Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Protection of Control Frames in Wireless Network

Praveen Naik* **, Manujakshi B C**
Computer Science Engg,AcIT,
India

Ambika Naik
IndustrialElectronics Engg,VDRIT,I
India

Abstract— Abstract— In the present communication scenario of 802.11 wireless local access network there is virtually no way to control frames and due to this a range of network allocation vector based denial of service attacks are possible. The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management.A novel approach for protecting control frames by generating a unique message authentication code using inter access point protocol for key distribution and key management is proposed.

Keywords— CTS, RTS, MAC, IAPP, WEP

I INTRODUCTION

The most common way to access internet now-a-days is by using wireless communication link. IEEE 802.11 Wireless Local Area Networks (WLAN) is most popular wireless technology all over the world because of low cost, easy deployment, simplicity and robustness against failures due to the distributed approach of its medium access control (MAC) protocol. In recent years, the popularity of real-time and multimedia applications is growing rapidly. A typical wireless network has an access point (which acts as a base station) and stations communicating using IEEE (Institute of Electrical and Electronics Engineers) 802.11 defined protocols [1]. IEEE 802.11 MAC layer (Medium Access Control) classifies communication in to three types of messages - Management, Data and Control messages. Currently IEEE is in the process of standardizing IEEE 802.11w standard (an extension to the current set of 802.11 standards)[6] to secure the management frames. For protecting data messages Wi-Fi Alliance [2] defined a set of standards called WPA (Wi-Fi Protected Access) [3]and WPA2[4] and later IEEE proposed 802.11i standard. Control frames which are commonly used for bandwidth reservation and acknowledgement purpose cannot be secured by the above mentioned standards making the network susceptible to attacks using these frames. The purpose of this paper is to protect the control work which is to protect the control frame in an infrastructure network. Due to this, ranges of network allocation vector based denial of service attacks are possible.

An attacker can use the control frames to make the medium unavailable by reserving the bandwidth using RTS-CTS (Request to Send – Clear to Send) or CTS to- self mechanism even if he is not part of the network. The attacker can replay the captured RTS frame or CTS frame or he can inject a fake CTS frames in to the network. Due to this all the stations present in the network will update their NAV (Network Allocation vector) timers and defer their transmissions. The proposed solution does not only protect the RTS and CTS frames but all the control frames including "Block Acknowledgment" introduced in IEEE 802.11e standard. This paper proposes a solution for protecting the control frames in an infrastructure network. As first step we propose the key generation and key distribution protocol using IAPP framework. Using this key we generate a message authentication code(MAC) for control frames. To countering replay attacks, we present a mechanism to generate sequence number which ensure that the MAC generated is unique.

In Section II we describe the related work done in this area. In Section III we describe the system model, and in Section IV we describe in detail the proposed model. In Section V we present evolution results, and in Section VI, we provide conclusion.

II RELATED WORK

A great deal of research has already been focused on 802.11 network security. IEEE 802.11 standard proposed WEP (Wired Equivalent Privacy) which uses RC4 algorithm to protect the data messages by using a pre-shared key. Most of this work has focused on weaknesses in the wired equivalency protocol (WEP) intended to provide data privacy between 802.11 clients and access points. As the RC4 algorithm has been identified to have vulnerabilities and weak keys. The Wi-Fi Alliance, working in conjunction with the IEEE, has brought a strong interoperable Wi-Fi security specification to market in the form of Wi-Fi Protected Access (WPA). Wi-Fi proposed a scheme named WPA (later WPA2) to protect the data messages by generating per-packet keys. Although no security solution can claim to be "bullet-proof," WPA represents a quantum leap forward in Wi-Fi security. WPA is built on standards-based interoperable security enhancements. It brings forward features of the forthcoming IEEE 802.11i standard that can be implemented immediately. WPA not only provides strong data encryption to correct WEP's weaknesses, it adds user authentication which was largely missing in WEP IEEE 802.11w standard proposed to provide security protection for all management frames. IEEE 802.11f [7] proposed a method to exchange secured data between access points. All of the above mentioned standards failed to protect control frames. A solution to protect against the denial of service (DoS) attacks caused by using RTS-CTS mechanism was proposed by John Bellardo and Stefan Savage [5] which uses prior transmitted RTS to validate the current received CTS. It also verifies whether data is being transmitted immediately after the received CTS and if there is no data message transmitted after the CTS frame then NAV update is invalidated. The above mentioned mechanism is insufficient against an intelligent attacker who can send a dummy RTS prior to transmission of CTS frame and dummy data packet after the transmission of CTS frame. Another significant issue is that there has been no solution proposed to protect the network from DoS attacks caused by an attacker using CTS-to-Self.

III. SYSTEM AND MODELS

A. *Network Model*

The architecture of the network model comprises of several access points (AP) and stations (STA1, STA2 ,Rogue Station) present in the same channel. All the stations and access points present in the network must be IEEE 802.11i/WPA/WPA2 and IEEE 802.11w compliant. This type of network ensures data integrity as well as management frame integrity. Fig.1 shows a prime example how WLAN network complements the IT and network solutions already being used by the households, enterprises and public organizations.

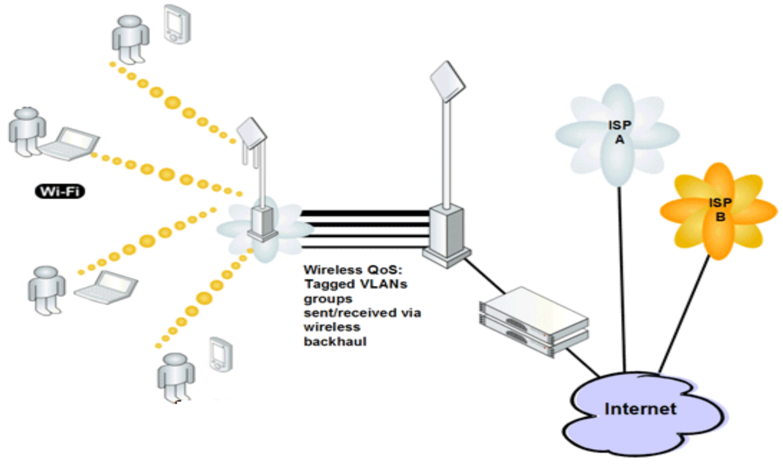

ISP A
ISP B
Wi-Fi
Wireless QoS: Tagged VLANs groups sent/received via wireless backhaul
Internet

Fig 1: Simple Wireless Network

B. *Attack Model*

Generally there are various types of attacks possible on the network by the rogue stations and rouge access points. We are assuming the attacks using rogue access points are not possible in this model, as access points need to authenticate with a trusted entity before they can obtain the keys for control frames. Attacks possible through rogue station and their consequences are explained in the following sections.

i) Attack Sources:

In this paper we are proposing solutions for attacks caused by outsider attackers. The goal of the attacker is to make the entire channel unavailable for the other STAs and APs to communicate by occupying the entire bandwidth. We do notice that an attacker can also be an insider, e.g., stations or APs part of the network. Since our solution is based on shared keys, it is not possible for the proposed solution to prevent insider attackers from forging others' packets. The security mechanism countering insider attackers is scheduled for our future work.

ii) Attack Methods and Consequences:

This sub-section describes the types of attacks possible and their consequences.

RTS replay attack: Suppose STA1 needs to send data to AP, then it can send an RTS frame with duration field set to the time required to transmit the data frame after DIFS (Distributed Inter-frame Space – Minimum time a station or an AP needs to wait before transmitting a frame using Distributed co-ordination function). AP verifying that the request is from a valid station will send the CTS response within SIFS (Short Inter-frame Space – maximum time within
Which the response frame needs to be transmitted) with duration field set to the duration requested. STA1 then sends the data frame to AP and receives the acknowledgement in return (confirming the receipt of the packet by AP). The rogue station can listen to the channel and capture the RTS frame sent by STA1 and retransmit it to the AP at a later time. This scenario is depicted in Fig 2. When the AP sends CTS in response to STA1 it is rejected as the actual sender of this replayed RTS was not STA1 but the rogue station. But STA2 on seeing the CTS frame will update its NAV timer. If the attacker is an intelligent attacker he can modify the duration field of the RTS frame with a very large value (according to the IEEE 802.11 standard [1] the maximum possible value is 32767 microseconds) making STA2 wait for long time to start before transmitting while STA1 can still transmit the packets because it has not updated the NAV timer

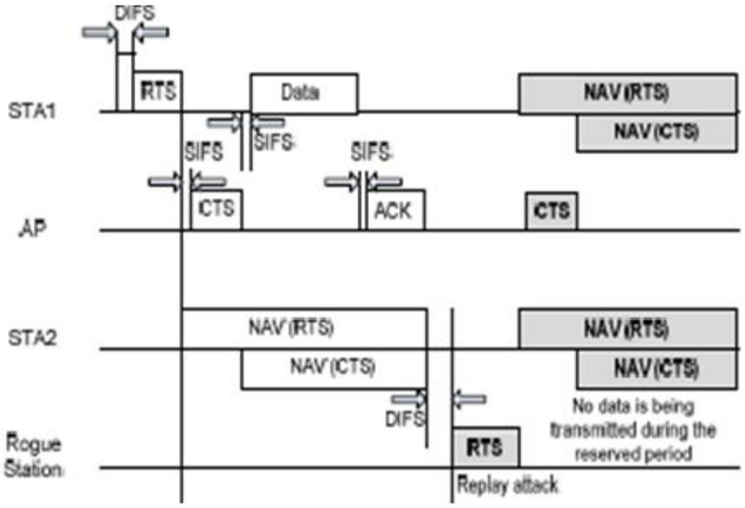


Fig 2:IEEE RTS replay attack

CTS replay attack: In this case the rogue station can listen to the channel and capture the CTS frame sent by an AP in response to any RTS sent by STA1 and replay the same frame. As in the previous case, STA1 rejects the CTS frame and will not update its NAV btimer. STA2 upon receiving the CTS frame updates its NAV timer with the duration field indicated in the CTS frame. Hence STA2 will defer transmissions until the NAV timer expires.

Injecting fake CTS frames: In this type of attack the rogue station can form fake CTS frames and transmit it. This type of attack is more powerful than all the above mentioned attacks as all the stations (STA1 and STA2 in this case) and APs present in the network will update their NAV timer. All the stations and APs present in the channel within hearing range will defer their transmissions as indicated by the CTS frame. An intelligent attacker can use this mechanism to put off others from transmitting data by periodically transmitting the CTS frame.

IV CONTROL FRAME PROTECTION APPROACH

To secure the control frames in a wireless network we start with a method for key generation and distribution using IAPP framework. Subsequently, a message authentication code (MAC) is generated using this key. This does not suffice to counter the replay attacks described in the section above. In order to counter this, we developed a sequence numbering scheme which will ensure that the MAC generated is unique.

The message authentication code can be applied to all types of control frames even for new frames like Block ACK Request, Block ACK defined in IEEE 802.11e and IEEE 802.11n standards. In this section we describe how key generation and

distribution is done and then proceed to explain the extensions to the existing control frames. Lastly, we describe how the sequence number is updated to counter the replay attacks.

A. Key Generation and Distribution

The proposed model uses the IAPP framework for key distribution and key generation. IAPP was introduced in IEEE 802.11f standard to achieve a multivendor access point interoperability with in a distribution system. Initially an AP scans the channel for other APs. If other APs are available then it establishes a TCP (Transmission Control Protocol) communication link to exchange the key and the current sequence number information. If the access point scan results show no APs in the same channel then it will generate a key ‘*K*’ using key generation protocol and initializes the sequence number – ‘*S*’ with a random value. Whenever a new station connects with the AP, the key ‘*K*’ and current sequence number ‘*S*’ maintained by the access point will be transmitted to the stationusing a TCP connection. Using TCP connection ensures that the key is disclosed to the station only after the 802.1x 4-way handshake is successful, which means that key information is given to station after it authenticates with the AP. The key ‘*K*’ also needs to be updated whenever a station disconnects with an AP present in the DS and also at periodic intervals to maintain confidentiality.

i) Generate Key:

Initially the AP scans the entire channel for a certain scan interval to find other active APs present in the same channel. During this interval if no other APs are found in the same channel, then “Generate Key” primitive is initiated.

The “Generate Key” primitive starts key generation process using a trusted entity generally a back-end authentication server and the key ‘*K*’ generated is passed on to the stations connected with the AP, as wells as to other access points that form an infrastructure network in the same channel.

ii) Key request:

If the scan result is successful (which means that other APs are found in the same channel) then the AP sends a “Key request” to the other access point using IAPP. If more than one AP is present in the channel, the AP can choose to request key from any AP present in the scan list.

iii) Key transfer:

This primitive is used whenever an AP gets a “Key Request”. The request is validated based on the authentication provided by the other AP and the key is transferred to the other AP using a secured communication channel, preferably a wired network.

iv) Key update initiate:

Any AP present in the channel can initiate this request and send an update request to all the other APs present in the channel. The new key ‘*K*´’ will be generated and is sent along with the request.

v) Key update response:

On receiving the “Key update initiate” request, the AP’s present in the channel send the key to the stations through the wireless medium. “Key update response” will be sent after updating the keys for all the stations connected to the AP.

Key update successful:

On receiving “Key update response” from all the APs the initiator who initiated the “key update initiate” request will send “Key update successful” message to all the APs. In return the APs send the timestamp information at which the new key ‘*K*´’ should replace ‘*K*’ to all the stations.

B. Control Frames format according to new model

Message authentication code is generated by using the HMAC [9] algorithm over the SHA-1 cryptographic hash function [10]. The reason for using SHA-1 cryptographic hash function is that many station adapters already have this cryptographic hash function in either their software or hardware layers.Using an existing algorithm reduces the overall cost of the updating the system, hence SHA-1 is preferred even though extensions for SHA-1 were proposed. The message authentication code is appended to the control frames using which the receiver validates theauthenticity of the message. SHA-1 cryptographic hash function generates a 160 bit message authentication code. Fig 3 represents process flow diagram.

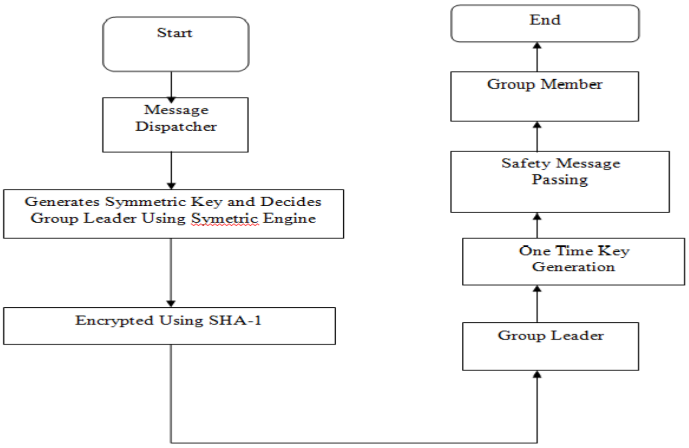


Fig 3: Process flow chart

To prevent replay attacks, the sequence number ‘*S*’ is appended to the message. A 4 byte sequence number is chosen to prevent replay attacks and also the key needs to be updated for every 212 hours of operation. (Considering that Sequence number is updated for every 178us as derived in the next section) The frame check sequence (FCS) which is the part of initial 802.11 RTS and CTS frame is removed to reduce the overhead as MAC can be used in the place of FCS. The extended RTS and CTS formats are depicted in Figure 4.

C. Updating Sequence number ‘S’

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 for every ‘*N*’ micro seconds. The station uses it own internal clock called ‘Real Time Clock’ (RTC) to update the sequence number. The sequence number ‘*S*’ is a 32 bit sequence number and once the sequence number reaches (232 -1) it will wrap. The sequence number is updated based on time interval rather than using packet count. Packet count requires that every control packet transmitted by the station or an access point be heard by all the stations, otherwise there is a chance that the CTS frame sent by a Station is rejected as duplicate or a replay. 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.

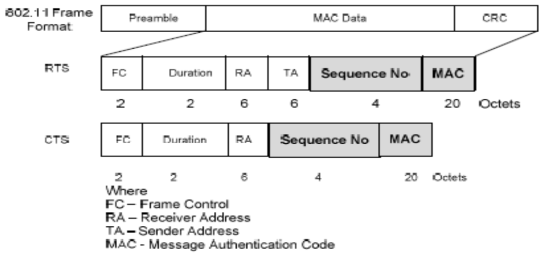


Fig 4: RTS and CTS frame formats according to new model

Estimation of ‘N’

We estimated the value of *N* considering that the station is transmitting a data packet of very small duration immediately after transmitting the CTS. To avoid replay for this case, the N should be equivalent to the duration value in the CTS frame. But there is chance that all the stations may not receive the CTS frame (hidden node problem), so the best way to approximate ‘*N*’ is by considering size of the smallest data packet and use that as reference to calculate duration:

$$N=(SIFS+Data_{dur}+SIFS+AC_{dur}+CTS_{replay\_preamble\_dur})$$

where,

SIFS: Short Inter-frame space.
Datadur: Time required for transmitting the data packet on air.
Ackdur: Time required for transmitting the Acknowledgement frame for the previous data packet on air.
CTS_replay_peamble_dur: CTS Packet preamble duration.

Using the above equation, we estimated the value of ‘*N*’ for all the supporting 802.11g and 802.11b rates. If the maximum speed supported by the network is 54Mbps then the sequence number must be updated for every 150us. Synchronization mechanism provided by the IEEE standard ensures that all the stations have the same RTC clock.

V. PERFORMANCE ASSESSMENT

Our proposed model is intended to counter the RTS or CTS replay attack as well as injecting fake CTS DoS attacks caused b y not securing the control channel. In this section, we present the simulation results showing that our proposed model counters the above three types of DoS attacks. In this section we first describe our security assessment and then proceed to protocol performance evaluation.

A. Security Evaluation

We have used NS2 (Network simulator 2) to mode l the network and the attacks. The rogue station is capable of replaying RTS and CTS frames and the injecting CTS-to-self frames in the network. The AP,STA1 and STA2 are modeled according to theproposed solution. All types of traffic TCP, UDP can be created between the stations and the AP. For each of the below mentioned attacks we evaluated the percentage of attacks that were successful.

B. RTS replay attack

This scenario is created by setting the RTS threshold of all the stations STA1, STA2 and AP in the network to a very less value and a TCP connection was setup between a station and an AP. The rogue station is programmed to capture the RTS frame sent by STA1 and retransmit the same after the previous
Exchange is complete. We have seen that the all the retransmitted RTS frames are being discarded by other stations and access points as sequence number present in the replayed RTS frame is no longer valid.

C. CTS replay attack

In this case after the rogue station retransmits a previously captured CTS frame, all the others STA’s and AP’s discarded the CTS frame as the sequence number indicates that the frame transmitted is a duplicate frame.

D. CTS attack

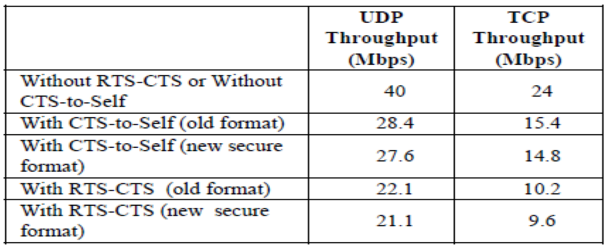
After observing the previous data transfers, the rogue station tries to approximate the sequence number and uses this to transmit the control frames with a previously captured MAC. At the receiving end, all the STA’s and AP’s discarded the CTS frames as the MAC of these frames is invalid. In all the above mentioned attacks, the percentage of attacks that were successful is 0%.

E. Protocol Performance Evaluation

The main computation overhead involved in this mechanism is in generating the Message Authentication code using SHA-1 algorithm. But the time required for generating this MAC depends upon the type of implementation - hardware / software and the speed of the processor etc. But according to our\ evaluation results the computation overhead involved in this process is almost negligible.

F. Communication Overhead due to changes in the control frame format

The changes to the control frame formats may result in reduce network throughput. We evaluated the throughput of an UDP stream with packet size 1500bytes at Data rate 54Mbps using CTS-to-Self mechanism and RTS-CTS mechanism (RTS Threshold – 1000 bytes) and we have observed that the throughput loss due to the changes in the control frame format is very less. The results are tabulated in Table 1. We also calculated the throughput of an FTP application at 54Mbps and we observed that on an average throughput loss of 0.6Mbps was observed for UDP applications.



	UDP Throughput (Mbps)	TCP Throughput (Mbps)
Without RTS-CTS or Without CTS-to-Self	40	24
With CTS-to-Self (old format)	28.4	15.4
With CTS-to-Self (new secure format)	27.6	14.8
With RTS-CTS (old format)	22.1	10.2
With RTS-CTS (new secure format)	21.1	9.6

Table 1: Throught Comparison Results (using old and new CTS frame formats)

G. Communication overhead due to key management and key distribution.

The communication overhead in this case depends upon the number of access points and stations present in the channel and the rate at which connections and disconnections happen in the network. Each connection and disconnection results in a key update.

The overhead in this case is evaluated based on the number of stations present in the channel.

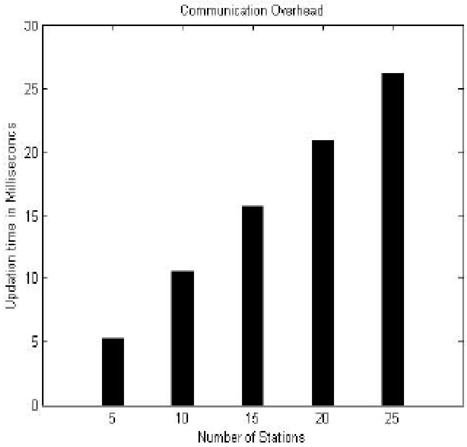


Fig 4: Communication overhead due to key management and key distribution

We can see from Fig. 4 that as the number of stations, present in the channel increase, the communication overhead becomes significant. Communication overhead among APs is not taken in to consideration, as wired communication can be used instead of wireless medium while doing key management and key distribution.

VI. CONCLUSION

A novel approach to counter the replay and fake CTS frame injection DoS attacks caused by not securing the 802.11 control frames is proposed. The solution to improve the current 802.11 control frame protection by generating a unique message authentication code using IAPP framework for key distribution and key management is proposed. SHA-1, the cryptographic hash function which is used in this proposed model to generate MAC for the control frames is supported by most of the current wireless station adapters which in turn makes this approach very cost effective. As a part of future work we would like to modify the current proposed scheme to counter the insider attacks as opposed to this model, where we were trying to make use of the current existing hardware for cost effectiveness.

REFERENCES

[1] IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007

[2] Wi-Fi Alliance: An Overview of the Wi-Fi Alliance Approach to Certification, September 2009

[3] WPA: Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, April 29, 2008

[4] WPA2: Wi-Fi Protected Access, Wi-Fi Alliance January,2008

[5] John Bellardo and Stefan Savage. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In Proceedings of USENIX Security Symposium, 2009

[6] Adrian Davis. Authentication across the airwaves. In Information security forum, February 2007

[7] IEEE Standard 802.11f: Multi-vendor access point interoperability via an Inter access point protocol across Distribution systems supporting IEEE 802.11 operation – 2007.

[8] http://www.wifi.org/wp/wifi-alliance-certification/

[9] H.Crawczyk, M.Bellare, R.Canneti. HMAC: Keyed-Hashing for Message Authentication, RFC 2104, February 2007.

[10]. D.Eastlake. US Secure Hash Algorithm 1 (SHA1), RFC 3174,September 2009.