create resilient networks, alternative paths and secondary equipment are required. The network is very efficient at both front and back end of the implementation. Interference of the can be detected easily by SDN. Data forwarding packets have some of the efficiency and it also easily attacked by the intruder in the network. It can be rectified by the terms of improving security to the system. It may then be necessary to hold some state between systems to ensure that should a failure occur, there is little or no interruption in service. Typical systems that require this functionality include network elements such as Load Balancers and Firewalls. Within a pure SDN environment, a single controller or group of controllers would provide control plane services for a wider number of data-forwarding nodes, thus allowing a system-wide view of network resources [2]. To overcome the network latency and to reduce network loads we can use IDS with decentralized multi agents. This can enhance the performance of IDS and also increase response time by its flexibility. It will delegate analysis functionality among the agents, and use the method of post processing to increase the precision of detection, as post processing of alerts is used to produce a many qualitative alert set in the system.

SDN as similar as the traditional network and it has high configuration in the system. It is interconnected with switches, routers, box appliances. SDN can interfere with the data nodes in the router and switches. The process is mainly based on data transmission in the node of data path. SDN is a open flow network with physical networking devices. It is a crucial approach with improved configuration and network compatibility. Because of high interoperability it can work efficient than other networks. The main difference resides in the fact that those traditional physical devices are now simple forwarding elements without embedded control or software to take autonomous decision. A logically centralized network that control system in the data plane with network intelligence and network operating system application. It delegates the function and analysis it type in the neural network. And also it is flexible for both preprocessing and post processing. These enable open interfaces dynamically in the program with open control enabler heterogeneously something difficult in traditional networks, due to the large variety of proprietary, closed interfaces and the distributed nature of the network. The main intern of the system is to improve the security of the system.

The prevention risk has become so usual from the effect of these attacks ranges from small to big. Fitting curve and time series has poor performance in the traditional network. A new original and improved technology also brings security difficulties.One of the important goals of data center networks is to avoid or mitigate the effect of network bottlenecks on the operation of the computing services offered. Linear bisection bandwidth is a technique that can be adopted for traffic patterns that stress the network by exploring path diversity in a data center topology. Such technique has been proposed in an SDN setting, allowing the maximization of aggregated network utilization with minimal scheduling overhead [5].

Machine learning algorithm can predict the hindrance in the path and sends alert message to the client, then the client can change the route of the data in other shortest path. The data travelled path is stored in the MAC table for further references. The OTP message will send to the user mail id whenever they login to prevent the intruder. Here the intruder cannot steal the data because the data is in encrypted format, the only thing the intruder can do is either crash the data or change the data path. The advantage of the system is security and accuracy improved by using SDN.

VI.CONCLUSION

Software defined network is the one of the emerging technology nowadays. It is the enhancement of traditional networking system and the wireless networking communication. SDN has some of the security issue and it is corrected

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

by using various techniques. In this project, time delay has been corrected by using machine learning algorithm. And by sending the data in alternate (shortest) path we can send more amount of data without traffic and connectionless problems. Data's are more secured. Capacity increases in the router side. By sending the data in encrypted format it becomes complicated for the intruder to steal the data from the system. Security and accuracy of the system get improved by using software defined network.

VII. FUTURE ENHANCEMENT

In future, the project has been enhanced by prevent the intruder before they enter into the system and by block them.By adding this feature the system will become cent percent secured. And the data which can be send from source to destination without any interference in the network and in the user side.

REFERENCES

[1] AtikuAbubakar, BernadiPranggono, "Machine Learning based Intrusion Detection System in Software Defined Network" International Conference on Emerging Security Technologies, IEEE,vol.31, pp.138-143,2017
[2] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A Survey of Security in Software Defined Networks," *Communications Surveys &Tutorials, IEEE*, vol. PP, pp. 1-1, 2015.
[3] N. McKeown*et al.*, "OpenFlow: Enabling innovation in campus networks,"*ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2,pp. 69–74, Apr. 2008.
[4] OpenNetworkingFroundation. (2017, 06/2017). Available: https://www.opennetworking.org/
[5] D.Kreutz, F. M. V. Ramos, P. EstevesVerissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, pp. 14-76, 2015.
[6] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J.Finnegan, *et al.*, "Are we ready for SDN? Implementationchallenges for software-defined networks," *CommunicationsMagazine, IEEE*, vol. 51, pp. 36-43, 2013.
[7] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," in *2016 International Conferenceon Wireless Networks and Mobile Communications (WINCOM)*,2016, pp. 258-263
[8] Security Requirements in the Software Defined Networking Model"," IETF Network Working Group Internet Draft.[Online].Available:https://datatracker.ietf.org/doc/draft-hartman-sdnsec-requirements/
[9] E. Haleplidis, J. HadiSalim, S. Denazis, and O. Koufopavlou, "Towards a network abstraction model for SDN," Journal of Network and Systems Management,pp.1–19,2014.
[10] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, \A Security Enforcement Kernel for OpenFlow Networks," in Proceedings of the 1st Workshop on Hot topics in Software De_ned Networks. ACM, 2012, pp. 121{126.
[12] P. Manandhar, "A Practical Approach to Anomaly-based Intrusion Detection System by Outlier Mining in Network Traffic," *MasdarInstitute of Science and Technology*,2014