Control Frame Protection from Denial-of-Service Attacks during Handover Process

Abdul Razaque[1], Saule Amanzholova[1], Azhar Sagymbekova[1], and Shakirt Makilenov[1,2]

[1] *International Information Technology University, Manas St. 34/1, Almaty, A15M0F0, Kazakhstan*
[2] *Al-Farabi Kazakh National University, al-Farabi Ave. 71, Almaty, A15E3B5, Kazakhstan*

Abstract

IEEE 802.11 remote Local Area Network (WLAN) has become increasingly important in recent years. WLAN provides mobility, ease of access, and moderate whether used as a simple range extender for a home wired Ethernet interface or as a wireless interface. The majority of the 802.11 remote system operates at 2.4GHz, making the system more dangerous and vulnerable than traditional Ethernet networks. IEEE 802.11, the most widely used wireless Medium Access Control (MAC) protocol, assumes that all nodes in the network are safe and cooperative. However, attackers may cause nodes to degrade network performance, obtain extra bandwidth, and consume resources. These MAC layer misbehaviors are known as Denial of Service (DoS) attacks, and they can cause network outages. There is no way to protect control frames in an 802.11 wireless local access network, which opens the door to a variety of network allocation vector-based DoS attacks. In fact, 802.11 is thought to be highly vulnerable to dangerous denial-of-service (DoS) attacks. We propose the Internet Access point protocol frame control (IAPPFC) for securing control frames in this paper. The characteristics of proposed IAPPFC provides the best features to generate a unique message authentication code for protecting control frames between different stations and clients. The proposed IAPPFC is implemented on network simulator-3. Based on the outcomes, it is proved that the proposed approach obtains better accuracy, and node detection capability.

Keywords

IAPPFC, Wireless, Security, IEEE802.11, MAC, DoS, Privacy

1. Introduction

Security has grown in importance due to vulnerability of wireless networking. The security protocols and key exchange mechanisms used in IEEE 802.11 networks have recently been the subject of extensive research [1], [2], [3]. However, due to the fact that DoS attacks frequently take place before security protocols are invoked, these networks are still vulnerable to them [4], [5], [6]. DoS attacks' primary goal is to prevent legitimate clients from accessing resources [7]. The IEEE 802.11 MAC protocol is weak because of vulnerabilities [8], [9], [10] and countermeasures for WLAN DoS attacks [11].

Communication is divided into three categories by the IEEE 802.11 MAC layer: management, data, and control messages. Currently, 802.11i standards are used to protect data frames and 802.11w standards are used to protect management frames. The above-mentioned standards are unable to secure control frames. These control frames are primarily used for bandwidth reservation and acknowledgement purposes, making the network vulnerable to attacks [12], [13], 14]. This paper discusses how to safeguard wireless network control frames. This makes a variety of denial of service

Proceedings of the 7th International Conference on Digital Technologies in Education, Science and Industry (DTESI 2022), October 20–21, 2022, Almaty, Kazakhstan
EMAIL: a.razaque@iitu.edu.kzv (Abdul Razaque); s.amanzholova@iitu.edu.kz (Saule Amanzholova); a.sagymbekova@iitu.edu.kz (Azhar Sagymbekova); shakirt.makilenov@gmail.com (Shakirt Makilenov)
ORCID: 0000-0003-0409-3526 (Abdul Razaque); 0000-0002-6779-9393 (Saule Amanzholova); 0000-0001-8878-3895 (Azhar Sagymbekova); 0000-0002-5330-4716 (Shakirt Makilenov)

attacks based on network allocation vectors possible. In this paper, we offer a method for using IAPPFC for control frame protection from being spoofed. The handover process is depicted in Figure 1.

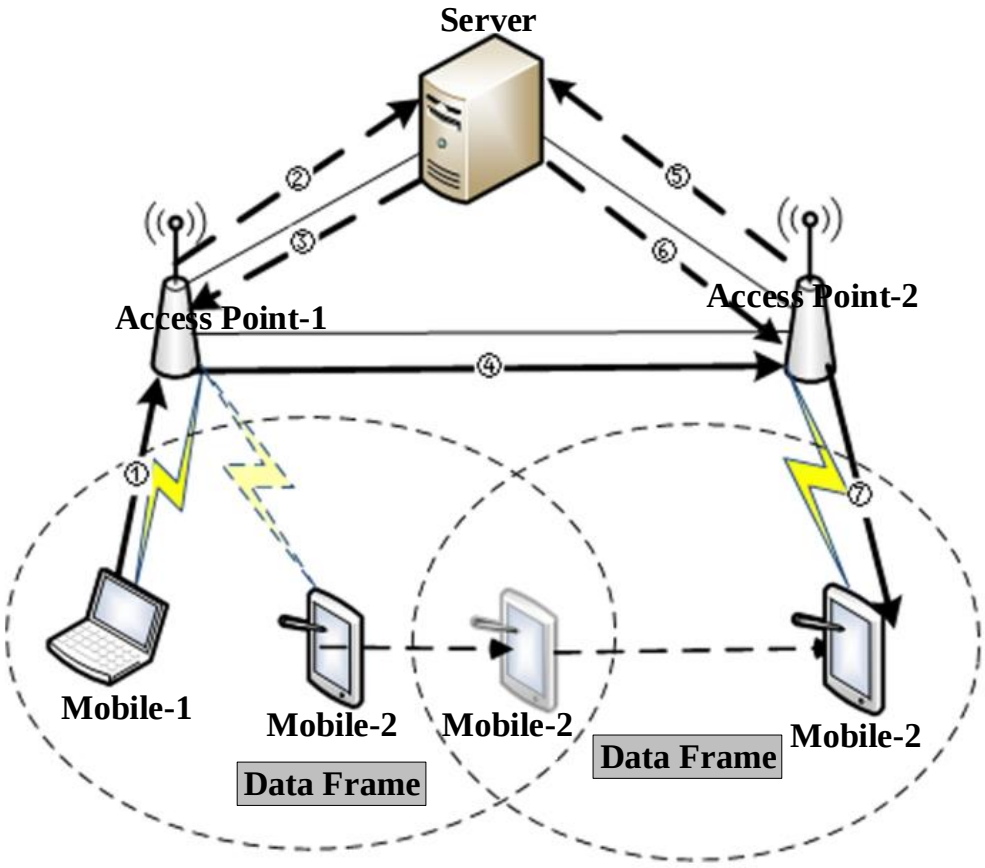

Figure 1: Handover process with data frame format

1.1. Paper Contribution

The main contributions of the paper are summarized as follows:

- The MAC layer can easily be exploited due to vulnerabilities of control frames that lead to DoS attacks. The IAPPFC is employed to secure the control frames from being attacked.
- A unique message authentication code is generated to protect the control frames while sending between clients and stations.
- The better node detection probability and accuracy are achieved.

1.2. Paper organization

The remainder of the article is structured as problem identification is presented in Section II. A comprehensive overview of the methods is provided in Section III. System model is provided in Section IV. Proposed plan & Implementation is in Section V, and References is in Section VI. Section VI provides the paper's conclusion.

2. Problem identification

An attacker can use control frames to gain bandwidth by using RTS-CTS (Request to Send - Clear to Send) or CTS to self-organization even if he is not a member of the network. The attacker can either replay the captured RTS or CTS frame or inject spoofed CTS frames into the network. As a result, all stations in the network will update their NAV (Network Allocation Vector) timers and cease

transmissions. The proposed solution protects not only the RTS and CTS frames, but also all control frames, including Block Ack.

3. Related work

Much research has already been conducted on 802.11 system security [15]. [16]. The majority of this work has focused on flaws in the wired equivalency protocol (WEP), which was proposed to provide information security between 802.11 customers and access points.

The IEEE 802.11 standard proposed WEP (Wired Equivalent Privacy), which uses the RC4 algorithm and a pre-shared key to protect data messages [17], [18]. The majority of this work has concentrated on flaws in the wired equivalency protocol (WEP), which is designed to provide data privacy between 802.11 clients and access points. Because the RC4 algorithm has been found to have flaws and weak keys. Wi-Fi Protected Access (WPA) is a strong interoperable Wi-Fi security specification developed by the Wi-Fi Alliance in collaboration with the IEEE. WPA is a scheme for protecting data messages by generating per-packet keys. Although no security solution can guarantee "bullet-proof" security, WPA represents a significant advancement in Wi-Fi security. It introduces the IEEE 802.11i standard. WPA not only provides strong data encryption to compensate for WEP's shortcomings, but it also provides user authentication, which WEP lacked [19], [20]. The IEEE 802.11w standard is proposed to provide security protection for all management frames [21].

4. System model

In the first step, we propose a key generation and distribution protocol based on the IAPPFC. We generate a message authentication code (MAC) for control frames using this key. To counteract replay attacks, we present a method for generating a unique sequence number. It validates the current received CTS using previously transmitted RTS. It also checks whether data is sent immediately following the received CTS, and if no data message is sent after the CTS frame, the NAV update is not validated. The network model's architecture consists of several access points (AP) and stations (STA1, STA2, Rogue Station) present in the same channel. All network stations and access points must be IEEE 802.11i and IEEE 802.11w compliant.

We propose solutions for attacks perpetrated by outsiders. The attacker's goal is to consume the entire channel, preventing other STAs and APs from communicating by occupying the entire bandwidth. In general, rogue stations can launch various types of attacks on the network. The following sections explain possible rogue station attacks and their consequences. This section describes the various types of attacks and their consequences.

A replay attack occurs when an attacker replays an authentication session in order to trick a computer into granting access.

RTS replay attack: If STA1 needs to send data to AP, it can send an RTS frame with duration set to the time required to send the data frame after DIFS (Distributed Inter-Frame Space - Minimum time a station/AP needs to wait before sending a frame using Distributed co-ordination function). When the AP determines that the request is from a legitimate station, it will send the CTS response within SIFS (Short Inter-Frame Space - the maximum time within which the response frame must be sent) with the duration field set to the requested duration. STA1 then sends the data frame to AP and waits for the acknowledgement.

The rogue station can listen to the channel, acquire the RTS frame sent by STA1, and later retransmit it to the AP. When the AP sends CTS to STA1, it will be rejected because the actual owner of this replayed RTS was not STA1 but its rogue station. When STA2 detects the CTS frame, it will update its NAV timer. If the attacker is a skilled attacker, he can change the duration field of the RTS frame to a very large value, causing STA2 to wait for a long time before transmitting while STA1 continues to produce packets because the NAV timer has not been updated.

CTS replay attack: In this case, the rogue station (attacker) can listen to the channel, obtain the CTS frame sent by an AP in response to any RTS sent by STA1, and replay the same frame. STA1 rejects the CTS frame and does not update its NAV b timer, as in the previous case. STA2 receives the CTS

frame and updates the bits NAV timer with the duration field from the CTS frame. As a result, STA2 will halt transmissions until the NAV timer expires.

Injecting Spoofed CTS Frames: In this type of attack, the rogue station can create and transmit spoofed CTS frames. This type of attack is more powerful than the others because every station (for example, STA1 and STA2) and AP in the network will update their NAV timer. All stations and APs in the channel within listening range will stop transmitting as indicated by the CTS frame. An attacker can use this method to prevent others from transmitting data by sending the CTS frame for a set period of time.

5. Control frame protection

To secure control frames in a wireless system, we begin with a key generation and distribution technique based on the IAPPFC method. As a result, a message authentication code (MAC) is generated using this key. This is insufficient to counter the replay attacks mentioned in the preceding section. In order to counteract this, we devised a sequence numbering scheme that ensures that the MAC created is unique. The message authentication code can be linked to a variety of control frames, including new frames such as Block ACK Request and Block ACK. We describe how key distribution and generation are accomplished before proceeding with the expansions to the current control frames.

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
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-512
19. If (Ma=true), then
20. message authenticated code is appended to control frames
21. Sequence number 'S' is appended to 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, the key is generated before initiating the key process. This process occurs when no active APs are found in the same channel. The generated K is distributed to all stations that are connected to the AP.

When other APs are active in the same channel, the generated Key would request the APs. IAPPFC is used to send the key request to another AP. If there are multiple active APs in the same channel, it chooses one. Following the completion of the key request, a key transfer occurs in which the AP sends the key request to another AP via an authenticated channel. Key update initiate allows an AP to send this request to other APs in the channel, and the new key K is sent to all APs.

When the key update response is finished, the key update is sent to all stations. After the key response is completed, the Key updating process is confirmed as successful or unsuccessful. If all APs successfully update their keys, the initiator who started the key update initiate will send a key update response to all APs. Instead of the Hash-based message authentication code algorithm, we use the SHA-512 algorithm in control frames.

The message authentication code field is added to the existing control frame fields, resulting in protected control frame fields. The existing frame check sequence in 802.11 RTS and CTS is removed, and the Sequence number is added in its place. When a station connects to an AP, it is assigned a sequence number, the station must update the sequence number S_n in every microsecond. The sequence number in this case is 32 bits. The control packets sent by stations or access points can be listened to by all stations, or the station's CTS frame is rejected. The attacker has enough time who can launch a replay attack. The duration value of the CTS frame is used to calculate S_n; if there are hidden nodes, the best value of S_n is the smallest size data packet. Thus, the best sequence can be determined as:

$$S_n = S_{itf} + Tt_{dp} + S_{itf} + Pp_{cts} + T_{ack}, \quad (1)$$

where Tt_{dp} is time required to send a data packet over the air, S_{itf} is the short time frame space, Pp_{cts} is the packet preamble time for CTS, and T_{ack} is the time spent on the air transmitting the Acknowledgement frame for the previous data packet.

5.1. Key Generation and Distribution

Initially, the AP scans the entire channel for a specific scan interval to detect other active APs in the same channel. If no different APs are found in the same channel during this interval, the Key primitive is started.

If the same channel result is effective (meaning that different APs are found in the same channel), the AP sends a Key request to a different access point using IAPPFC. If more than one AP is available in the channel, the AP can choose to request a key from any AP in the scan list.

This primitive is used whenever an AP receives a Key Request. The request is validated based on the verification provided by the previous AP, and the key is transferred to the next AP via a secure communication channel.

Any AP in the channel can initiate this request and send an update request to the other APs in the channel. The new key K will be created and sent with the request. When the Key update initiate request is accepted, the APs in the channel send the way to the stations via the wireless medium. When the initiator who started the key update initiate request receives a Key update response from each of the APs, the initiator will send a Key update successful message to all of the APs. In exchange, the APs send to all stations the time stamp information at which the new key K should replace K.

5.2. New Control Frames Format

The HMAC algorithm is used to generate the message authentication code over the SHA-512 cryptographic hash function. The SHA-512 cryptographic hash function is used because many station adapters already have this cryptographic hash function in their software or hardware layers. Because using an existing algorithm reduces the overall cost of updating the system, SHA-512 is preferred, despite the fact that extensions for SHA-512 have been proposed. The message authentication code is appended to the control frames, and the receiver uses it to validate the message's authenticity. A 512-bit message authentication code is generated by the SHA-512 cryptographic hash function. The sequence number S is appended to the message to prevent replay attacks, as shown in Fig 2. To prevent

replay attacks, a 4-byte sequence number is chosen, and the key must be updated. (Considering that the Sequence number is updated every 178us, as shown in the following section) Because MAC can be used in place of FCS, the frame check sequence (FCS) that is part of the initial 802.11 RTS and CTS frame is removed to reduce overhead.

When a station connects to an access point, it receives the initial network sequence number. The station must then update the sequence number every microsecond. The sequence number S is a 32-bit sequence number that will wrap when it reaches (232 -1). Rather than using packet counts, the sequence number is updated based on time intervals. Because synchronization in the wireless medium is not very accurate, the time interval by which the sequence number is updated should not be too short. At the same time, the time interval should not be too long because the attacker can use the replay mode to attack.

We calculated S_n by assuming that the station is transmitting a very short data packet immediately after transmitting the CTS. In this case, the N should be equal to the duration value in the CTS frame to avoid replay.

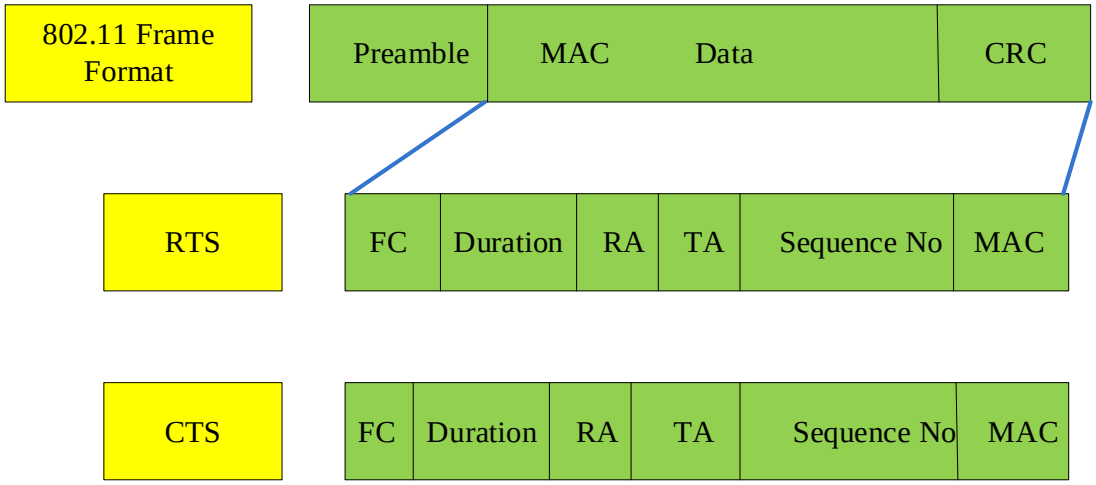

Figure 2: RTS & CTS Frame format, *where*: FC- frame control; RA- receiver Address; TA- sender Address; MAC- Message Authentication Code.

Thus, the best way to calculate duration is to consider the size of the smallest data packet and use that as a reference. A novel approach is proposed to counter replay and fake CTS frame injection DoS attacks caused by unsecured 802.11 control frames. The IAPPFC for key distribution and key management is used to generate a unique message authentication code, which is then used to improve the current 802.11control frame protection. Most current wireless station adapters support SHA-512, the cryptographic hash function used in this proposed model to generate MAC for control frames, making this approach very cost-effective.

5.3. New Control Frames Format Protection

The new frame format is protected during the handover to avoid potential threat of DoS attack. The algorithm-2 shows the Non-malleable encryption process to protect the frame format. In step-1, initialization of variables is described. In steps 2-3, input and output are shown respectively. In step 4, User and Server are specified to send the message and accept the message respectively. At step 5-6, the sender's account and 2 different keys are created (the first for encryption using the Caesar method, the second using POT1) and stored in the database. At step 7, the sender writes a message to the recipient in clear text. Step 8 shows that the Caesar and Rot1 method is already implemented on the server. In step 9, one encryption process is shown using the Caesar method and the first key, and finally, ROT1 and the second key are additionally applied to the Caesar method in step 10. In the last step, the message is transmitted to the server.

Algorithm 2: Dual encryption using Non-malleable cryptographic process

1. Initialization: {S: Server; U: User; M: Message; I_u: Sender's ID ; E_s: Single encryption; T_p : Plain text; E_d: Dual encryption; C_a : Caesar; R_1: ROT1; D : Database; K_1: Key for Caesar method; K_2: Key for ROT1 method }
2. Input: $\{T_p\}$
3. Output:$\{ E_d\}$
4. Set U & S
5. Create I_u & K_1 & K_2
6. I_u & K → D
7. Set $M = T_p$
8. Set C_a & R_1
9. Apply $E_s = C_a \,\&\, K_1 \rightarrow T_p$
10. Apply $E_d = R_1 \,\&\, K_2 \rightarrow E_s$
11. Do $U \rightarrow E_d \rightarrow S$

The algorithm-3 shows the Non-malleable decryption process. In step-1, initialization of variables is presented. In steps 2-3, input and output are shown respectively. In step 4-6, Receiver creates an account and the data is stored in a database. At stage 7, the program searches in the database keys attached to the sender's ID. At stage 8, the program receives the message in dual encrypted form. Step 9 show that the message with double encryption is decrypted using the ROT1 method and the second key. The resulting text is then decrypted using the Caesar method and the first key in step 10. As a result, the recipient has the clear text in step 11.

Algorithm 3: Dual decryption using Non-malleable cryptographic process

1. Initialization: {S: Server; R : Receiver ; M: Message; D_s: Single decryption; T_p : Plain text; D_d: Dual decryption; C_a : Caesar; R_1: ROT1; D : Database; I_u: Sender's ID; I_r: Receiver's ID; E_d: Dual encryption; K_1: Key for Caesar method; K_2: Key for ROT1 method }
2. Input: $\{E_d\}$
3. Output:$\{ M\}$
4. Set U & S
5. Create I_r
6. I_r → D
7. $Get\ D \rightarrow I_u \,\&\, K_1 \,\&\, K_2$
8. S → E_d
9. Apply $D_s = E_d \rightarrow R_1 \,\&\, K_2$
10. Apply $T_p = D_s \rightarrow C_a \,\&\, K_1$
11. Set M = T_p

As depicted in Figure 3. It shows the process of encryption of the message. User types the message, which is now considered as a plaintext, and presses the "send" button. The plain text automatically goes to the server, where all the information about user and message is saved. Message then is encrypted in the system program, firstly, with the Caesar encryption method. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. The received single encrypted text is now encrypted for the second time with the ROT1 encryption method. The code ROT for Rotation (which most common variant is Caesar Cipher) is the easiest shift-based encryption cipher. In order to prevent the MiM attack we get twice encrypted message, which is very difficult for attacker to decrypt. We get two absolutely different texts from the first and the second encryption processes. It means that having even the first key or the single encrypted text it is actually impossible to define the final version of dual encryption process.

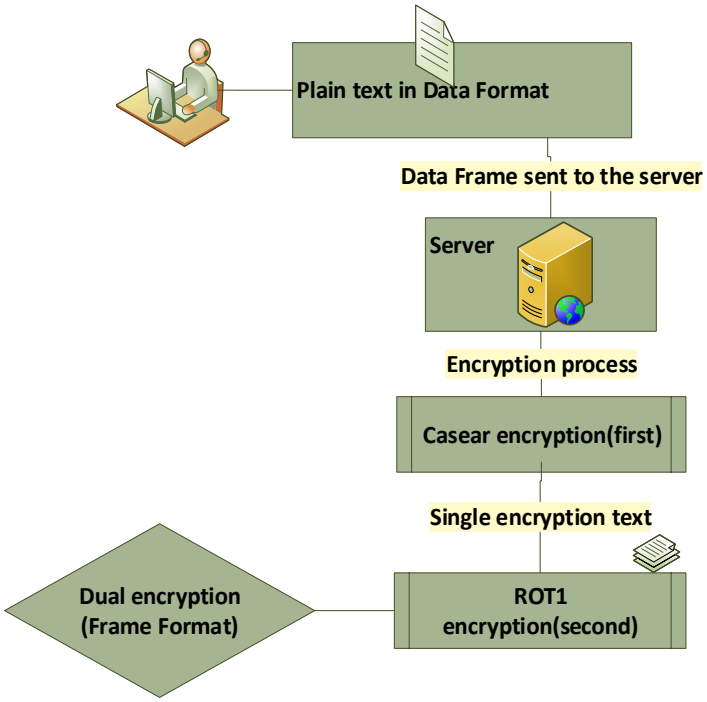

Figure 3: Process of data frame format encryption

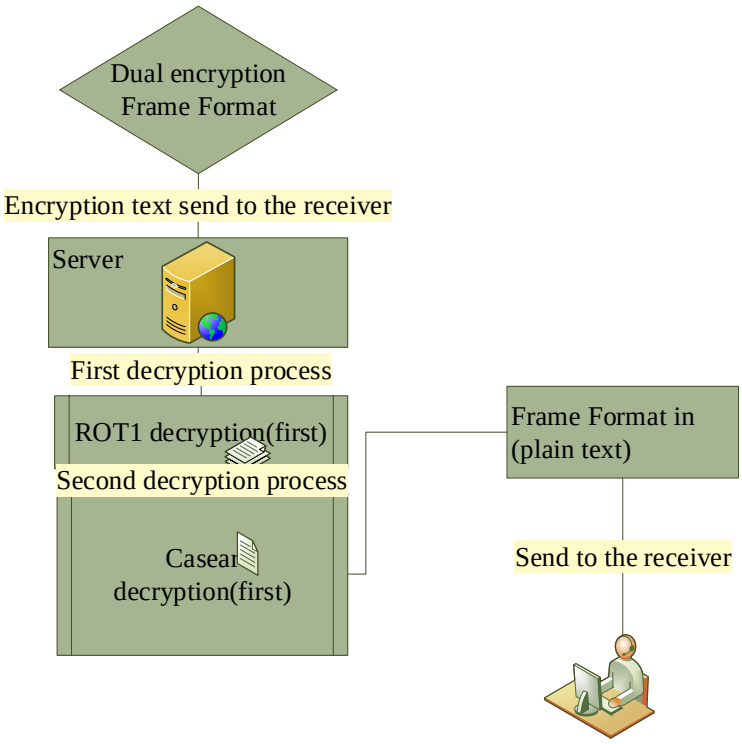

Figure 4: Process of data frame format decryption

As proposed system is depicted in Figure 4. It shows the process of decryption of the dual encrypted message. This message is taken from the server, where it is saved automatically after every encryption process. The first decryption process begins in the system program. Vice a versa now it begins to decrypt firstly with the ROT1 cryptographic method. It is the first decryption process. The second decryption process contains the decryption of the received from the first process text with the Caesar

cryptographic method. The obtained plain text goes to receiver as a common readable but highly secured message.

6. Experimental results

We used NS3 on the Ubuntu 14.04 operating system to simulate the scenario of a new control frame protection environment. The simulation's primary goal is to generate a unique message authenticated code (MAC) using the IAPPFC framework's key. The simulation scenario has 100 nodes. IAPPFC is used in handoff and by an attacker to trick the bandwidth. The nodes are distributed uniformly and at random across a 600 * 600 square meter area. The simulation lasts 100 seconds. The results show an average of two simulation runs. In our experiment, the Handoff mechanism is activated, and hundred nodes are created, eight of which are dedicated to access points and the remaining to mobile nodes. The total simulation time is 100 seconds, and the mobile nodes shift or move from one access point to another during the specified times. While data is being transmitted to the receiving mobile nodes, the mobile nodes move from one AP to another. Because mobile nodes should not lose signal or messages while data is being transmitted, IAPPFC, which provides the handoff mechanism, provides undisturbed signal strength to user mobile nodes even when transferring from one AP to another AP. Now, the attacker node steals the data by not allowing it to reach the required user mobile nodes. We generate the attack here by randomly generating traffic using control frame messages (RTS & CTS) of sender and receiver nodes. The random generation is accomplished through the use of a random app procedure, which randomly assigns traffic to different nodes for each simulation runs. The complete simulation parameters are explained in Table 2.

Table 1
Simulation parameters

Parameters	Description
Number of Nodes	100
Queue length	50 packets
Type of Network	Wireless
Sensing range of nodes	30 meters
Data rate	55Mbps
RTS Threshold	1000 bytes
Packet size	1500 bytes
Simulation time	100 sec
Size of Network	600*600 square meters

6.1. Handover Accuracy

In Figure 5, the accuracy has been detected during the handover process. When mobile phones initiate the handover, then data frame format cannot highly be affected due to DoS attacks. Thus, the accuracy remains higher which is observed at 99.94% during 18 handover processes. It is proved that the proposed IAPPFC cannot be affected due to handover processes.

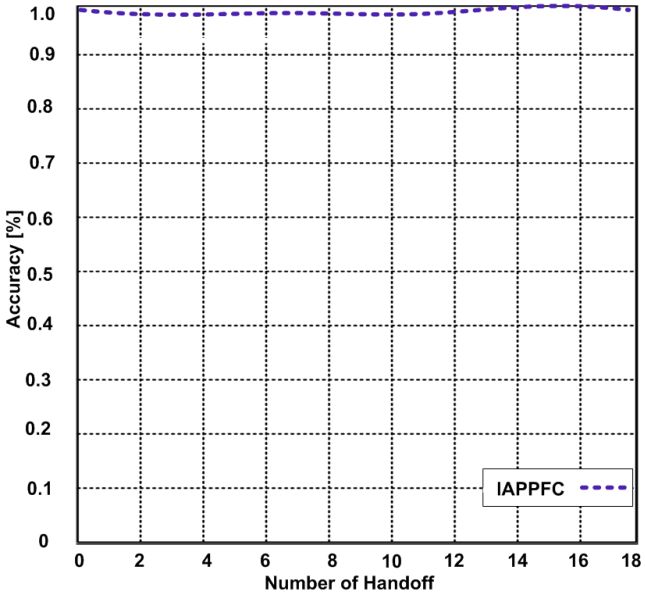

Figure 5: Accuracy with maximum 18 handovers

6.2. Malicious Node Detection

The malicious node detection process is depicted in Figure 6. In this experiment, 27 malicious nodes participated, then the proposed IAPPFC takes just 0.84 seconds to detect all malicious nodes. This malicious detection node time is much shorter.

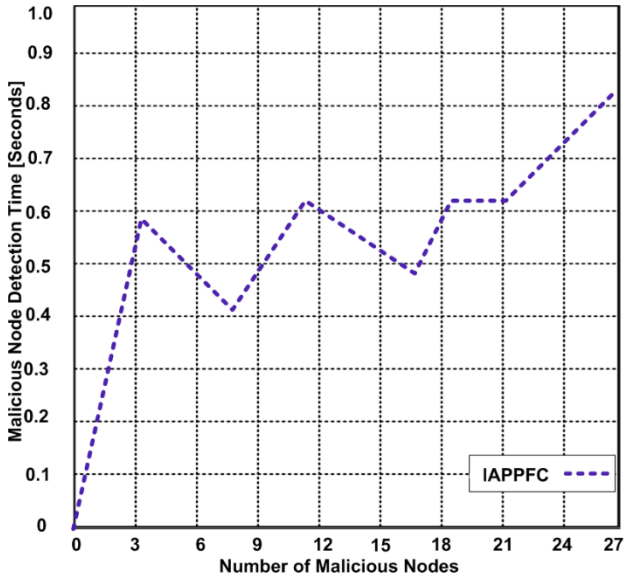

Figure 6: Malicious node detection time with various number of nodes

6.3. Control Frame with IAPP and without IAPP protection

A maximum of 4500 control frames have been generated to determine the malicious attempts shown in Figure 7. In this experiment, the IAPP protocol is tested with our proposed frame format and without frame format. Based on the results, it is confirmed that malicious node probability is obtained higher which is almost 99.92%, whereas the malicious node probability is lower when the number of control frames increases which is found at 72.5%. Thus, it is confirmed that the proposed approach IAPPFC has a much better malicious node detection probability.

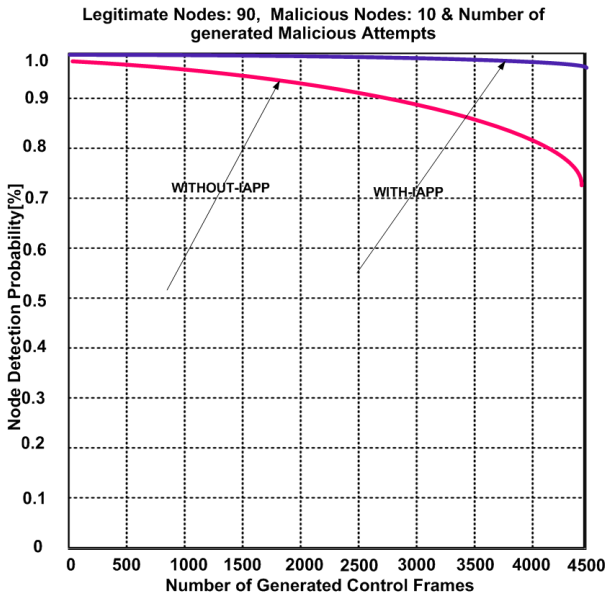

Figure 7: Node detection probability with maximum 4500 control frames

7. Conclusion

The Inter access point protocol is introduced to combat DoS attacks involving reply and fake CTS frame injection. The sequence number and message authentication code have been appended in the standard control frame format, the proposed method modifies the standard control frame format. The key generated by the IAPPFC method is used to generate the message authentication code. SHA-512 is used to generate message authentication code for control frames, which is then supported by the majority of wireless adapters and is relatively inexpensive. To move nodes (users) from one access point to another, the IAPPFC employs a handoff mechanism. As a result, the attacker's trick is limited when wasting or misleading bandwidth by replaying or repeating the same RTS or CTS frames. In the future, we will try to investigate various Quality of Service parameters to see how they are affected by DoS attacks.

8. References

[1] Sh. K. Memon, K. Nisar, M. H. A. Hijazi, B. S. Chowdhry, A. H. Sodhro, S. Pirbhulal, and J. P. C. Rodrigues, A survey on 802.11 MAC industrial standards, architecture, security & supporting emergency traffic: Future directions, Journal of Industrial Information Integration 24 (2021) 100225.

[2] R. R. Chowdhury, S. Aneja, N. Aneja, and P. Emeroylariffion Abas, Packet-level and IEEE 802.11 MAC frame-level network traffic traces data of the D-Link IoT devices, Data in Brief 37 (2021) 107208.

[3] N. Unk, A. Trivedi, and A. Razaque, Dynamic allocation of slot using MAC protocol, in Proceedings of the 2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT, IEEE, 2016, pp. 1-5.

[4] J. Zhang, W. Qing-Guo, M. Tshilidzi, and S. Jitao, Neural network-based control for RRP-based networked systems under DoS attacks with power interval, Automatica 145 (2022) 110555.

[5] J. Shao, Z. Ye, D. Zhang, H. Yan, and J. Zhu, Injection attack estimation of networked control systems subject to hidden DoS attack, ISA transactions (2022).

[6] M. Almiani, A. AbuGhazleh, Y. Jararweh, and A. Razaque, DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network, International Journal of Machine Learning and Cybernetics 12.11 (2021) 3337-3349.

[7] K. Kavitha, T. Babitha, V. Praveena, and P. Devika, Identifying legitimate user in DDoS attack using Petri net, Materials Today: Proceedings (2022).

[8] Ch. Yu. Park, Developing an asynchronous NoAck-based full-duplex MAC for IEEE 802.11 networks in a systems approach, Computer Communications 174 (2021) 172-189.
[9] E. Chatzoglou, G. Kambourakis, and C. Kolias, How is your Wi-Fi connection today? DoS attacks on WPA3-SAE, Journal of Information Security and Applications 64 (2022) 103058.
[10] M. Thankappan, H. Rifà-Pous, and C. Garrigues, Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review, arXiv preprint arXiv:2203.00579 (2022).
[11] A. Razaque, F. Amsaad, M. J. Khan, S. Hariri, Sh. Chen, Ch. Siting, and X. Ji, Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain, IEEE Access, 7 (2019) 168774-168797.
[12] R. R. Chowdhury, S. Aneja, N. Aneja, and P. E. Abas, Packet-level and IEEE 802.11 MAC frame-level network traffic traces data of the D-Link IoT devices, Data in Brief 37 (2021) 107208.
[13] G. Kumar, Ankit, and T. G. Venkatesh, Design and analysis of IEEE 802.11 based Full Duplex WLAN MAC protocol, Computer Networks 210 (2022) 108933.
[14] R. Amin, and Sh. Hossain, An RTS–CTS based medium access control protocol for full-duplex wireless local area networks, Ad Hoc Networks 132 (2022) 102858.
[15] H. Moura, A. R. Alves, J. R. A. Borges, D. F. Macedo, and M. A. M. Vieira, Ethanol: A software-defined wireless networking architecture for IEEE 802.11 networks, Computer Communications 149 (2020) 176-188.
[16] E. Chatzoglou, G. Kambourakis, and C. Kolias, Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset, IEEE Access 9 (2021) 34188-34205.
[17] A. Amoordon, V. Deniau, A. Fleury, and C. Gransart, A single supervised learning model to detect fake access points, frequency sweeping jamming and deauthentication attacks in IEEE 802.11 networks, Machine Learning with Applications 10 (2022) 100389.
[18] L. Davoli, L. Belli, A. Cilfone, and G. Ferrari, From micro to macro IoT: Challenges and solutions in the integration of IEEE 802.15. 4/802.11 and sub-GHz technologies, IEEE Internet of Things Journal 5.2 (2017) 784-793.
[19] T. Guo, Yu. Zh. Feng, and Yu. H. Fu, A new form of initialization vectors in the FMS attack of RC4 in WEP, Procedia Computer Science 183 (2021) 456-461.
[20] B. I. Reddy, and V. Srikanth, Review on wireless security protocols (WEP, WPA, WPA2 & WPA3), International Journal of Scientific Research in Computer Science, Engineering and Information Technology (2019): 28-35.
[21] A. Razaque, V. Alexandrov, M. Almiani, B. Alotaibi, M. Alotaibi, and A. Al-Dmour, Comparative Analysis of Digital Signature and Elliptic Curve Digital Signature Algorithms for the Validation of QR Code Vulnerabilities, in: Proceedings of the 2021 Eighth International Conference on Software Defined Systems, SDS, IEEE, 2021, pp. 1-7.