Advances in Parallel Computing Technologies and Applications
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC210126

Framework for Authentication 802.1X Security Protocol of WNAS as RFC Access Management Device Associated with RFC Authentication Management Technique

Fathima T [a,1], and Vennila S M [b]

[a] *Research Scholar, PG & Research Department of Computer Science, Presidency College, TamilNadu, India*

[b] *Associate Professor and Head, PG & Research Department of Computer Science, Presidency College, Chennai, TamilNadu, India*

Abstract. IEEE 802 is used in LAN networks that expose or provide sensitive data to complex applications or services. These are protocols for accessing, managing and controlling access to network-based services and applications in general. Port-controlled network access controls network access and prevents the transmission and reception of nameless or unauthorized persons, leading to network interruption, service theft and data loss. This paper introduces a new approach to investigate whether a data packets in wired networks transferred to a management device is authenticated packet. The data packets are sent to the SDN from RAR and share the information associated with each packet with a limited rate for the access management and are received by the RFC. Here it detects whether the data packet arrived is accepted or restricted. The speed at the authentication start packet is restricted to manage the number of terminals that enter later authentication, and it avoids avalanche impact of wireless authentication which may cause faults to lots of terminals which enter later authentication at the same time.

Keywords. Authentication, RFC (Request For Comments), Network security, SDN (Software Defined Networks).

1. Introduction

The IEEE 802.1X specifies a standard method for port-based network access with the aim of providing optimal authentication PSK, authentication and cryptographic key acquisition methods to enable secure communication between devices connected to the local network (LAN). IEEE Class 802.1 AE (TMS) outlines the principles for establishing MAC security firms. Radius assists in the implementation of industry standardization and accreditation processes network virtualization to generally (Figure 1) separate physical infrastructure and "topology" from "logical" topologies or infrastructure by cre-

[1] Taskeen Fathima, PG & Research Department of Computer Science, Presidency College, TamilNadu. E-mail:taskeenfathima2011@gmail.com.

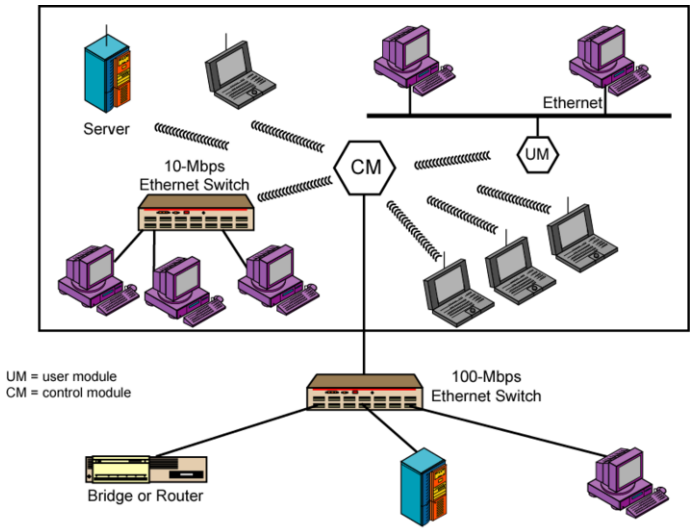


Figure 1. Physical Infrastructure.

ating RFC overlay network. Network Coverage physical networks support a variety of applications across infrastructure and areas, transforming them into cloud-based multi-tenancy physical infrastructure and "topology" from "logical" topologies or infrastructure by creating RFC overlay network. and scalable networks . It basically distinguishes physical infrastructure tops and topologies from "logical" topologies by (Figure 1) creating RFC overlay network, and the ability to collect and disconnect as a whole. Network overlays physical networks can support applications from infrastructure and scales and fields, transforming them into cloud-based multi-tenancy and scalable networks . In IEEE802.1X [1], 802.15 and 802.3 are nodes connected to IAE 802 Technology, PSK [2] coordinator and intermediate register. LAN's new wiring is SDN connected to protocol RFC is an upgraded variant of SDN that incorporates the features of a remote cross stock.

2. Related Work

Security is the top challenge for every wired and Wi-Fi neighborhood location community in an organization setting [3, 4]. These days' agencies like government, non-public [5], and public sectors construct their workplaces with Wi-Fi neighborhood place networks imparting entire safety to their beneficial facts belongings and safety from unauthorized user which should be a difficult task. The findings of the literature exhibits that the existing protection fashions tackle completely RFC genuine extent of protection troubles and all have their own limitations. Therefore, in this paper, a company new safety layout is developed referred to as a multi-layered [6] protection layout for any organizations' WLAN [7].

3. Research Methodology

Authentication Protocol (EAP) is used inside the wired and wi-fi community that helps more than one authentication techniques like secret digital certificates and public key infrastructure. PSK typically consists of three entities especially supplicant, authenticator, and authentication server. A supplicant is CCMP (Counter Mode with CBC-MAC) entity that wants to use the provider provided through the managed port on the TKIP (Temporal Key Integrity Protocol) has the administration over a crew of ports, and a community will have a couple of authenticators. In IEEE 802.11, the administration port represents to PAC (Protected Access Credential) affiliation between supplicant and authenticator. The former authenticates by the critic to a [8] central authentication server. The 802.1X makes use of Remote Authentication Dial-in User Ser-vice (RADIUS) as RFC authentication server, that directs the CTR (user Counter Mode) to produce an entry for productive authentication. 802.1X usually gives for centralized authentication and dynamic key distribution in 802.11 designs and for using 802.1X [9] with RADIUS. 802.1X is employed for conversation between the Wi-Fi buyers and AP's, where as RADIUS operates between AP and authentication server. The authentication approach between authentication server SDN supplicants is carried over protocol (EAP). The key protocol in 802.1X is termed EAP over a laptop community (EAPOL) [10].

4. Framework of Components

The distance between the EAP cable and the Ethernet cable is not long: the cable is still limited to a maximum length of 100 meters (328 feet) limits cable to 90 meters in length, at both ends. Historically, this medium was coaxial copper cable MIC, but today it is usually twisted pair or fiber optic cable. Most industrial control components in current production (Figure 2) run at 10 / 100BaseT. Industrial networks should only use 5E Shielded Trusted Pair (STP) cables and cables with Shielded RJ-45 connectors only. Optical fiber conversation entails sending indicators to skinny wires of glass or plastic fibers. The mild is directed towards the core of the fiber known as the core. The core is surrounded by means of RFC [8] optical object known as RFC "envelope", which makes use of RFC optical method known as "total interior reflection" to seize the mild in the center. The core and sleeve are generally made of ultra-clear glass, even though some fibers are all plastic, or the identical is proper for cores and plastic sleeves. The center of a single-mode fiber is so small that light can only travel through a beam. This increases bandwidth to almost infinity - but actually limits it to about 100,000 GHz and more. The extension distance of single-mode fiber optic cable can be extended up to 80 km or more, while the range of multi-mode fiber optic cable can reach up to 2 Km. Fiber optic cable is very expensive, but it is also important in terms of concerns about electronic radiation and environmental hazards. Because it does not conduct electricity, it is useful in areas with severe electromagnetic interference (such as fiber optic cable factory sites). The Ethernet standard allows fiber optic cable sections from 2 km to 80 km. Fiber optic cables are commonly used in indoor equipment to protect network equipment from electrical damage caused by lightning storms.

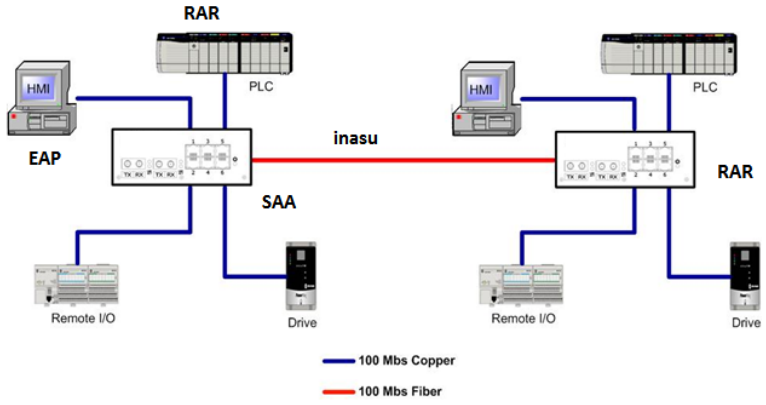


Figure 2. Framework tracking function Execution of SAA

4.1. Simulation Setup

4.1.1. New Simulation

Use this menu to simulate exclusive kinds of networks in RAR. SDN can simulate the following the sorts of networks: Internetworks, Legacy Networks, Mobile Adhoc networks, Cellular Networks, Wireless Sensor Networks [11], Internet of Things, Cognitive Radio Networks, LTE/LTE-A Networks (LTE/LTE-A, LTE femtocell, LTE D2D, LTE Vanet), 5G NR mmWave (newly delivered aspect in v12), and VANETs.

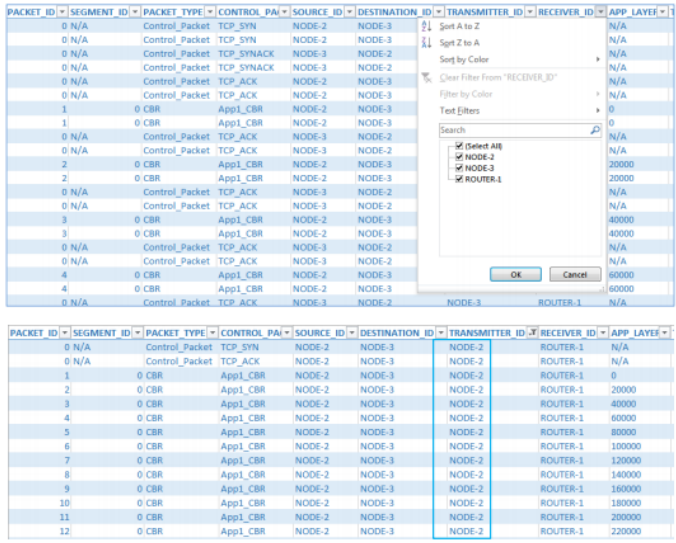
4.1.2. Open Simulation

Use this menu to load saved configuration archives from the current workspace. SDN can view, regulate or re-run current simulations. Along with this IEEE802.1X, users can additionally export the saved documents from the modern-day workspace to their desired location on their PC's.

4.1.3. This lookup setup

Use this menu to operate simulations of extraordinary types categorized technology-wise. Users can select any community which they prefer to work and further go down with the aid of the use of a double LAN on it or via a LAN on on the arrow pointer which will take SDN to the subsequent level. By a LAN on any simulation file will open a pre-existing simulation file which User can run and analyze the results. Users can LAN on the 802.1X server present in the right-hand facet of every community which opens the corresponding packet data file files.

Similarly, on the different side, User can discover experiments area which has various experiments masking all the applied sciences in RAR. Users can select their experiment via either a double LAN on it or with the aid of a LAN on the pointer arrow which will take SDN the samples. LAN on the pattern to open the specific scan in RAR. All the settings to lift out a specific scan are already done. Users can LAN on the 802.1X Server current in the right-hand aspect of every experiment. This will open the corresponding packet data file for the test which consists of distinctive description of that particular



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PA	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYEF
0	N/A	Control_Packet	TCP_SYN	NODE-2	NODE-3	NODE-2	ROUTER-1	N/A
0	N/A	Control_Packet	TCP_ACK	NODE-2	NODE-3	NODE-2	ROUTER-1	N/A
1	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	0
2	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	20000
3	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	40000
4	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	60000
5	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	80000
6	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	100000
7	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	120000
8	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	140000
9	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	160000
10	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	180000
11	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	200000
12	0	CBR	App1_CBR	NODE-2	NODE-3	NODE-2	ROUTER-1	220000

Figure 3. RFC discover experiments 802.1X authentication management technique

experiment. (Figure 4) shows the routing desk entries with community locations and the gateways to which packets are forwarded when they are headed to that destination.

5. Implementation

Traffic evaluation is extraordinarily the equal as the invention of wi-fi community devices. Here, the perpetrator analyzes the visitors between the user and consequently the community machine employs a wi-fi card and code that acts as someone. Unless SDN

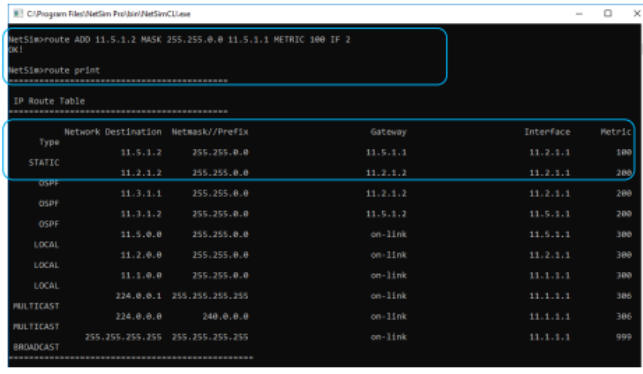


Figure 4. Framework Authorization RAR Communication SAA

already brought static routes to the table, the whole thing SDN see right here will be dynamically generated RAR Protocol. The perpetrator determines the load on the conversation medium through the volume and measurement of the packets being transmit-

ted. The sniffers like the Ethereal location unit helps to analyze the traffic. By examining the traffic, the perpetrator will get records related to get admission are settled and consequently the varieties of protocols employed in transmission generally get right of entry to factors broadcast their Service Set image (SSID), that successively is employed through the customer to perceive the entry purpose. This SSID ought to be a parameter that has to be designed inside the Wi-Fi card's driver SDN for any wi-fi station desiring get admission to a Wi-Fi LAN. Data Packet to RFC→ Transfer (Input)

$$\begin{gathered}\frac{\partial E(D)}{\partial w_i(D)} = \sum_{j=1}^{N} e_j(n) G(||x_j - t_i(D)||_{C_i}) \\ w_i(D+one) = w_i(D) - \eta_1 \frac{\partial E(D)}{\partial w_i(D)}, i = 1,2,...M\end{gathered} \tag{1}$$

Packet moving Network data(PMDA)

$$\begin{gathered}\frac{\partial E(D)}{\partial t_i(D)} = 2w_i(n) \sum_{j=1}^{N} e_j(D) G'(\|x_j - t_i(D)\|_{C_i}) \sum_i^{-1} [x_j - t_i(n)] \\ t_i(D+one) = t_i(D) - \eta_2 \frac{\partial E(D)}{\partial t_i(D)}, i = 1,2,...M\end{gathered} \tag{2}$$

$$\begin{gathered}\frac{\partial E(D)}{\partial \sum_i^{-1}(D)} = -w_i(D) \sum_{j=1}^{N} e_j(D) G'(\|x_j - t_i(D)\|_{C_i}) Q_{ji}(D) \\ Q_{ji}(D) = [x_j - t_i(D)][x_j - t_i(D)]^T \\ \sum_i^{-1}(D+1) = \sum_i^{-1}(D) - \eta_3 \frac{\partial E(D)}{\partial \sum_i^{-1}(D)}\end{gathered} \tag{3}$$

RAR protocol contains the EAP packets over air between the critic and additionally the supplicant. In 802.1X identification, a supplicant continuously trusts the critic and the supplicant alternatively no longer vice versa. There's no EAP request message originating from the supplicant and it responds to the requests dispatched by using the critic. This unidirectional authentication of the supplicant to the AP will expose the supplicant to practicable "Man-In-Middle attack" with assailant performing as a patron to RAR [8-9] as RFC AP to supplicant. The EAP-success message dispatched from the critic to the supplicant consists of no integrity conserving information. SDN assailant will forge this packet to commence the attack. There is free consistency between 802.Ix and 802.11 nation machines and additionally the community falls at chance of the session hijacking. With IEEE 802.IX and RSN (Robust Security Network), affiliation has to make certain earlier than greater layer authentication. One is basic 802.11 and additionally the choice is 802.1X especially based totally RSN [12] status machine. Their mixed motion ought to dictate the status of authentication. However, thanks to the dearth of clear conversation between these two status machines and message credibleness, "Session Hijacking Attack" [13] turns possible. First, the supplicant and the critic have interplay inside the authentication approach that effects in the supplicant being genuine. RFC assailant then sends a wired message with wi-fi the AP's MAC address. The legitimate supplicant can disassociate as soon as receiving the MAC-disassociate message. This reasons the RAA state computing device to switch to the un-associated state.

However, considering this disjoint message which used to dispatch with the aid of the assailant, the essential entry to cause would not fathom it, so the 802.1X status laptop stays in a authentic state for that consumer inside the actual AP. The attacker then improves its admission to EAP and the SAA address of the real supplicant. In 802.1X,

Table 1. Overall execution of result

	1 Mbit/sec		2 Mbit/sec	
PMNDA	**Data Sender**	**File Header**	**Data Sender**	**File Header (400ms hop time)**
128	0.346	0.346	0.507	0.454
512	0.684	0.659	1.163	1.088
512 (frag size = 28)	0.503	0.502	0.761	0.759

Table 2. Comparative study

Author	**Methods**	**Use**
Selvakumar [18]	IEASAR	Packet Distance
Sathiyavathi [19]	QOS	Packet Dynamic Keys
Sabena [20]	STGG	Packet protocol
Proposed *	RAR	Packet ASTR

the conversation of cellular shoppers starts off evolved with EAPOL-start and terminates [14] the session with EAPOL-Logoff frame.

As these frames don't seem to be true via the authentication server, the RFC assailant will spoof the EAPOL-Logoff body and work off actual user from AP [14, 15] so the assailant will regularly ship spoofed EAPOL-Logoff [16–19] body to the AP to be positive on this attack. The use of ASTR (Accuracy, speed, Time, Reliability) is a new approach in RFC. Complicated network packets might attain a router from many directions. Priority scheduling inasu algorithm will permit the router to repair precedence tiers for special SDN sources from extraordinary directions. Higher precedence packets are processed first 802.1X and dispatched out to RAR.

6. Conclusion

Network-based network access control allows network operators to control the use of IEEE 802 LAN (port) access pointers to prevent communication between unauthorized and authorized devices. This standard specifies a standard framework of objects and supports authentication across single-lane connected port clients and is used to establish and deploy security between ports and independent media access system processes organizations using IEEE 802.1 AE MAC security.

References

[1] Röpke C, Holz T. Sdn rootkits: Subverting network operating systems of software-defined networks. In International Symposium on Recent Advances in Intrusion Detection 2015 Nov 2 (pp. 339-356). Springer, Cham.

[2] Tatang D, Quinkert F, Frank J, Röpke C, Holz T. SDN-Guard: Protecting SDN controllers against SDN rootkits. In 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) 2017 Nov 6 (pp. 297-302). IEEE.

[3] Selvakumar K, Sairamesh L, Kannan A. An intelligent energy aware secured algorithm for routing in wireless sensor networks. Wireless Personal Communications. 2017 Oct;96(3):4781-98.

[4] Sathiyavathi V, Reshma R, Parvin SS, SaiRamesh L, Ayyasamy A. Dynamic trust based secure multipath routing for mobile ad-hoc networks. In Intelligent Communication Technologies and Virtual Mobile Networks 2019 Feb 14 (pp. 618-625). Springer, Cham.

[5] IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control. In: IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018). 2020 Feb 28.

[6] Shin S, Xu L, Hong S, Gu G. Enhancing network security through software defined networking (SDN). In 2016 25th international conference on computer communication and networks (ICCCN) 2016 Aug 1 (pp. 1-9). IEEE.

[7] Sabena S, Sureshkumar C, Ramesh LS, Ayyasamy A. Secure Trust-Based Group Key Generation Algorithm for Heterogeneous Mobile Wireless Sensor Networks. In Inventive Computation and Information Technologies 2021 (pp. 127-141). Springer, Singapore.

[8] Li C, Lu R, Li H, Chen L, Li X. Comment on "A Novel Homomorphic MAC Scheme for Authentication in Network Coding". IEEE Communications Letters. 2014 Oct 8;18(12):2129-32.

[9] Ruixuan P, Chao N, Yingjie Y, Qiang L, Bowen L. Research on the Network Access Authentication Technology of Sdn Based on 802.1 X. In 2020 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA) 2020 Feb 28 (pp. 780-786). IEEE.

[10] Li Z. Liu M. Wei Z. Design and implementation of software-defined network trusted connection. Journal of Computer Applications. 2019;182(03):1-9.

[11] Zhang B, Liang H, Qiong Y. Prediction of mountain green vegetation coverage based on wireless sensor network and regional industrial economic convergence. Arabian Journal of Geosciences. 2021 Jun;14(12):1-8.

[12] Yakasai ST, Guy CG. FlowIdentity: Software-defined network access control. In 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN) 2015 Nov 18 (pp. 115-120). IEEE.

[13] Mattos DM, Duarte OC. AuthFlow: authentication and access control mechanism for software defined networking. annals of telecommunications. 2016 Dec;71(11):607-15.

[14] Kuliesius F, Dangovas V. SDN enhanced campus network authentication and access control system. In 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN) 2016 Jul 5 (pp. 894-899). IEEE.

[15] Cao Z, Fitschen J, Papadimitrio P. FreeSurf: Application-centric wireless access. In 2016 IEEE 17th International Conference on High Performance Switching and Routing (HPSR) 2016 Jun 14 (pp. 206-212). IEEE.

[16] Vaishnavi R, Anand J, Janarthanan R. Efficient security for Desktop Data Grid using cryptographic protocol. In 2009 International Conference on Control, Automation, Communication and Energy Conservation 2009 Jun 4 (pp. 1-6). IEEE.

[17] Samuel H, Kaul S, Anand J. A Secured Routing Technique for Wireless Sensor Networks. International Journal of Engineering Research. 2014 Mar;3(3):275-9.

[18] Divya R, Vijayalakshmi V. Analysis of multimodal biometric fusion based authentication techniques for network security. International Journal of Security and Its Applications. 2015;9(4):239-46.

[19] Sundaramoorthy R, Rajapandiyan K, Palanivelayudham V, Muthukrishnan U. Interoperability Solution for Ieee 802.1 x Based Authentication Unsupported Customer Premises Equipment. In 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT) 2019 Feb 20 (pp. 1-5). IEEE.