A Lightweight Statistical Authentication Protocol for Access Control in Wireless LANs

Haoli Wang, Joel Cardo, Yong Guan

ECE, Iowa State University

ASWN 2004

Introduction

- Emergence of visitor networks
  - Visitor Networks:
    - LANs that are most often deployed in *public* places and enable the public network access on an ad-hoc basis.
    - ISPs desires *user authentication* before granting the right to access Internet and then *charges* users accordingly.
- Traditional authentication protocols for wired networks do not work well in wireless
    - error-prone wireless transmission medium, node mobility, power conservation constraints
  - Current wireless authentication protocol, such as WEP, has some security flaws.
- Dilemma in wireless security
  - Vulnerable wireless networks need strong security protocols, resulting in enormous power consumption.

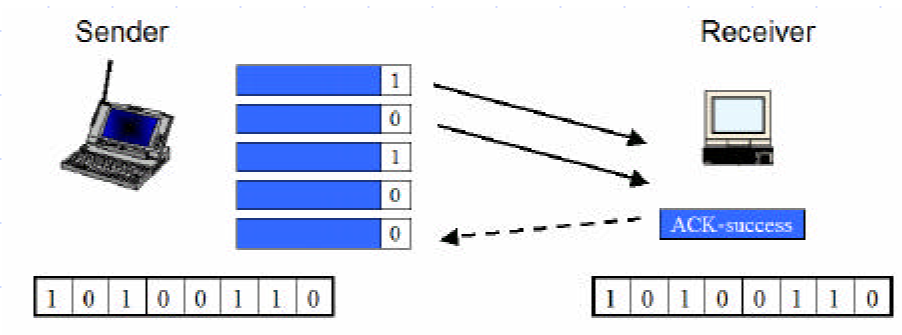
Shepherd Overview

- Design goals
  - ***Secure***: An attacker should be able to gain the access to the network only with a very low probability.
  - ***Robust****:* The protocol must effectively resist the attacks and the unexpected situations.
  - ***Efficient****:* The protocol must be efficient in term of overhead, bandwidth and CPU cycles.
  - ***Detectable***: If the attacker tries to gain the access to the network, the protocol will be able to detect it.

- Characteristics
  - ***Lightweight***: good for power conservation
  - ***Probabilistic method***: good for node mobility and error-prone channel

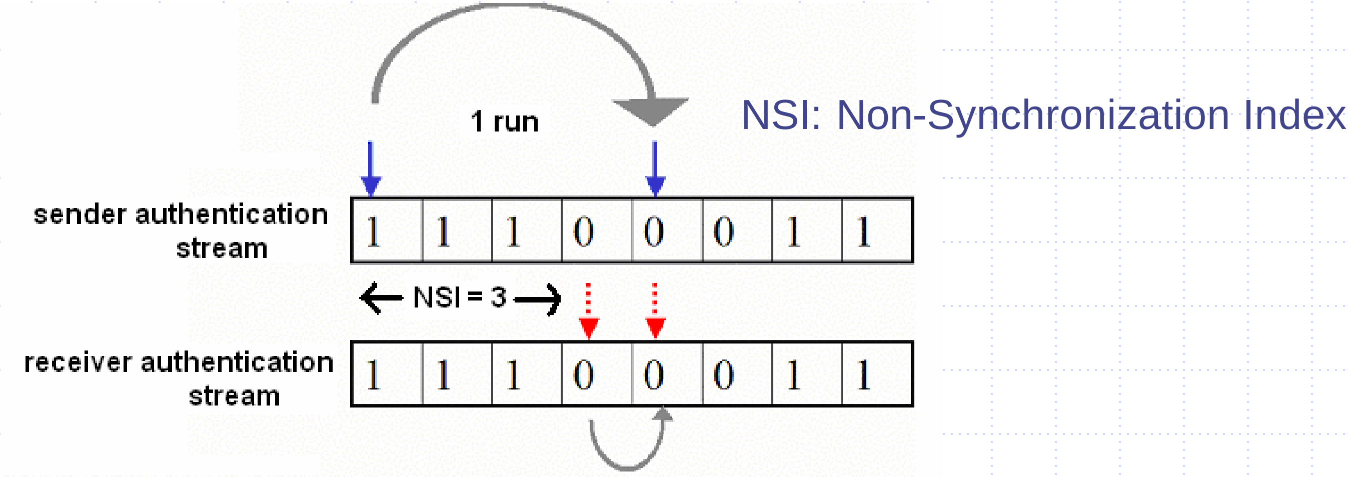
Shepherd

- How Shepherd works
  - AP and MN generate authentication bit streams by the same random number generator under the same shared seed as a key.
  - Authentication bit is piggybacked in exchanged frame from MN to AP.
  - AP determines the legitimacy of MN by continuously checking a series of randomly generated authentication bits.
- Unsynchronization Problem
  - Frame loss may cause UnSync problem between AP and MN.
  - UnSync problem leads to check error at AP.



Sync Scheme 1

- Receiver's pointer always moves forward one step after replying DATA frame.
- Sender's pointer moves after receiving ACK(+/-)
  - ACK+: move forward one step
  - ACK- : move forward to "opposite bit" + 1

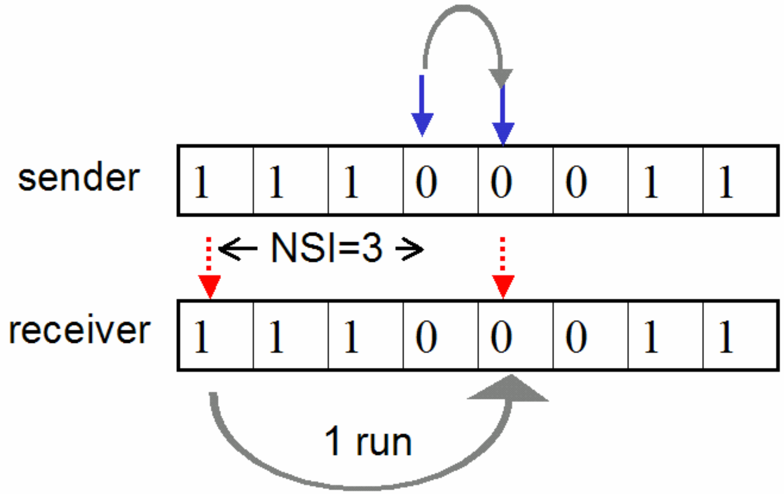


+: Loss of ACK frame causes non-sync problem.

- : Sender is aware of the checking results.

Sync Scheme 2

- Sender's pointer always moves forward one step after sending DATA
- Receiver's pointer moves after replying DATA frame.
  - If checking bit correct, move forward one step
  - If checking bit uncorrected, move forward to "opposite bit" + 1

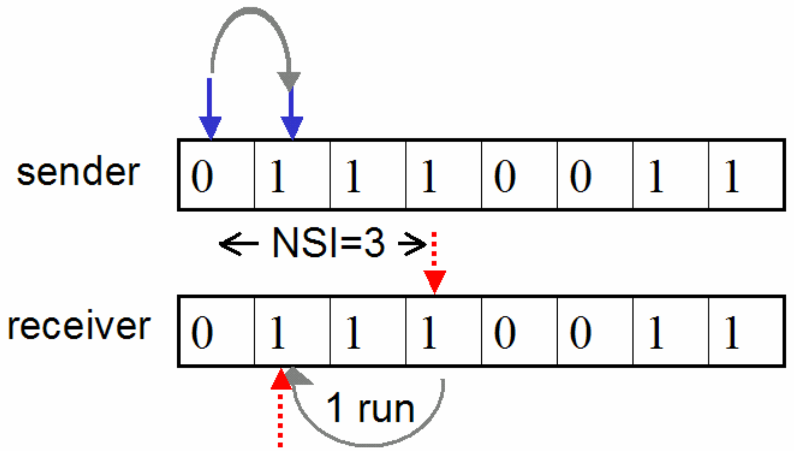


+: Sender is *unaware* of the checking results.

-: Loss of DATA frame causes non-sync problem.

Sync Scheme 3

- Sender's pointer always moves forward one step after sending DATA
- Receiver's pointer moves after replying DATA frame.
  - If checking bit correct, move forward one step
  - If checking bit uncorrected, move back to "opposite bit" + 1



+: Loss of ACK frame causes non-sync problem.

Sender is *unaware* of the checking results.

-: Some bits may be reused.

Statistical Method

- In scheme 1, The probability of this mobile station *H* being a legitimate one can be derived by

$$Pr(H = legal|w, s) = \frac{\delta^s(1-\delta)^{w-s}}{2^{-w} + \delta^s(1-\delta)^{w-s}} \quad (1)$$

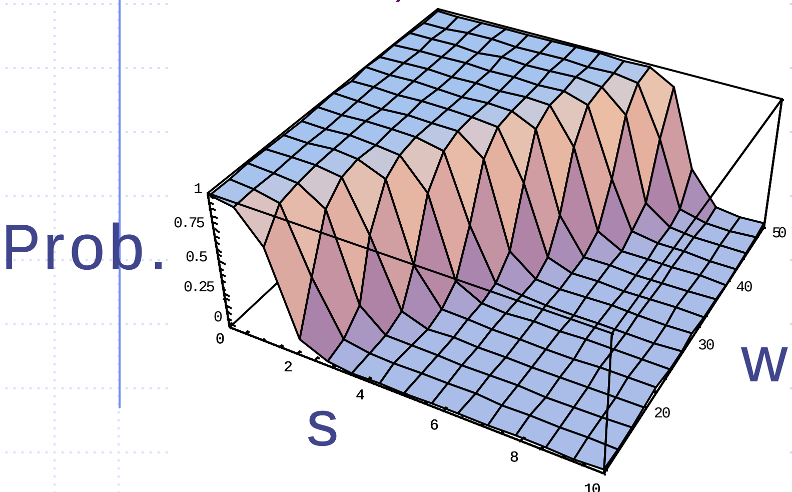
where δ is the average authentication bit error rate and calculated as

$$\delta = \sum_{i=1}^{G}[(L_{ACK} \times BER)^i \times \frac{i+1}{2}] \quad (2)$$

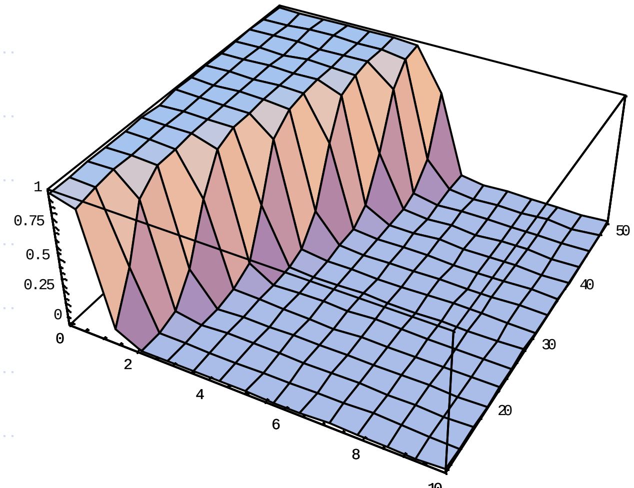
s: number of syncs
w: number of checks
G: Max number of consecutive frame losses
L_{ACK}:ACK frame length

Numerical Analysis Results

Scheme 1, BER=10^{-4}

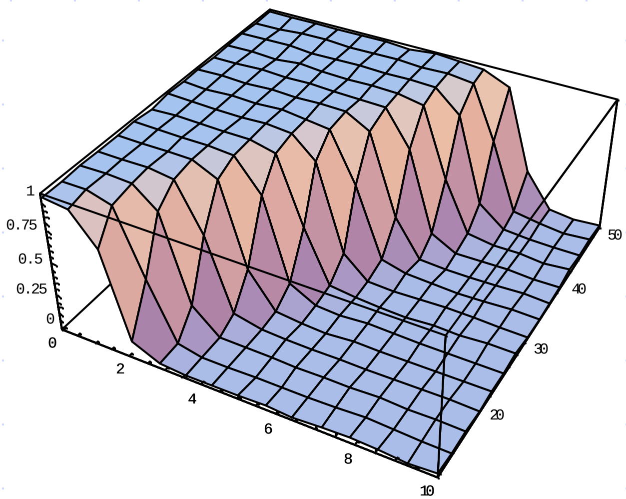


Scheme 1, BER=10^{-5}

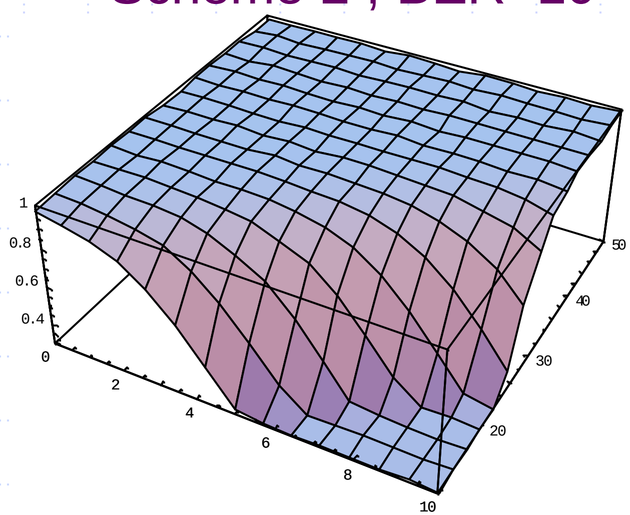


Shepherd works better with lower BER.

Scheme 3 , BER=10^{-4}

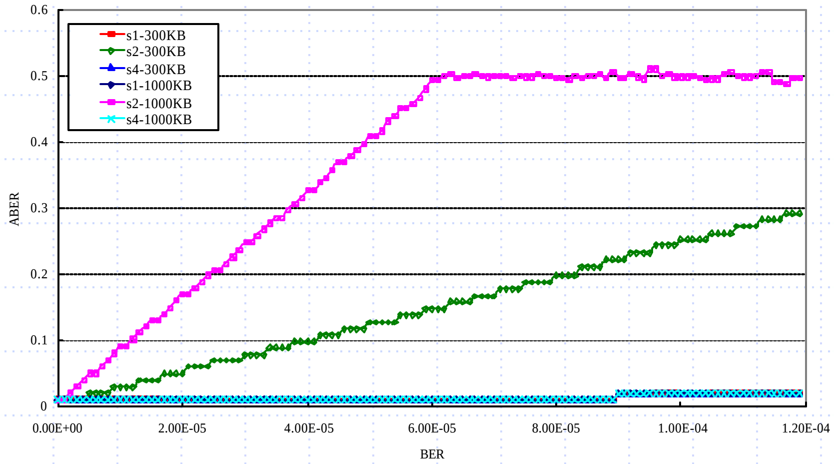


Scheme 2 , BER=10^{-4}

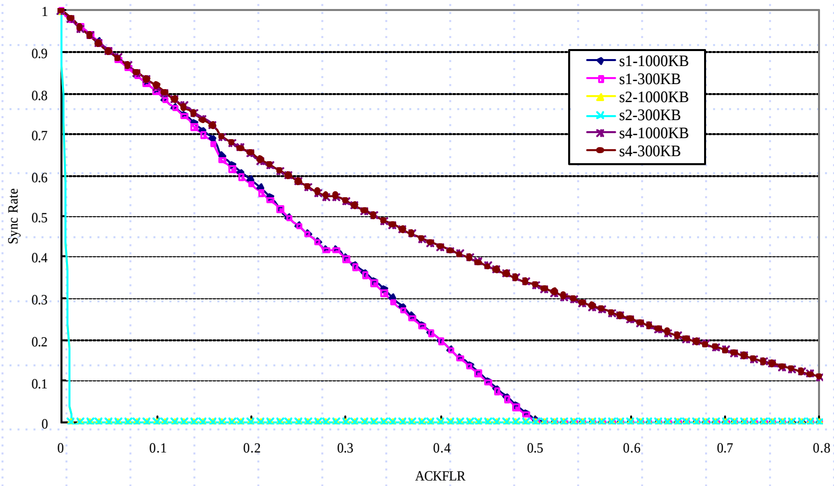


Scheme 3 excels among 3 schemes.

Simulation Results



1. For a legal node, authentication bit error rate increases with increasing BER.
2. A good scheme is able to increase slowly with increasing BER.
3. Scheme 2 increases quickly. Scheme 3 increase slower than scheme 1.



1. For a legal node, Sync rate drops with increasing FLR.
2. A good scheme is able to drop slowly with with increasing FLR.
3. Scheme 2 drops quickly. Scheme 3 drops slower than scheme 1.

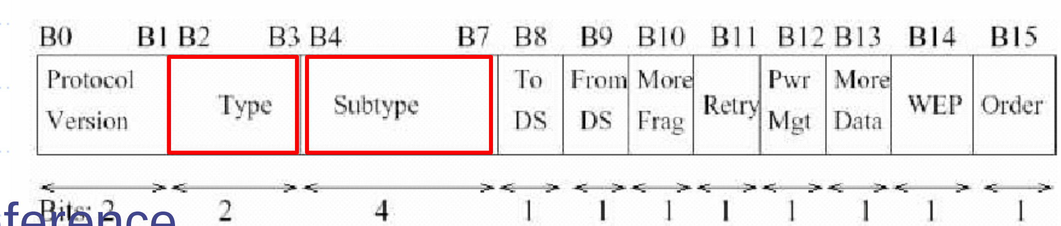
Comparison

	Shepherd	SOLA	RBWA
Random bit	V	V	V
UnSync Problem	V	V	
Algorithm Workable	V		

- RBWA uses the sequence number in each IP packet to avoid sync problem, but we argue that SN is not reliable.
- A problem exists in the sync algorithm in SOLA.

Summary

- A lightweight probabilistic authentication protocol is proposed for wireless networks.
  - Three synchronization schemes for UnSync Problem.
- Implementation Consideration
  - Type and subtype fields are adapted from IEEE 802.11.



Frame Control Field

- Reference

  - H. Wang, A. Velayutham and Y. Guan, A Lightwight Authentication Protocol for Acess Control in IEEE 802.11, IEEE GLOBECOM, 2003
  - H. Wang, J. Cardo and Y. Guan, Shepherd: A Lightweight Probablistical Authentication Protocol for Wireless Networks, in submssion.

Thank You