An Improved Mechanism for SDN Flow Space to Control Oriented Authentication NAA Network

Taskeen Fathima, S. Mary Vennila

Abstract: ***The Open Daylight platform with its power by working with IEEE 802.1X port level authentication for wired and wireless networks has been very supportive because of the massive deployments at mean charge for main design considerations. Within the current marketplace, 802.1X has flourished the ground works for wireless, wire stability, LAN stability and authentication methods. EAP (Extensible Authentication Protocol) supports long time protection of the supplicant and the authentication software till the end condition of the RADIUS (Remote Authentication Dial-In User Service) server is met. This paper is focused on the RAR (RADIUS Access Request) unique identification about the users on the network with SAA (Supplicant, Authenticator and Authentication server) system which records on the attribute cost of RFC 2865 according to the forwarding server. NAA (Non-Adaptive Algorithm) using FlowVisor based virtualization packages drive inward the network timescales or statistics, dynamically controlling the flow space of switches to control the speed and results in scaling of networks. NAA is an application level protocol that contains authentication and configuration information between a Network Access Server and a shared authentication server. It avoids the attacker from listening for requests and responses from the server and calculates the improved MD5 client secret key of the response.***

Keywords: Software Defined Networking, Non Adaptive Algorithm, 802.1X, FlowVisor, Flow space, Radius Access Request.

I. INTRODUCTION

The Open Daylight (ODL) is a portable platform for tuning and authenticating networks of any measure and balance. It focuses on network programmability, it aroused for commercial solutions to address a variety of use cases in flourishing complex environments. ODL is most randomly installed open source SDN controller [1]. However, previous lookups have focused on unicast operations no longer appear to mandate multicast or broadcast services to comply with 3GPP (3rd Generation Partner Projects) standards, which is the place of interest. As contemporary multicast networks go along with the lack of flexibility, openness, adaptiveness and scalability issues, SDN is primarily based on cellular multicast footprints that emerge from reality. According to Mill Bear Lab, the rule on IPTV is a service that facilitates to suit customers will become challenging radius tuning, offering customized multicast capabilities through social programming. This enables service companies to adapt unique overall performance requirements of a wide variety of scenarios. SDN has dramatically improved NAA community resource utilization due to its strong technical characteristics, multicast based management facilities and then controlling the operating cost. It runs on Openflow regarding the IP multicast protocol as it relates to robust construction and multicast trees. If a person changes its location, the multicast arbor can be reconstructed efficiently or with flow guidelines. Therefore, SDN is a flexible solution to modern network problems, facilitating the expansion and management of objectives, there by promoting innovation and development.

II. RELATED WORK

In recent years, the concise Brief OS (2013) [2] and others debate connecting the SDN of cellular networks ,80 percent think about the reality, so SDN is brave enough to adapt the revolution in the cell network. The ONF is responsible for the standardization of the Openflow protocol, but in order to empower the community, the SDN architecture has been described as an effigy due to cell network. The author extends the work between X.Do. et.al. (2016) [3] and in a short life of long range planetary technique is used to solve the scaling problem of a heterogeneous controller. Mobile custom core community based SDN did not discuss the smooth handover due to multicast, because they provided initial options for adoption of structural functions. This multicasting style over SDN network is evolving these days.To connect two SDN domains, W. Stallings et.al. (2013) [4] API's are interfaces between controllers that are commonly seen as extended applications of social operating systems. SDN domains haves specific verbal transmission protocols between controllers, whose basic functions are log based structures, access to different SDN domains and security symphonies about networks.In line with [5] integration of H. Yin, et.al. (2012), inter-domain flows often alter the ability information to go with the requirements flow system.

Revised Manuscript Received on December 08, 2019

Taskeen Fathima, Research Scholar, Assistant Professor, Department of Computer Science, JBAS College for Women, Chennai, TamilNadu, India.

Dr. S. Mary Vennila, Associate Professor and Head, PG & Research Department of Computer Science, Presidency College, Chennai, TamilNadu, India.

III. RESEARCH METHODOLOGY

An application specific run-time monitoring and management tool is recommended. With that tool the application logic depends on the consumer power system[6]. It focuses on the entire features of the software and delivers it to the customer.

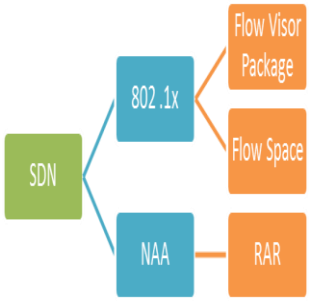

Fig. 1.Flow space based authentication

Since each release of basic features is sent after application logic, the incompatibility of any feature is no longer a problem. Enable app consumers determine the popularity of 802.1X assets so that they can be used even after the app is rooted.

Metadata

1. Access rule policies. 2. Data fairness checks. 3. Dissemination policies. 4. Life duration. 5. ID regarding a trust server. 6. ID on a security server. 7. Application based information.

IV. IMPLEMENTATION

There is internal conflict of traffic patterns and for this the IDs can be configured to look similar, and firewalls are configured to exclude certain sections according to their access. In addition, hardware mainly uses identification tokens with deep encryption to comply with the identifier [7]. The need for security related to native gadgets can disrupt the host and provide an additional road for terminal devices to attack astronaut networks for malicious purposes. A computing device for the Radius Native Host Desktop 802.1X solution can stand well in the network area and all cellular devices with a rise in speed and accuracy levels in the current network are a compact laptop. Although related to the safety of the site of the Star provider[8], web users cannot notice most binary machines after addressing the EAP. The lack of security on a field host IP net mask organizes the star and its sources for other users based on the SDN protocol. NAA consumers rely on mobile machines to gain access to EAP by regular astronaut data, which expose the risk of compliance with the Reserve and the loss and damage to network packet data units. The SDN flow open devices require an emotional authentication mechanism, the astronaut does not get damaged, and then the NAA requires viewers' privacy to maintain the cryptographic activity site. Since this location is for the safety of the consumer, there is a measure, the provider can consider after setting its security SLA (Service Level Agreement). New strategies for complying with high-security computing, enabling the environment within the planet for RAR, allows for a more sophisticated security mechanism. Users are compatible with the cloud near their local military machines. In particular, multi-star facts that store technologies require customers to follow the keys used to understand encrypted information and the NAA keys store them in a regional equipment. If malicious services in the cloud work together with a local computing device or have the right to enter these keys, the confidentiality of the records stored in the air is at risk. The user RFC3588 is used according to SDN's attack in anticipation of running the user's laptop, with harmful articles damaging the provider's side resources, which affects not only the provider, but also its poor consumers.

NAA Algorithm

1. Planar equation: a x + b y + c z + d = 0.
2. Let N = (a, b, c, d).
(Note: (a, b, c) is normal vector)
3. Let P = (x, y, z, 1) be a point in planeπ.
4. Planar equation: N • P = 0.
5. M is an affine transformation matrix. (MT is M transpose.)
6. Let P' = M PT.
7. Find N' such that N' • P' = 0 (transformed planar equation)
8. N • P = 0;
9. N PT = 0;
10. N (M-1 M) PT= 0;
11. (N M-1) (M PT) = 0;
12. (N M-1) P'T= 0;
13. So N' = NM-1
14. To put in column-vector form, (N')T = (NM-1)T = (M-1)TNT
15. So N' = ((M-1)T NT)T and (M-1)T is the transformation matrix to take NT into N'T
16. If M is a rotation matrix, (M-1)T = M.

Test procedure: Configure 100k flows within the OpenFlow network load restart community mininet, wait till an affirmation over flows is re-programmed.

$$r_{A,B} = \frac{\sum_{i=1}^{n}(a_i - \bar{A})(b_i - \bar{B})}{(n-1)\sigma_A\sigma_B} = \frac{\sum_{i=1}^{n}(a_i b_i) - n\bar{A}\bar{B}}{(n-1)\sigma_A\sigma_B} \quad (1)$$

n stands for number of data packets; A and B are their respective instruments; standard deviation of A and B and the sum [9] of cross product AB is shown. If rA, B> 0: A and B are positively correlated (the value of A will increase to B), High, strong communication speed increase; If rA,B = 0:A and B are independent; If rA,B<0:A and B negatively correlated.

$$a'_k = (a_k - mean(A)) / std(A) \quad (2)$$

$$b'_k = (b_k - mean(B)) / std(B)$$
$$correlation(A, B) = A' \bullet B'$$

V. SIMULATION RESULTS

Energy is saved when the formulation produces a positive number in Table I. A SDN Control board has viii × eighth = sixty four positions. Each player controls 16 portions at the commencing of the game. Each section may additionally remain in about the 64 possible locations then needs 6 bits to represent the location. To represent a SDN present day state as shown in Table-I, it is adequate in accordance with state that 6 bits × 32 bits = 192 bits = 24 bytes; this is smaller than a typical wireless packet[10]. Performing encryption then stenographic techniques earlier than sending facts requires partial extra processing on the system. (1)When SP (Supplicant Port) discusses possible routes, each NP (Network Policy) can negotiate the authority. (2) There is no chance of losing control now as NP agents provide a route (Table-II) to exit the selected range. (3) Complying with the choice of the most accurate path is among the best government, as the SP advises it to pass. (4) Because SDN is used, it makes the network flexible. (5) The route through the SP is chosen from each of the routes provided by the NP, mainly in relation to overall efficiency or cost and everyone has the same ability[11]. (6) Each network dealer can determine the cost of waterproofing using several SDN parameters. Finally select Request and service cost. Round trip time [12] distance between Data packet Accuracy generation and receipt of related consent Load payload speed performance is measured as the ratio between the numbers is shown in Fig. 2. The desired locations receive the payload bytes and all the bytes in packets are in circulation in the network. The response time is measured as intervals. When the administrator receives a request for a new entry, the controller sends the appropriate input speed and accuracy, the immediate time.

Table-I: Overall Accuracy with speed in SDN

MD5 Diffusion Tubes Measurements										FlowVisor Automatic Method		NAA Data Quality Check	
PROTOCOL	SDN	SDN+NAA	Tube 1 $\mu g\ m^{-3}$	Tube 2 $\mu g\ m^{-3}$	Tube 3 $\mu g\ m^{-3}$	Triplicate Mean	Standard Deviation	Coefficient of Variation (CV)	98 % CI of mean	Period Mean	Data Capture (% DC)	ACCURACY	SPEED
1	OPEN FLOW	MTV	88.3	88.3	77.6	85	6.2	7	15.5	66	44	Good	Poor Data Capture
2	FLOW SPACE	NAA	32	38	33.4	34	3.1	9	7.8	44	77	Good	Good
3	CONTROL	NBI	32	44	33.3	36	6.6	18	16.3	66.44	44.55	Good	Poor Data Capture
4	FLOW SPACE	NAA NBI+802.X	43	34.3	44.3	41	5.4	13	13.5	67	88.33	Good	Good
5	RADIUS	RAR	34.5	33.9	33	34	0.8	2	1.9	68	44.55	Good	Poor Data Capture
6	FLOW SPACE	NAA+ NBI	34.7	46.5	33	38	7.3	19	18.2	67	88.78	Good	Good
7	OPEN FLOW	EAP	34	34.6	77.4	49	24.9	51	61.9	77	77.6	Poor Precision	Good
8	SP	NBI	34	33	33	33	0.6	2	1.4	89	88.88	Good	Good
9	RGDD	MTV	67	55.6	44.3	56	11.3	20	28.1	99.99	88.77	Poor Precision	Good
10	FLOW SPACE	NAA + 802.1X	76.7	88.9	88.3	85	6.9	8	17.1	78.88	99.77	Good	Good

Table-II: New approach to NAA using SDN

Accuracy +SPEED SDN calculated using 5 periods of data		(with 98% confidence interval)
RAR factor A	1.5 (1.01 - 2.89)	
Bias B	-33% (-65% - -1%)	
Diffusion Tubes Mean:	46 µg m^{-3}	
Mean CV (Precision):	10	Caution
Automatic Mean:	69 µg m^{-3}	
Data Capture for periods used:	89 %	
Adjusted Tubes Mean:	96 (134 - 38) µgm^{-3}	

Accuracy+ SPEED SDN calculated using 7 periods of data		(with 98% confidence interval)
RAR factor A	1.56 (1.19 - 2.25)	
Bias B	-36% (-55% - -16%)	
Diffusion Tubes Mean:	48 µgm^{-3}	
Mean CV (Precision):	18	Caution
Automatic Mean:	75 µgm^{-3}	
Data Capture for periods used:	87 %	
Adjusted Tubes Mean:	75 (57 - 108) µgm^{-3}	

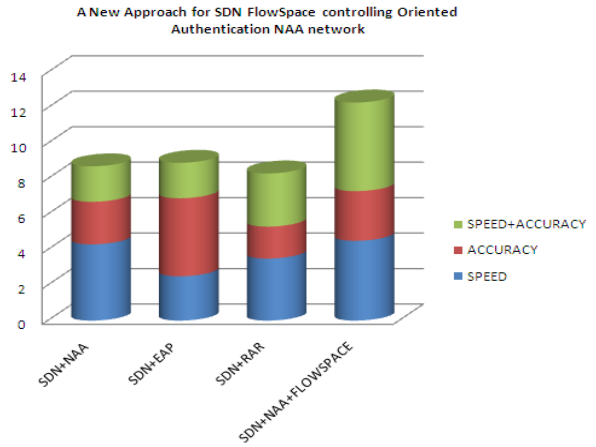

Fig. 2.SDN Flowspace using proposed NAA Accuracy with speed

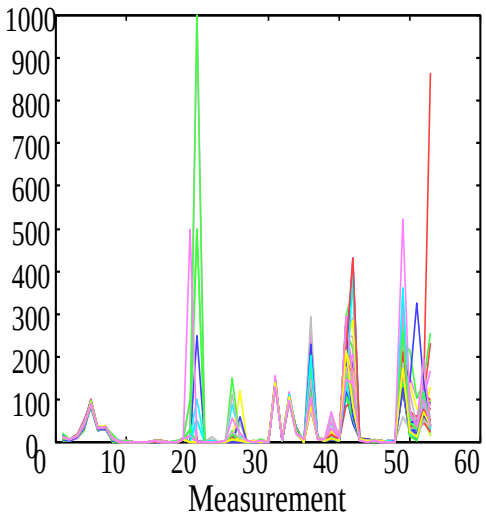

Fig. 3. NAA Layer nodes updated status

Whenever a node changes, the controller sends new coordinates to that particular node and its immediate [13] layer. The nodes are up to date about their status and their immediate layer as shown in Fig. 3. Using geographic routing, a node can send a packet with only FSK one request to the controller for the target coordinates and then all forwarding authorities [14] are made independent of each node in the communication path is determined by the controller. In the case of geographical route[15] for multicast, the path that the packet should follow to reach all the nodes in the group and the algorithm is used to create this path is the IEEE 802.1X tree, which is complex based on the size of the whole network. However, when using geographic routing, the Euclidean IEEE 802.1X tree algorithm can be taken advantage of [16], which is a problem that depends only on the number of nodes in the multicast group. Note that the proposed algorithm can introduce IEEE 802.1X (branch) points, which are not compatible with the nodes of the multicast data stream [17], although they are necessary to improve the route. In fact, IEEE 802.1X points is artificial because their coordinates [18] have the same network node. In this situation, the closest point of these coordinates is selected as the IEEE 802.1X point. If a node wants to send multicast packets, it sets the address to the destination and advances a request to the controller. Then, to send packets to each multicast or IEEE 802.1X node, the controller computes responses along the target coordinates of the next multicast or IEEE 802.1X node, as described above. When a multicast or IEEE 802.1X node receives a packet, a request is sent to the controller to the controller, which returns the next multicast IEEE 802.1X node. Until the packet multicast does not reach all the nodes [22] the process replays.

VI. CONCLUSION

As it inherits Internet software or hardware resources, it can be of help in deployment of applications. A theoretical or test result of NAA has application-independent, ruler-independent, minimal features and reliable communication-related features. The NAA supports common IP purposes or novel applications by integrating two related SDN domains on an IP network. It is of important theoretical and sensible value. Next quarter following the development of RAR, to provide safe, reliable guidance for the range related to key regulators and current API's to support various network applications after education. Computing can be effective in finding compliance solutions to security issues, complying and finding strategies and then strategies within the terms of loss of control to resolve this NAA with multiple tenant issues. Since NBI (North Bound Interface) can provide an unformatted SDN pipeline with older devices, it is taking more time in favor of older devices. Considering past experience, as SP is more concerned with the entire community, it can be placed in suitable positions if the RAR boundary occupation is too low or necessary. Since NBI only provides those paths according to its policy, they can proceed with personal safety rather than violating the policy of others. According to 802.1 X specifications, each client should use a separate shared secret. The common secret is to be a random string of at least 16 bytes of bits and must be generated by NAA. A secret password is shared between the client and NAA must be at least as long as the password is large and unchecked. It is desirable to have at least 16 numbers in this secret. Avoid these attacks on the server in the future.

REFERENCES

1. Brief OS, "OpenFlow™ Enabled Mobile and Wireless Networks," White paper, September 2013.
2. T. -X. Do, V. -G. Nguyen and Y. Kim, "SDN-based mobile packet core for multicast and broadcast services, Wireless Networks," (2016), 1–14doi:10.1007/s11276-016-1433-6.
3. W.Stallings," Software-defined networks and OpenFlow," The Internet Protocol Journal, vol.16. no.1, 2013.
4. H. Yin, et al., "SDN: A Message Exchange Protocol for Software Defined Networks across Multiple Domains, Internet Draft," Internet Engineering Task Force, June 2012.
5. Angelos-Christos Anadiotis, Laura Galluccio, Sebastiano Milardo, Giacomo Morabito, Sergio Palazzo, "SD-WISE: A Software-Defined Wireless Sensor network," Computer Networks, vol.159, 2019, Pages 84-95, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2019.04.029.
6. J. Medved, R. Varga, A. Tkacik, K. Gray, "OpenDaylight: towards a model-driven SDN controller architecture," in: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, 2014, pp. 1–6, doi:10.1109/WoWMoM.2014.6918985.
7. L. Galluccio, G. Morabito, S. Palazzo, "Geographic multicast (GEM) for dense wireless networks: protocol design and performance analysis," IEEE/ACM Transactions on Networking 21 (4) (2013) 1332–1346, doi:10.1109/TNET.2012.2236351.
8. Ming Chen, Ke Ding, JieHao, Chao Hu, GaogangXie, Changyou Xing, Bing Chen, "LCMSC: A lightweight collaborative mechanism for SDN controllers," Computer Networks, vol. 121, 2017, Pages 65-75, https://doi.org/10.1016/j.comnet.2017.04.029.
9. Yahui Li, Zhiliang Wang, Jiangyuan Yao, Xia Yin, Xingang Shi, Jianping Wu, Han Zhang, "MSAID: Automated detection of interference in multiple SDN applications," Computer Networks, vol. 153, 2019, Pages 49-62.
10. Guido Maier, Martin Reisslein,"Transport SDN at the dawn of the 5G era, Optical Switching and Networking, vol. 33,2019,Pages 34-40.
11. M. Banikazemi, D. Olshefski, A. Shaikh, J. Tracey, G. Wang, " Meridian: an SDN platform for cloud network services," IEEE Commun Mag, 51 (2) (2013), pp. 120-127
12. F. Callegati, W. Cerroni, C. Contoli, R. Cardone, M. Nocentini, A. Manzalini, "SDN for dynamic NFV deployment," IEEE Commun Mag, 54 (10) (2016), pp. 89-95.
13. Q. Duan, N. Ansari, M. Toy, "Software-defined network virtualization: an architectural framework for integrating SDN and NFV for service provisioning in future networks," IEEE Netw, 30 (5) (2016), pp. 10-16
14. Senthil, P. (2017). Enhancement VLC to Sushisen Algorithms Using BER Performance of the FSK Communication Network Asian Journal of Electrical Sciences ISSN: 2249 – 6297, Vol. 7, No. 1, 2018, pp. 42-46.
15. Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., &Shenker, S. (2008), "NOX: Towards an operating system for networks," ACM SIGCOMM Computer Communication Review, 38(3), 105–110.
16. H. Polat and O. Polat, "The effects of DoS attacks on ODL and POX SDN controllers," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 554-558 doi: 10.1109/ICITECH.2017.8080058.
17. S. V. Morzhov and M. A. Nikitinskiy, "Development and research of the PreFirewall network application for floodlight SDN controller," 2018, Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, 2018, pp. 1-4 doi: 10.1109/MWENT.2018.8337255.
18. O. Salman, I. H. Elhajj, A. Kayssi and A. Chehab, "SDN controllers: A comparative study," *2016, 18th Mediterranean Electrotechnical Conference (MELECON)*, Lemesos, 2016, pp. 1-6. doi: 10.1109/MELCON.2016.7495430
19. A. Lara, A. Kolasani and B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 493-512, First Quarter 2014. doi: 10.1109/SURV.2013.081313.00105
20. Erickson, D. (2013), "The Beacon OpenFlow controller," In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, ser. HotSDN'13, New York, NY, USA: ACM, pp. 13–18.
21. Cai, Z., Cox, A. L. & Ng, T. S. E. (2011), "Maestro: A system for scalable openflow control," Rice University, Tech. Rep.
22. J. H. Cox, S. Donovan, R. J. Clarky and H. L. Owen, "Ryuretic: A modular framework for Ryu," MILCOM 2016 - IEEE Military Communications Conference, Baltimore, MD, 2016, pp.1065-1070.doi: 10.1109/MILCOM.2016.7795471.

AUTHORS PROFILE

Taskeen Fathima, received her Bachelor of Science degree in Mathematics from Justice Basheer Ahamed Sayeed College for Women, India in 1993, Master of Computer Applications degree from Justice Basheer Ahamed Sayeed College for Women, India in 1996 and M.Phil in Computer Science in the year 2006 from Mother Teresa University. She is a part-time Ph.D. student in Presidency College, Chennai, India. She is currently working as an Assistant Professor in Justice Basheer Ahamed Sayeed College for Women, India. Her current research areas include computer networks and security, wireless communications.

Dr. S. Mary Vennila, is an Associate Professor & Head of the PG & Research Department of Computer Science, Presidency College, Chennai, TamilNadu, India. She has more than 26 years of teaching experience in Computer Science. She has been guiding several M.Phil candidates and is guiding research scholars. Her research interests are in Networks, Cloud security and Data mining.