Token-Based Security Protocol for Wireless Local Area Networks

Se Hyun Park*, Aura Ganz* and Zvi Ganz**
* Multimedia Wireless LAN Laboratory
ECE Department, University of Massachusetts
Amherst, MA 01003
shpark,ganz@tikva.ecs.umass.edu
** AIM Engineering Inc.
zvi@aime.com

September 15, 1997

Abstract

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 the noisy wireless channel, limited bandwidth and limited computational power. In this paper, we introduce a token based protocol that provides privacy and authentication, and is designed to reduce security overheads while taking into account the WLAN characteristics.

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 (ST), called a *basic service set* (BSS), and an *Access Point* (AP) which arbitrates the access of the wireless stations to the shared communication media.

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 initial spreading code like the paging code. Therefore, their conclusion was that in order to ensure secure wireless LANs, additional security mechanisms must be incorporated.

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 adopted.

In this paper we present a security protocol that takes 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 make provisions for suitable retransmissions of our security messages.

The proposed security protocol is designed with a polling based media access control mechanism in mind.

2 Wireless LANs

In this section we first describe the polling based media access control protocol and the WLAN characteristics that are relevant to the design of our security protocol.

2.1 Polling Based Media Access Control Protocol

The media access control in the WLAN system is based on a centralized polling mechanism. Polling schemes are efficient if the round trip propagation delay is small and the number of stations in the system is relatively small. These two conditions will lead to a relatively reduced polling overhead apriori to transmission. Since these conditions are generally satisfied by WLANs, the polling based protocols can be applied in such environments [23].

This polling mechanism will be initiated by the Access Point (AP). AP will poll each one of the stations in its basic service area. The polling sequence as well as the time allocation

for each polled station will be determined at the AP and will be a function of the traffic loads, priorities, quality of service, etc.

The following desirable properties can be easily realized in the centralized polling based scheme:

- Efficient utilization of the WLAN bandwidth resources, since no bandwidth is lost due to contention
- Provides preferential and guaranteed bandwidth allocations to real-time traffic streams.
- Adaptive to changes in traffic conditions.
- Graceful degradation in Service Quality.
- Facilitates the implementation of security functions.

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 proposed 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.

As described in the next section, our goal is to design security protocols for WLAN systems that take into account the above characteristics of the WLANs, the use of an AP and the polling based media access control protocol.

3 Token-Based Wireless Security Protocol

3.1 WLAN Assumptions and Notations

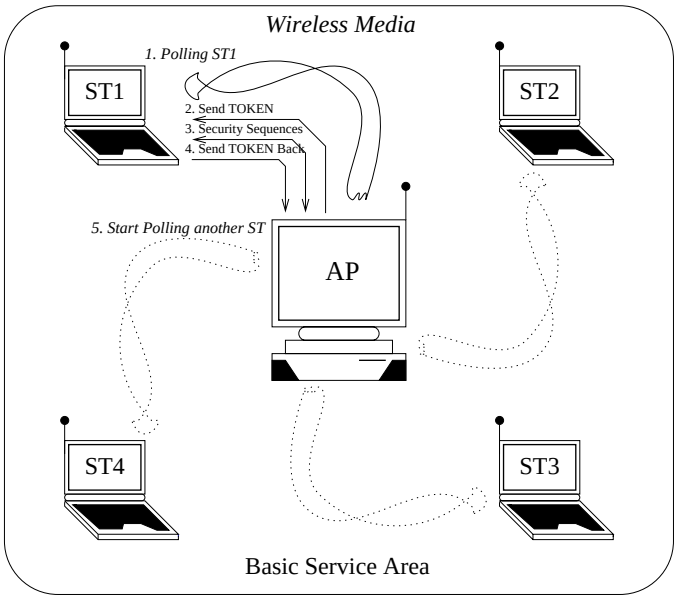


Figure 1: The token-based wireless LAN configuration in the same BSS

The following assumptions and design principles will guide us to the development of the token based security protocol for WLANs:

- AP maintains a list of wireless stations within its BSS and updates it whenever a new wireless station joins or a known station leaves the area.
- The sequence of polling is determined by the AP. Once polled, the station receives the token which determines the connection duration. When the connection time expires, the ST that holds the token stops its transmission and sends the token back to the AP. AP sends the token to the next ST based on the polling sequence. Fig. 1 shows the token-based WLAN in a same BSS.
- AP serves as the authentication agent of the basic service set.
- 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 AP for privacy at the initiation time of the polling sequence.
- The known BSS session key is used for the initial talk to poll the wireless ST and create a unique session key.

- A number of timers are used in both AP and ST 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 AP or ST1 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 TOKEN is emitted
- L : the life time of the nonce
- $TOKEN$: contains N, T, and L
- XX_{ID} : XX's IP address
- Pub_{XX} : XX's public key
- Pri_{XX} : XX's private key
- $MD(PP)$: Hash function (e.g. MD5) value of parameter PP
- $E(X, \langle YYs \rangle)$: encryption of YYs using key X
- $[\{IIs\}, C]$: xor IIs with the session key C
- Mess. #n ReTr : Message #n Retransmission

3.2 Token Based Protocol Description

We assume that ST1 wants to establish a session with ST2. The proposed protocol proceeds as follows:

- *Step 1 ($AP \rightarrow ST1$)*

  step.1.1 AP creates N

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

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

  step.1.4 To broadcast the token for ST1, AP has to send its IP address AP_{ID}. After appending AP_{ID} to the encrypted data, AP xors the message with the BSS session key ($SessionKey$).

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

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

- *Step 2 ($AP \leftarrow ST1$)*

  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 TOKEN destined for itself, and proceed to the next step. If ST1 can not decrypt the message, go back to the receive mode since the message is not destined for ST1.

  step.2.3 ST1 detects whether AP_{ID} is correct or not. If AP_{ID} is valid, proceed to the next steps. If not, proceed to the 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 AP 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 AP. ST1 encrypts $ST1_{ID}$ and SK_N using the public key of AP. 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 :
  $[\{MD(N), E(Pub_{AP}, \langle ST1_{ID}, SK_{NEW}\rangle)\}, SessionKey]$

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

- *Step 3 ($AP \rightarrow ST1$)*

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

  step.3.2 AP 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 AP routine.

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

  step.3.4 AP computes SK_N using SK_{NEW}.

step.3.5 T and L are generated to compute TOKEN.

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

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

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

step.3.9 The moment AP sends Message #3, the timer starts running for the beginning of the communication stage. After receiving Message #3, ST1 has to send information to AP or another wireless station within the time-out period of the timer of AP. According to our token-based protocol, an information message keeps AP informed that ST1 is alive and sending data. If no data from ST1 is detected in a timing threshold, AP will retransmit the message. The number of retransmissions is bounded. If start of communication has been detected. AP starts another timer that is working based on L, the life time of TOKEN. If AP does not get the event of Message #4 within a chosen time, AP returns control to main AP routine.

- *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 AP 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 to ST2 until TOKEN expires.

step.4.4 If TOKEN expires, ST1 xors the hash value of L using SK_N. ST1 identifies itself to AP with L based on the unique session key (SK_N).

step.4.5 ST1 transmits Message #4 :
$[\{MD(L)\}, SK_N]$

- *Step 5 (from AP)*

step.5.1 AP xors Message #4. If the mutual authentication is verified using $MD(L)$ and SK_N, AP determines that this session is over, and then returns control to the main AP routine. AP will start to poll another ST. If AP can not xor Message #4 or $MD(L)$ is not valid, AP goes back to the receive mode.

The flow chart of this protocol is described in the Appendix, and The detailed proof using BAN logic [8][22] is provided in [24].

3.3 Comparison with Other Wireless Security Techniques

Our 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 token based protocol we have implemented a number of properties that are derived from the WLAN characteristics, e.g., the use of a polling based media access control protocol and unique session key techniques.

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 AP is the one that creates and distributes the token. 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 protocol can eliminate the risk that can be caused by attacks to the unencrypted nonce.

The advantage of the using SK_N is that we can eliminate at least one expensive private key computation. This elimination is due to the fact that TOKEN is encrypted under the pubic key of ST1 and the message is xored by the unique session code SK_N.

The proposed token based 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 WLAN polling mechanism with the public-key encryption for the limited bandwidth environments of WLAN systems. 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 protocol and other wireless schemes is summarized in Table 1.

	Proposed Security Protocol	Aziz-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.*
**Th basic secuirty protocol among CDPD proposals [11] is selected for a fair comparison.*

Table 1: Comparison with other wireless approaches

4 Conclusions

In this paper we have proposed a token-based security protocol which achieves authentication and privacy in wireless LAN environments using an access point, unique session codes for each connections, and the private/public key cryptographic algorithms. The proposed security mechanism is integrated the polling based media access control protocol. This integration and the use of the session code 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 AP. The authentication and privacy features of the proposed protocol have been proven in [24] using the original and modified BAN logic.

References

[1] C.F. Chiasserini and A. Ganz, "Security in Wireless LAN," Draft of Wireless LAN Lab., UMass, Dec. 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, Dec. 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, pp. 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*, vol. 82, no. 4, April 1994, pp. 572-584.

[11] Y. Frankel *et al.*, "Security Issues in a CDPD Wireless Network," *IEEE Personal Communications*, Aug. 1995, pp. 16-27.

[12] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, Nov. 1976, pp. 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, "Wirelss 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*, vol. 13, no. 5, June 1995, pp. 839-849.

[16] B.C. Neuman, "Security, Payment, and Privacy for Network Commerce," *IEEE Journal of Selected Ares in Communications*, vol. 13, no. 8, Oct. 1995, pp. 1523-1531.

[17] H. Imai, "Information Security Aspects of Spread Spectrum Systems," *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 Series on Computer Communications*, 1995.

[19] V.K. Grag and J.E. Wilkes, "Wireless and Personal Communications Systems," *Prentice-Hall PTR*, 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, pp. 281-295.

[22] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, Feb. 1990, pp. 18-36.

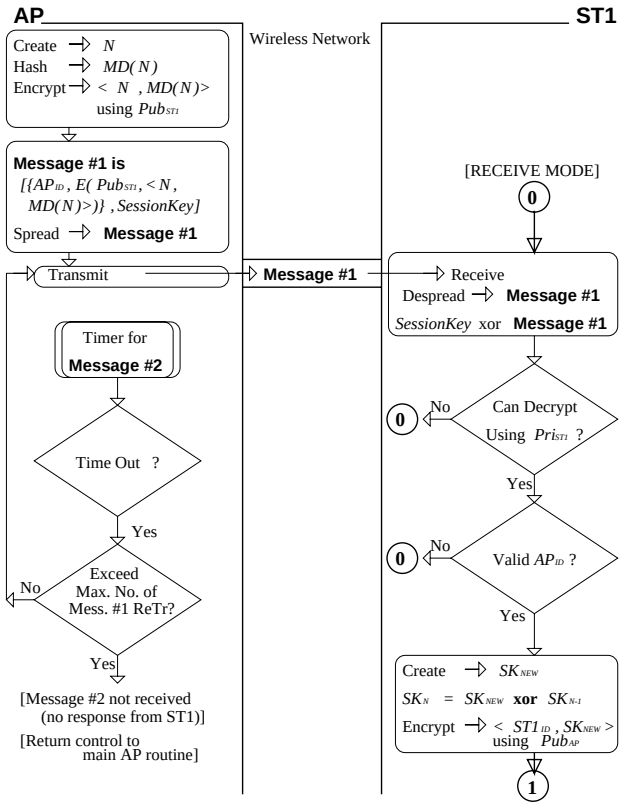
[23] E. Agu, "Data Link Protocols for Wireless Local Area Networks," Master's Thesis, Wireless LAN Lab., UMass, May, 1996.

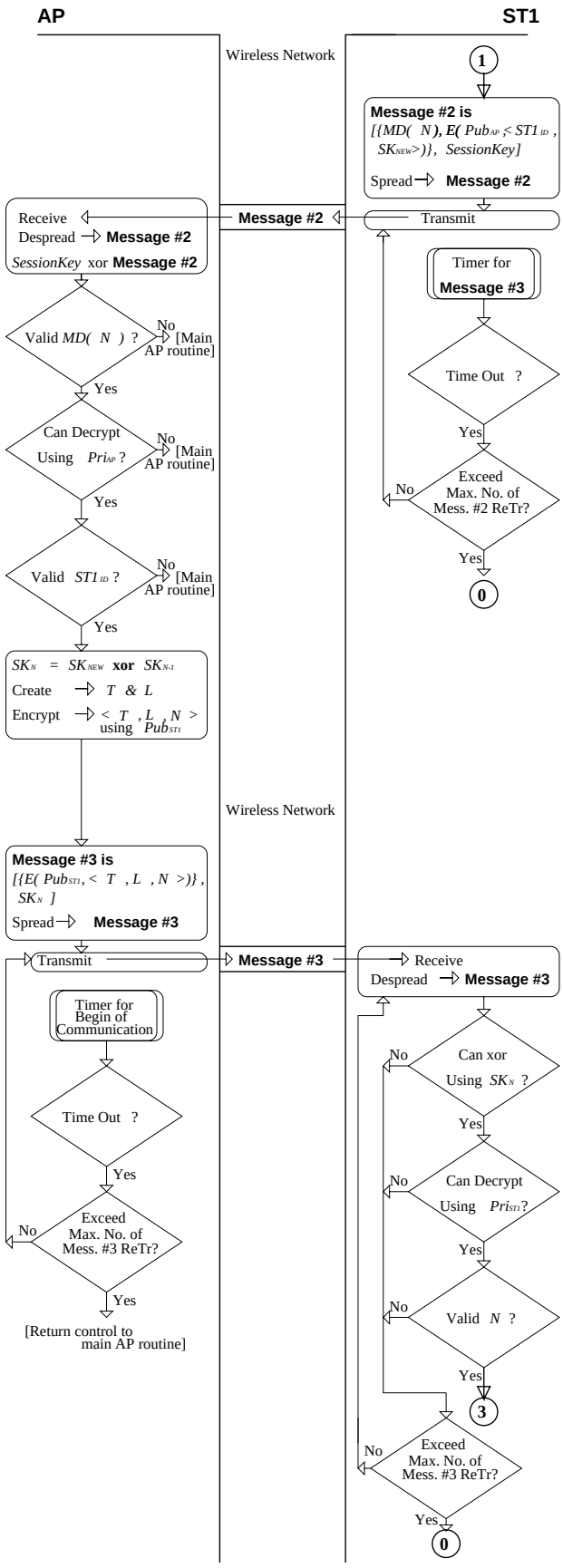
[24] S.H. Park, A. Ganz, and Z. Ganz, "Token-Based Security Protocol for Wireless Local Area Networks," TR-CSE97-1, Technical Report, *Multimedia Wireless LAN Lab.*, UMass, Mar. 1997.

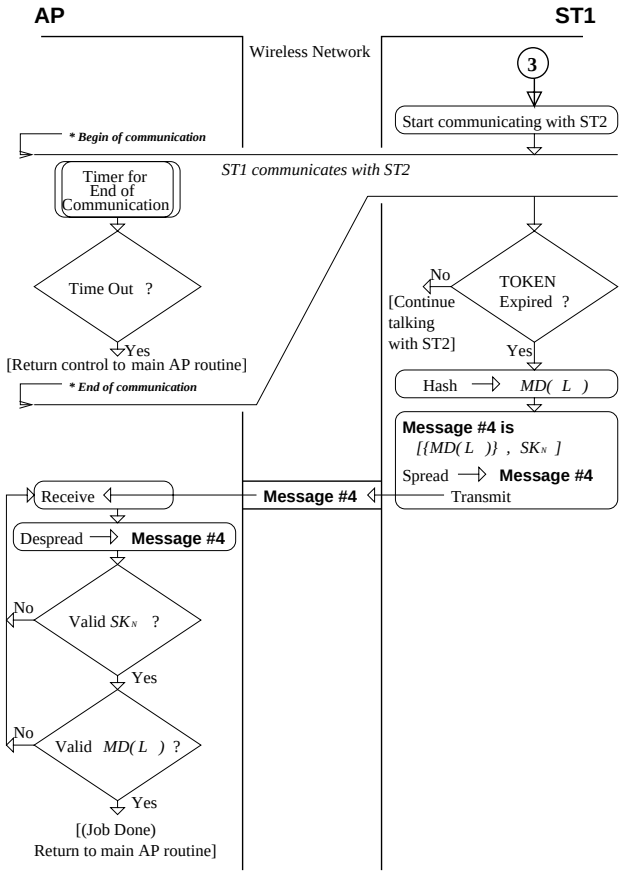
The Flow Chart of Token-Based Security Protocol

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
$E(X, <YYs>)$	: 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 TOKEN is emitted
L	: The life time of the nonce
TOKEN	: (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




AP
ST1
Wireless Network
1
Message #2 is
[{MD(N), E(Pub_AP ,< ST1_ID , SK_NEW >)}, SessionKey]
Spread → Message #2
Receive
Despread → Message #2
SessionKey xor Message #2
Message #2
Transmit
Timer for
Message #3
Valid MD(N) ?
No
[Main AP routine]
Yes
Time Out ?
Yes
Can Decrypt
Using Pri_AP ?
No
[Main AP routine]
Yes
Exceed
Max. No. of
Mess. #2 ReTr?
No
Yes
Valid ST1_ID ?
No
[Main AP routine]
Yes
0
SK_N = SK_NEW xor SK_N-1
Create → T & L
Encrypt → < T , L , N > using Pub_ST1
Wireless Network
Message #3 is
[{E(Pub_ST1, < T , L , N >)}, SK_N]
Spread → Message #3
Transmit
Message #3
Receive
Despread → Message #3
Timer for
Begin of
Communication
Time Out ?
Yes
Exceed
Max. No. of
Mess. #3 ReTr?
No
Yes
[Return control to
main AP routine]
No
Can xor
Using SK_N ?
Yes
No
Can Decrypt
Using Pri_ST1?
Yes
No
Valid N ?
Yes
3
No
Exceed
Max. No. of
Mess. #3 ReTr?
Yes
0


AP
ST1
Wireless Network
3
Start communicating with ST2
* Begin of communication
ST1 communicates with ST2
Timer for End of Communication
Time Out ?
Yes
[Return control to main AP routine]
* End of communication
No
[Continue talking with ST2]
TOKEN Expired ?
Yes
Hash → MD(L)
Message #4 is
[{MD(L)} , SKN]
Spread → Message #4
Transmit
Message #4
Receive
Despread → Message #4
No
Valid SKN ?
Yes
No
Valid MD(L) ?
Yes
[(Job Done)
Return to main AP routine]