4th International Conference on Automation, Control Engineering and Computer Science (ACECS - 2017)
Proceedings of Engineering and Technology – PET
Vol.19, pp.88-93

Control Frame Protection during Hand off Process

[1]Abdul Razaque
Computer Science Department
New York Institute of Technology (NYIT)
[1]arazaque@nyit.edu

[2]M. Abdulghafour
Computer Science Department
New York Institute of Technology (NYIT)
[2]mabdulgh@nyit.edu

***Abstract*— Currently IEEE 802.11 remote Local Area Network (WLAN) turns out to be the most important for data communication. It is straightforward extent extender for a home-wired Ethernet interface, or as a wireless interface, WLAN produces the mobility, ease of access and moderation. The majority of the 802.11 remote systems utilize the recurrence of 2.4GHz, which often drives the system to be risky and more vulnerable than conventional Ethernet networks. IEEE 802.11 is the most predominant Wireless Medium Access Control (MAC) protocol, which *attempts to make* all the nodes to remain safe and cooperative in the network. However, attackers may attempt to make nodes misbehave in their performance of the network by consuming an additional bandwidth and resources. The MAC layer misbehaviors can be caused by several malicious threats, but the Denial-of-Service (DoS) attack is extremely critical as it can disrupt the network operation and performance. Thus, control frame protocol in IEEE 802.11 is the most important component to avoid the network allocation dilapidation and vector-based DoS attacks. IEEE 802.11 is highly susceptible DoS attacks. In this paper, we propose an Internet Access Point Protocol for Frame Control (IAPPFC) for securing control frames. Our proposed Access Point protocol guarantees the control frame protection by generating a unique message authentication code using inter-access (between different stations & clients) point protocol for key distribution and key management. The validation of the proposed IAPPFC is confirmed by using Network simulator-3 (NS3).**

Keywords: CTS, RTS, MAC, IAPPFC, WEP, IEEE 802.11.

I. INTRODUCTION

Security has become an ever important issue in the case of wireless networking. Recently, there has been a huge amount of research on the security protocols and key exchange mechanisms in IEEE 802.11 networks [1]. However, these networks are still vulnerable to DoS attacks [2] because these attacks commonly happen prior to invoking the security protocols. The main purpose of DoS attacks is to stop a legitimate client from accessing resources. Vulnerabilities create the weak point in IEEE 802.11 and IEEE 802.15 MAC header [3-4] and Counter measures for WLAN Denial of Service attacks. IEEE 802.11 MAC [5-8] layer classifies communication into three types of messages: Management, Data and Control messages. Currently standards 802.11i is used to protect data frames and 802.11w [9] for protecting management frames. Control frames which are mostly used for bandwidth reservation and acknowledgement purposes cannot be secured by the above mentioned standards [10-13]. As a result, it causes the network to be attacked using these frames. Due to this weakness, a wide range of network allocation vector based DoS attacks are possible. The purpose of this paper is to protect the control frames in a wireless network. In this paper, we provide the solution how to protect the control frames being spoofed from DoS and vector-based DoS attacks. This paper contributes new protocol IAPPFC to secure the control frames during the handoff process. The IAPPFC generates unique authentication code to improve the key distribution and key management processes.

The remainder of the paper is organized as follows: Section II presents problem Identification. Section III gives complete overview of the existing techniques. Section IV presents the problem formulation and description. Section V presents the proposed approach to protect the control frames. Section VI discusses the experimental results and analysis and finally, the entire paper is concluded in section VII.

II. PROBLEM IDENTIFICATION

An attacker can use the control frames to provide the medium unavailable by gaining the bandwidth using RTS & CTS (Request- to-Send & Clear- to-Send) or CTS to self-organization even if it is not part of the network[]. The attacker can replay the captured RTS frame or CTS frame or it can inject the spoofed CTS [11] frames into the network. Due to this situation, all the stations present in the network attempt to update their Network Allocation vector (NAV) timers and terminate their transmissions. Thus, there is need to introduce such solution that should not only protect the RTS and CTS frames, but it should protect all control frames including Block Ack.

III. RELATED WORK

In this section salient features of the existing approaches are discussed. A lot of attention has already been paid on

ISSN 2356-5608

the security of IEEE802.11. However, the majority of the work has focused on the shortcomings in the wired equivalency protocol (WEP) for providing the protection between 802.11 customers and access points [6].

IEEE 802.11standard proposed the WEP (Wired Equivalent Privacy) which uses RC4 algorithm to protect the data messages by using a pre-shared key [10]. Most of this work has focused on weaknesses in the WEP intended to provide data privacy between clients and access points. As the RC4 algorithm has been identified to have vulnerabilities and weak keys [14] The Wi-Fi Alliance, working in conjunction with the IEEE, has brought a strong interoperable Wi-Fi security specification to the market in the form of Wi-Fi Protected Access (WPA). A scheme named WPA protects the data messages by generating per packet keys [15]. However, no security solution could provide the "bullet-proof. Thus, WPA represents a quantum leap forward in Wi-Fi security. It brings forward IEEE 802.11i standard [1], [3]. WPA not only gives strong data encryption to rectify WEP's weaknesses, but it gives user authentication which is missed in WEP, IEEE 802.11w standard proposed to provide security protection for all management frames. All existing solutions brought substantial improvement from security perspective, but addressed the issue of static nodes. Our approach attempts to resolve the security problem of RTS and CTS control frames in mobile node when they initiate the handover process. In addition, our approach addresses the accuracy and malicious node detection probability.

IV. PROBLEM FORMULATION AND DESCRIPTION

As a first step we propose the key generation and key distribution protocol using IAPPFC framework. Using this key, we produce a message authentication code (MAC) introduced in [3-4] for control frames. The unique sequence numbers are generated to avert the counter reply attack. We use earlier transmitted RTS to validate the current received CTS. We also verify whether data is being sent immediately after receiving the CTS. And if there is no data message is sent after the CTS frame, then Network Allocation Vector (NAV) update is not validated. The architecture of the network model comprises of several access points (APs) and stations (STA1, STA2, Rogue Station) are available in the same channel. All the stations and access points available in the network must be compatible with IEEE 802.11i and IEEE 802.11w.

Here, we focus on the attacks caused by outsider attackers. The goal of the attacker is to consume the entire channel of STAs and Aps. As a result, the attacker occupies the entire bandwidth. The attacker attempts to generate different types of attacks such as replay attack, RTS reply attack, CTS reply attack and Injecting Spoofed CTS frames.

In a replay attack, an authentication session is replayed to confuse the system into granting access. In a RTS replay attack, if STA1 needs to transmit data to AP, then the rogue station(attacker) can hear the channel and acquire the RTS frame [sent by STA1 and retransmit it to the AP at a later time. When the AP sends CTS in accordance to STA1 that is rejected. The actual owner of the replayed RTS] is not STA1, but actually its rogue station. Once STA2 sees the CTS frame, then it l updates its NAV timer. If the attacker is an expert, then it can change the duration field of the RTS frame with a very large value while making STA2 wait for the longer time. In CTS replay attack, the rogue station can hear to the channel and acquire the CTS frame sent by an AP in response to any RTS sent by STA1.The rogue station replays the same frame. As in the earlier case, STA1 rejects the CTS frame and does not update its NAV timer. Once, STA2 receives the CTS frame; then it updates bits of NAV timer with the duration field indicated in the CTS frame. Hence STA2 terminates transmissions until the NAV timer expires.

In Injecting Spoofed CTS frames, the rogue station forms the spoofed CTS frames and transmits it. This type of attack is more powerful than all the above mentioned attacks as every station (example STA1 and STA2) and APs existing in the network update their NAV timer. All the stations and APs presented in the channel within listening range stop their transmissions as suggested by the CTS frame. An attacker can use this method to stop others from transmitting data by spreading the CTS frame for a certain period.

V. CONTROL-FRAME PROTECTION

To secure the control frames in a wireless system, we begin with a technique for key generation and distribution utilizing IAPPFC structure. Therefore, a message authentication code is produced utilizing this key. This does not suffice to counter the replay attacks mentioned in the above section. With a specific end goal to counter this, we built up a sequence numbering scheme which guarantees the message authentication code that can be connected to a wide range of control frames even for new frames like Block ACK Request and Block ACK [13]. We describe how key distribution and generation processes are done, and after that, continue to replicate [proceed] the expansions to the current control frames. In conclusion, we describe how the sequence number is redesigned to counter the replay attacks.

Algorithm 1: Protection of Control Frames Process
1. Generation of key 'k'
2. If ((APP ∈ C1)&&(APP= false)) then
3. beginning of key process
4. end if

ISSN 2356-5608

5. Kr is send to other AP using IAPPFC
6. else if (AAP>1 && AAP ∈ C1), then
7. one AP will be selected
8. else, none of the AP's will be selected
9. end if
10. if (Ca ∈ C1), then
11. AP sends Kr to other AP's
12. end if
13. New key Ku is initiated
14. The update key 'Ku' will be sent to all the stations connected to AP's
15. If (Ku==K), then
16. updating of key is successful
17. else, not successful
18. Creation of one-time key generation by encryption using SHA-256
19. If (Ma=true), then
20. message authenticated code is appended to control frames
21. Sequence number 'S' is appended to the message to prevent reply attack
22. For every 'N' micro second, stations should update sequence number
23. While (CTS frame not approved), then
24. Control packets will not be sent by AP
25. else if (Tp=long), then
26. using reply attack, the attacker can attack
27. end if

First *key* generation is done where key process is initialized when there are no active APs found in same channel. Generated Key 'K' and distributed to all stations connected to AP. Thee generated Key requests for the AP, when other APs are active in same channel. Key request is sent to other AP using IAPPFC. It selects one AP if more than one active Aps are available in the same channel. After key request process, the key transfer procedure is started. AP sends key request to other AP based on authenticated channel. In Key update, an initiated AP can send this request to other APs available in the channel and new key 'K' is sent to all APs.) Then, Key update response is sent to all the stations. After key response is done, then Key updating is performed whether it is successful or not. Once key update is successful from all Aps, the initiator who started key update will send key update response to all APs. Here in control frames, we use SHA-256 algorithm instead of HMAC algorithm. Message authentication code field is added to existing control frame fields which gives protected control frame fields. The existing frame check sequence which is present in 802.11 RTS & CTS is replaced with add Sequence number. The sequence number is given to all stations when it connects to AP. Then station needs to update sequence number every 'N' micro second. Here sequence number is 32 bit. The control packet sent by stations or access point will be listened to by all stations, or else CTS frame sent by a station is not approved. If the time period is longer, then the attacker can attack using replay attack. The Calculation of 'N' is done by using duration value of CTS frame if there are hidden nodes. The best value of 'N' is the smallest size data packet that can be calculated using equation (1).

$$N = S_f + D_{re} + S_f + t_{ack} + t_{pr} \quad (1)$$

TABLE 1: Notation and description of given variables

Notation	Description
S_f	Short Inter-frame space
D_{re}	Time required for transmitting the data packet in air
t_{ack}	Time required for transmitting the Acknowledgement frame for the previous data packet on air
t_{pr}	CTS Packet preamble duration

A. Key Generation and Distribution

Initially the AP checks the whole channel for a certain scan interval to discover other active APs presented in the same channel. During this interval, if no different APs are found in the same channel, then Key primitive generation process is started.

In the event, the scanned-result is effective (which implies that different APs are found in the same channel), then the AP sends a Key request to alternate access point utilizing the IAPPFC. On the other hand, there is a possibility of more than one APs existing in the channel. Thus, the AP can decide to demand for the key from any AP available in the scan list. This primitive is utilized at whatever point an AP gets a key request. The request is validated taking into account the verification provided by the other AP. Furthermore, the key is transferred to the next AP utilizing a secured communication channel.

Any AP present in the channel can start this request and send an update request to the various APs present in the channel. The new key 'K' is produced and sent alongside the request. On accepting the Key update initiate is asked for. The APs present in the channel are sent to the stations through the wireless medium. On accepting Key update response from every one of the Aps, the initiator who started the key update initiate request will send key update successful message to all of the APs. In return the APs send the time stamp information at which the new key $'K_n'$ should replace existing key 'K' to all the stations.

B. Control Frames Format According to New Model

Message authentication code is generated by using the SHA-256 cryptographic hash function. The reason for using SHA-256 cryptographic hash function is that many station adapters already have this cryptographic hash function in either their software or hardware layers. It reduces the overall cost of the updating the system. The message authentication code is appended to the control frames and validated the authenticity of the message from the authenticated receiver.

ISSN 2356-5608

To prevent replay attacks, the sequence number $'S_n'$is appended to the message as depicted in Figure 1. The sequence number with 4 bytes is chosen to prevent replay attacks and also the key needs to be updated. (Considering that sequence number is updated after every 178us. We conducted several tests by using variable time for update, but 188us is optimized time. The Frame- Check Sequence (FCS) which is the part of initial 802.11 RTS and CTS frame removed to reduce the overhead as MAC can be used in the place of FCS. The initial network sequence number is given to the station whenever it connects to the access point. From there the station needs to update the sequence number after every 'N' micro seconds. The sequence number 'S' is a 32-bit and once the sequence number reaches (232 -1), it wraps. The sequence number is updated based on time interval rather than using packet count. The time interval by which the sequence number is updated should not be too short as synchronization in wireless medium is not too accurate. At the same time, the time interval should not be too long as the attacker can attack using the replay mode. We estimated the value of 'N' assuming that the station is transmitting a data packet of very small size immediately after transmitting the CTS. To avoid replay for this case, the 'N' should be equivalent to the duration value in the CTS frame.

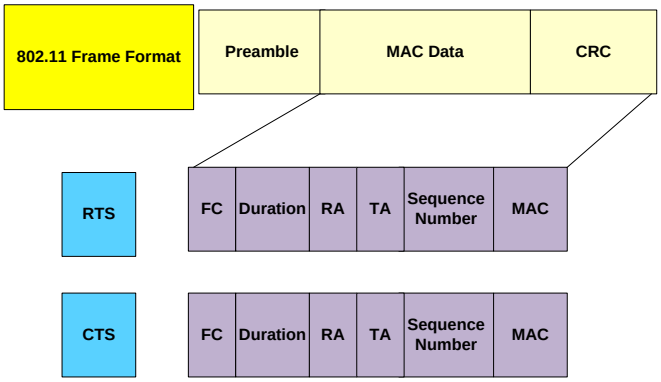


Figure 1. RTS & CTS Frame form

Where
FC- frame control
RA- receiver Address
TA- Transmitter Address
MAC- Message Authentication Code

Therefore, the best way is to make approximation for 'N' while considering the size of the smallest data packet. In addition, use the size of the packet as reference to calculate the duration. The solution is to improve the current 802.11control frame protection by generating a unique message authentication code using IAPPFC framework for key distribution and key management processes. The cryptographic SHA-256 hash algorithm is used to generate MAC for the control frames that are supported by most of the current wireless station adapters which in turn makes this approach as an inexpensive.

VI. EXPEREMENTAL RESULTS

Here, we simulated the scenario having new control frame protection environment using NS3. The primary goal of the simulation is to generate a unique message authenticated code (MAC) using the key generated through IAPPFC framework. The simulation scenario consists of 50 nodes. IAPPFC is used in handoff and generated for the attackers to mislead the bandwidth. The nodes are randomly placed in a uniform fashion in the area of 1200 * 1200 square meters. The total simulation time is 100 seconds. The results demonstrate an average of 08 simulation runs.

Our experiment depicts the Handoff mechanism is initiated where 50 nodes are created; out of them 10 nodes are dedicated for the access points and the remaining are set to be mobile nodes. The total simulation time is 100 seconds. The mobile node can freely move from one access point to other access point throughout the simulation time. The mobile nodes also maintain the network connectivity when forwarding the data frame. Hence, IAPPFC provides the undisturbed signal strength to user mobile nodes even when initiating handoff process and transmitting data.

Now, the attacker node which takes the data by not allowing it to go to required user mobile nodes. Here, we generate the attacks by randomly generating traffic using control frame messages (RTS & CTS) of sender & receiver nodes. The random generation is done by using random app procedure, so this assigns the traffic randomly to different nodes during simulation time. The Summarized simulation parameters are explained in Table 2.

TABLE 2: simulation parameters

Parameters	**Description**
Number of Nodes	50
Queue length	50 packets
Type of Network	Wireless
Sensing range of nodes	40 meters
Data rate	55Mbps
RTS Threshold	1000 bytes
Packet size	1500 bytes
Simulation time	100 sec
Size of Network	1200*1200 square meters

Based on simulation, we targeted following results

- Handover Accuracy

ISSN 2356-5608

- Malicious Node Detection
- Control Frame with IAPPFC and without IAPPFC

A. Handover Accuracy

Handover accuracy is of paramount [16]. Figure 2 shows the accuracy of the handover process of the mobile nodes. The graph X-axis describes the number of handoff taken place in the network and Y-axis describes the accuracy of handoff/handover. Here the nodes are 50 in the network. As, 18 nodes are initiating the handoff process, we generate 10% malicious nodes which cause the handoff process to be increased and reduced the accuracy, However, our approach has been capable to maintain 99.9% handover accuracy that results in stabilizing the network performance.

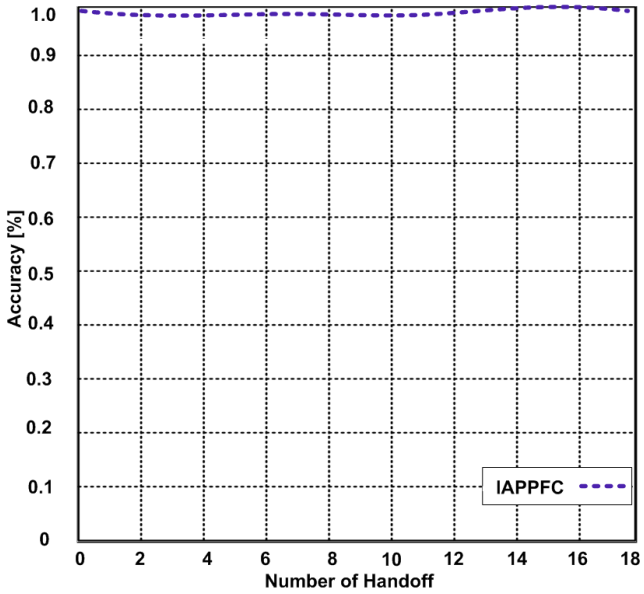


Figure 2: Accuracy based on different number of handoff processes

A. Malicious Node Detection

Figure 3 shows the number of malicious nodes that can be detected during detection time. Using the IAPPFC protocol, we generate the number of malicious nodes on X-axis from 0 to 27 and detection time in [seconds] on Y-axis from 0 to 1 Seconds. Here, the trend increases with respect to number of malicious nodes. As there are more malicious nodes time taken to detect the malicious nodes would be more at different intervals of time. Here 3 malicious nodes are detected at 0.59 seconds and 7 nodes are detected at 0.4 seconds and so on 27 malicious nodes are detected at 0.8 seconds. Thus, our approach provides the variable time for detection process because of depending on the nature of handover process and malicious node's capacity.

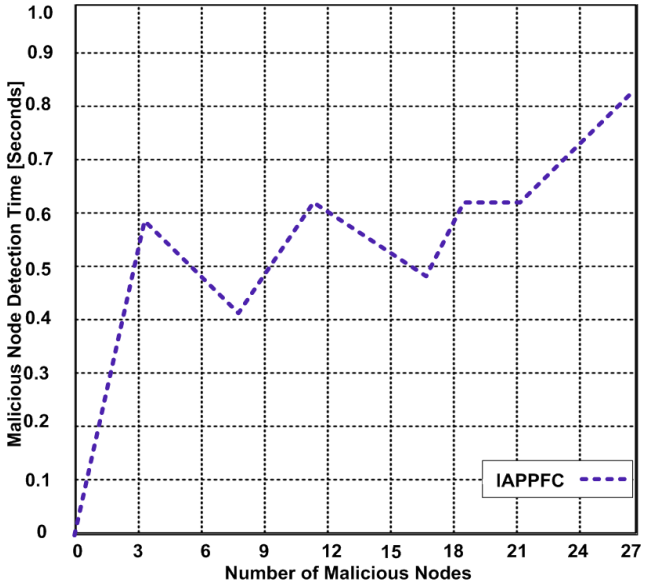
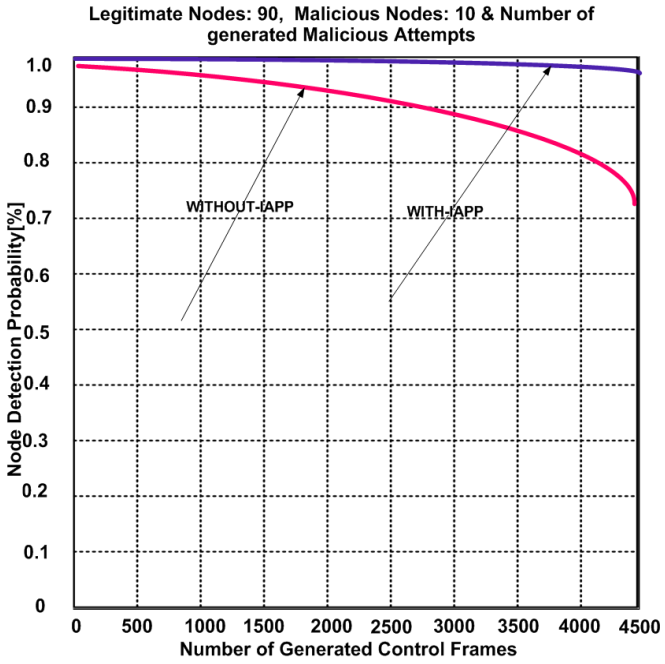


Figure 3: Malicious detection time for different malicious nodes

C. Control Frame with IAPPFC and without IAPPFC protection

Figure 4 reflects the difference between control frame with IAPPFC & without IAPPFC. The X-axis provides the information of the number of generated control frames and Y-axis provides the information of node detection probability [%]. Here when using without IAPPFC, the capability of malicious node detection would be reduced and even the performance also decreases.



ISSN 2356-5608

Figure 4: Node detection probability based on generated control frames

With our IAPPFC protocol, the malicious node detection capacity increases. As a result, it leads to increase the performance of the network. By using the proposed scheme, we get the desired objectives.

VII. CONCLUTION

Internet Access Point Protocol for Frame Control is introduced to secure the network traffic when node is initiating the handoff process. Our approach detects the reply and fake CTS frames injected by Daniel of service attacks. The standard control frame is modified with new control frame format by appending a sequence number and message authentication code (MAC). The MAC is generated by using the key produced by IAPPFC framework. Existing hash function (SHA-256) is applied to produce MAC for the control frames which in turn is supported by most wireless adapters that is also cost effective. The IAPPFC uses the handoff mechanism to switch the nodes or users from one access point to other access point, and malicious attacks are generated to consume additional bandwidth or mislead the bandwidth by replaying or repeating the same RTS or CTS frames. Our proposed approach IAPPFC is validated using NS3. The experimental results confirm the effectiveness of our proposed approach.

REFERENCES

[1] Razaque, Abdul, Savitesh Jain, MNK Sai Santosh Irrinki, Fathi H. Amsaad, and Musbah Abdulgader. "Simultaneous Priority and Detection based Carrier Sense Multiple Access protocol." In *Electro Information Technology (EIT), 2016 IEEE International Conference on*, pp. 0111-0116. IEEE, 2016.

[2] Sheng, Yong, Kokkiong Tan, Guanling Chen, David Kotz, and Arnett Campbell. "Detecting 802.11 MAC layer spoofing using received signal strength." InINFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.

[3] Razaque, Abdul, and Khaled M. Elleithy. "Energy-efficient boarder node medium access control protocol for wireless sensor networks." *Sensors* 14, no. 3 (2014): 5074-5117.

[4] Hemin Nilesh Dalal,Nisarg V Soni, Abdul Razaque, "Header encryption of IEEE802.15.4",Conference: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT): DOI: 10.1109/LISAT.2016.7494140

[5] Chong Han, Mehrdad Dianati,Rahim Tafazolli,Ralf Kernchen,Xuemin Shen, "Analytical Study of the IEEE 802.11p MAC Sublayer in Vehicular Networks", Journal of IEEE Transactions on Intelligent Transportation Systems archive Volume 13 Issue 2, June 2012, PP: 873-886.,

[6] Rizwan Khan,Sonia Aissa,Charles Despins, "MAC layer handoff algorithm for IEEE 802.11 wireless networks",IEEE Symposium on Computers and Communications, 2009. ISCC 2009, PP:1530-1346:DOI:10.1109/ISCC.2009.5202350.

[7] Richard W. Pazzi, Zhenxia Zhang, Azzedine Boukerche. "Design and evaluation of a novel MAC layer handoff protocol for IEEE 802.11 wireless networks", Elsevier Journal of Systems and Software. Vol. 83(8), August 2010, PP: 1364–1372.

[8] Sung Hoon Seo, JooSeok Song, Haitao Wu,Yongguang Zhang, "Achievable Throughput-Based MAC Layer Handoff in IEEE 802.11 Wireless Local Area Networks",EURASIP Journal on Wireless Communications and Networking20092009:467315: DOI: 10.1155/2009/467315.

[9] Jyoti Sachan, Anant Kr. Jaiswal, "Reducing the Latency of IEEE 802.11 MAC Layer Handoff using Virtual Access Point", International Journal of Engineering Research & Technology,Vol.2(2),2013.M.Gineste,N.V.Wambeke,E.Exposito,C. Chassot, L.Dairaine, "A Cross-Layer Approach to Enhance QoS for Multimedia Applications Over Satellite", Wireless Pers Commun (2009) 50: 305. doi:10.1007/s11277-008-9591-1.

[10] Gerla, Mario, Ken Tang, and Rajive Bagrodia. "TCP performance in wireless multi-hop networks." In Mobile Computing Systems and Applications, . Proceedings. WMCSA. Second IEEE Workshop on, pp. 41-50. IEEE,.

[11] Lei, Zhongding, and Stephen J. Shellhammer. "IEEE 802.22: The first cognitive radio wireless regional area network standard." IEEE communications magazine 47, no. 1: 130-138.

[12] Xiao, Yang, Haizhon Li, and Sunghyun Choi. "Protection and guarantee for voice and video traffic in IEEE 802.11 e wireless LANs." In INFOCOM. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 2152-2162. IEEE,

[13] Ni, Qiang. "Performance analysis and enhancements for IEEE 802.11 e wireless networks." Network, IEEE 19, no. 4: 21-27.

[14] Ramani, Ishwar, and Stefan Savage. "SyncScan: practical fast handoff for 802.11 infrastructure networks." In INFOCOM. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, pp. 675-684. IEEE.

[15] Lae Lae Khine, "A New Variant of RC4 Stream Cipher",World Academy of Science, Engineering and Technology, International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering Vol:3, No:2, 2009.

[16] Razaque, Abdul, Syed S. Rizvi, Meer J. Khan, Qassim B. Hani, Julius P. Dichter, and Reza M. Parizi. "Secure and quality-of-service-supported service-oriented architecture for mobile cloud handoff process." *Computers & Security* 66 (2017): 169-184.

ISSN 2356-5608