Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

REVAMPING SDN TO MINIMIZE THE ASCENDANCY OF ROGUE ACCESS POINTS

P.G.Siva Sharma Karthick[1], R.Poongodi[2], G.Revathi[3]

Assistant Professor/CSE,Nadar saraswathi college of engineering and technology,Theni [1]
U.G Student, Department of computer science and engineering, Nadar saraswathi college of engineering and technology ,Theni [2]
U.G Student, Department of computer science and engineering, Nadar saraswathi college of engineering and technology ,Theni [3]

Abstract— *Software Defined Networking (SDN) is an emerging technology which provides network programmability and encompasses multiple kinds of network technologies designed to make the network more flexible. Rogue access point one of the most challenging issues in security of software defined network. Rogue Access Points are serious threats which steal sensitive information from the network. To overcome above, we propose an approach to detect and minimize the entry of Rogue Access Point from software defined network. Along with rogue access point detection, our works also improve the capabilities of software defined network by using: 1) mininet to create software defined network with SDN controller. 2) Sequential hypothesis algorithm to detect RAPS 3) miniedit as a simulator 4) wire share as a network analyser.*

Keywords—*Rogue Access Point(RAP), Software defined network(SDN), Network flow guard(NFG), mininet ,pox;*

I. INTRODUCTION

Network safety is a specialized field in laptop networking that involves securing a computer network infrastructure. It presents security to a network from unauthorized access and dangers. It's miles the responsibility of community directors to adopt preventive measures to defend their networks from ability protection threats. Community safety is usually handled by way of a community administrator or device administrator who implements the safety policy, network software and hardware needed to protect a network and the resources accessed thru the community from unauthorized get right of entry to and also make certain that employees have ok access to the community and sources to paintings. Community security is defined as the system of taking bodily and software preventative measures to guard the underlying networking infrastructure from unauthorized get right of entry to, misuse, malfunction, change, destruction, or flawed disclosure, thereby developing a at ease platform for computer systems, users and packages to perform their authorized vital capabilities within a comfortable surroundings.

One of the maximum common wi-fi protection threats is the rogue access factor and it is used in many attacks, each DDoS and information theft. Many different rogue get admission to factors, but, are deployed by means of personnel wanting unfettered wireless access factor .those get right of entry to factors are known as tender get entry to points. Different rogues are located in neighboring organizations the use of your network without cost gets right of entry to. Normally low-value and patron-grade, those get entry to factors often do now not broadcast their presence over the wire and might handiest be detected over-the-air. Due to the fact they're commonly set up in their default mode, authentication and encryption are not enabled, thereby developing a safety hazard. Due to the fact wi-fi LAN alerts can traverse building walls, an open access point connected to the company network the proper target for struggle riding. A rogue get entry to factor is a tool now not sanctioned via an administrator, but is working at the community anyway. This can be an access factor set up through both an employee or with the aid of an intruder. Any consumer that connects to a rogue get entry to point must be taken into consideration a rogue patron. Rogue get admission to factors and their clients undermine the security of a company network by using probably allowing unchallenged get right of entry to the community through any wireless user or patron within the bodily area. Rogue get entry to points can also intervene with the operation of your company network. Rogue access factors can do the subsequent harm:

- Allow a hacker to behavior a person-in-the-middle attack. The attacker makes unbiased connections with the sufferers and relays messages among them, making them trust that they are speaking without delay to each other over a non-public connection, while in fact the complete conversation is controlled by the attacker.
- Flood the network with useless statistics, growing a denial of carrier.
- Ship faux SSIDs advertising and marketing appealing capabilities including loose net connectivity. As soon as a user connects, the fake SSID is introduced to the customer's wireless configuration and the purchaser begins to broadcast the faux SSID, thereby infecting other clients. .
- Offer a conduit for the robbery of business enterprise records.

To stumble on those gadgets, our framework, called community go with the flow defend (NFG), offers a hybrid method, made out of both passive and active measures, to detect and isolate RAPs. The passive strategies used by NFG

already stumble on the majority of feasible RAPs. But, for those now not right now detectable, NFG additionally passively monitors patron site visitors for signatures of RAP conduct. Suspected RAPs are then flagged, and NFG briefly redirects the suspected consumer's visitors to its relied on Agent for lively testing. Clients who fail the take a look at are isolated from community services. Additionally, our active testing introduces minimum burden to the community and may be implemented in a random or rotational manner to periodically test all clients if favored

II. BACK GROUND

A. *Software Defined Network*

Software program-described networking (SDN) is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and garage infrastructure of the cutting-edge records center. The intention of SDN is to allow network engineers and directors to reply quickly to changing commercial enterprise necessities. In a software-defined network, a network administrator can shape traffic from a centralized manage console while not having to touch individual switches, and can deliver offerings to wherever they may be wished in the network, without regard to what unique devices a server or different hardware additives are related to. The important thing technology for SDN implementation is functional separation, network virtualization and automation through programmability.

B. *Rogue access points*

A rogue get admission to factor is a wi-fi get admission to factor that has been established on a comfortable network without specific authorization from a local network administrator, whether or not added by a properly-that means worker or with the aid of a malicious attacker.

III. LITERATURE REVIEW

In 2007 Lanier Watkins, Raheem Beyah and Cherita Corbett proposed a passive detection approach for rogue access point detection. In 2008 Gayathri Shivaraj, Min Song and Sachin Shetty proposed Hidden Markov Model Based Approach to detect rogue access point. In 2014 Prof. Sandeep Vanjale and. Dr. P.B.Mane,,Ph.D Research Scholar use novel approaches to eliminate rogue access point in wireless network. Jacob H. Cox Jr, Russel Clark, and Henry Owen members of IEEE performed a study on RAPs (2017) .They use NFG rogue detection framework with trusted agent and open flow switch to detect unauthorized access point from SDN.

IV. RELATED WORKS

There are a number of unauthorized access point detection techniques. Techniques use the concept of MAC Address verification, SSID, wireless traffic analysis for the detection of malicious access points. But now a day's attacker can easily overcome these techniques of traditional approaches. There are number of software tools available which are used in network for detection of malicious access points e.g. Air tights WIPS, Aero hived. In general malicious access point detection can be classified into two different approaches which include client side and server side. The server side approach is again divided into two parts centralized and decentralized approaches. Some techniques use a hybrid approach. In server side approach software tool have been installed on the central node basically called server which handle whole network and detect malicious access point. The client side approach is challenging because there is no prior information about network which can be used as a reference. Even client doesn't know about the authorized access point list. Even nodes don't have any sophisticated software tool available within it.

V. OUR APPROACH

Previously, we have discussed about diverse detection strategies and we are able to now deal with our approach to stumble on rogue get admission to point and to decorate the SDN capabilities. The proposed device is a mininet based totally technique and it does now not require additional hardware, nor does it want to preserve facts approximately new wi-fi gadgets. On this phase, we first explained about modules. There are six modules and based on every module SDN is similarly detected to discover rogue get entry to factors and in next section we defined standard process via the structure. Sooner or later, the algorithms are explained within the segment followed by architecture.

VI. ARCHITECTURE

The general design goal of SDN is to enable important features of subsequent-technology wi-fi networks, along with self-resolvability, rapid-adaptability, multi-service mutli-technology convergence, most spectrum performance. Any system or device connected to a community is likewise known as a node. For instance, if a community connects a file server, five computer

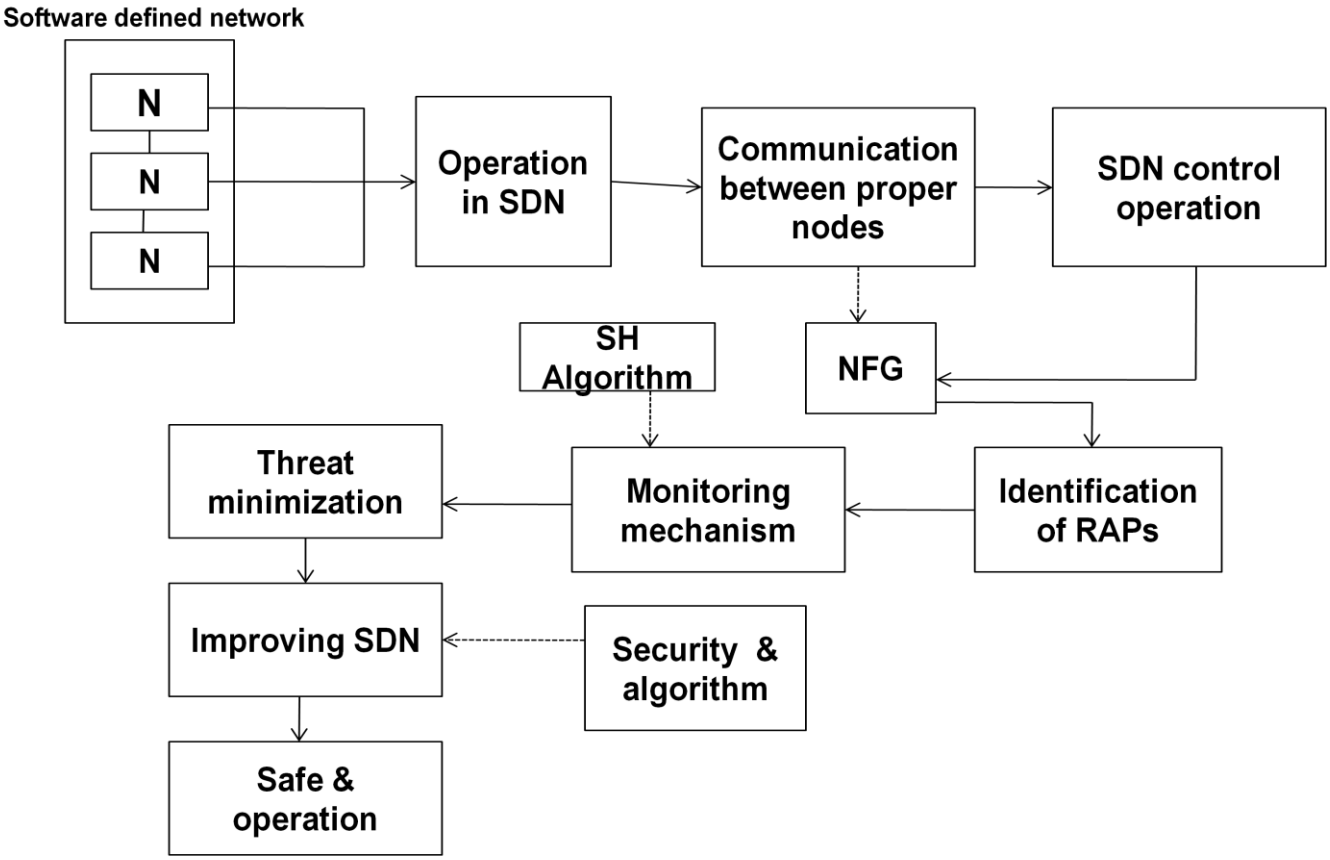

Fig 1: Architecture of software defined network

Systems, and printers, there are 8 nodes at the community. Every tool at the network has a network address, consisting of a MAC cope with, which uniquely identifies each device. This allows hold song of where statistics is being transferred to and from at the network. A node also can talk over with a leaf, which is a folder or document to your difficult disk. In physics, a node, or nodal factor, is a point of minimum displacement or in which a couple of waves converge, developing a internet amplitude of zero. We have created four nodes and configure then by way of the usage of their IP cope with. Nodes get created while a flow is deployed, they may send and obtain some messages at the same time as the flow is running and they get deleted whilst the subsequent flow is deployed. After creating node we've got supplied a operation of the fundamental components of SDN: the SDN devices, the controller, and the applications. Communications refers to the transmission of this virtual records between two or extra computer systems and a laptop community or information community is a telecommunication community that allow the computer systems to alternate information. Software program-defined aren't bodily related. This enables you convert your community faster and extra effectively for example, if you want greater IP addresses or you've got a brand new task that desires a network, an administrator to create the important setup immediately. SDN controller makes it feasible which will address your records middle wishes with an open architecture that allows programmable community manage and an abstracted underlying infrastructure. The Flow Guard carrier reliably protects you against not unusual form of DDOS assaults inclusive of IOT, UDP flood, ICMP flood , ICMP attack, syn flood, ping of dearth, ping flood, HTTP flood gradual Loris, utility level assault / Layer 7 attack, Degradation of service attack, Multi-vector assault, zero Day DDoS, DNS Amplification assaults, Smurf attacks, ACK attack and Teardrop assault Flow Guard systematically monitors and evaluates unique data go with the flow changes, even as attack safety is immediately activated while giant anomalies are detected. Via this method, waft guard guarantees the resistance of your community infrastructure in opposition to modified or absolutely unknown types of attacks. After that rogue access point may be identified and decrease its threads via the use of sequential hypothesis set of rules.SDN can advanced by means of the use of safety features.

VII. EXPERIMENTAL SETUP

Now we flip our consciousness to implementing a way to the Rogue get entry to factor trouble.

A. MIninet

Mininet is a community emulator which creates a network of digital hosts, switches, controllers, and hyperlinks. Mininet hosts run trendy Linux community software program, and its switches support Open Flow for enormously bendy custom routing and software-described Networking. Mininet helps studies, improvement, mastering, prototyping, checking out, debugging, and some other responsibilities that could advantage from having an entire experimental network on a pc or

other laptop. Mininet provides a smooth way to get correct device conduct (and, to the extent supported by way of your hardware, performance) and to experiment with topologies. Mininet networks run real code along with standard Unix/Linux network packages in addition to the actual Linux kernel and network stack (consisting of any kernel extensions which you may have available, so long as they're well suited with network namespaces.)Due to this, the code you increase and take a look at on Mininet, for an Open Flow controller, changed switch, or host, can move to an actual device with minimum modifications, for actual-world testing, overall performance assessment, and deployment. Importantly this means that a layout that works in Mininet can normally pass immediately to hardware switches for line-charge packet forwarding.

Mininet:

- Provides a simple and inexpensive network test bed for developing Open Flow applications
- Enables multiple concurrent developers to work independently on the same topology
- Supports system-level regression tests, which are repeatable and easily packaged
- Enables complex topology testing, without the need to wire up a physical network
- Includes a CLI that is topology-aware and Open Flow-aware, for debugging or running network-wide tests
- Supports arbitrary custom topologies, and includes a basic set of parameterized topologies
- is usable out of the box without programming, but
- also Provides a straightforward and extensible Python API for network creation and experimentation

B. Formation of SDN

There is want to model hosts, switches, hyperlinks and SDN. Mininet permits creating topologies of very big scale length up to thousands of nodes and perform check on them very without problems. It has very simple command line gear and API. Mininet allows the consumer to easily create, personalize, share and test SDN networks. Mininet is freely to be had open source software that emulates Open Flow devices and SDN controllers. Mininet can simulates SDN networks, can run a controller for experiments. It lets in emulating actual international community scenarios Couple of SDN controllers are protected with in Mininet VM. Mininet contains number of default topologies together with minimum, single, reversed, linear and tree. The usage of Mininet, you may easily create custom topologies.

C. SDN Operation

On this, we've configure device in software program described network and we provided an operation of the primary additives of SDN: the SDN devices, the controller, and the applications. The SDN gadgets incorporate forwarding functionality for identifying what to do with every incoming packet. The devices also include the information that drives those forwarding choices. The facts itself is in reality represented with the aid of the flows defined by means of the controller, as depicted within the upper-left portion of every device. A flow desk is living on the network tool and includes a sequence of flow entries and the movements to carry out while a packet matching that flow arrives on the device. Whilst the SDN device gets a packet, it consults its flow tables looking for a fit. These flow tables were built formerly while the controller downloaded suitable flow rules to the tool. If the SDN device finds a suit, it takes the best configured action, which generally includes forwarding the packet. If it does no longer find a match, the switch can either drop the packet or skip it to the controller, relying on the model of Open Flow and the configuration of the transfer The SDN controller is accountable for abstracting the network of SDN devices it controls and offering an abstraction of these network sources to the SDN applications jogging above. The controller allows the SDN software to define flows on gadgets and to assist the application reply to packets that are forwarded to the controller through the SDN devices.

D. NFG Implementation

In this work, our aim is to design a sturdy SDN fire wall that helps network-huge get entry to control by way of correctly dealing with firewall policy violations in dynamic Open Flow-based networks. To reap our goal and address the aforementioned demanding situations and limitations we seek a solution that fulfills following layout requirements: Accuracy, Flexibility, efficiency. We recommend a complete framework, flow guard, to house our layout requirements flow guard addresses several significant demanding situations in constructing SDN fire walls to facilitate correct detection in addition to flexible decision of firewall coverage violations in dynamic Open Flow networks in conjunction with an expansion of toolkits for visualization, optimization, migration, and integration of SDN fire walls. We next articulate the core components inside the flow guard framework.

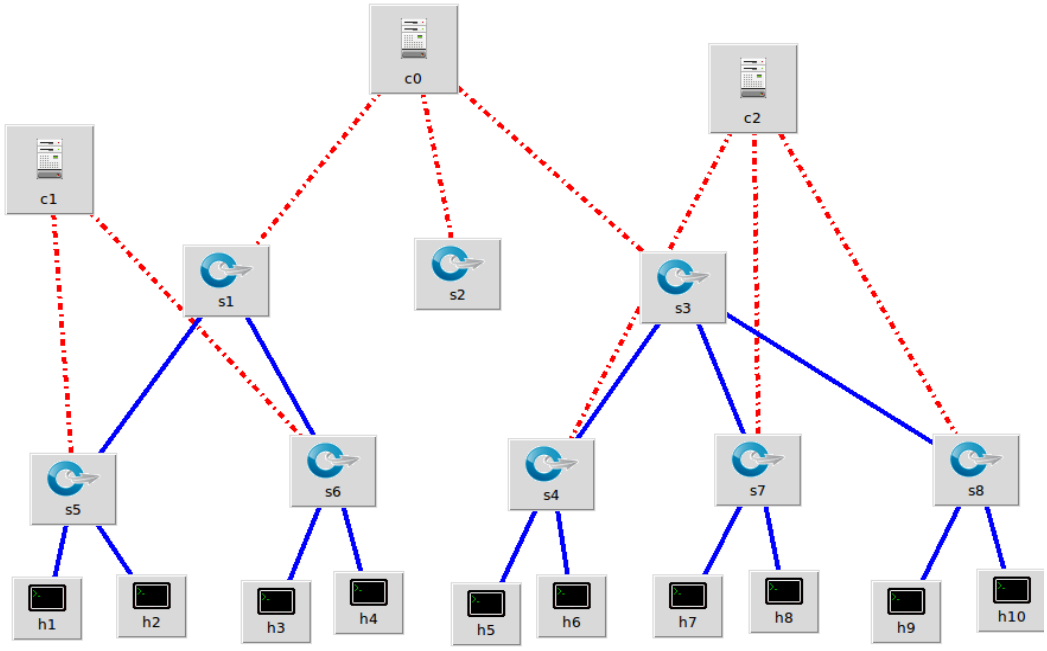

Fig 2: SDN Formation

E. Identification of RAPs

Rogue tool detection is a vital aspect in wireless security. The presence of rogue get right of entry to factors is a chief risk to corporate information structures. Here's what characterizes the problem, a way to hit upon rogues and what you may do to increase the security of your network. one of the maximum essential safety concerns of IT managers nowadays is the possibility that rogue wireless get right of entry to factors can be present on the corporate community. A rogue get right of entry to point is one which the enterprise does not authorize for operation. We've got used sequential hypothesis to perceive rogue get entry to point.

F. Minimization of Threats

Rogue get right of entry to factor can cause so many threats like man in the middle of attack and DDOS .If an attacker installs an get entry to point they may be able to run various varieties of vulnerability scanners, and as opposed to having to be physically in the business enterprise, can attack remotely - possibly from a reception location, adjoining constructing, automobile park, or with a excessive benefit antenna, even from several miles away. We are able to decrease the threats by using the usage of sequential set of rules. It is simple to formulate solution to a query with sequential algorithm.

G. Removal of RAP and Revamping SDN

On this, we have eliminated Rogue get admission to factor. The access points are determined to be a rogue and not doubtlessly legitimate. If the SSID being broadcast is the identical or much like considered one of our SSID's the offending access factor have to be disabled wirelessly and on the switch port as quickly as viable. The remark in ONA ought to be "Disabled because of Rogue access points". If the access points is exposing the college of Waterloo networking with none safety it should be disabled wirelessly and at the transfer port as soon as possible. The comment in ONA needs to be "Disabled because of Rogue access points". Determine the overall vicinity for the rogue using airwave visualRF as being on campus. Contact the laptop guide for that area to analyze the rogue. Determine who owns the access points (e.g., name on the workplace, consumer sitting with it in a cubicle, ask humans in the location) discover from the owner why the access points has been setup. Also direct the proprietor to the rogue access point exception/authorization documentation. If the user is complaining approximately wi-fi sign, a short test need to be accomplished to degree the signal and then a price tag created for IST. If the person has setup the access points for research functions direct them to the rogue access points exception/ authorization documentation The port the rogue connects to (if acknowledged) is disabled and commented in ONA. The remark in ONA has to be "Disabled because of Rogue access points". And through using protection set of rules we improve the performance and protection to software program defined network.

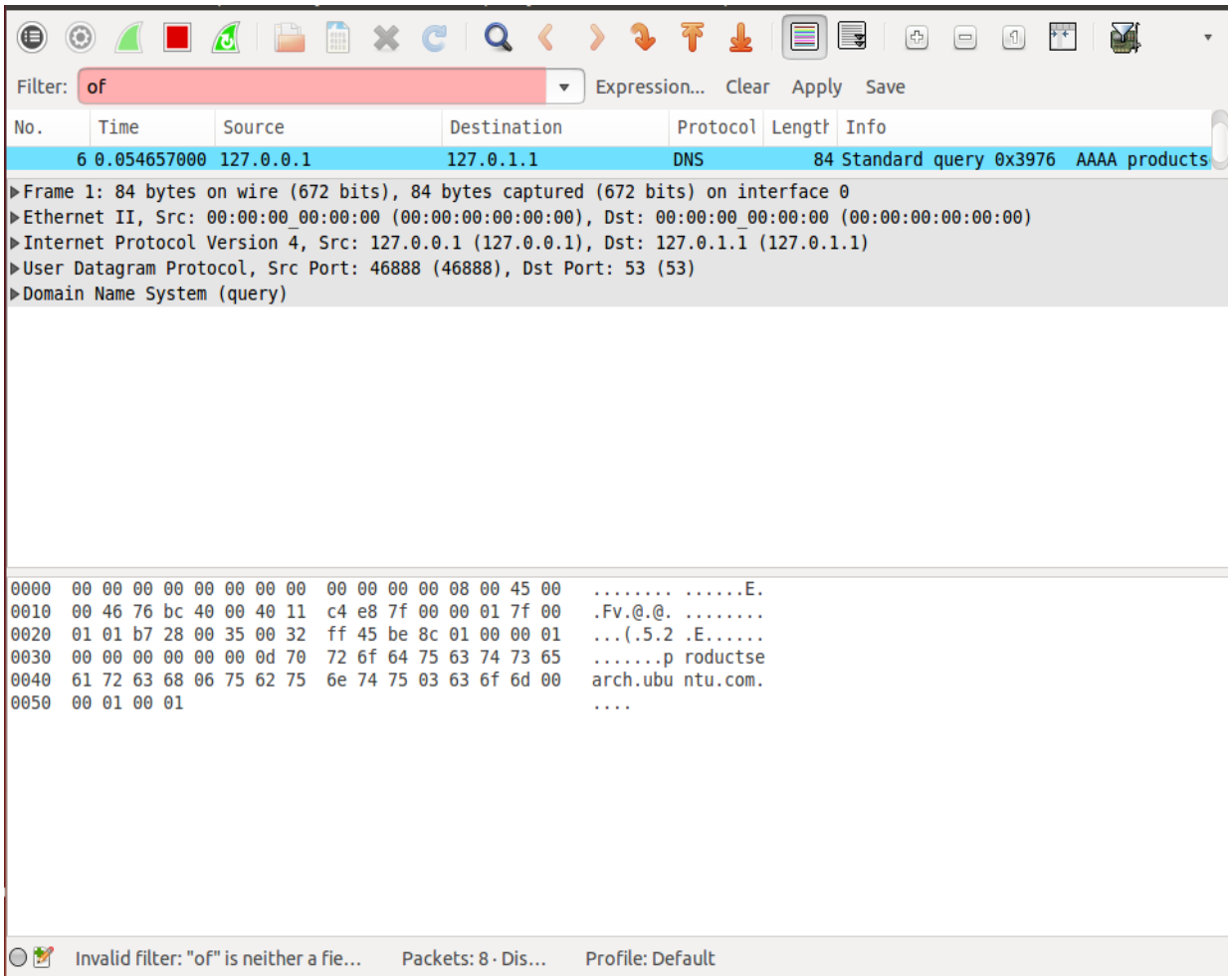

Fig 3: Packets analysis

VIII. ALGORITHMS

A. *Sequential hyphothesis Algorithm*

Sequential analysis is the department of data that offers with decision making as the samples are being collected. It differs from classical speculation trying out in that conclusions are reached extra speedy, regularly before the give up of the experiment. Therefore, it is right for detection, sign processing, clinical trials and different packages. In trendy, sequential decision issues involve one or extra sensors and a fusion middle in which the very last selection is made. Inside the centralized placing, all of the facts received by means of the sensors are made available on the fusion center. However, in the decentralized case, the sensors themselves are part of the choice method and relay partial facts in preference to all of their observations.

IX. CONCLUSION

From this experimental result, the revamping of SDN is accomplished with the support of Mininet and SDN controller. We have done SDN-based approach to detecting and preventing RAPs. Our work contributes a new RAP detection method that is applicable to both SDNs and traditional networks. Other contributions of our work include its use case for the newly developed wireless network emulation framework (i.e., Mininet) Using Mininet, we implement a test bed capable of supporting wireless switches, wireless routers, and wireless hosts (stations). In doing so, our work further validates Mininet viability towards wireless security application development and testing. All of these contributions work together to demonstrate a hybrid testing methodology consisting of passive and active techniques for detecting RAPs connected to an organization's network.

X. REFERENCE

[1] https://people.cs.clemson.edu/~hongxih/papers/HotSDN2014.pdf
[2] http://www.brianlinkletter.com/how-to-install-mininet-sdn-network-simulator/.
[3] https://smartech.gatech.edu/bitstream/handle/1853/58242/COX-DISSERTATION-2017.pdf
[4] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, "Sphinx: Detecting security attacks in software-defined networks.," NDSS, 2015
[5] J. Cox, R. Clark, and H. Owen, "Leveraging SDN for ARP Security," SouthEast-Con 2016, IEEE, 2016, pp. 1–6.
[6] http://ieeexplore.ieee.org/document/5422999/detecting and eliminating rogue access points in ieee-802.11 wlan - a multi-agent sourcing methodology
[7] Karygiannis,T., Owens, L. "Wireless Network Security 802.11, Bluetooth and Handheld Devices." National Institute of Standards and Technology, Special Publication 800-48.
[8] https://intronetworks.cs.luc.edu/current/uhtml/mininet.html
[9] https://uwaterloo.ca/information/systemstechnology/about/organizational-structure/technology-integrated-services-tis/network services/resources/rogue-access-point-ap-removal-process
[10] https://www.giac.org/paper/gsec/4060/rogue-wireless-access-point-detection-remediation/106460
[11] https://arxiv.org/pdf/1307.7451.pdf
[12] https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/wireless/wireless_rogue_ap_detection_enable_c.html
[13] http://www.cs.columbia.edu/~lierranli/coms6998-8SDNFall2013/papers/FortNox-HotSDN2012.pdf http://www.dca.fee.unicamp.br/~chesteve/pubs/DRAFT-survey-on-SDNs.pdf S. Vanjale and P. Mane, "A novel approach for elimination of rogue access point in wireless network," in 2014 Annual IEEE India Conference (INDICON).IEEE,2014,PP.
[14] G. Shivaraj, M. Song, and S. Shetty, "A hidden markov model based approach to detect rogue access points," in Military Communications
[15] Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008, pp. 1–7. K.-F. Kao, I.-E. Liao, and Y.-C. Li, "Detecting rogue access points using client-side bottleneck bandwidth analysis," computers & security,vol. 28, no. 3, pp. 144–152, 2009
[16] B. Alotaibi and K. Elleithy, "Rogue access point detection: Taxonomy, challenges, and future directions," Wireless Personal Communications,pp. 1–30, 2016.
[17] S. M. Bellovin, "A technique for counting natted hosts," in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment. ACM, 2002, pp. 267–272.
[18] S. Mongkolluksamee, K. Fukuda, and P. Pongpaibool, "Counting natted hosts by observing tcp/ip field behaviors," in Communications (ICC),2012 IEEE International Conference on. IEEE, 2012, pp. 1265–1270.
[19] H. Han, B. Sheng, C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue ap detection," Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 11, pp. 1912–1925, Nov 2011.
[20] H. Hou, R. Beyah, and C. Corbett, "A passive approach to rogue access point detection," in IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference. IEEE, 2007, pp. 355–360.
[21] S. Shin, L. Xu, S. Hong, and G. Gu, "Enhancing network security through software defined networking (sdn)," in Computer Communicationand Networks (ICCCN), 2016 25th International Conference on.IEEE, 2016, pp. 1–9.

