# SOLA: A One-bit Identity Authentication Protocol for Access Control in IEEE 802.11


Henric Johnson, Arne Nilsson
Blekinge Institute of Technology
SE-371 79 Karlskrona
Sweden

Judy Fu
Motorola Labs
1301 East Algonquin Rd
Schamburg, IL 60196

S. Felix Wu
UC Davis
One Shields Avenue
Davis, CA 95616

Albert Chen
Integrated System Solution Corp
2F-6, No. 6, Lane 99, Puding Rd
Hsinchu, Taiwan, R.O.C

He Huang
Nortel Networks
4004 E. Davis Drive
RTP, NC 27709



***Abstract*–Given the wide deployment of IPSec/VPN (Virtual Private Networks) technology, there might be a redundancy in security protection in some configurations. Various commercial companies have replaced 802.11 security with IPSec/VPN to protect the wireless LAN (Local Area Network). How to do it in an efficient and lightweight way is a challenging research problem. This paper introduces a new lightweight identity authentication protocol, SOLA (Statistical One-bit Lightweight Authentication), for access control well suited for IEEE 802.11 networks with IP connections. This protocol prevents unauthorized access on a per packet basis. Since SOLA only adds one identity bit to each packet it will have a low impact on the network bandwidth and power consumption. The performance and efficiency of the SOLA protocol together with IEEE 802.11 is analyzed and evaluated via simulation.**


## I. Introduction

For organizations and individuals all future signs point to that every laptop, handheld device, and also desktop PC is connected wirelessly to the corporate network. Wireless connectivity gives the users access to data anywhere and anytime. Today, most of the enterprises are deploying wireless infrastructure based on the IEEE 802.11 standard [8], which offers access to enterprise intranet or Internet data services.

Wireless network access technology raise new concerns when it comes to security and those who manage the wireless network must ensure that new vulnerabilities are not introduced to the corporate network. New challenges arrive when it comes to secure the wireless network and protect it against possible security threats like unauthorized use of the network. However, this threat is also present in traditional LANs, but wireless LANs have significantly concerns caused by uncontrollable signal propagation. This means that potential intruders do not need to be physically located within an enterprise area.

In this paper, a new identity authentication protocol is proposed to detect unauthorized access in 802.11, called SOLA (Statistical One-bit Lightweight Authentication). SOLA is a new option for access control with less identity authentication overhead than in traditional packet authentication mechanism. This is notable since wireless networks have limited bandwidth resources and the challenge for wireless networks is to be both secure and lightweight in bandwidth consumption.

The main idea is to compute an identical random identity authentication stream in the Mobile Station (STA) and the Access Point (AP), and then only add one bit from this stream into the MAC-layer header for identity authentication. Mutual authentication should also be performed since APs are untrusted devices from the STA's point of view. The goals in the design of SOLA are the following:

- *Secure and useful*: an attacker should with low probability be able to gain access to the network.
- *Cheap:* by presenting an optimized one-bit identity authentication method for resource-constrained environments like wireless networks, a cheap and efficient access control procedure is obtained.
- *Robust:* due to lossy channels in wireless communications a synchronization algorithm is required for the generated random authentication streams in the STA and the AP.

The paper is organized as follows: Section II describes the 802.11 access control mechanisms. Section III outlines the related work. In section IV the proposed solution is introduced in an overview and detailed description. Section V gives an evaluation with simulation results of the SOLA protocol and, finally, section VI concludes the paper.

## II. The Ieee 802.11 Access Control Mechanisms

This section specifies three basic methods of securing access to the wireless APs in IEEE 802.11. They are the Wired Equivalent Privacy, Media Access Control Address filtering, and Service Set Identifier. Some of the weaknesses are also described in these access control mechanisms.

### *A. Wired Equivalent Privacy (WEP)*

WEP is specified for encryption and authentication between the STA and the AP and is based on the RC4 encryption algorithm. The 802.11 standard describe two types of authentication services. It is the *Open System Authentication* and the *Shared Key Authentication*.

The 802.11 does not provide a per packet authentication, only encryption using WEP. Thus, packet authentication is optional. However, a series of theoretical and practical attacks against WEP have been published [10, 3].

### B. Media Access Control Address Filtering

Each AP can be configured with a list of MAC addresses that are allowed access to the AP, and the MAC address is associated with a STA. If the STA's MAC address is not in the AP's access list, the AP will deny access. This is a practical security solution if the network is small since the work of manually updating lists of all the MAC addresses limits the scalability of this approach. Unfortunately, MAC addresses are easily sniffed by an eavesdropper since they appear in the clear even when the functionality of WEP is enabled. Also, most of the wireless cards provide the 'service' of changing the MAC address via software, which makes it very easy to spoof a valid MAC address.

### C. Service Set Identifier (SSID)

The SSID allows a network to be divided into multiple networks. In order to be able to access any of these networks, the STA must be configured with the correct SSID identifier. Several management frames contain the SSID identifier, and are broadcasted in the clear by AP or STA. This causes, however, a vulnerability to the network since an attacker can easily sniff the SSID and use it in order to gain access to the protected network. Therefore, there is need for a secure lightweight packet identity authentication mechanism.

## III. Related Work

IEEE has been motivated to work on standards that focus on restricted access. IEEE 802.11 Task Group I is specifying a Robust Security Network (RSN) to address security issues with infamous WEP encryption as well as WEP based authentication. IEEE 802.1x port-based access control [6] is used and extended in RSN to conduct mutual authentication. In the 802.1X standard, no specific protocol for authentication is specified. Instead, it specifies that the Extensible Authentication Protocol (EAP), standardized by IETF in Request For Comments (RFC) 2284 [4], will be used. Another form of the EAP protocol is the Lightweight Extensible Authentication protocol (LEAP). Temporary Key Initiation Protocol (TKIP) and Advanced Encryption Standard (AES) are defined to perform packet-based encryption and authentication. The defined encapsulation process with TKIP or AES has expanded original MAC Service Data Unit (MSDU) by 12 bytes, 4 for replay counter field, and 8 for the Message Integrity Check (MIC). Compared to these methods, SOLA achieves access control in a lightweight way by introducing one bit per packet for identity authentication.

Canetti et al., describe a scheme with a low communication overhead [5] similar to SOLA. They consider a Message Authentication Code with a single bit output that is ½-per-message unforgeable, and the scheme uses a MAC with a single bit output from current constructions of MACs.

The IPSec/VPN solution is becoming very popular. It is, for instance, available in Windows 2000, Windows XP operating system [1], and Linux/FreeBSD. The combination of IPSec/VPN and 802.11 is widely used and some commercial companies (e.g., Reefedge) have replaced 802.11 security with IPSec to protect the wireless LAN. Two key RFCs for overall IP security and for the IPSec protocol suite are RFC 2401 [7], and RFC 2411 [9]. In IPSec, the total length of an Authentication Header is 24 bytes (192 bits). If attached to every packet the Authentication Header constitutes a relatively big load of bits over the radio link as compared to the one-bit SOLA protocol, even though SOLA provides identity authentication at the MAC layer.

## IV. Contribution

This section demonstrates SOLA, the proposed identity authentication protocol for access control in 802.11. A brief overview is given followed by a more detailed description of the implementation.

### A. SOLA Overview

By introducing SOLA one will get a robust lightweight one-bit identity authentication protocol without the need for expensive authentication mechanisms. As mentioned earlier, VPNs are used to provide protection for areas where current 802.11 solutions are weak. Unless some strong authentication mechanisms (such as IPSec AH/ESP, WEP or AES+OCB in IEEE 802.11 Task Group I, all of which are somewhat expensive) are used to protect the "data packets", we have no assurance generally about whether some "malicious" neighbors are impersonating a non-malicious user. On the other hand, if strong authentication is used between the STA and the AP, the user's data packets might be authenticated (unnecessarily) twice: one time between STA and AP, and second between STA and CH (Correspondent Host), as shown in Fig 1. The combined solution of WEP and IPSec is a drawback in a constrained wireless environment since both WEP and IPSec are used simultaneously over the radio link. However, it is most common that an IPSec/VPN tunnel is used to protect the traffic without any encryption or authentication at the link layer. Therefore, to still be able to obtain access control, a new option is presented at the link layer for per packet identity authentication. Unlike a traditional packet verification mechanism, the decision is

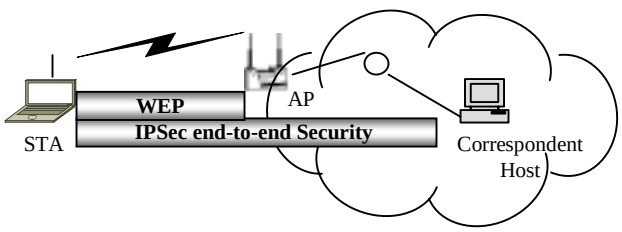


Fig 1. WEP and IPSec/VPN solution in an 802.11 network.

made on per packet basis, SOLA determines legitimacy of a series of packets. Ideally, since the attacker does not have the right key, the probability for the attacker to guess continuously n bits correctly is as small as $2^{-n}$. With the SOLA algorithm there is only one bit for identity authentication, which greatly reduces bandwidth overhead and thus preserves the scarce wireless bandwidth resource without compromising security. An attacker cannot steal service or launch attack with fake addresses by bypassing identity authentication without being detected.

Both the STA and the AP will have a module called the Authentication Stream Generator (ASG), which will generate a particular random bit stream. Only one bit is added to each transmitted packet from the STA to the AP for the outbound traffic. Normally, without any packet loss or security attacks, each bit will be used once, and a new bit will be used for each new packet.

The 802.11 standard only offers a weak one-way authentication. The trust assumption that is reflected from this design is that the APs are trusted devices, which might be a misjudgment. Therefore, it is strongly recommended that the SOLA protocol should be used in a bi-directional way.

SOLA offers the following nice properties:

- *Originator Sender Identity Authentication:* If the authentication bit is verified correctly, the receiver has a statistical assurance that the packet originated from the claimed sender. This also includes data freshness and replay protection.
- *Low Communication Overhead*: Only one bit is added to each packet for identity authentication.

### *B. SOLA Implementation*

Due to the nature of wireless communication with unreliable communication links, the implementation of the SOLA protocol is a major challenge. Therefore, the bit stream synchronization between the AP and the STA is critical because, in a wireless and insecure network environment, packets might get lost or tampered unintentionally or even intentionally. Bits can also become corrupted because of noise. SOLA introduces a synchronization algorithm to handle the wireless lossy environment. Thus, one of the goals is to provide a secure and robust solution.

The SOLA protocol has multiple phases and will be described with the following key words: ASG, packet format, and synchronization algorithm.

**ASG:** Technically, any secure random bit generator can be used as an Authentication Stream Generator. The purpose is to generate an authentication stream that cannot be guessed by an attacker. In the design it is assumed that the STA and the AP will share a session key provided from the connection setup. Based on this session key the random authentication stream is generated from the ASG. A practicable implementation of the ASG, which is used in our simulations, is to apply a device similar to the encryption engine in the Bluetooth specification [2].

**Packet Format:** One important issue in SOLA is about where in the packet to insert this new identification bit. It can be in either MAC or IP header, and it really depends on the standardization groups such as IEEE or IETF to make the final decision. In the following description, it is assumed that it is embedded in the IEEE 802.11 MAC header.

The 802.11 standard [1] specifies an overall MAC packet format. The one bit for identity authentication will be inserted in the data packet and the "failed" or "success" bit, from the AP to the STA, will be inserted in the response acknowledgement packet. In the simulations we are currently using the most significant bit in the sequence control field for the data packet and the most significant bit in the duration field for the ACK packet.

**Synchronization Algorithm:** Conceptually, both the STA and the AP has a pointer pointing to the bit for the next outgoing packet. Ideally, both the STA and the AP will have their pointers pointing at exactly the same bit and advance synchronously. However, due to packet loss and other failures or noise, it is almost certain that the bit pointers between the STA and the AP not will be synchronized. We then weaken the synchronous condition a little: STA's bit pointer must be equal with or behind the pointer of AP in bit advancing (i.e., continue to the next bit in the random authentication stream). In the analysis and fault tolerance section, we show how to guarantee this condition to be true in the protocol, and how to re-synchronize once the STA is indeed behind the AP.

*Analysis:* this section describes the analysis part of the synchronization algorithm.

**Lemma 1.1.** If the STA advances regularly then the AP must have advanced. Since the STA will not advance unless it receives the acknowledge (ACK) packet together with the result of the verification of the authentication bit, i.e., "failed" or "success".

**Lemma 1.2.** If the STA advances to the next opposite bit (the opposite bit is the next bit in the authentication stream with an opposite value of the current bit), it will not advance more than the AP.

Lemma 1.2 is proved by contradiction. Assume that the bits can be represented as an array $Bit[\gamma]$. STA is currently using $Bit[\alpha]$, while the AP is currently using $Bit[\beta]$. Before the failure, $\beta$ is greater than or equal to $\alpha$. Assume that $Bit[\alpha]$ is not equal to $Bit[\beta]$, and that the AP will issue a failed verification of the authentication bit, at the same time as it increases $\beta$ to opposite bit + 1. Assume also that $Bit[\alpha+\delta]$ is equal to $Bit[\beta]$, where $\delta$ is the minimal. It is now easy to see that $\alpha+\delta$ is equal to or less than $\beta$. Otherwise $\delta$ is not minimal. Therefore, we have $\alpha+\delta+1$ less or equal to $\beta+1$.

*Fault Tolerance:* If no message gets lost, $\beta$ is equal to $\alpha$ and therefore $Bit[\alpha]$ is equal to $Bit[\beta]$. Any loss of a packet will result in $\alpha$ less than or equal to $\beta$. But the next packet will be "failed" by the AP while the STA can re-transmit. If packet is "failed", the AP will increase $\beta$ to opposite bit + 1. If the STA did not receive the AP's ACK packet it will use the same bit $Bit[\alpha]$ for the retransmission and it will not advance (i.e.,

increase the value of $\alpha$). Eventually, it should receive an ACK packet from the AP and find out about the failure and also increase $\alpha$ to opposite bit + 1. In any case, it is safer to stay at the same bit unless the STA heard the ACK message from the AP. The synchronization algorithms explained above can partially be described with the following pseudo code:

```
Algorithm for AP
1.  // AP receives data packet with Bit[α]
2.      if Bit[α] == Bit[β] then
3.          β++
4.          AP → STA: Packet{ACK, success}
5.      else if Bit[α] ≠  Bit[β] then
6.          β = β + opposite bit + 1
7.          AP → STA: Packet{ACK, failed}
End Of Algorithm

Algorithm for STA
1. //   STA receives ACK packet with success or
        failed bit from STA
2.      if bit == success then
3.          α++
4.      else if bit == failed then
5.          α = α + opposite bit + 1
End Of Algorithm
```

The IEEE 802.11 MAC header contains a sequence number (also a fragment number). However, this sequence number is not possible to use for synchronization. The reason is that the bits in the authentication stream must advance regularly to the next bit in the identity authentication stream. In the case of retransmission of packets the sequence number in the IEEE 802.11 MAC header remains constant, and will not contribute to any advancement in the identity authentication stream.

A concern is if the authentication bit is corrupted by noise. This could result in the fact that the STA's bit pointer is not equal with or behind the pointer of AP in bit advancing. To solve this problem four different solutions are proposed:

1. Rely on the 4 bytes Frame Check Sequence (FCS) in the 802.11 standard to check for transmission errors in the packet.
2. Apply the proposed synchronization algorithm but achieve redundancy by placing the one-bit in different locations of the packet. The receiving station now has higher probability to decide the value of the received bit.
3. Apply the proposed synchronization algorithm but divide the authentication stream into window segment of length $N$. Then allocate $\log_2 N$ bits in the packet for bit positioning of the bit-pointer in the window. For instance, if $N$ is equal to 8 we need 3 bits in the packet for bit positioning of the bit pointer.
4. In the extreme case when the two authentication streams cannot be synchronized one have to re-negotiate a new session key and compute new identity authentication streams. The decision of re-negotiation could be based on factors like the number of incorrect identity authentication bits due to packet loss, synchronization performance, or an attack.

## V. EVALUATION

This section discusses the synchronization algorithm evaluation and the security evaluation. All the simulations have been implemented under the ns-2 environment. The simulations have been carefully chosen to be realistic in order to illustrate the behavior and performance of the SOLA protocol. In the simulations a session is established between two mobile devices with TCP data sources and an FTP application on top for traffic generation. To simulate an ASG, a device similar to the encryption engine in the Bluetooth specification [2] is implemented. Furthermore, the MAC protocol used in the simulations is IEEE 802.11.

### *A. Synchronization Algorithm Evaluation*

The performance of the synchronization algorithm is evaluated in terms of failure rate, duration, and drop probability for acknowledgement (ACK) packet only. The number of failed packets (packets in which the identification bit is wrong) is recorded and summed up. Then, the failure rate is derived by the ratio between the total number of "failed" packets and the total number of "checked" packets. The duration is the value of the successive numbers of dropped acknowledgement packets. That is if one drops an acknowledgement packet the coming acknowledgement packets after that one will also be dropped, and the number of successive dropped packets depends on the duration value. By increasing the duration value one will stress the synchronization algorithm. In the simulations the duration value differs from 1 to 6.

As shown in Fig 2, the synchronization algorithm resynchronizes without any problems, even when the duration and the dropping probability for the acknowledgement packets increase. The highest failure rate is 50 % and this is due to the randomness of the identification bit generated by the ASG. All this demonstrates that the algorithm has high robustness, which was one of the major goals in the design of the SOLA protocol.

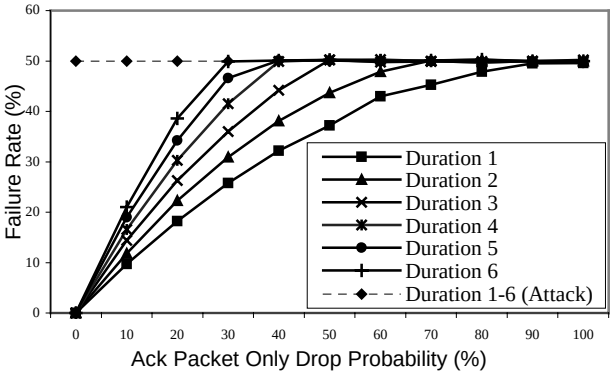


Fig 2. The failure rate vs. the drop probability and duration for ACK packets only. The dotted line is an attack in which the adversary guesses the identity authentication bit.

### B. The Security Evaluation

While attacks on the network access might not occur very often, it is necessary to have a framework to detect and respond to this problem when it does happen. However, the SOLA protocol major purpose is to detect an attack, and it offers a statistical way to "identify" the origin of the packets for the purpose of access control. In this section, fault/intrusion detection and response is discussed for four possible attacks: *Denial-of-Service* attack, *overwrite* attack, *Man-in-Middle* attack, and *guessing the identity authentication bit* attack.

A *Denial-of-Service* attack from an adversary could, for instance, be launched by the transmission of "failed" acknowledgement packet even if the data packet with corresponding identity bit was correctly received. The goal for the attacker is to corrupt the identity authentication bit synchronization between the STA and the AP. This type of attack is easy to detect by the nature of the SOLA protocol since the failure rate will increase to an abnormal value. The fault/intrusion detection and response to this attack would be to set a failure rate threshold, and if a user's profile does exceed the threshold then try to re-establish its connection to make sure that the shared key is synchronized. If this will not help, then one should suspect an ongoing attack and if necessary turn on a less lightweight access control method like IPSec or locally investigate the source of the problem. Interesting is that by only adding one bit to each packet it is possible to detect the *Denial-of-Service* attack of this kind, and then one might use a method (like IPSec) that requires more computational power to defend against the attack.

An "*overwrite*" attack is an attack in which the adversary "overwrites" the content in a packet with a very high power signal, something which we believe is very hard to do. In such an attack, the identity authentication bit remains the same but the payload or header contains new data. In this scenario the SOLA protocol do not detect the attack. If one believes that this attack is possible to obtain then IPSec could be used with the authentication option, and the end user will detect the malicious content in the payload or header. Similarly, an adversary who receives a packet with the identity authentication bit, and modifies the content and not the identity authentication bit in the payload or header field, could launch a *Man-in-Middle* attack. The goal of the adversary with these attacks could, for instance, be to steal bandwidth from another STA. If someone tries to steal the bandwidth, by a *Man-in-Middle* attack, the attacked STA will not advance in the identity authentication stream and send new TCP data packets due to the nature of the absence of TCP response packets. Therefore, a *Man-in-Middle* attack of this kind would not succeed against the SOLA protocol.

A "*guessing the identity authentication bit*" attack is an attack in which an adversary tries to obtain access to the secure network by guessing the identity authentication bit for each successive packet. Also, in this case the SOLA protocol will detect the attack and, as shown in Fig 2, an adversary who tries to guess the identity authentication bit will cause a failure rate of 50 % for all values of the acknowledgement packet drop probability. Similar to the *Denial-of-Service* attack, a threshold for the failure rate could be set in order to determine if it is an attack or not. This is done so as to be able to decide whether the failure rate of the authentication bit follows the normal packet loss behavior or not. In the case in which an adversary does not try to guess all successive packets but instead a few packets at the time, the failure rate will be less than 50 %. Therefore, a failure rate threshold with a lower value than 50 % needs to be set. The response of this statistical access control method from the AP would be not to grant access to the secure network.

## VI. Conclusion

In this paper, a lightweight protocol for access control in IEEE 802.11 networks has been presented. The proposed SOLA protocol inserts an identity authentication bit from a stream known only to the two communicating stations. Any secure random bit generator could generate the identity authentication bit. The challenge has been the synchronization between the two end points due to a lossy and shared wireless channel. Therefore, a synchronization algorithm has been given to handle packet loss and simulation results were presented to evaluate the synchronization behavior and show the robustness of the algorithm.

Finally, the SOLA protocol is well suited in a wireless constrained environment since the communication overhead for the protocol is low: only one bit. Furthermore, it is possible to develop a framework to detect, for instance, *Denial-of-Service* attacks or an adversary who tries to attack the secure and protected network by guessing the identity authentication bit for successive packets.

## References


[1] A. Ayyagari and T. Fout. *Making IEEE 802.11 Networks Enterprise-ready*. Whitepaper, Microsoft Corporation, May 2001.

[2] Bluetooth, The Bluetooth Specification, v.1.0B, November 1999.

[3] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11."

[4] L. Blunk and J. Vollbrecht. *PPP Extensible Authentication Protocol (EAP).* RFC 2284, March 1998.

[5] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, *Multicast Security: A Taxanomy and Some Efficient Constructions*, 1999.

[6] Institute of Electrical and Electronics Engineers (IEEE). *Standard for port based Network Access Control*. IEEE Draft P802.1X/D11, March 2001.

[7] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, Nov. 1998.

[8] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE Standard 802.11, 1997 Edition," 1997.

[9] R. Thayer, N. Doraswamy, R. Glenn, IP Security Document Road Map, RFC 2411, Nov. 1998.

[10] J. Walker, "Unsafe at any key size: an analysis of the WEP encapsulation, " Tech. Rep. 03628E, IEEE 802.11 committee, March 2000.