Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 105675, 16 pages
doi:10.1155/2011/105675

Research Article

Design and Implementation of a Lightweight Security Model to Prevent IEEE 802.11 Wireless DoS Attacks

Mina Malekzadeh, Abdul Azim Abdul Ghani, and Shamala Subramaniam

Faculty of Computer Science and Information Technology, Universiti of Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

Correspondence should be addressed to Mina Malekzadeh, minarz@gmail.com

Received 9 August 2010; Revised 29 November 2010; Accepted 20 January 2011

Academic Editor: I. Moerman

The protection offered by IEEE 802.11 security protocols such as WEP, WPA, and WPA2 does not govern wireless control frames. The control frames are transmitted in clear-text form, and there is no way to verify their validity by the recipients. The flaw of control frames can be exploited by attackers to carry out DoS attacks and directly disrupt the availability of the wireless networks. In this work, focusing on resource limitation in the wireless networks, a new lightweight noncryptographic security solution is proposed to prevent wireless DoS attacks. In order to prove the ability of the proposed model and quantify its performance and capabilities, a simulation topology is developed, and extensive experiments are carried out. Based on the acquired results, it is concluded that the model successfully prevents wireless DoS attacks, while the security cost is not remarkable compared to the model achievements.

1. Introduction

Wireless control frames facilitate and complement delivery of data frames. These frames include request-to-send (RTS), clear-to-send (CTS), acknowledgment (ACK), and contention-free control frames which are CF-End and CF-End-ACK [1]. The RTS frame is used to address the hidden node problem in the virtual carrier sensing mechanism. The CTS frame is transmitted as a respond to the RTS frame. The ACK frame is used to acknowledge the successful reception of the data frames. The contention-free control frames are applied to reset the network allocation vector (NAV) and subsequently release the channel [1].

The general structure of RTS, CTS/ACK, and CF-End/CF-End-ACK control frames are presented in Tables 1(a), 1(b), and 1(c), respectively.

As deliberated in the structure of the control frames, these frames consist of duration field which reserves the channel for the duration time required to transmit the data frames. All the wireless stations utilize this duration value to set the NAV. The maximum NAV value is 32767 μs, and the wireless stations are not allowed to transmit until the NAV reaches zero [1].

While the duration field and the NAV mechanism while are used to minimize the collision probability, they present a prime opportunity for the attackers to trigger DoS attacks on the wireless networks. The attacker continuously transmits forgery control frames with large duration to exhaust the memory and processing capacity of the wireless network. Since there is no way for the recipients to verify validity or duplication of the received control frames, these forgery frames are accepted by the target wireless network [2, 3].

The DoS attack quickly consumes all available bandwidth, resulting in the network no longer being able to operate in the way it was designed to. These attacks directly target the network availability and disrupt the normal communication between the wireless stations. The main purpose of the attacker is to cause a complete loss of availability and prevent legitimate use of the resources by the authorized users [4].

The emerging benefits from the available solutions in the literature still pose some notable weak points. Most of these solutions are diverted towards the wireless DoS attacks using some specific type of control frames while ignoring the other pertinent factors. There is no evidently consideration in the solutions to protect contention-free control frames

Table 1

(a) 802.11 RTS control frame

Frame control	Duration	Receiver address	Sender address	FCS
Octets 2	2	6	6	4

(b) 802.11 CTS and ACK control frames

Frame control	Duration	Receiver address	FCS
Octets 2	2	6	4

(c) 802.11 CF-End and CF-End-ACK control frames

Frame control	Duration	Receiver address	BSSID	FCS
Octets 2	2	6	6	4

from being exploited by the attackers. In addition, these solutions are not able to simultaneously ensure low overhead and less computation power while maintaining strong level of security. A mechanism to prevent replay attacks is also further ignored.

On the other hand, utilizing cryptographic-based solutions to protect wireless control frames and prevent DoS attacks are expensive solutions in terms of excessive overhead and resource consumption caused by the encryption and decryption operations. Thus, there is a need to develop a security mechanism to protect all types of control frames while supporting the required aspects such as less overhead, legacy compatibility, replay attack protection, and sufficient level of security.

In this work, we present the ACFNC model as a lightweight noncryptographic security solution by encompassing these required aspects to provide a countermeasure against DoS attacks based on the control frames in wireless networks. In order to implement the ACFNC model and evaluate its performance and effectiveness, we use the OMNeT++ simulator. Different experiments with the explicit purposes are conducted to quantify capabilities of the ACFNC model under different network conditions.

The rest of the paper is organized as follows. Section 2 presents the related works with respect to the wireless DoS attacks. The structure of the proposed ACFNC model is explained in Section 3. Section 4 describes the simulation system. In Section 5, the experimental design to conduct the experiments is described. Results from the implementation of the model and corresponding analysis are presented in Section 6. Finally, in Section 7, we draw our conclusions.

2. Related Works

In order to mitigate DoS attacks on the wireless networks, several schemes have been proposed. These schemes can be categorized into three general groups which are cryptographic-based [2, 5, 6], detection [7, 8], and the NAV validation methods [9–11].

The authors in [2] investigated the control frames vulnerabilities and adopted enhanced hmac-md5 and hmac-sha1 (EHMAC) algorithms. The format of RTS, CTS, and ACK frames was modified by adding extra 80 to 160 bits to include the output of hmac algorithms. They also added a 48 bits transmitter address to the CTS and ACK frames. However, the most important drawback of the model is the lack of ability to prevent the replay attacks which keeps the model vulnerable to DoS attacks. In addition, the overhead of the model is high, while still DoS attacks are possible against wireless network by exploiting contention-free control frames.

To address the DoS attacks, the authors in [5] proposed a packet-by-packet encryption scheme for the RTS and CTS control frames. The formats of the control frames were modified by adding extra 160 bits to attach the encrypted fields. Two new fields as a 32-bit timestamp and a 32-bit sequence number were considered to avoid replay attack. However, implementation of the model demands high computation power for the overall encryption and decryption process. Besides, the model is unable to prevent the attacks via other types of control frames.

In [6], a per-packet authentication scheme was proposed based on a modified pseudorandom function (PRF-16) authentication mechanism using hmac-sha1 with 16 bits output results. They utilized a new CRC-16 algorithm instead of the current CRC-32 algorithm. However, in addition to modification of the CRC-32 algorithm, the very short authentication element length is considered as the other issue of the model. Besides, the model is unable to prevent the replay attacks, and wireless DoS attacks are still possible against the wireless networks.

The prevention of wireless DoS attacks based on the NAV validation methods was initially deliberated by Bellardo and Savage [9]. In the proposed scheme, a limit was set on duration value of the control frames. However, the model does not specify the prevention of contention-free control frames DoS attacks. The NAV validation methods also have been discussed in [10, 11]. Furthermore, the DoS detection schemes have been presented in [7, 8], which limit their scope to detect the attacks but not preventing them.

3. Proposed ACFNC Model

In order to prevent DoS attacks in wireless networks by exploiting the control frames vulnerabilities, we propose a new lightweight authenticator control frame based on

noncryptographic solutions (ACFNC) model. By considering the resource limitation in the wireless networks, the main objectives throughout design of the ACFNC model are providing sufficient level of security and accuracy, avoiding unnecessary overheads, and preserving high efficiency. Furthermore, the model is legacy compatible and can be implemented only with firmware upgrades, and thus eliminating the need for massive replacement of the existing network hardware. The details of the ACFNC structure are as follows.

3.1. Define TS Security Field. The ACFNC model defines a new field as a placeholder to carry out security element. This field is called TS with 4 bytes in size which is appended at the end of wireless control frames before the FCS to provide secure control frames.

3.2. Secure Time Synchronization Function (STSF). In the wireless communication, time synchronization is an important function for time-critical applications, in which the order or simultaneously launching of the events is necessary. To achieve this goal, IEEE 802.11 defines a synchronization function which is called timing synchronization Function (TSF). The TSF utilizes the beacon frames to present the new system clock as a timestamp field [12]. At each beacon interval, which is every 100 ms, the TSF presents the current system clock, while all other stations must set their clock according to this value.

The ACFNC model is rely on synchronization between the access point and the wireless stations. Thus, providing accurate synchronized time is important in the ACFNC model to perform its respective functions. The TSF specified by the 802.11 standard, despite its efficiency in term of communication overheads, has been designed without taking into account security [13]. Consequently, the unprotected beacon frames can be exploited by the attackers to desynchronize the wireless stations through the following synchronization attacks [14, 15].

(i) Manipulation attacks: the beacon frames are not protected [16], thus the attacker can modify their timestamp field to assign incorrect values.

(ii) Spoofing attacks: the attacker can forge new beacon frames with wrong timestamp.

(iii) Replay attacks: the attacker may replay a beacon frame with some delay latter.

All the above attacks on time synchronization have one main goal, which is to mislead the TSF protocol. The attackers perform either of these attacks by sending false beacon frames with wrong clock information to convince the wireless stations to adjust their clock based on the erroneous information. Once this happens, the stations will be out of synchronization with the access point. Losing the synchronization can cause problems on the ACFNC model which relies on the accurate synchronized time. The synchronization attacks may lead to discarding the frames including control frames. Consequently, the wireless stations request the retransmission of the missed frames, resulting in resource exhaustion which affects the bandwidth, latency, and loss rate. Hence, secure time synchronization is prerequisite to limit the attacker's ability and thereby to guarantee the correct operation of the ACFNC model.

Many mechanisms have been proposed to address time synchronization issue in the wireless networks [17–19]. However, most of these mechanisms do not take into account security to address TSF vulnerabilities against the synchronization attacks. The authors in [20] propose a secure time synchronization mechanism called TESLA to authenticate the broadcast beacon frames. However, TESLA is not suitable for limited recourses wireless networks for two main reasons [21]. First, TESLA utilizes the digital signatures which are too expensive to compute in wireless networks. Second, TESLA has an overhead of about 24 bytes per each beacon frame which is large overhead for wireless networks. Thus, TESLA introduces high computation and communication overheads and cannot directly be applied in the resource constrained wireless networks.

In order to detect malicious synchronization attacks using the beacon frames, we use the secure clock synchronization proposed in [22] which is based on μTESLA [21], a simplified version of TESLA. It is a lightweight broadcast authentication mechanism based on efficient one-way hash chains to provide authenticity and integrity for the beacon frames. The mechanism is suitable for infrastructure wireless networks and is included in the access point as the base station [23]. We give a short description of the mechanism, while more details can be found in [13, 21, 23, 24].

The mechanism uses one-way hash chains which are much faster than asymmetric algorithms and can be performed in an on-the-fly way such that it causes almost no additional delay [25]. The secure time synchronization is calculated by the access point and verified by the wireless stations as follows.

(A) Access Point Side. The access point chooses random number k_n and generates a sequence of keys (key chain) by repeatedly applying the one-way hash function H with n bits length so that $k_i = H(k_{i+1})$ for all n, where $n > i \geq 0$. Due to one-way nature of hash functions, given $k_i + 1$, everybody can calculate forward to obtain $k_0, \ldots, k_i$. However, nobody by given $k_0, \ldots, k_i$, can calculate backward to obtain k_{i+1}. The access point divides the time into intervals and associates each key from the key chain with one interval. During the ith interval, the access point calculates the tag over the beacon frame with k_i from the key chain. Then, the beacon frame with its tag is transmitted to the stations. The access point discloses the k_i after a certain period of time. This means that each beacon frame discloses the previous key and that the k_i cannot be used to spoof beacon frames after the ith interval time.

(B) Receiver Side. Upon receiving the beacon frame, the receiver station first authenticates the disclosed key then the beacon frame itself. Thus, the receiver first must verify that the beacon frame has not yet disclosed. If the condition

Table 2: System parameters and related values.

Parameter	Value
Short interframe space (SIFS)	10 μs
Slot time, S_t	20 μs
Basic bitrate, B_r	2 Mbps
Physical bitrate, PHY$_r$	1 Mbps
Physical header, PHY$_h$	192 bits
Propagation delay time, P_t	1 μs

was not meet, the beacon frame is discarded, otherwise, the receiver stores it in the buffer. Now, the receiver station is assured that the key is known only by the access point, and it has not been forged by the attackers. Then, at the time of the key disclosure when the access point reveals the key, the receiver uses the disclosed key to authenticate the beacon frame.

We utilize this mechanism to make a secure TSF (STSF) for the ACFNC model. The SHA1 is used as the one-way hash function to create the key chain, while the length of each key in the key chain is considered 64 bits. Adoption of a 64-bit key extends the time taken to crack to a few thousand years [26].

3.3. Replay-Preventing Mechanism. Based on the STSF, further extensions are done by designing and developing a replay attack protection mechanism in the ACFNC model based on the threshold time windows to validate the freshness of the received control frames. The replay preventing mechanism is accomplished by tagging each outgoing control frame with an identifier which is creation time of that control frame. We formulize five distinct threshold time windows which are related and mapped to the five control frames and represent their maximum acceptable age. In order to determine these five threshold time windows, some IEEE 802.11 standard notations [1, 27] are used which are identified in Table 2.

In the IEEE 802.11 standard, except for the unicast data and management frames that are transmitted in the normal data rates, the other frames including multicast, broadcast, and control frames are transmitted in the basic bitrate [28, 29]. Considering this rule, we define T_{CF} as the required time for the transmission of the entire control frame including its physical header as follow:

$$T_{\text{CF}} = \frac{L_{\text{CF}}}{B_r} + \frac{\text{PHY}_h}{\text{PHY}_r}. \tag{1}$$

In (1), L_{CF} is the length of the secure control frames after adding the TS security field. The T_{CF} is the required time considered for all types of control frames as T_{RTS}, T_{CTS}, T_{ACK}, $T_{\text{CF-End}}$, and $T_{\text{CF-End-ACK}}$ for transmission of the secure RTS, CTS, ACK, CF-End, and CF-End-ACK control frames, respectively. The calculation of these timeout values by the ACFNC model is accomplished as follows.

(A) Amount of T_{CTS} and T_{ACK}. Since the length of the secure CTS and ACK control frames are the same, the required time for their transmission also is the same. In order to calculate the amount of T_{CTS}, and T_{ACK} we have

$$T_{\text{ACK}} = T_{\text{CTS}} = \frac{8 \times 18\,(\text{b})}{2 \times 10^6\,(\text{bps})} + \frac{192\,(\text{b})}{10^6\,(\text{bps})} = 264\ \text{us}. \tag{2}$$

(B) Amount of T_{RTS}, $T_{\text{CF-End}}$, and $T_{\text{CF-End-ACK}}$. Since the length of the secure RTS, CF-End, and CF-End-ACK frames are the same, the required time for their transmission also is the same, and we calculate them as follow:

$$T_{\text{RTS}} = T_{\text{CF-End}} = T_{\text{CF-End-ACK}} = \frac{8 \times 24\,(\text{b})}{2 \times 10^6\,(\text{bps})} + \frac{192\,(\text{b})}{10^6\,(\text{bps})} = 288\ \text{us}. \tag{3}$$

The basic idea of our proposed replay attack protection mechanism is to use distinct threshold time windows for each control frame. Thus, we calculate the maximum amount of the time window at which the control frame is expected to be sensed in the wireless channel. This threshold presents a time window at which a received control frame is valid. Thus, if the control frame is sensed after this threshold timeout, it is regarded as an old frame and is discarded by the receiver. We call the timeout window for the RTS, CTS, ACK, CF-End, and CF-End-ACK frames as TO_{RTS}, TO_{CTS}, TO_{ACK}, $\text{TO}_{\text{CF-End}}$, and $\text{TO}_{\text{CF-End-ACK}}$, respectively.

It is important to note that determining the value of each timeout window must be accomplished carefully with sufficient duration to avoid any unexpected network behavior. Each timeout value must be large enough to avoid any increase in the number of retransmissions and must be small enough to avoid unnecessary delays. Assigning the right value for each timeout has a direct impact on the wireless network performance so that a wrong value can significantly degrade the performance due to retransmissions or collisions.

We formulize and calculate the threshold time windows related to the secure control frames in the ACFNC model as follows:

$$\begin{aligned}
\text{TO}_{\text{ACK}} &= T_{\text{ACK}} + P_t + S_t + \text{SIFS} = 295\ \text{us},\\
\text{TO}_{\text{CTS}} &= T_{\text{CTS}} + P_t + S_t + \text{SIFS} = 295\ \text{us},\\
\text{TO}_{\text{RTS}} &= T_{\text{RTS}} + P_t + S_t + \text{SIFS} = 319\ \text{us},\\
\text{TO}_{\text{CF-End}} &= T_{\text{CF-End}} + P_t + S_t = 309\ \text{us},\\
\text{TO}_{\text{CF-End-ACK}} &= T_{\text{CF-End-ACK}} + P_t + S_t = 309\ \text{us}.
\end{aligned} \tag{4}$$

Then, we define two new attributes, which are the following.

(i) Creation time of the control frames: it represents the time at which the control frame has been created to be placed into the channel for transmission. The creation time is tagged into the TS field.

(ii) Current clock time (CCT): it is the current system time which is assigned by the STSF in the secure

beacon frames and represents arrival time of the control frames.

Creation time of each outgoing control frame is tagged into the TS field, and then the control frame is transmitted to the destination address. Upon receiving the control frame, the recipient must verify if its TS value is fresh. In order to accomplish this verification, the recipient utilizes the following equation:

$$0 \leq \text{CCT} - \text{ received TS} \leq \Delta t, \tag{5}$$

where Δt is corresponding threshold time window.

The two major advantages of the proposed replay attack protection mechanism are as follows.

(i) Wireless networks are limited in terms of their resources such as bandwidth, buffer, computation power, and battery lifetime [30]. In this regard, since the overall process of the protection mechanism is based on a simple subtraction, the entire process of the ACFNC model is very fast which enable the model to be highly efficient for the limited resources wireless networks. The recipient of the control frame only needs to do a simple subtraction to verify the validity of the received control frames using (5).

(ii) By using this mechanism, there is no need to keep track of the control frames or their reception sequence. The model is not memory dependent, which reduces the overall algorithm complexity without demanding extra cache or memory.

The flowchart of the proposed replay attack prevention mechanism is provided in Figure 1 .

3.4. Procedure of the ACFNC Model. The process of DoS attacks prevention by the ACFNC model consists of two main phases which are generation phase and verification phase. The details are as follows.

(A) Generation Phase. This phase is carried out by the sender station to generate value of the TS security field. In this phase, the sender station determines creation time of the outgoing control frame. Then, this value is tagged into the TS field of the control frame and the frame is transmitted to the receiver.

(B) Verification Phase. This phase is carried out by the receiver station to verify the validity of the received control frames. Upon receiving the control frame, if the frame does not have the TS field, it is immediately discarded due to its wrong format. Otherwise, the receiver applies (5) and subtracts the CCT from the value of the TS field in the received control frame. This is to check whether the result is less than or equal to the corresponding timeout value. If the required condition is met, the receiver considers the control frame as a fresh frame. Now, if the frame is ACK, CTS, or RTS frame, it is accepted by the receiver as a valid control frame and the corresponding function is implemented. In contrast, if the frame is CF-End or CF-End-ACK, the receiver must verify duration field of these frames. If the duration field of these frames is not zero, the frame is discarded as an invalid frame due to its wrong format. However, zero duration in the frame results in accepting the frame by the receiver as a valid control frame. The general process of the ACFNC model along with its two corresponding phases is presented in Figure 2.

4. Simulation System Description

Using the OMNeT++ simulator, we develop two simulation environments which are called A and B. The simulation environment A is related to the IEEE 802.11 current model and the simulation environment B is related to the ACFNC model. The topology of the two environments is identical to provide fair conditions to compare the results. The size of the simulation environments is $300 \times 300\,\text{m}^2$ which include two areas as authorized and attacker area. The details are as follows.

4.1. Simulation of the IEEE 802.11 Current Model. The simulation environment A is developed to implement the IEEE 802.11 current model. It consists of two areas as authorized and attacker. The authorized area consists of two wireless stations associated to the access point which follow the IEEE 802.11 standard MAC layer. The attacker area belongs to the attacker station who launches different types of wireless DoS attacks against the authorized wireless network. Figure 3 shows the simulation environment A to implement the IEEE 802.11 current model.

In order to carry out different types of wireless DoS attacks by the attacker, we need to develop a new network interface card (NIC) for the attacker station. Therefore, we created a new wireless host which is named 80211DoS-Host with the 80211DoS-NIC. This new node is considered as the attacker and includes a new MAC layer to conduct the wireless DoS attacks. We have written the new MAC layer in C++ code and have added it to the OMNeT++ as a simple module which is called the 80211DoS-MAC. This new MAC layer is able to generate all types of forgery control frames with large duration value as $32767\,\mu$s to trigger different types of wireless DoS attacks.

4.2. Simulation of the ACFNC Model. In order to implement the ACFNC model, the simulation environment B is developed. It consists of two areas as authorized and attacker. The authorized area consists of two protected wireless stations associated to the protected access point which follow the ACFNC model. The attacker area belongs to the attacker to launch different types of wireless DoS attacks and synchronization attack against the ACFNC model in the protected wireless network. The simulation environment B to implement the ACFNC model is shown in Figure 4.

Implementation of the ACFNC model comprises two phases. The first phase is done in the MAC layer to secure the control frames. The second phase is done in the management sublayer (mgmt) to secure time synchronization using the STSF mechanism as follows.

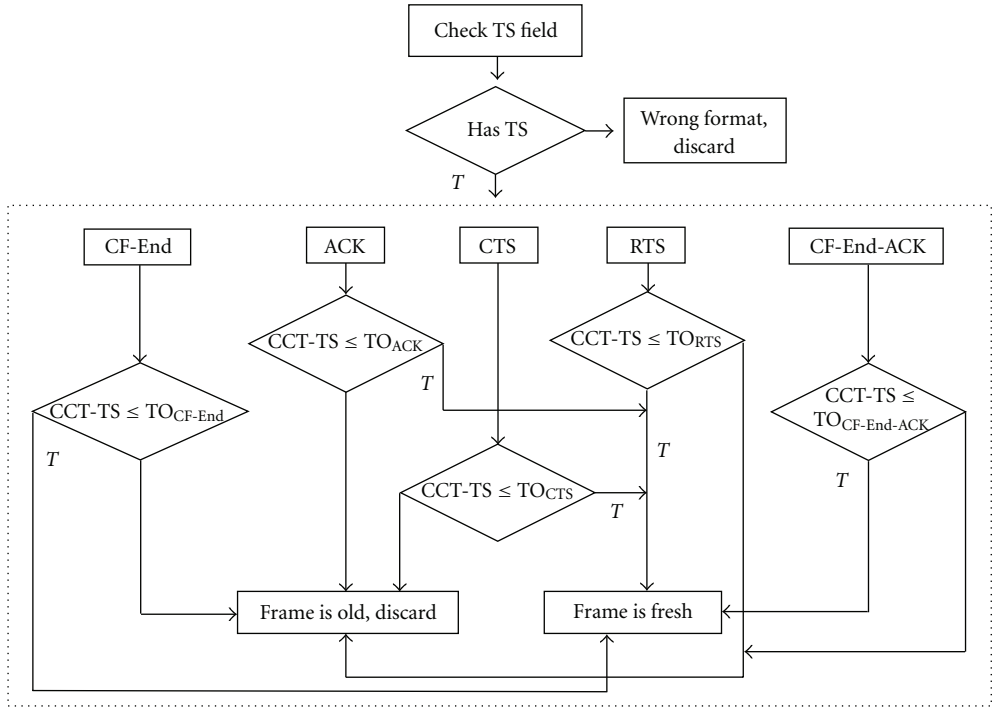


Figure 1: Replay attack preventing mechanism in the ACFNC model.

Phase 1: Secure MAC Layer. The ACFNC model focuses on the provisioning the secure control frames at the MAC layer. Thus, we need to develop a new secure MAC layer and include the respective ACFNC codes in the both wireless stations and access point. Therefore, we created a wireless NIC which is called 80211-ACFNC-NIC. This secure NIC includes a secure MAC layer which is called 802.11-ACFNC-MAC layer. The ACFNC code to secure control frames has been written in C++ and included in the 802.11-ACFNC-MAC layer.

Phase 2: Secure Time Synchronization (STSF). The synchronization process is a service related to the MAC sublayer management entity (MLME). The MLME is part of the MAC layer to monitor the events and create appropriate MAC management services such as beacon transmission and synchronization. Thus, in order to implement the STSF, we created a new management sublayer in the 80211-ACFNC-NIC for the wireless stations and access point which are called 80211MgmtSTA-STSF and 80211MgmtAP-STSF, respectively. The ACFNC source code to secure time synchronization in the access point and wireless stations is included in the 80211MgmtAP-STSF and 80211MgmtSTA-STSF sublayers, respectively.

The structure of the 80211-ACFNC-NIC for the access point including the secure MAC layer and secure Mgmt sublayer is presented in Figure 5.

5. Experimental Design

In order to quantify and evaluate the performance of the ACFNC model, we conduct variety types of experiments. The methodology to conduct the experiments and obtain the results is described in the following subsections.

5.1. Characterization of Traffic Type. For all the experiments, we apply both types of data communications as connection-oriented and connectionless. This enables us to extensively evaluate the impact of the traffic type on the performance of the ACFNC model in the wireless network. Three types of traffics are considered, which are the following.

(i) For the connection oriented traffic, we apply the FTP packets. The FTP traffics source is set to a constant bit rate, while the length of each packet is 1000 B. The FTP packets are transmitted with interval times of 0.5 seconds.

(ii) For the connectionless traffic video packets are transmitted as a video stream with maximum size of 10000 MB. The length of video packets in this stream is 1000 B, which are transmitted at constant bit rate of 0.5 seconds intervals.

(iii) We use ICMP packets to obtain results from packets lost due to the attacks and also to obtain the average of round trip response time. The properties of the ICMP packets are set as the default in real world with 56 bytes length and interval of every 1 second.

5.2. Performance Measures. The following performance metrics are investigated.

(i) *End-to-end delay*. It is defined as the amount of time taken by a packet to travel from the originating node

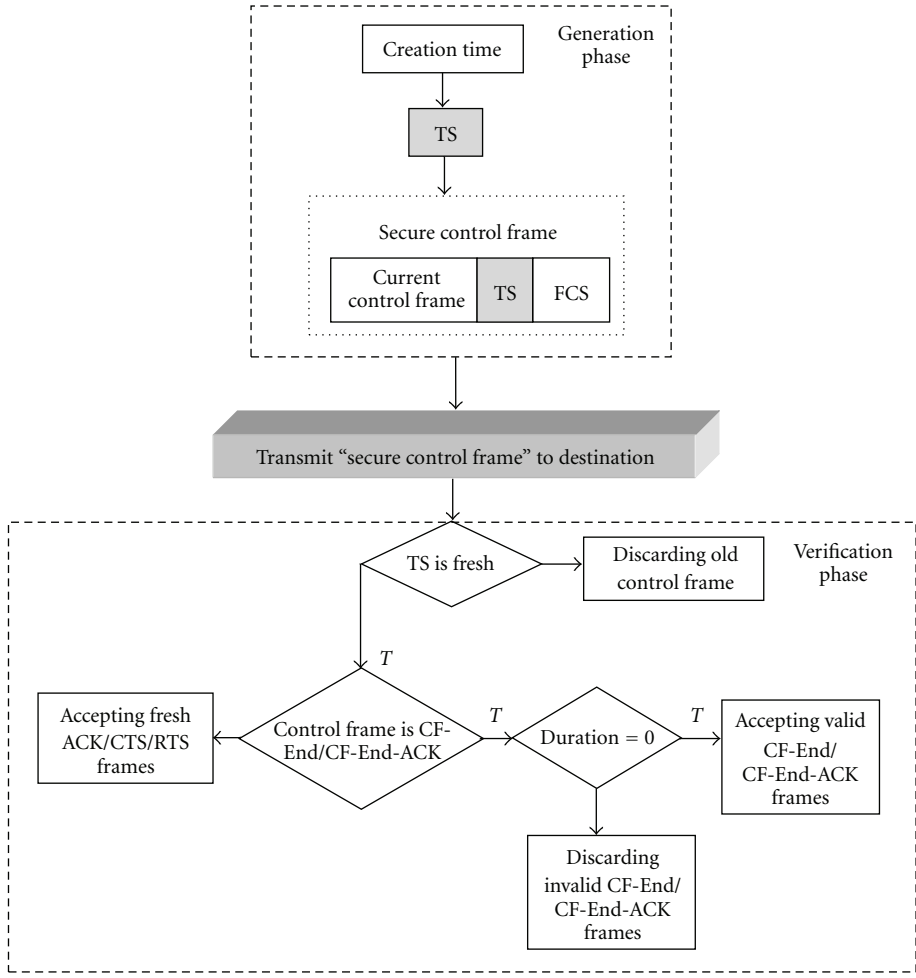


Figure 2: Algorithm of the ACFNC model.

until it is successfully received at the destination node.

(ii) *Throughput*. It is computed by dividing the amount of data successfully received by destination node with the time taken to arrive at this node.

(iii) *Packet lost ratio (PLR)*. The PLR is measured as the number of dropped packets divided by the total number of sent packets during data transmission.

(iv) *Round trip response time (RTT)*. The RTT is the time required for a packet to travel from the source to the destination and back again.

(v) *Detection accuracy*. Accuracy of the ACFNC model is investigated in terms of false negative (FN), false positive (FP), true negative (TN), and true positive (TP) [31]. The FN is when the received forgery control fames incorrectly are regarded and accepted as valid control frames by the recipient. The FP is the incorrectly discarding of a valid control frame which is considered as a forgery frame by the recipient. The TN is the correctly discarding of the forgery control frames by the receiver. The TP is the correctly acceptance of the valid control frames by the recipient.

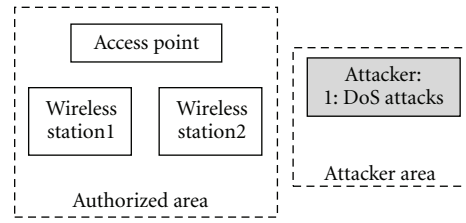


Figure 3: Simulation environment A for the IEEE 802.11 current model.

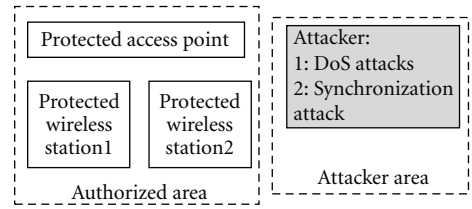


Figure 4: Simulation environment B for the ACFNC model.

Furthermore, the security cost of the ACFNC model is taken into account. In order to determine the security cost,

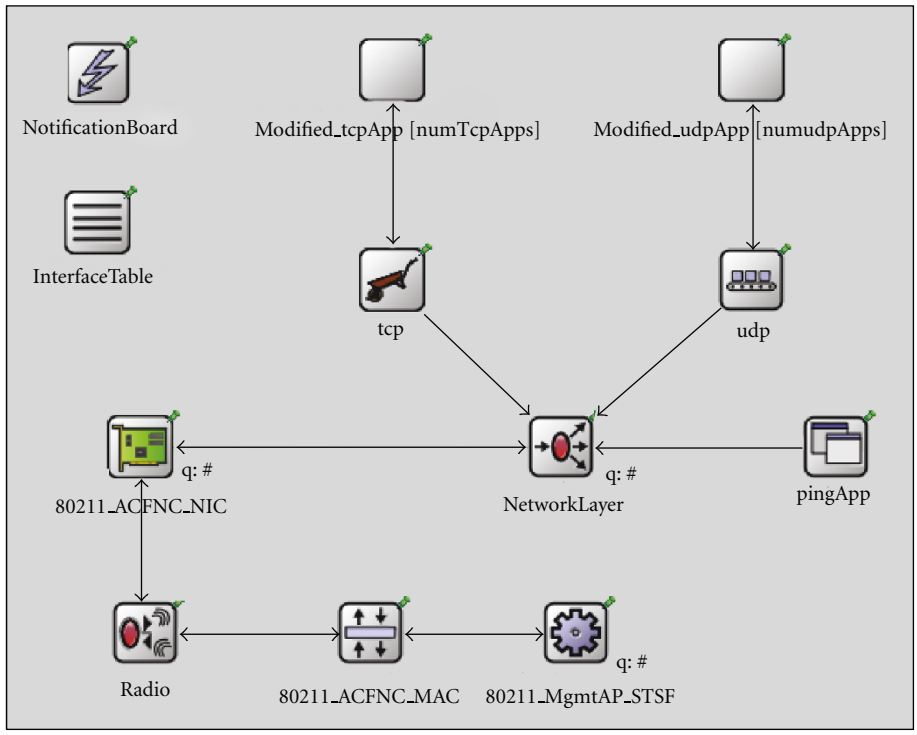


Figure 5: Structure of the protected 80211-ACFNC-NIC in the simulation environment B.

the percentage of performance degradation is calculated as compared to the current model under normal conditions without any DoS attacks.

5.3. Attacks Scenarios. The performance of the ACFNC model is evaluated in terms of its ability to prevent both wireless DoS attacks and synchronization attacks as the following scenarios.

5.3.1. DoS Attacks. The details of the strategy to conduct variety types of wireless DoS attacks against the ACFNC model is described in the following.

(i) The total simulation time for each experiment is 90 seconds, which is further divided into three parts. The first 30 seconds is considered a duration at which the network is under normal conditions with no attack. The second 30 seconds is the attack duration. During the entire period, different types of DoS attacks are conducted separately over the ACFNC and the current model. The third 30 seconds presents conditions of the wireless network after the attacks.

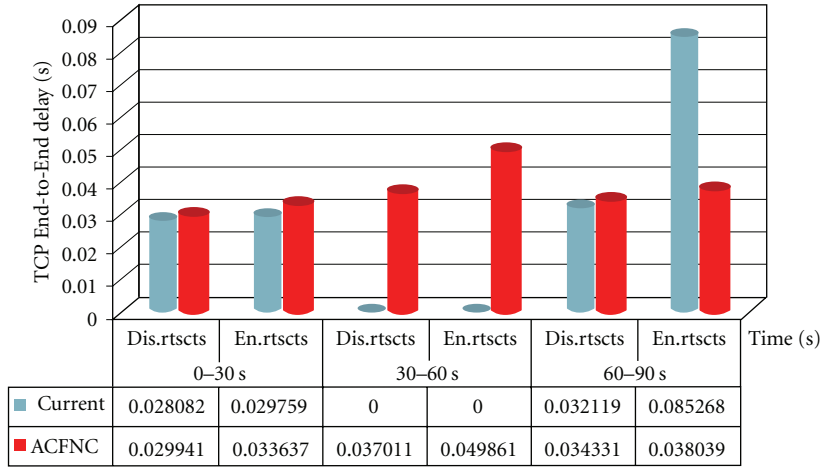
(ii) For all types of the DoS attacks, the attack cycle is considered to be 100 forgery control frames per second (0.01 s attack rate).

(iii) We set duration field of the forgery control frames to the maximum possible value which is 32767 μs.

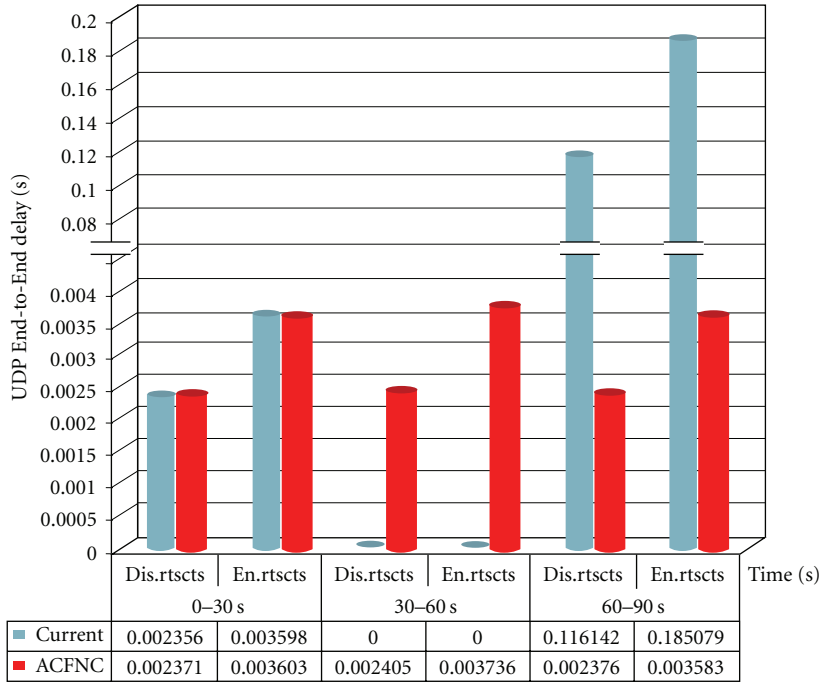
(iv) According to the IEEE 802.11, there are two types of communication modes in wireless networks as enabled and disabled RTS/CTS handshake [1]. Since our proposed model directly deals with the wireless control frames, enabling or disabling of the RTS/CTS handshake can provide significant differences in the network performance in terms of the metrics. Therefore, all the experiments are performed under the both communication modes. The disabled RTS/CTS handshake is denoted as Dis.rtscts, and the enabled RTS/CTS handshake is denoted as En.rtscts.

(v) The experiments are also implemented in the baseline mode which evaluates the performance of the ACFNC model under normal conditions without the presence of the attackers. The results provide helpful insight to demonstrate the security cost of the ACFNC model compared to the current model.

5.3.2. Synchronization Attacks. The synchronization attack is conducted against the ACFNC model to evaluate its performance. Like before, the total implementation time is 90 seconds, which is divided in three intervals. The first 30 seconds is considered a duration at which the wireless network is under normal condition with no attack. At the second 30 seconds, the attacker launches synchronization attack against the ACFNC model. The forgery beacon frames with incorrect timestamp values (higher and lower than the CCT) are broadcasted to the wireless stations to maliciously desynchronize them. The attack rate is double compared to the normal beacon interval (100 ms) to cause more instability in the system clock. The results in terms of MAC loss rate and end-to-end delay are measured under the both enabled and disabled RTS/CTS handshake to evaluate



(a)



(b)

Figure 6: (a) TCP, (b) UDP delay comparison under attacks.

performance of the STSF in the ACFNC model compared to the TSF. The third 30 seconds presents conditions of the wireless network after the synchronization attacks.

6. Results and Discussion

In this section, the performance of the ACFNC model is evaluated and compared with the current model under the attacks and in the baseline mode as follows.

6.1. Performance Evaluation of the ACFNC Model under DoS Attacks. The experiments are carried out for the TCP and UDP traffics separately to evaluate the effectiveness of the ACFNC model to prevent wireless DoS attacks.

6.1.1. TCP/UDP Delay Comparison. The results of the TCP and UDP delay are presented in Figures 6(a) and 6(b), respectively.

As represented by the above results, we can confirm the effectiveness of the ACFNC model to successfully prevent the wireless DoS attacks. During the attacks in the protected wireless network using the ACFNC model, normal traffics (FTP and video packets) are exchanged between the authorized users and the attacks are not able to disrupt the normal communications.

In contrast, as the both TCP and UDP results show, during 30 seconds attacks times (30–60 s), the current model entirely fails to maintain the regular communication. The wireless network completely is overwhelmed by the forgery control frames and the performance practically drops to null. In the TCP experiment, we observe that when the attacks start, instantly the connection between the wireless nodes is broken, and they are unable to transmit or receive any data. The queued packets before the attacks have to wait until the attack comes to an end. This is the reason of high delay for TCP packets in the standard model after the attacks period. However, the UDP results represent different behavior during the DoS attacks. Unlike the TCP, due to connectionless nature of the UDP traffics, when the attacks start the UDP transmission is possible. However, all the packets go in the queue and are not transmitted to the destination. The UDP packets enter in the queue until the queue becomes full, and the rest of the packets are dropped. Al these UDP packets in the queue must wait there until the end of the attacks. Therefore, in the standard model, delay of the UDP packets after the attacks is higher than the TCP packets.

6.1.2. TCP/UDP Throughput Comparison. The results of the TCP and UDP throughput are presented in Figures 7(a) and 7(b), respectively.

The above findings and results lead us to conclude that the ACFNC model, unlike the standard model, is able to successfully prevent the wireless DoS attacks. In the standard model before the attack (0–30 s), the amount of throughput is observed normal. But during the attacks (30–60 s), the network is flooded with high volume of the forgery control frames which consumes the available bandwidth so that the network is not able to handle the valid requests made from the authorized users. Consequently, the communication between the users is broken, and the network throughput quickly drops to null. Comparing the null throughput of the current model during the attacks with the high throughput of the proposed model further advocates that the ACFNC model is able to successfully block the attacks and significantly improve the performance of the IEEE 802.11 wireless networks (100%) under the DoS attacks.

6.1.3. RTT/PLR Comparison. We measure the average round trip response time of the ACFNC model and compare it with the current model. The result of this comparison is presented in Figure 8.

Based on the above results, the RTT of the proposed model and the current model before the attacks (first 30 seconds) are similar in the achievement. However, when the standard model goes under the attacks, the network completely is rendered unusable and the provided resources are unavailable for the intended users. During the attacks over the standard model, the RTT is null because there is no traffic. The forgery frames of the attacker make buffer of the access point full of useless frames such that it is no longer able to respond to the legitimate requests. The packets in the queue must wait there until termination of the attacks, thus they experience high delay after the attacks (60–90 s).

Table 3: PLR comparison.

Model	# Sent	# Received	# Lost	PLR %
Current	90	56	34	36
ACFNC	90	90	0	0

While the current model absolutely fails to prevent the wireless DoS attacks, the proposed model successfully prevents the attacks. Comparing the very high RTT of the standard model with the normal RTT of the ACFNC model after the attacks further justifies that the protected wireless network has not been affected by the DoS attacks.

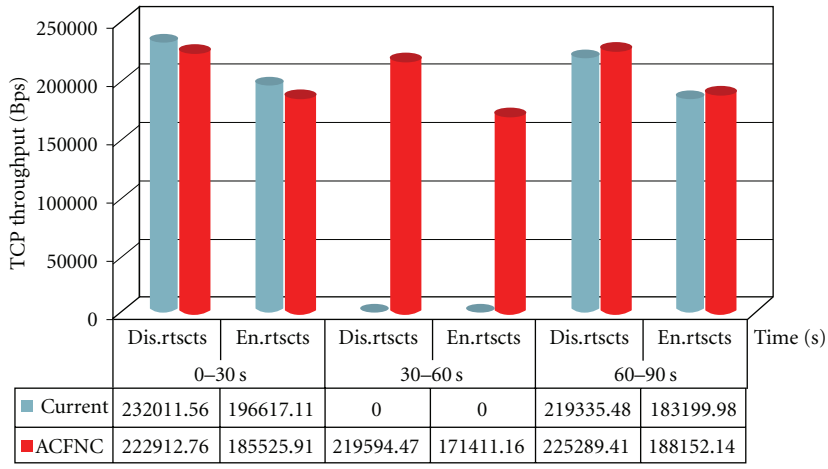
We also provide comparison over the number of lost packets between the standard model and the ACFNC model. The results of this comparison are presented in Table 3.

As the above results indicate, the number of packets lost due to the attacks in the current model is very high. From the 90 transmitted ICMP packets, about 34 packets lost during the attacks which increase the amount of lost ratio substantially to about 36%. The very high amount of lost ratio in the current model proves its weakness and disability to confront the DoS attacks. However, in the wireless network protected by the ACFNC model, it is observed that all the 90 transmitted ICMP packets are successfully received by their destination and number of lost packets is zero. The null amount of lost ratio in presence of the ACFNC model provides evidence for strong ability of the model to prevent DoS attacks over the wireless networks.

6.2. Performance Evaluation of the ACFNC in the Baseline Mode. The previous experiments have been accomplished in presence of the attacker and forgery control frames. In this section, we investigate the performance of the ACFNC model in baseline mode. We study the wireless network behavior during the time at which there are only legal users and their legal traffics over the wireless network. Evaluation of the proposed model in baseline mode determines very helpful insights to demonstrate lifetime overhead and overall security cost imposed to the wireless networks using the ACFNC model under normal conditions. The results are provided as follows.

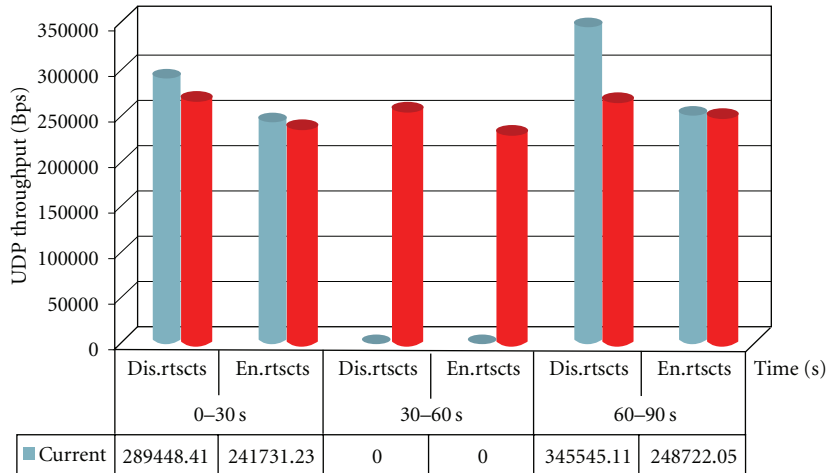
6.2.1. TCP/UDP Delay Comparison. The impact of the ACFNC model on delay of the TCP and UDP packets are presented in Figures 9(a) and 9(b), respectively.

As the above results show, regardless of the type of traffic or the models, the amount of delay is higher when the handshake is enabled. The best performance for the current model and the ACFNC model is achieved when this handshake is disabled throughout the communications. The TCP and UDP results show that delay of the ACFNC model and standard model have the same pattern and level of variations. This proves that the four bytes overhead imposed by the TS security field do not have remarkable impact over the performance of the IEEE 802.11 wireless networks.



	Dis.rtscts	En.rtscts	Dis.rtscts	En.rtscts	Dis.rtscts	En.rtscts
Current	232011.56	196617.11	0	0	219335.48	183199.98
ACFNC	222912.76	185525.91	219594.47	171411.16	225289.41	188152.14

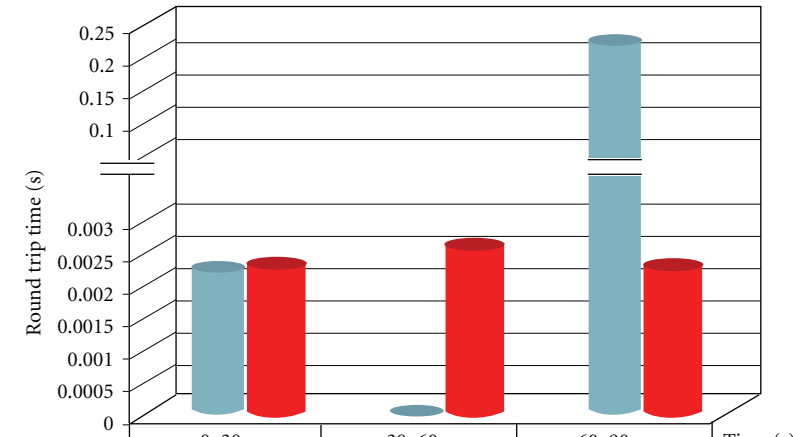
(a)



	Dis.rtscts	En.rtscts	Dis.rtscts	En.rtscts	Dis.rtscts	En.rtscts
Current	289448.41	241731.23	0	0	345545.11	248722.05
ACFNC	267761.51	235630.13	253378.38	228463.58	265425.72	246340.59

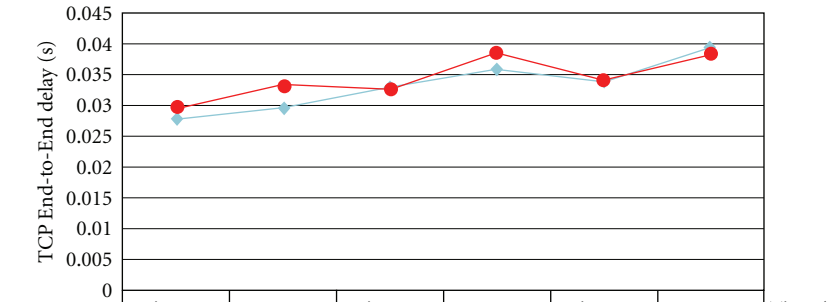
(b)

Figure 7: (a) TCP, (b) UDP throughput comparison under attacks.



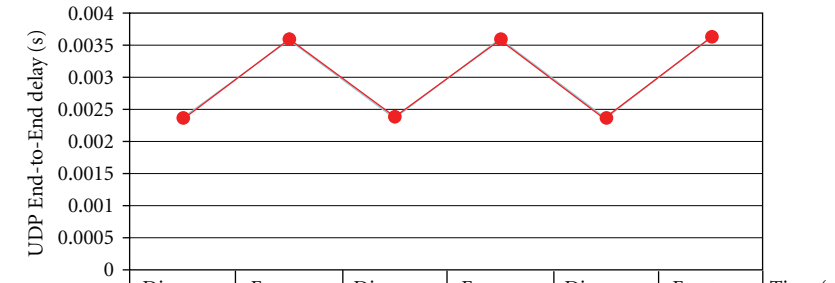
	0–30 s	30–60 s	60–90 s
Current	0.002265	0	0.220087
ACFNC	0.002313	0.002655	0.002328

Figure 8: RTT comparison under attacks.



	Dis.rtscts 0–30 s	En.rtscts 0–30 s	Dis.rtscts 30–60 s	En.rtscts 30–60 s	Dis.rtscts 60–90 s	En.rtscts 60–90 s	Time (s)
Current	0.028082	0.029759	0.033512	0.03604	0.033986	0.039527	
ACFNC	0.029941	0.033637	0.033004	0.038813	0.034398	0.038748	

(a)



	Dis.rtscts 0–30 s	En.rtscts 0–30 s	Dis.rtscts 30–60 s	En.rtscts 30–60 s	Dis.rtscts 60–90 s	En.rtscts 60–90 s	Time (s)
Current	0.002356	0.003599	0.002362	0.003545	0.002359	0.003641	
ACFNC	0.002371	0.003603	0.002383	0.003607	0.002371	0.003619	

(b)

Figure 9: (a) TCP, (b) UDP delay comparison in baseline mode.

6.2.2. TCP/UDP Throughput Comparison. The impact of the ACFNC model on the TCP and UDP throughput are presented in Figures 10(a) and 10(b), respectively.

As for the throughput, the results complement the delay results. Based on the findings, it is clear that applying the ACFNC model does not cause substantial security cost to the wireless networks. The security cost caused by the ACFNC model due to additional overhead (TS field) compared to the standard model is about 4% and 6% when the handshake is disabled and enabled, respectively. The 4% or 6% security cost prove high efficiency and practically of the ACFNC model when comparing with devastating impact of the DoS attacks on the wireless networks.

Furthermore, based on the results, we observe that there is a linear relationship between delay and throughput regardless of the type of traffic. It is observed that they are negatively correlated so that whenever one of them increases, the other one decreases.

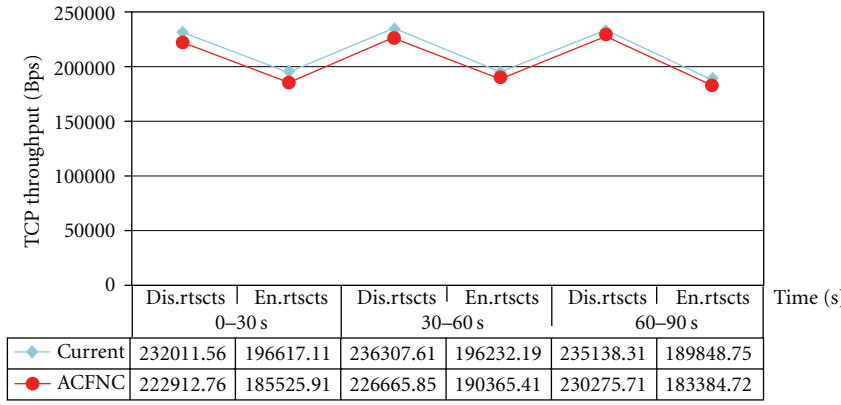
6.2.3. RTT Comparison. This experiment is carried out to evaluate impact of the proposed model over the RTT in the wireless network. The results are presented in Figure 11.

The above results represent almost the same amount of RTT for the standard model and the ACFNC model. This proves that by using the ACFNC model in the wireless networks, the packets do not experience any significant changes in the response time compared to the standard model.

6.3. Detection Accuracy. In order to evaluate accuracy of the ACFNC model, we investigate the probability of the correct/incorrect detection of the valid/forgery control frames by the ACFNC model. The results are presented as follows.

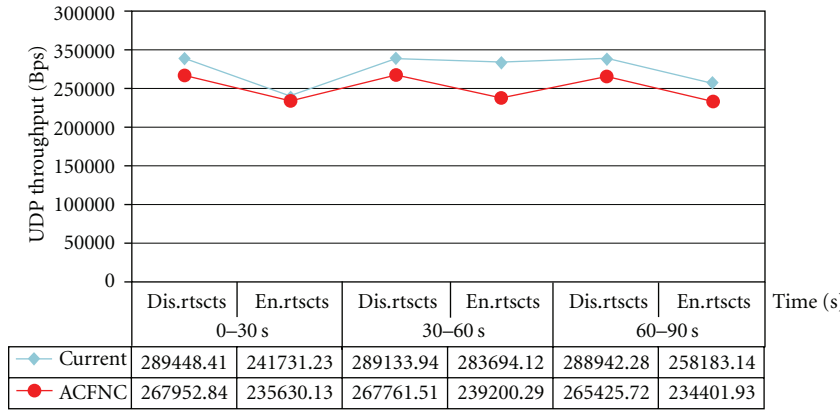
6.3.1. False Negative (FN). From implementation of the ACFNC model, we observed that during the DoS attacks, only the first forgery control frame is verified as a valid control frame and accepted by the recipient. Accepting one forgery control frame out of the 3000 transmitted forgery control frames provides 0.033% FN rate. In contrast, the standard model accepts all the 3000 forgery control frames as valid frames to implement. Thus, comparing very low FN rate of the ACFNC model with 100% FN rate of the standard model proves strong ability of the ACFNC model to prevent wireless DoS attacks.

6.3.2. False Positive (FP). During the entire implementation time, we observed that the ACFNC model like the standard model does not discard any valid control frames. The 0% FP



	Dis.rtscts 0–30 s	En.rtscts 0–30 s	Dis.rtscts 30–60 s	En.rtscts 30–60 s	Dis.rtscts 60–90 s	En.rtscts 60–90 s
Current	232011.56	196617.11	236307.61	196232.19	235138.31	189848.75
ACFNC	222912.76	185525.91	226665.85	190365.41	230275.71	183384.72

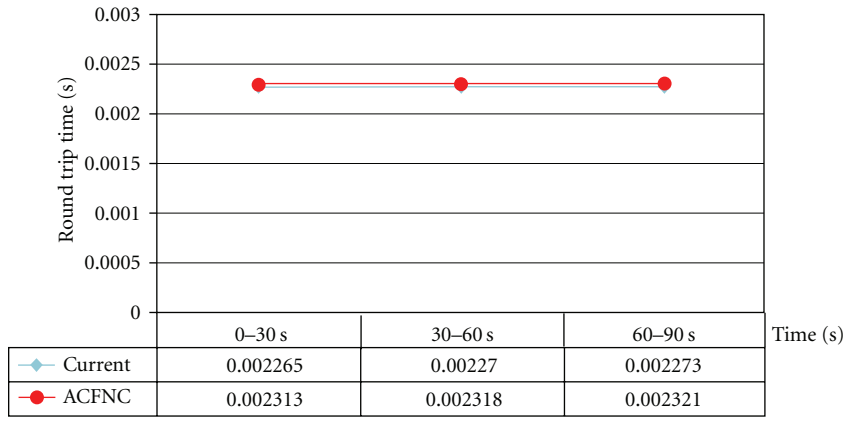
(a)



	Dis.rtscts 0–30 s	En.rtscts 0–30 s	Dis.rtscts 30–60 s	En.rtscts 30–60 s	Dis.rtscts 60–90 s	En.rtscts 60–90 s
Current	289448.41	241731.23	289133.94	283694.12	288942.28	258183.14
ACFNC	267952.84	235630.13	267761.51	239200.29	265425.72	234401.93

(b)

Figure 10: (a) TCP, (b) UDP throughput comparison in baseline mode.



	0–30 s	30–60 s	60–90 s
Current	0.002265	0.00227	0.002273
ACFNC	0.002313	0.002318	0.002321

Figure 11: RTT comparison in baseline mode.

rate proves that the ACFNC model correctly follows the IEEE 802.11 standard.

6.3.3. True Negative (TN). Based on results of the ACFNC implementation, we observed that other than the first forgery control frame the rest of 2999 forgery control frames are correctly discarded by the recipient. Thus, discarding forgery control frames by the ACFNC model provides 99.966% TN rate. Comparing significantly high TN rate of the ACFNC model with the 0% TN rate of the standard model proves that the ACFNC model strongly prevents DoS attacks against the wireless network.

6.3.4. True Positive (TP). During the implementation of the ACFNC model, we observed that like the standard model, the ACFNC model correctly accepts all the valid control frames

Table 4: Detection accuracy of the ACFNC model.

Detection	ACFNC model	Current model
FP	0%	0%
FN	0.033%	100%
TP	100%	100%
TN	99.966%	0%

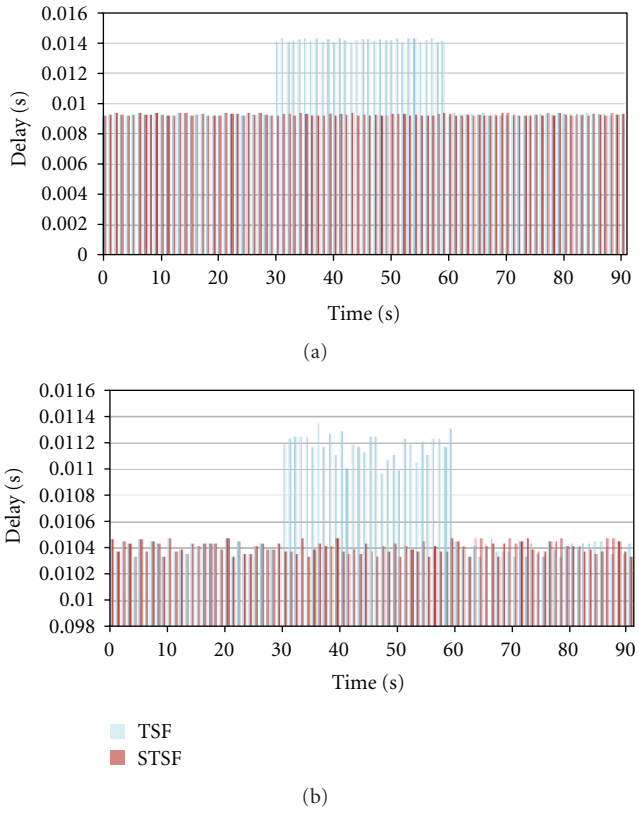


Figure 12: Impact of synchronization attack on delay: (a) for the disabled handshake and (b) for the enabled handshake.

without any mistake. Hence, successful acceptance of the all valid control frames provides 100% TP rate for the ACFNC model which is identical to the standard model.

The summary of comparison between the accuracy rate of the ACFNC model and the standard model is provided in Table 4.

6.4. Performance Evaluation of the STSF in the ACFNC Model. In this section, we evaluate performance of the STSF in the ACFNC model compared to the current TSF. The delay and MAC loss rate are measured under the normal conditions and under synchronization attack as follows.

6.4.1. Delay Comparison: STSF versus TSF. The results of delay under synchronization attack against the ACFNC model for the disabled and enabled handshake are presented in Figures 12(a) and 12(b), respectively.

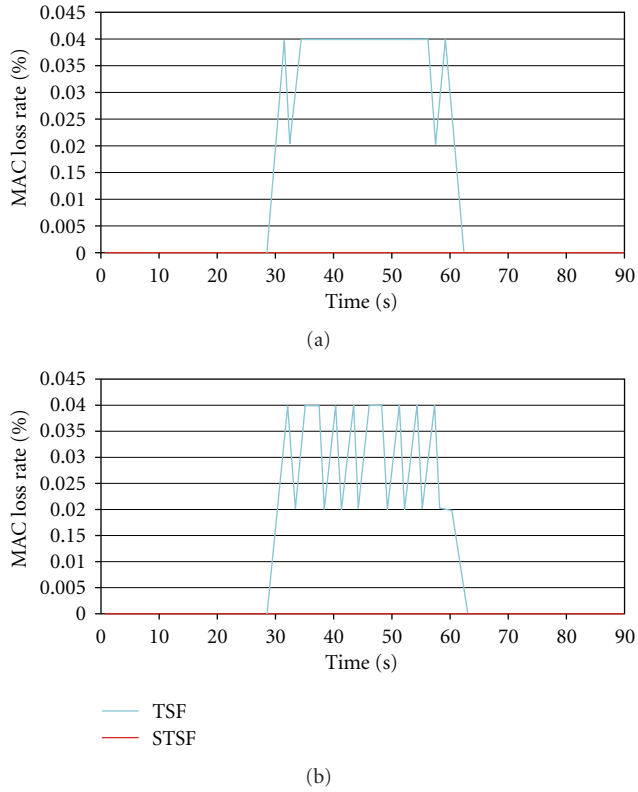


Figure 13: MAC loss rate comparison: (a) for the disabled handshake and (b) for the enabled handshake.

As the above results show, the forgery beacon frames with incorrect timestamps have direct impact on the delay of the TSF. During the 30 seconds attack time (30–60 s), the delay is higher in presence of the TSF compared to the STSF. Comparing the delay of the disabled and enabled handshake shows interesting results. When the handshake is disabled, under normal conditions (i.e., before and after the synchronization attack) the delay is lower than the enabled handshake. However, during the attack, the results are opposite so that in the disabled handshake, the delay is higher than the enabled handshake. The reason is that when the handshake is enabled, the attack causes to drop mostly the RTS and CTS frames which lead to their retransmission. In contrast, when the handshake is disabled, the attack causes to drop the ACK frames, which consequently lead to retransmission of the data frames that is more time consuming than the retransmission of the RTS or CTS frames. As a result, using the TSF, the attacker can intentionally delay the beacon frames by sending low rate forgery beacon frames.

In contrast, the synchronization attack does not have any impact over the normal performance of the ACFNC model. The STSF mechanism preserves the correct and valid synchronization between the authorized stations in the wireless network.

6.4.2. MAC Loss Rate Comparison: STSF versus TSF. The results of the MAC loss rate under the synchronization attack

against the ACFNC for the disabled and enabled handshake are presented in Figures 13(a) and 13(b), respectively.

Based on the above results it is observed that during 30 seconds synchronization attack (30–60 s) over the TSF, the attacker's forgery beacon frames interrupt the active connection between the wireless stations. The attacker sends double forgery beacon frames compared to the normal beacon frames interval. This leads to more instability in the current clock and causes significant desynchronization and dropping the packets.

In contrast, the MAC loss rate is zero in presence of the STSF regardless of the handshake status which shows that the ACFNC model is robust against the synchronization attack. The ACFNC model can detect malicious synchronization attack and prevent the wireless network from being desynchronized by the forgery beacon frames with erroneous time values. As a result, the attacker is not able to modify or destroy the clock information sent by the authorized access point and the ACFNC model correctly performs its respective functions.

7. Conclusion

In this work, we proposed a noncryptographic security model, ACFNC, to prevent the wireless DoS attacks based on control frames vulnerabilities. The ACFNC model has been implemented and further evaluated for validation through a series of extensive experiments to compare with the IEEE 802.11 standard model.

Our findings and results have clearly lead us to the conclusion that while the IEEE 802.11 standard model is highly vulnerable to prevent the DoS attacks, the ACFNC model has been successful in overcoming the drawbacks and strongly prevents the wireless DoS attacks. Based on the results, we deduce that the simple structure of the ACFNC model does not demand remarkable computational resources. The security cost of the ACFNC model is negligible and comparable with the standard model under normal conditions.

The lack of complexity through the simplicity of the overall computation and implementation process, legacy compatibility, high accuracy, and small security cost and communication overhead are the substantial advantages of the ACFNC model which make it practical and efficient in the limited resources wireless networks.

References

[1] IEEE 802.11, "Information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements—part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2007.

[2] A. Rachedi and A. Benslimane, "Impacts and solutions of control packets vulnerabilities with IEEE 802.11 MAC," *Wireless Communications & Mobile Computing*, vol. 9, no. 4, pp. 469–488, 2009.

[3] K. Bicakci and B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 931–941, 2009.

[4] R. Bansal, S. Tiwari, and D. Bansal, "Non-cryptographic methods of MAC spoof detection in wireless lan," in *Proceedings of the 16th International Conference on Networks (ICON '08)*, pp. 1–6, New Delhi, India, December 2008.

[5] Y. Zhou, D. Wu, and S. M. Nettles, "Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems," in *Proceedings of the IEEE Workshop on Broadband Wireless Services and Applications (BWSA '04)*, San Jose, Calif, USA, 2004.

[6] M. A. Khan and A. Hasan, "Pseudo random number based authentication to counter denial of service attacks on 802.11," in *Proceedings of the 5th IEEE and IFIP International Conference on Wireless and Optical Communications Networks (WOCN '08)*, pp. 1–5, Surabaya, Indonesia, May 2008.

[7] W. Chen, D. Chen, G. Sun, and Y. Zhang, "Defending against jamming attacks in wireless local area networks," in *Proceedings of the 4th International Conference on Autonomic and Trusted Computing: Bringing Safe, Self-x and Organic Computing Systems into Reality (ATC '07)*, vol. 4610 of *Lecture Notes in Computer Science*, pp. 519–528, Hong Kong, July 2007.

[8] Z. Zhang, J. Wu, J. Deng, and M. Qiu, "Jamming ACK attack to wireless networks and a mitigation approach," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 4966–4970, New Orleans, La, USA, 2008.

[9] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proceedings of the 12th USENIX Security Symposium*, Washington, DC, USA, August 2003.

[10] R. Negi and A. Rajeswaran, "DoS analysis of reservation based MAC protocols," in *Proceedings of the IEEE International Conference on Communications (ICC '05)*, vol. 5, pp. 3632–3636, Seoul, Korea, May 2005.

[11] D. Chen, J. Ding, and P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming," in *Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03)*, San Diego, Calif, USA, September 2003.

[12] A. Safonov, A. Lyakhov, and S. Sharov, "Synchronization and beaconing in IEEE 802.11s mesh networks," in *Proceedings of the International Conference on Telecommunications (ICT '08)*, pp. 1–6, Saint-Petersburg, Russia, June 2008.

[13] L. Chen and J. Leneutre, "A secure and scalable time synchronization protocol in IEEE 802.11 ad hoc networks," in *Proceedings of the International Conference on Parallel Processing Workshops (ICPP '06)*, pp. 207–214, Columbus, Ohio, USA, August 2006.

[14] K. Xing, S. Srinivasan, M. Rivera, J. Li, and X. Cheng, "Attacks and countermeasures in sensor networks: a survey," Tech. Rep. GWU-CS-TR-010-05, The George Washington University, 2005.

[15] G. Khanna, A. Masood, and C. N. Rotaru, "Synchronization attacks against 802.11," in *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS '05)*, San Diego, Calif, USA, February 2005.

[16] L. Wang and B. Srinivasan, "Analysis and improvements over DoS attacks against IEEE 802.11i standard," in *Proceedings of the 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC '10)*, vol. 2, pp. 109–113, Wuhan, China, April 2010.

[17] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," in *Proceedings of the 5th Symposium on Operating Systems Design and*

Implementation (OSDI '02), vol. 36, pp. 147–163, Boston, Calif, USA, 2002.

[18] S. Ganeriwal, R. Kumar, and M. B. Srivastava, "Timing-sync protocol for sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 138–149, Los Angeles, Calif, USA, November 2003.

[19] M. Maróti, B. Kusy, G. Simon, and A. Lédeczi, "The flooding time synchronization protocol," in *Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 39–49, Baltimore, Md, USA, November 2004.

[20] S. Fries and H. Tschofenig, "RFC 4442. Bootstrapping Timed Efficient Stream Loss-Tolerant Authentication (TESLA)," 2006.

[21] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[22] K. Sun, P. Ning, C. Wang, AN. Liu, and Y. Zhou, "TinySeR-Sync: secure and resilient time synchronization in wireless sensor networks," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 264–277, Alexandria, Va, USA, November 2006.

[23] Y. Zhou and Y. Fang, "BABRA: batch-based broadcast authentication in wireless sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '06)*, pp. 1–5, San Francisco, Calif, USA, December 2006.

[24] T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," *IEEE Transactions on Computers*, vol. 59, no. 8, pp. 1120–1133, 2010.

[25] L. Chen and J. Leneutre, "Toward secure and scalable time synchronization in ad hoc networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2453–2467, 2007.

[26] A. Talbot, "Beacon timestamp. A proposal allowing automatic QSL information to be appended to beacon transmissions," November 2006, http://www.g4jnt.com/BeaconTimestamp.pdf.

[27] L. Green, K. Balmy, and M. Emmelmann, "Theoretical throughput limits," doc. 11-06/928, IEEE 802.11 TGt Wireless Performance Prediction Task Group, San Diego, Calif, USA, July 2006.

[28] A. Sheth and R. Han, "SHUSH: reactive transmit power control for wireless MAC protocols," in *Proceedings of the 1st International Conference on Wireless Internet (WICON '05)*, pp. 18–25, Budapest, Hungary, July 2005.

[29] M. Youssef, E. Thibodeau, and A. C. Houle, "Fairness enhancement of IEEE 802.11 ad hoc mode using rescue frames," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications* , pp. 311–316, Springer, New York, NY, USA, 2007.

[30] M. K. Denko, "Detection and prevention of denial of service (DoS) attacks in mobile ad hoc networks using reputation-based incentive schemes," *Journal of Systemics, Cybernetics and Informatics*, vol. 3, no. 4, pp. 1–9, 2005.

[31] Y. Peng, G. Kou, and Y. Shi, "Knowledge-rich data mining in financial risk detection," in *Proceedings of the 9th International Conference on Computational Science (ICCS '09)*, vol. 5545 of *Lecture Notes in Computer Science*, pp. 534–542, Baton Rouge, La, USA, May 2009.