Security protocol for IEEE 802.11 wireless local area network

Se Hyun Park [a], Aura Ganz [a] and Zvi Ganz [b]

[a] *Multimedia Wireless LAN Laboratory, ECE Department, University of Massachusetts, Amherst, MA 01003, USA*
[b] *AIM Engineering Inc., USA*

As Wireless Local Area Networks (WLANs) are rapidly deployed to expand the field of wireless products, the provision of authentication and privacy of the information transfer will be mandatory. These functions need to take into account the inherent limitations of the WLAN medium such as limited bandwidth, noisy wireless channel and limited computational power. Moreover, some of the IEEE 802.11 WLAN characteristics such as the use of a point coordinator and the polling based Point Coordination Function (PCF) have also to be considered in this design. In this paper, we introduce a security protocol for the IEEE 802.11 PCF that provides privacy and authentication, and is designed to reduce security overheads while taking into account the WLAN characteristics. We prove this protocol using the original and modified BAN logic.

1. Introduction

In the near future, Wireless Local Area Networks (WLANs) are expected to constitute one of the largest segments in the market for wireless products [14]. Wireless Local Area Networks will facilitate ubiquitous communications and location independent computing in restricted spatial domains such as offices, factories, enterprise facilities, hospitals, and campuses. In such environments, WLANs will complement and expand the coverage areas of existing wired networks. The main attractions of WLANs include: cost effectiveness, ease of installation, flexibility, tether-less access to the information infrastructure, and support for ubiquitous computing through station mobility. One particular advantage of WLANs is the fact that they can be quickly installed in an Ad Hoc configuration by non-technical personnel, without pre-planning and without a supporting backbone network.

A WLAN consists of a set of wireless stations (STx), called a *Basic Service Set* (BSS), and a *Point Coordinator* (PC) which arbitrates the access of the wireless stations (figure 1).

Radio WLANs may employ either Narrow Band or Spread Spectrum (SS) techniques. In the United States, a license is typically required to operate non-spread spectrum narrow band transmitters [14]. However, licenses are not required to operate spread spectrum equipment in the Industrial Scientific Medical (ISM) frequency bands (902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz bands). Spread spectrum techniques provide resistance to intentional jamming by another source and the degrading effects of multipath transmission. The characteristics of SS modulation are also advantageous from the security standpoint, since both direct sequence (DS) SS and frequency hopping (FH) SS distribute the bits of transmission information for a chip duration [4]. The security aspects of SS communication have been investigated in [17]. The authors concluded that the use of SS as the only security mechanism will not be sufficient. The active intruders in the same service area can easily know or detect the spreading code. Therefore, their conclusion was that in order to ensure highly efficient and secure wireless communication systems cryptographic techniques that incorporate the SS features must be used.

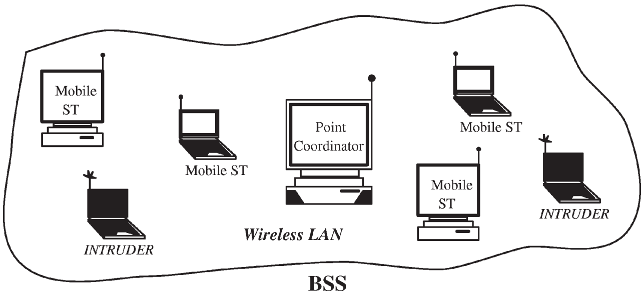


Figure 1. Wireless LAN configuration.

The currently proposed security methods require a symmetric (private key) system or/and an asymmetric (public key) system to authenticate the packet. Moreover, to efficiently derive an authentication technique, a mutual challenge-response protocol based on a random nonce is employed in most protocols proposed for wireless systems [7,11].

However, since in wireless LANs the bandwidth and the computing resources are limited, complex cryptographic protocols such as those requiring extensive computations and transmissions can not be considered. So far, no security protocols for Wireless LANs were proposed for the IEEE 802.11 WLAN.

In this paper we propose a security protocol that is designed for the IEEE 802.11 PCF (Point Coordination Function) and also takes into account the characteristics of a WLAN environment such as limited bandwidth, limited computational power and noisy wireless channel. The limited bandwidth dictates a small number of messages to be exchanged for providing security services. The limited computational power limits the use of sophisticated cryptographic techniques. For the noisy environment we will

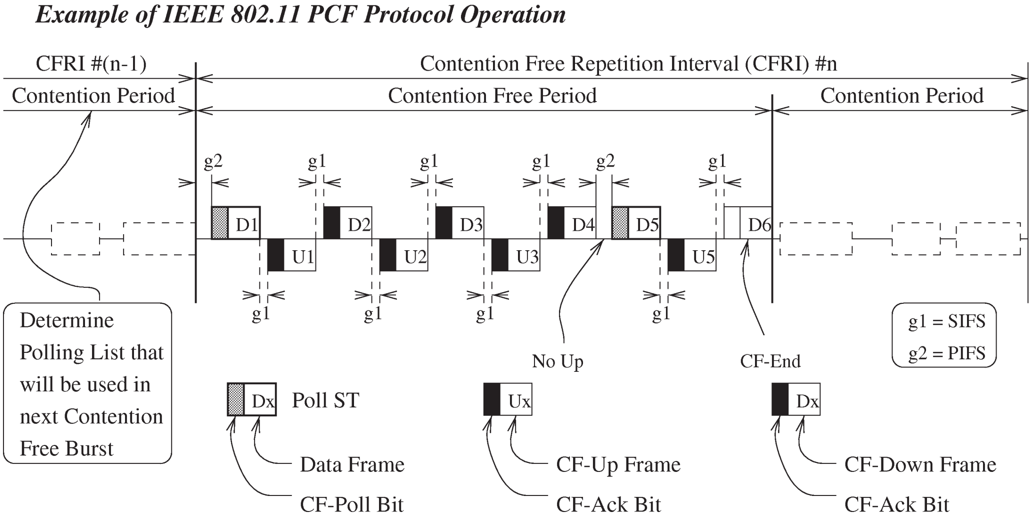


Figure 2. IEEE 802.11 PCF protocol operations.

make provisions for suitable retransmissions of our security messages.

The privacy and the authentication of this security protocol are proved using the original and modified BAN logic presented in [8,22].

2. Wireless LANs

In this section we first describe IEEE 802.11 PCF and the WLAN characteristics that are relevant to the design of our security protocol.

2.1. IEEE 802.11 Point Coordination Function (PCF)

As defined in the IEEE 802.11 standard [5], both the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF) coexist without interference. The seamless integration of the two access methods is obtained by the use of a superframe denoted as Contention Free Repetition Interval. As shown in figure 2, the first period of the Contention Free Repetition Interval follows the contention-free PCF and the second part of the frame follows a contention period.

The PCF protocol is based on a Polling Scheme controlled by the Point Coordinator (PC). Data frames sent from the PC to station STx are denoted as CF-Down (*Dx*) (which includes a CF-Poll bit) frames and Data frames sent from STx to the PC are termed CF-Up (*Ux*) (which includes a CF-Ack bit) frames. The PC sends *Dx* frames between the start of the contention free and the CF-End using the SIFS (Short Inter-Frame Space) except in cases where a transmission by another STx is expected by the PC and an SIFS gap elapses without the receipt of the expected transmission. In such cases, the PC sends the next *Dx* frame a PIFS (Priority Inter-Frame Space) after the end of the last *Dx* [5].

The CF-Poll bit in the *Dx* frames will allow the station to send its *Ux* data. The station immediately responds to the CF-Poll Bit by sending the frame with CF-Ack bit after a SIFS gap. Also the *Dx* frames will contain the CF-Ack bit to acknowledge the preceding *Ux* data [5].

Based on the above PCF access procedure, we propose a security mechanism that will be initiated by the Point Coordinator (PC).

2.2. WLAN characteristics

In this subsection we will discuss the WLAN characteristics that are pertinent to security protocols design.

- *Roaming*: It is the ability to deliver services to wireless stations outside of the basic service area. When a wireless station is roaming, new authentication through the wireless medium must be performed to ensure the new origination of communication and the new session key from unauthorized access and use. In this case it is desirable that the new security mechanisms performed in the new service area should be kept minimal to assure seamless transfer between the areas.
- *Reduce power consumption*: Since the WLANs are intended for portable battery operated wireless stations, low power consumption is a very important consideration. Therefore, the security mechanisms developed should use relatively low complexity cryptographic algorithms.
- *Limited bandwidth*: The limited ISM frequency band allocated by the FCC and the requirement to use spread spectrum communication limit the data rate. For example in the IEEE 802.11 standard the data rate is up to 2 Mbps. This characteristic will require security protocol design that minimizes the number of messages exchanged over the wireless medium.
- *Noisy channel*: In WLANs the bit error rate is high relatively to wired transmission medium. This characteristic will dictate security protocols that incorporate appropriate provisions for erroneous messages and retransmission procedures.

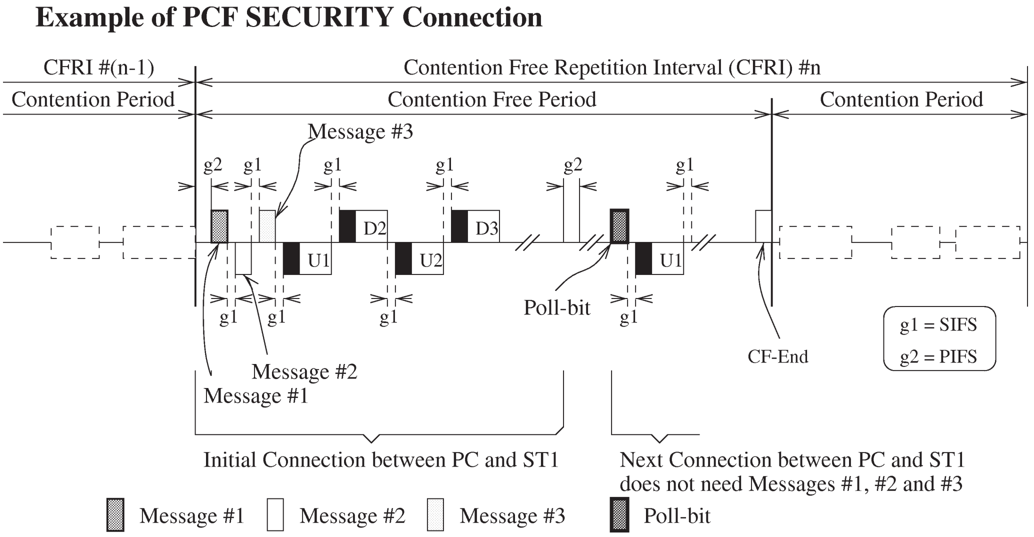


Figure 3. Proposed PCF security protocol operations.

The security protocol proposed here takes into account the above characteristics of the WLANs, the use of a PC and the polling based PCF.

3. Proposed wireless security protocol for IEEE 802.11 PCF

3.1. WLAN design principles and notations

The following assumptions and design principles will guide us in the development of the PCF based security protocol.

- PC maintains a list of wireless stations within its BSS and updates it whenever a new station joins or a station leaves the BSS.
- The stations register for PCF service during the DCF period.
- The polling sequence is determined by the PC.
- PC serves as the authentication agent of the basic service set.
- Since the communication in the PCF period is connection oriented, the proposed security protocol will be executed only at the connection initiation, i.e., after the station registers through the DCF period. As depicted in figure 3, the proposed security procedure consists of three messages (three way handshake) that replace the *Dx* frame that includes CF-Poll.
- Public-key cryptography is used to authenticate and update the session key, and shared-key cryptography is used to provide privacy [7]. In addition, the public-key cryptography is used by PC for privacy.
- The known BSS session key is used for the initial talk to poll the STx and create a unique session key to enhance the bandwidth.
- A number of timers are used in both PC and STx to reduce security overheads and therefore increase the system bandwidth. These timers will be set based on the characteristics of the wireless environment. If there is no response within the allocated time, the PC or STx will retransmit the message. This retransmission may occur up to a maximum number of times which will be determined by the channel quality, the applications that need to be services, etc.

We will present a number of notations used in the remaining part of the paper:

- N: a valid random nonce,
- T: the time at which POLL is emitted,
- L: the life time of the nonce,
- *POLL*: contains N, T, and L,
- $\mathit{XX}_{\mathit{ID}}$: XX's IP address,
- $\mathit{Pub}_{\mathit{XX}}$: XX's public key,
- $\mathit{Pri}_{\mathit{XX}}$: XX's private key,
- *MD*(*PP*): Hash function (e.g., MD5) value of parameter *PP*,
- $E(X, \langle \mathit{YYs} \rangle)$: encryption of *YYs* using key X,
- $[\{\mathit{IIs}\}, C]$: xor *IIs* with the session key C,
- Mess. #n ReTr: Message #n Retransmission.

In the next subsection, we will specifically discuss the security protocol operation which is depicted in figure 3.

3.2. Proposed PCF security protocol description

We assume that the PC wants to establish a session with ST1 in a contention free period. The proposed PCF security protocol proceeds as follows:

- *Step 1 (PC → ST1)*

  step 1.1 PC creates N.

  step 1.2 PC computes MD(N), the hash value of the message digest [13], to ascertain ST1's turn.

step 1.3 N and MD(N) are encrypted with the public key which belongs to ST1.

step 1.4 To broadcast the poll for ST1, PC has to send its IP address PC_{ID}. After appending PC_{ID} to the encrypted data, PC xors the message with the BSS session key (*SessionKey*).

step 1.5 PC transmits Message #1: $[\{PC_{ID}, E(Pub_{ST1}, \langle N, MD(N)\rangle)\}, SessionKey]$

step 1.6 PC starts the timer for Message #2 the moment Message #1 is sent. If there is no reply from ST1, PC will retransmit the message up to a maximum number of times Mess. #1 ReTr. If no reply, the PC returns control to the main PC routine.

- *Step 2 (PC ← ST1)*

step 2.1 ST1 xors Message #1using BSS session key.

step 2.2 ST1 verifies the ciphertext of both N and $MD(N)$ using its private key. If ST1 can decrypt the message under its private key (Pri_{ST1}), ST1 realizes that this message is a POLL destined for itself, and proceeds to the next step. If ST1 can not decrypt the message, proceed to receive mode since the message is not destined for ST1.

step 2.3 ST1 detects whether PC_{ID} is correct or not. If PC_{ID} is valid, proceed to the next steps. If not, proceed to receive mode.

step 2.4 ST1 creates SK_{NEW}, the new session key. The length of SK_{NEW} is variable according to the channel environment, the priority of message, or security.

step 2.5 ST1 creates SK_N, the current session key for PC and ST1. The current session key (SK_N) is xoring the new session key (SK_{NEW}) and the previous session key (SK_{N-1}). If it is the first connection, the current session key (SK_N) is the new session key (SK_{NEW}).

step 2.6 ST1 uses $ST1_{ID}$ to identify itself to PC. ST1 encrypts $ST1_{ID}$ and SK_N using the PC public key. Then, this encrypted data is appended to $MD(N)$.

step 2.7 ST1 xors the message using BSS session key (*SessionKey*).

step 2.8 ST1 transmits Message #2: $[\{MD(N), E(Pub_{PC}, \langle ST1_{ID}, SK_{NEW}\rangle)\}, SessionKey]$

step 2.9 The timer is started for Message #3. If there is no response from PC in a predetermined time, ST1 assumes the traffic is lost in the wireless network. In such an event, ST1 will retransmit Messages #2. The number of retransmissions will be bounded by Mess. #2 ReTr.

- *Step 3 (PC → ST1)*

step 3.1 PC xors Message #2 with BSS session key.

step 3.2 PC validates the hash value of N. If MD(N) is valid, go to next step. If MD(N) does not match, the wireless station suspects an attacker and control is returned to the main PC routine.

step 3.3 PC ensures that it can decrypt the ciphertext using its private key (Pri_{PC}). If PC can decrypt and verify ST_{ID} along with MD(N), PC starts generating Message #3. If PC can not decrypt the message or ST_{ID} is not the authentic station that PC intended to poll, the conversation is disconnected and PC returns control to the main PC routine.

step 3.4 PC computes SK_N using SK_{NEW}.

step 3.5 T and L are generated to compute POLL.

step 3.6 PC encrypts all factors of POLL using Pub_{ST1}. This encrypted data based on N performs the mutual authentication.

step 3.7 To provide additional mutual authentication between PC and ST1, we use a unique current session key (SK_N). PC xors the encrypted data using SK_N to identify itself to ST1.

step 3.8 PC transmits Message #3: $[\{E(Pub_{ST1}, \langle T, L, N\rangle)\}, SK_N]$

step 3.9 The moment PC sends Message #3, the timer starts running for the beginning of the communication stage. After receiving Message #3, ST1 has to send information to PC or another wireless station within the time-out period of the timer of PC. According to our PCF security protocol, an information message keeps the PC informed that ST1 is alive and sending data. If no data from ST1 is detected in a timing threshold, PC will retransmit the message. The number of retransmissions is bounded by Mess. #3 ReTr.

- *Step 4 (from ST1)*

step 4.1 ST1 xors Message #3 to achieve mutual authentication using SK_N. If ST1 can xor, the next step is performed. Otherwise, the party sending the message is suspected to be an attacker or the message was damaged due to channel noise. Thus, ST1 goes back to the receive mode. The number of times ST1 can fail to xor is bounded by Mess. #3 ReTr.

step 4.2 ST1 makes sure that the ciphertext is correctly decrypted using its private key. If ST1 can decrypt and verify an authentic PC based on a valid random nonce (N), ST1 starts the next step. If not, ST1 goes back to the receive mode. The number of times ST1 can fail to decrypt or validate (N) is bounded by Mess. #3 ReTr.

step 4.3 ST1 starts sending information.

The flow chart and the proof using BAN logic [8,22] of this protocol are described in the Appendix.

The proposed security protocol takes into account the characteristics of a WLAN environment such as limited bandwidth, limited computational power and noisy wireless channel. The limited bandwidth dictates a small number of messages to be exchanged for providing security services. We only have three messages. The limited computational power limits the use of sophisticated cryptographic techniques. We use xor function and public key encryption. For the noisy environment we have incorporated provisions for suitable retransmissions of our security messages.

3.3. Comparison with other wireless security techniques

Our security protocol is different from the recently published security techniques for wireless LANs [7] and CDPD network [11] in a couple of aspects such as: a) privacy in the first step, b) exposure of the nonce and c) the number of expensive computations required to complete the authentication process.

In the proposed PCF security protocol, we have implemented a number of additional properties that are derived from the WLAN characteristics, e.g., the use of the polling based PCF and a Point Coordinator.

In the recently published protocols for wireless communication, the first authentication occurs in the second message. However, in this proposed protocol, authentication starts to occur in the first message. This feature can be obtained due to the fact that PC is the one that creates and distributes the poll in a contention free burst. The proposed protocol also has a unique merit as compared with other approaches which use mutual authentication protocols or hand-shake methods, because we never expose the nonce. Therefore, this security protocol can eliminate the risk that can be caused by attacks to the unencrypted nonce.

The advantage of the using SK_N which is constructed by the public-key and the shared-key algorithms at the initial connection is that we can eliminate at least one expensive private key computation. This elimination is due to the fact that POLL is encrypted under the public key of ST1 and the message is xored by the unique session code SK_N. If ST1 can synchronize and xor using SK_N, ST1 will start to send information.

The proposed PCF security protocol provides an unique session key which is dynamically changeable corresponding to the wireless medium environment, the priority of message, or security. Even though the session key due to the simple xor operation may not be applied for strong secure assurance by itself, it is successfully operated in PCF polling mechanism with the public-key encryption. Therefore, we can effectively reduce the total number of expensive computations calculated in currently proposed protocols [7,11] to three.

The comparison between the proposed PCF protocol and other wireless schemes is summarized in table 1.

4. Conclusions

In this paper, we have proposed a security protocol for IEEE 802.11 PCF which achieves authentication and privacy in wireless LAN environments using a point coordinator, unique session codes for each connection, and the private/public key cryptographic algorithms. The proposed security mechanism is integrated with the polling based PCF. This integration and the use of the session code sequence as one more key result in an efficient security mechanism in a low bandwidth ISM band with relatively reduced computation power at the wireless stations and PC (Point Coordinator). The authentication and privacy features of the proposed protocol have been proven using the original and modified BAN logic.

Table 1
Comparison with other wireless approaches.

	PCF Security Protocol	Aziz and Diffie [7]	CDPD network basic security [11]
# of expensive computations	3	4	NA
Authentication in first step	YES	NO	NO
Privacy of Nonce	YES	NO	NO

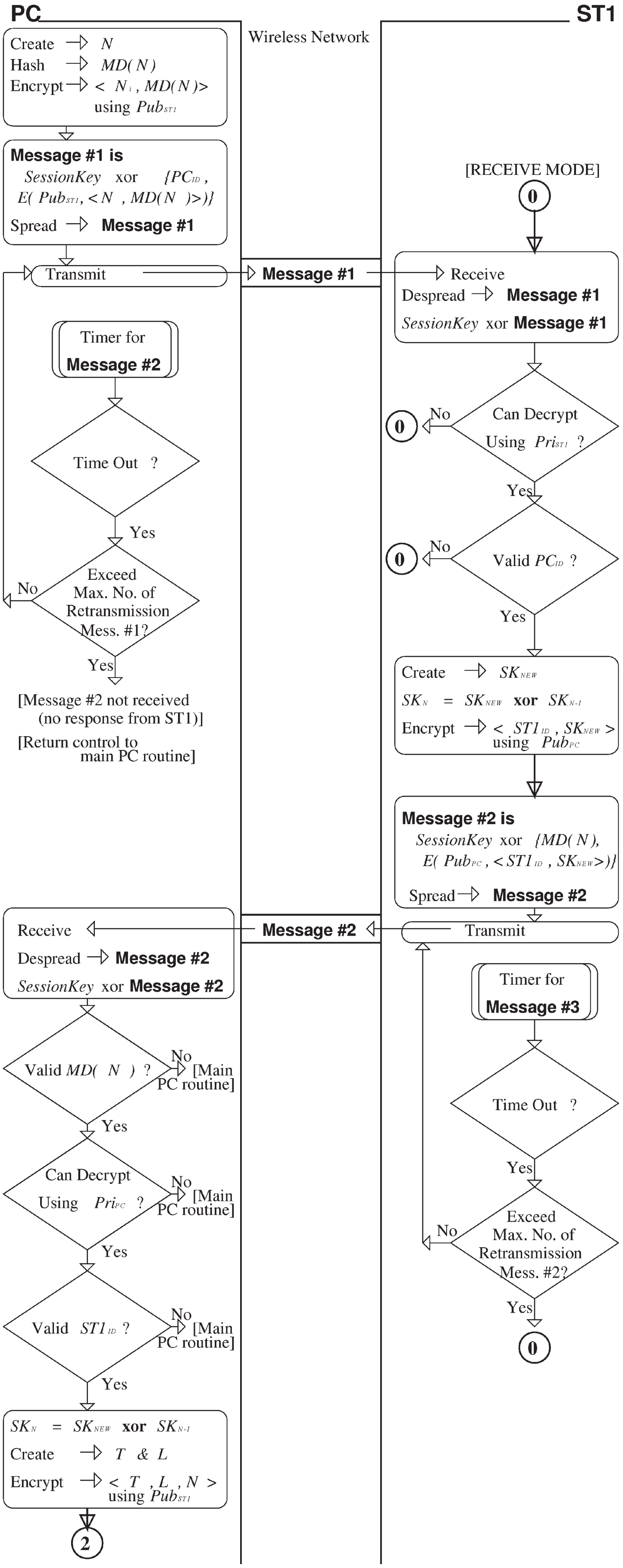
[*] In view point of wireless LAN, CDPD network protocol is not available for the first comparison.

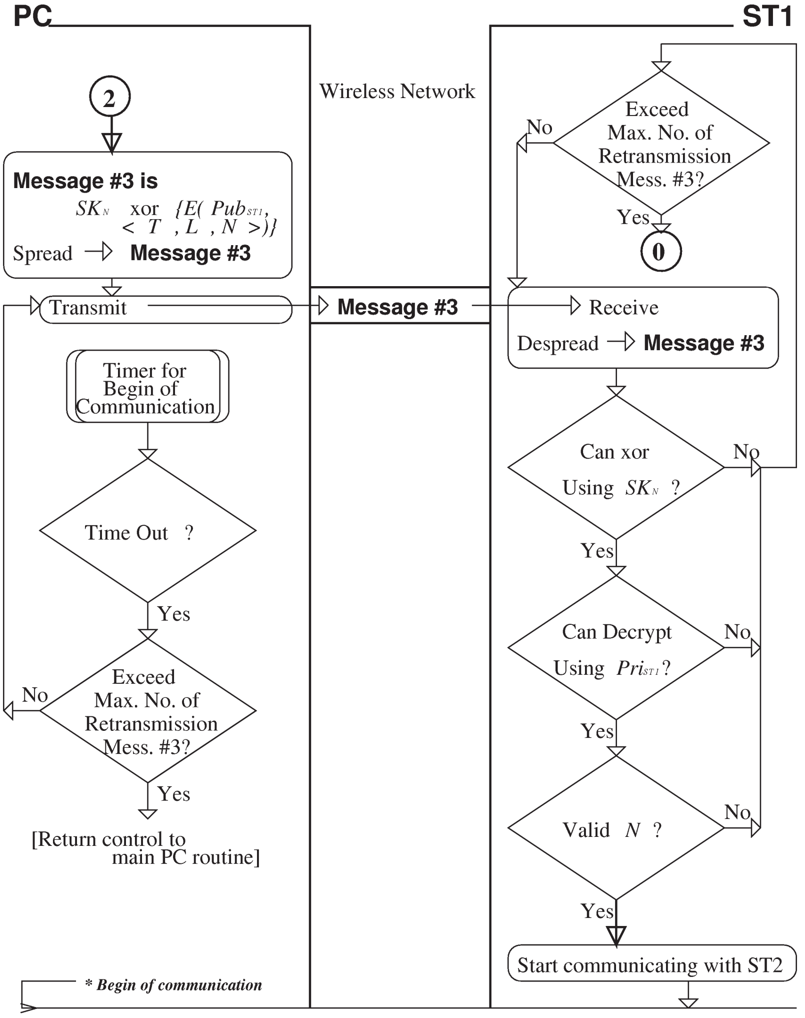
[*] The basic security protocol among CDPD proposals [11] is selected for a fair comparison.

Appendix A. The flow chart of proposed PCF security protocol

Notations

XX_{ID}	: XX's IP address
PC_{ID}	: PC's IP address
$ST1_{ID}$	: ST1's IP address
Pub_{XX}	: XX's public key
Pub_{PC}	: PC's public key
Pub_{ST1}	: ST1's public key
Pri_{XX}	: XX's private key
Pri_{PC}	: PC's private key
Pri_{ST1}	: ST1's private key
$E(X, \langle YY_s \rangle)$	: Encryption of YYs under key X
$MD(PP)$	: Hash function (e.g., MD5) value of parameter PP
$MD(N)$	: Hash function (e.g., MD5) value of parameter N
$MD(T)$	: Hash function (e.g., MD5) value of parameter T
$MD(L)$	: Hash function (e.g., MD5) value of parameter L
N	: A valid random nonce
T	: The time at which POLL is emitted
L	: The life time of the nonce
POLL	: (N, T, L)
$[\{IIs\}, C]$	: xor IIs with session key C
SK_i	: ith session key (e.g., spreading code)
SK_{N-1}	: Previous session key
SK_{NEW}	: New session key
SK_N	: Current session key: $SK_N = SK_{N-1}$ **xor** SK_{NEW}
SessionKey	: The BSS session key
Mess, #n ReTr	: Message #n Retransmission


PC
Wireless Network
ST1
Create → N
Hash → $MD(N)$
Encrypt → $< N_1, MD(N)>$ using Pub_{ST1}
Message #1 is
$SessionKey$ xor $\{PC_{ID}, E(Pub_{ST1}, <N, MD(N)>)\}$
Spread → Message #1
Transmit
Message #1
Timer for Message #2
Time Out ?
Yes
No
Exceed Max. No. of Retransmission Mess. #1?
Yes
[Message #2 not received (no response from ST1)]
[Return control to main PC routine]
[RECEIVE MODE]
0
Receive
Despread → Message #1
$SessionKey$ xor Message #1
Can Decrypt Using Pri_{ST1} ?
No
Yes
Valid PC_{ID} ?
Create → SK_{NEW}
SK_N = SK_{NEW} xor SK_{N-1}
Encrypt → $< ST1_{ID}, SK_{NEW} >$ using Pub_{PC}
Message #2 is
$SessionKey$ xor $\{MD(N), E(Pub_{PC}, <ST1_{ID}, SK_{NEW}>)\}$
Spread → Message #2
Transmit
Message #2
Timer for Message #3
Time Out ?
Exceed Max. No. of Retransmission Mess. #2?
Receive
Despread → Message #2
$SessionKey$ xor Message #2
Valid $MD(N)$?
[Main PC routine]
Can Decrypt Using Pri_{PC} ?
Valid $ST1_{ID}$?
SK_N = SK_{NEW} xor SK_{N-1}
Create → T & L
Encrypt → $< T, L, N >$ using Pub_{ST1}
2


PC
ST1
Wireless Network
2
Message #3 is
SK_N xor {E(Pub_ST1, < T , L , N >)}
Spread → Message #3
Transmit
Message #3
Timer for Begin of Communication
Time Out ?
Yes
No
Exceed Max. No. of Retransmission Mess. #3?
Yes
[Return control to main PC routine]
* Begin of communication
Exceed Max. No. of Retransmission Mess. #3?
No
Yes
0
Receive
Despread → Message #3
Can xor Using SK_N ?
No
Yes
Can Decrypt Using Pri_ST1 ?
No
Yes
Valid N ?
No
Yes
Start communicating with ST2

ST1 Starts Transmission

Appendix B. Proof of proposed PCF security protocol for WLAN

B.1. Authentication proof using BAN logic

To prove the authentication provided by the proposed security protocol, we use the logic of authentication developed by Burrows, Abadi and Needham (BAN logic) [8]. Since the conventional notation for security protocols is not convenient for manipulation in the logic of authentication, they introduced the rules to annotate protocols transforming each message into a logic formula. BAN logic is the most widely used logic for analyzing authentication protocols [6]. By using this logic of authentication, flaws in several protocols, including Needham–Schroeder have been found and redundancies in many protocols including Yahalom, Needham–Schroeder and Kerberos [6] have been discovered. Therefore, the BAN logic was successfully used to prove security features in a number of papers [6,7,23,24]. We propose a different notation for the specific session key. We assume that from the security viewpoint, the function of the unique session key is the same as for a public key. This is due to the fact that in our scheme we have a master (the PC). (We use the same notation as used in [8].)

More notations

A : is PC.
B : is ST1.
S_{AB} : Unique session key between A and B
S_{BSS} : BSS session key

More constructs

$|\overset{S}{\rightsquigarrow} P$: P has S as a session key.

Security protocol

1. $A \rightarrow B : \{A_{ID}, \{N\}_{K_B}\}_{S_{BSS}}$
2. $A \leftarrow B : \{H(N), \{B_{ID}, S_{NEW}\}_{K_A}\}_{S_{BSS}}$
3. $A \rightarrow B : \{\{L, N\}_{K_B}\}_{S_{AB}}$

Idealized protocol

1. $A \rightarrow B : \{|\overset{K_A}{\rightarrow} A, \{N\}_{K_B}\}_{S_{BSS}}$
2. $A \leftarrow B : \{H(A \overset{N}{\rightleftharpoons} B), \{|\overset{K_B}{\rightarrow} B, A \mid\equiv (A \overset{S_{AB-1}}{\rightleftharpoons} B), A \overset{S_{NEW}}{\rightleftharpoons} B\}_{K_A}\}_{S_{BSS}}$

3. $A \rightarrow B : \{\{< A \overset{L}{\rightleftharpoons} B >_N\}_{K_B}, B \mid\equiv (A \overset{S_{AB}}{\leftrightarrow} B)\}_{S_{AB}}$

Proof. Assumptions:

1. $A \mid\equiv \mid\overset{K_A}{\rightarrow} A$
2. $A \mid\equiv \mid\overset{S_{BSS}}{\leadsto} BSS$
3. $B \mid\equiv \mid\overset{K_B}{\rightarrow} B$
4. $B \mid\equiv \mid\overset{S_{BSS}}{\leadsto} BSS$
5. $BSS \mid\equiv \mid\overset{K_A}{\rightarrow} A$
6. $BSS \mid\equiv \mid\overset{K_B}{\rightarrow} B$
7. $BSS \mid\equiv \mid\overset{S_{BSS}}{\leadsto} BSS$
8. $B \mid\equiv A \overset{S_{AB-1}}{\rightleftharpoons} B$
9. $A \mid\equiv (B \mid\Rightarrow A \overset{S_{NEW}}{\rightleftharpoons} B)$
10. $B \mid\equiv (A \mid\Rightarrow A \overset{L}{\rightleftharpoons} B)$
11. $B \mid\equiv (A \mid\Rightarrow A \overset{N}{\rightleftharpoons} B)$

From Assumption 6 and message 1, we obtain:
$\mathrm{B} \lhd \{\mid\overset{K_A}{\rightarrow} A, \{N\}_{K_B}\}_{S_{BSS}}$
$\mathrm{B} \mid\equiv \mid\overset{K_A}{\rightarrow} A$

In Message 2, we apply the Hash function rule. Using Assumption 11, we obtain:
$\mathrm{B} \mid\equiv \mathrm{A} \mid\sim N$
$\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{A} \overset{N}{\rightleftharpoons} B$

In addition, from Assumption 1, and B $\mid\equiv \mid\overset{K_A}{\rightarrow} A$, we get:
$\mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{A} \overset{N}{\rightleftharpoons} \mathrm{B}$

Applying the rules of message meaning to Message 2, we get:
$\mathrm{A} \lhd \{H(A \overset{N}{\rightleftharpoons} B), \{\mid\overset{K_B}{\rightarrow} B, A \mid\equiv (A \overset{S_{AB-1}}{\rightleftharpoons} B), A \overset{S_{NEW}}{\rightleftharpoons} B\}_{K_A}\}_{S_{BSS}}$
$\mathrm{A} \mid\equiv \mathrm{B} \mid\sim \{\mid\overset{K_B}{\rightarrow} B, A \mid\equiv (A \overset{S_{AB-1}}{\rightleftharpoons} B), A \overset{S_{NEW}}{\rightleftharpoons} B\}_{K_A}$

Using Assumption 8 and the fact that B uses public key K_A with $\mid\overset{K_B}{\rightarrow} B$, A authenticates that the message if from B. So, we obtain:
$\mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \overset{S_{NEW}}{\rightleftharpoons} \mathrm{B}$

Now, A is able to use S_{NEW} to compute S_{AB}.
$\mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \overset{S_{AB}}{\leftrightarrow} \mathrm{B}$

In Message 3, A uses S_{AB} to get:
$\mathrm{B} \lhd \{\{< A \overset{L}{\rightleftharpoons} B >_N\}_{K_B}, B \mid\equiv (A \overset{S_{AB}}{\leftrightarrow} B)\}_{S_{AB}}$

Applying the rules of message meaning, we obtain:
$\mathrm{B} \mid\equiv \mathrm{A} \mid\sim \{\{< A \overset{L}{\rightleftharpoons} B >_N\}_{K_B}, B \mid\equiv (A \overset{S_{AB}}{\leftrightarrow} B)\}$
$\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{A} \overset{S_{AB}}{\leftrightarrow} \mathrm{B}$

From Hash function rule, and public key K_B, we get:
$\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{B} \mid\equiv < A \overset{L}{\rightleftharpoons} B >_N$

In addition, using the shared secret L and Assumption 10, we get:
$\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \mid\equiv A \overset{L}{\rightleftharpoons} B$

Thus, the authentication results are:

- $\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{A} \overset{N}{\rightleftharpoons} B$
- $\mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{A} \overset{N}{\rightleftharpoons} \mathrm{B}$
- $\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \mid\equiv A \overset{L}{\rightleftharpoons} B$
- $\mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \overset{S_{NEW}}{\rightleftharpoons} \mathrm{B}$
- $\mathrm{A} \mid\equiv \mathrm{B} \mid\equiv \mathrm{A} \overset{S_{AB}}{\leftrightarrow} \mathrm{B}$
- $\mathrm{B} \mid\equiv \mathrm{A} \mid\equiv \mathrm{A} \overset{S_{AB}}{\leftrightarrow} \mathrm{B}$

□

B.2. Privacy proof

In this subsection, we analyze the proposed security protocol from the privacy viewpoint. Since the logic of authentication was developed only to prove authentication, we modify it. We use all the notations and rules to annotate protocols in the logic of authentication. We also assume that from the privacy standpoint the adaptive binding session key has the same function as the public key. This is due to the fact that only one pair of stations can recognize the message that is coupled by the unique session key in the PCF security protocol. To transform each message into a logic formula of privacy, we create more constructs. We use the same assumptions as in B.1. In order to drive results, we first modify the idealized protocol of the logic of authentication for the privacy version.

More constructs
$P \mid\overset{\diamond}{\Rightarrow} X$: Only P has jurisdiction over X.
$\ll X \gg_T$: X is protected by T.
$\sqsubseteq X \sqsupseteq_T$: The privacy of X is obtained using T.

Idealized protocol for privacy

1. $A \rightarrow B : \{A_{ID}, \ll N \gg_{K_B}\}_{S_{BSS}}$
2. $A \leftarrow B : \{H(A \overset{N}{\rightleftharpoons} B), \ll B_{ID}, A \mid\equiv (A \overset{S_{AB-1}}{\rightleftharpoons} B), A \overset{S_{NEW}}{\rightleftharpoons} B \gg_{K_A}\}_{S_{BSS}}$
3. $A \rightarrow B : \ll\ll\ll A \overset{L}{\rightleftharpoons} B >_N \gg_{K_B}, B \mid\equiv (A \overset{S_{AB}}{\leftrightarrow} B) \gg_{S_{AB}}$

In Message 1, since only stations in the same BSS can recognize the polling signal with S_{BSS}, we obtain:
$\mathrm{B} \mid\equiv \ll A_{ID}, \ll N \gg_{K_B} \gg_{S_{BSS}}$

Then, we obtain the privacy of A_{ID} in the same BSS.
B $\mid\equiv \sqsubseteq A_{ID}, \ll N \gg_{K_B} \sqsupseteq_{S_{BSS}}$

From the proof of authentication, we have obtained:
B $\mid\equiv$ A $\mid\sim N$

Using Message 1, Assumptions 6 and 7 (provide in B.1.) and the fact that N is encrypted using public key K_B, we obtain:
B $\mid\equiv$ (A $\mid\overset{\diamond}{\Rightarrow} \sqsubseteq A_{ID}, \sqsubseteq N \sqsupseteq_{K_B} \sqsupseteq_{S_{BSS}}$)

Applying Hash function rule to Message 2, we obtain:
A $\mid\equiv \ll\sqsubseteq N \sqsupseteq_{H(N)}, \ll B_{ID}, A \mid\equiv (A \overset{S_{AB-1}}{\rightleftharpoons} B), A \overset{S_{NEW}}{\rightleftharpoons} B \gg_{K_A} \gg_{S_{BSS}}$

Using Assumption 8 and the rules of message meaning, $A \mid\equiv (A \overset{S_{AB-1}}{\rightleftharpoons} B)$, B uses public key K_A to protect elements from the eavesdropper. So, we get the result of privacy from Message 2 as follows:
A $\mid\equiv$ (B $\mid\overset{\diamond}{\Rightarrow} \sqsubseteq\sqsubseteq N \sqsupseteq_{H(N)}, \sqsubseteq B_{ID}, S_{NEW} \sqsupseteq_{K_A} \sqsupseteq_{S_{BSS}}$)

Now, only A and B are able to compute S_{AB} using S_{NEW} and S_{AB-1}. So, we obtain:
A $\mid\equiv$ A $\overset{S_{AB}}{\rightleftharpoons}$ B
B $\mid\equiv$ A $\overset{S_{AB}}{\rightleftharpoons}$ B

Since in Message 3, A uses S_{AB} to protect the privacy of the poll parameters from the eavesdropper, we obtain:
B $\mid\equiv$ A $\mid\sim \sqsubseteq\ll< A \overset{L}{\rightleftharpoons} B >_N \gg_{K_B} \sqsupseteq_{S_{AB}}$

From the replay of N which is used in Message 2 with Hash function, we obtain:
B $\mid\equiv$ A $\mid\sim \sqsubseteq\ll L, \ll L \gg_N \gg_{K_B} \sqsupseteq_{S_{AB}}$

Since A uses public key K_B to convince B, we get:
B $\mid\equiv$ (A $\mid\overset{\diamond}{\Rightarrow} \sqsubseteq\sqsubseteq L \sqsupseteq_{K_B} \sqsupseteq_{S_{AB}}$)

We summarize the results from the logic of privacy:

- B $\mid\equiv$ (A $\mid\overset{\diamond}{\Rightarrow} \sqsubseteq A_{ID}, \sqsubseteq N \sqsupseteq_{K_B} \sqsupseteq_{S_{BSS}}$) from Message 1
- A $\mid\equiv$ (B $\mid\overset{\diamond}{\Rightarrow} \sqsubseteq\sqsubseteq N \sqsupseteq_{H(N)}, \sqsubseteq B_{ID}, S_{NEW} \sqsupseteq_{K_A} \sqsupseteq_{S_{BSS}}$) from Message 2
- B $\mid\equiv$ (A $\mid\overset{\diamond}{\Rightarrow} \sqsubseteq\sqsubseteq L \sqsupseteq_{K_B} \sqsupseteq_{S_{AB}}$) from Message 3

In summary, every element that includes the stations' ID in each message meets the requirements of privacy.

References

[1] C.F. Chiasserini and A. Ganz, Security in Wireless LAN, Draft of Wireless LAN Lab., UMass (December 1995).

[2] B. Sklar, *Digital Communications: Fundamentals and Applications* (Prentice-Hall, 1988).

[3] TIA/EIA Interim Standard, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System* (1993).

[4] R.E. Ziemer and W.H. Tranter, *Principles of Communications: Systems, Modulations, and Noise* (Houghton-Mifflin, 1995).

[5] Draft Standard IEEE 802.11, *Wireless LAN*, P802.11/D1 (December 1994).

[6] B. Schneier, *Applied Cryptography* (Wiley, 1996).

[7] A. Aziz and W. Diffie, Privacy and authentication for Wireless Local Area Networks, IEEE Personal Communications, First Quarter (1994) 25–31.

[8] M. Burrows, M. Abadi and R. Needham, A logic of authentication, DEC SRC Res. Rep. 39 (1990).

[9] R.H. Baker, *Network Security* (McGraw-Hill, 1996).

[10] D.T. Magill, F.D. Natali and G.P. Edwards, Spread-spectrum technology for commercial applications, Proceedings of the IEEE 82(4) (April 1994) 572–584.

[11] Y. Frankel et al., Security issues in a CDPD Wireless Network, IEEE Personal Communications (August 1995) 16–27.

[12] W. Diffie and M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22(6) (November 1976) 644–654.

[13] R.L. Rivest, The MD5 message-digest algorithm, Request for Comments 1321, RSA Data Security Inc. (April 1992).

[14] K. Pahlavan and A.H. Levesque, *Wireless Information Networks* (Wiley, 1995).

[15] A. Myles, D.B. Johnson and C. Perkins, A mobile host protocol supporting route optimization and authentication, IEEE Journal of Selected Ares in Communications 13(5) (June 1995) 839–849.

[16] B.C. Neuman, Security, payment, and privacy for network commerce, IEEE Journal of Selected Ares in Communications 13(8) (October 1995) 1523–1531.

[17] H. Imai, Information security aspects of spread spectrum systems, in: *Proceedings of the Advances in Cryptography – ASIACRYPT '94* (1994) pp. 195–208.

[18] P.T. Davis and C.R. McGuffin, *Wireless Local Area Networks* (McGraw-Hill, 1995).

[19] V.K. Grag and J.E. Wilkes, *Wireless and Personal Communications Systems* (Prentice-Hall, 1996).

[20] R.J. Bates, *Wireless Networked Communications: Concepts, Technologies, and Implementation* (McGraw-Hill, 1994).

[21] L. Gong and N. Shacham, Multicast security and its extension to a mobile environment, Wireless Networks 1 (1995) 281–295.

[22] M. Burrows, M. Abadi and R. Needham, A logic of authentication, ACM Transactions on Computer Systems 8(1) (February 1990) 18–36.

[23] R.J. Anderson, A second generation electronic wallet, in: *ESORICS 92* (Springer-Verlag, 1992) pp. 411–418.

[24] B.C. Neuman and S. Stubblebine, A note on the use of timestamps as nonces, Operating Systems Review 27(2) (April 1993) 10–14.

Se Hyun Park is currently a Research and Teaching Assistant with the Multimedia Wireless LAN Laboratory at the University of Massachusetts, Amherst, where he is pursuing the Ph.D. degree. He received the B.S. and M.S. degrees in electronic engineering from Chungang University, Seoul, Korea, in 1986 and 1988, respectively. From 1988 to 1994, he was a senior research engineer designing the VLSI chips in the field of CDMA Viterbi Decoder, high-resolution sigma delta AD/DAC, ISDN interfaces, DSPs and high-speed voice modems at ETRI, Korea. His research interests include real-time security protocols and management for wireless LAN, mobile networks and heterogeneous networks, and high-speed integrated circuit design related to wireless communication, ATM and cryptography.
E-mail: shpark@tikva.esc.umass.edu

Aura Ganz received her Ph.D. degree in computer science from Technion – Israel Institute of Technology, Haifa. She is currently an Associate Professor in the Department of Electrical and Computer Enginering at the University of Massachusetts, where she serves as the director of the Multimedia Wireless LAN Laboratory. Her research interests include design of multimedia wireless LANs, protocol and architecture design of wireless networks, security issues in wireless networks, modeling and performance evaluation. She served as co-chair of the 1997 Massachusetts R&D Telecommunication conference. She is editor of Computer Networks and ISDN Systems and has been active in the program committees for a number of conferences such as IEEE Infocom, IEEE Globecom and IEEE ICC.
E-mail: ganz@tikva.ecs.umass.edu

Zvi Ganz serves as the president of AIM Engineering Inc., which provides business solutions using Internet and Intranet technologies, engineers business processes and develops wireless network solutions for multimedia and data applications. Before joining AIM, he worked in management and engineering capacities for corporations like the Travelers Insurance Companies. He holds a Ph.D. from the University of Massachusetts at Amherst in industrial engineering and operations research and M.Sc. and B.Sc. from the Technion in Israel.
E-mail: zvi@aime.com