Fast Initial Authentication

Authors:

Date: 2010-03-17

Name	Company	Address	Phone	email
Hiroshi MANO	ROOT Inc.	8F TOC2 Bldg. 7-21-11 Nishi-Gotanda, Shinagawa-ku, Tokyo 141-0031 JAPAN	+81-3-5719-7630	hmano@root-hq.com
Hitoshi MORIOKA	ROOT Inc.	#33 Ito Bldg. 2-14-38 Tenjin, Chuo-ku, Fukuoka 810-0001 JAPAN	+81-92-771-7630	hmorioka@root-hq.com
Paul A Lambert	Marvell	Marvel lane, MS 2-201 Santa Clara, CA 95054	+1-408-222-9522	paul@marvell.com
Marc Emmelmann	TU Berlin	Einsteinufer 25 10587 Berlin Germany	+49-30-314 24580	emmelmann@ieee.org
Hiroki Nakano	Trans New Technology	Sumitomo-Seimei Kyoto Bldg. 8F, 62 Tukiboko-cho Shimogyo-ku, Kyoto 600-8492 JAPAN	+81-75-213-1200	cas.nakano@gmail.com cas@trans-nt.com
Mineo Takai	Space Time Engineering	609 Deep Valley Drive, Suite 200 Rolling Hills Estates, CA 90274, USA	+1-310-265-4441	mineo@ieee.org

Agenda

- Motivation and background of proposal
- Prospect of use case
- Feasibility with existing standard
- Problems with existing Standard
- Next step
- Motion

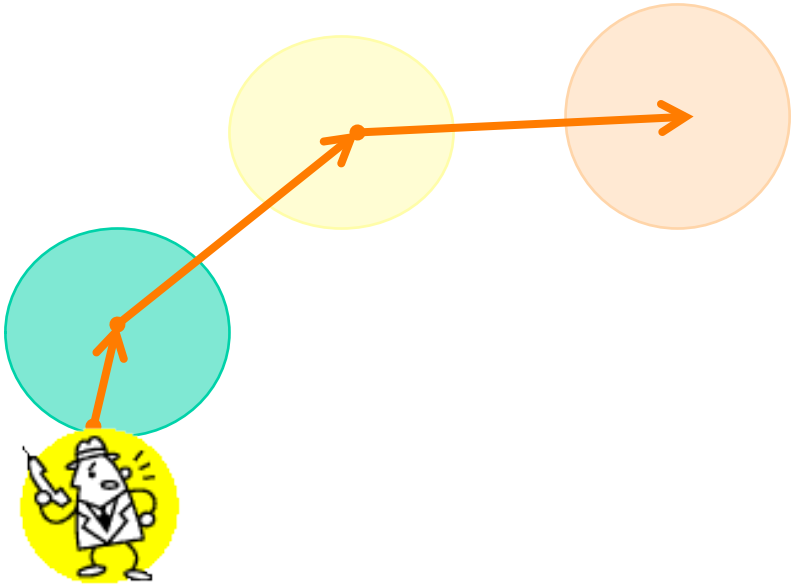
Limitation of market growth in the existing 802.11

- **IEEE802.11 evolved greatly for the past ten years and got big success in a market**
  - Bandwidth :
    - 11/2Mbps →11b/11Mbps→11g/54Mbps →11n/300Mbps
  - Securities :
    - WEP->WPA->WPA2
  - Service device
    - Desktop PC → Note Book → PDA → Portable game, Digital Camera → Hybrid cell phone.

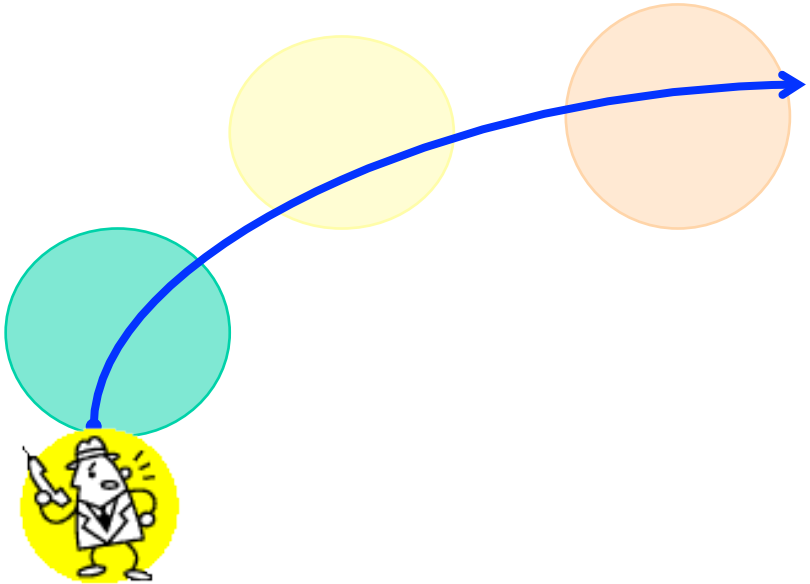
- **However**
  - We are still in nomadic services.

Nomadic Vs Mobile

- **Nomadic**
- **STA must be stationary while in use.**



- **Mobile**
- **STA do not need stop while in use.**



Reference :RECOMMENDATION ITU-R F.1399-1
"Vocabulary of terms for wireless access" MWA & NWA

Today's market back ground

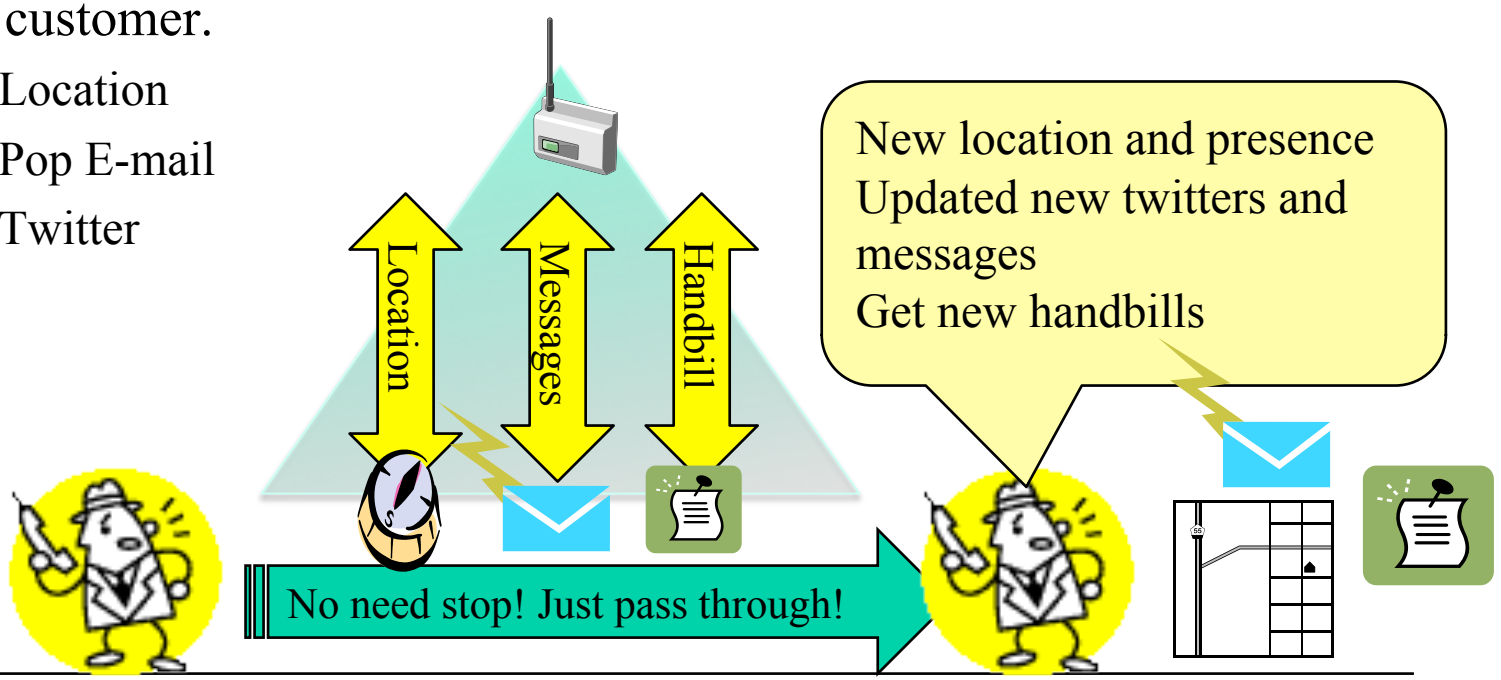
- Growth of portable device
  - Number of portable device which incorporate Wi-Fi is more than PC's
  - Low power consumption device realized the use of the always-on connection type service.
- New application's request (Twitter, Face book…)
  - Push Notification Service
  - Quick update
    - Only cell phone provide these service
- Highly bandwidth
  - Very SMALL CELL of each AP
- True mobile usage
  - Users frequently pass through (isolated) hot spots while on the move

➔ The dwell time of a user within a cell is short

➔ Isolated hot spots cause frequent initial association / authentication

Prospect of use case 1

- **Quick update contents and push service.**
  - New messages and location data are updated while just passing an AP‘s coverage.
  - So you do not have to stop many times like serious landing operation.
  - Service provider can distribute the handbill without stopping the foot of the customer.
    - Location
    - Pop E-mail
    - Twitter



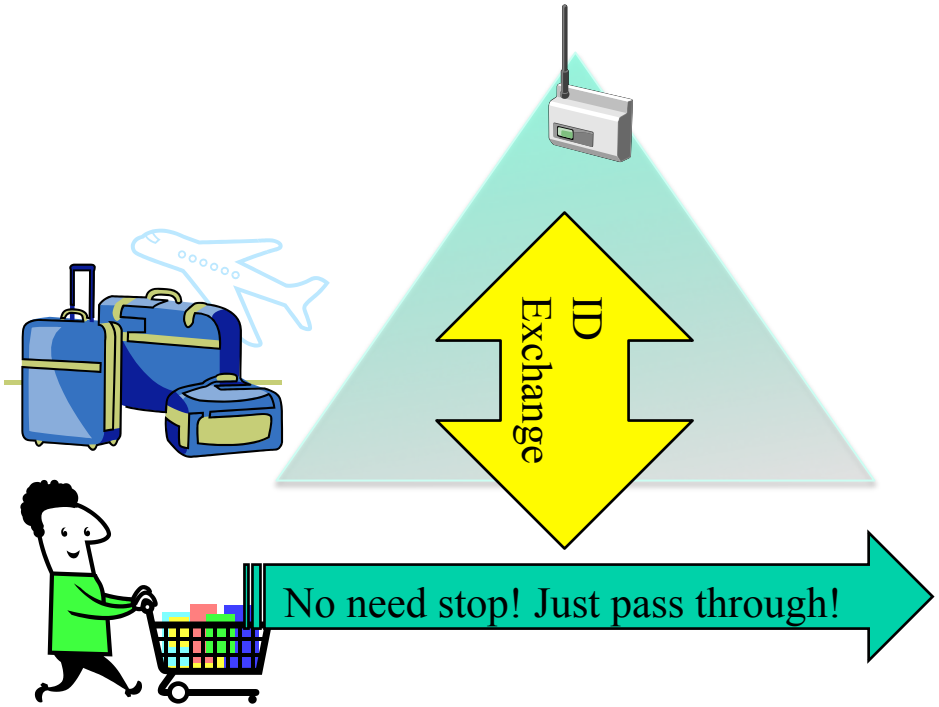
Prospect of use case 2

RF Tag application

- **Automatic Electrical Cash Register**
- **Security Gate**

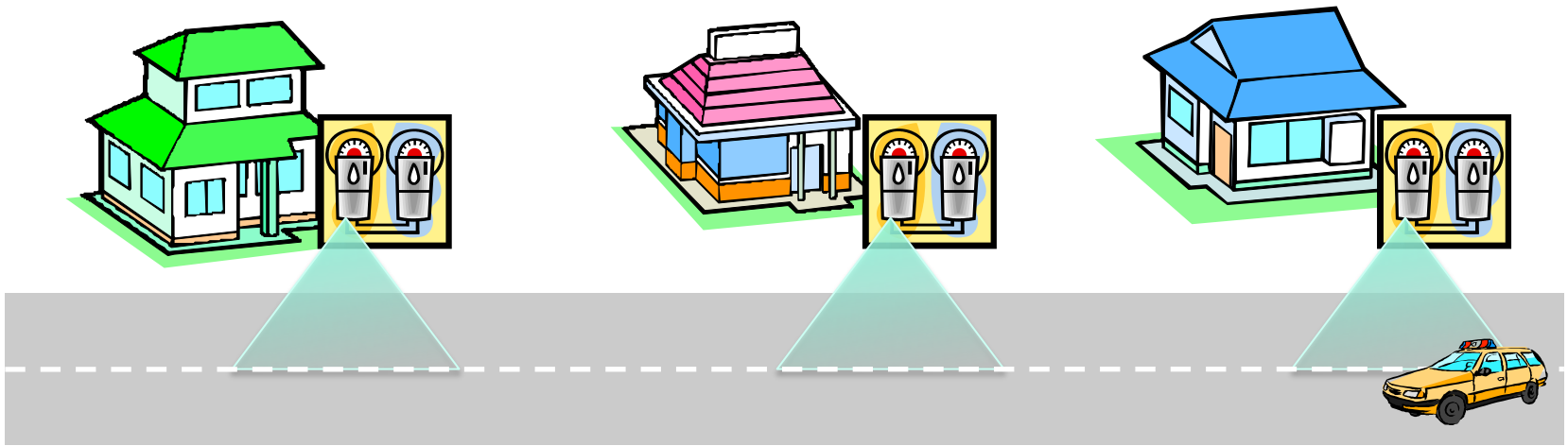
Digital Signage + Info Stand

Distribute information



Prospect of use case 3

- **Automatic metering**
  - Power electric
  - Water meter
  - Gas meter
  - etc..



What is feasible today with existing standard?

Network Discovery ✔

= **Scanning and other means**

- Goal: Find other BSSs in reach
- Active / passive scanning
  → not mandatory for network discovery but only for synchronizing TSF timer
- Implicit knowledge (11k neighborhood reports) in combination with localization
- Existing approaches e.g. background scanning can reduce the delay to tens of ms

→ **Associated delay theoretically not noticeable if we can avoid requiring synchronization of TSF timer before authentication / association**

Upper Layer Aspects

→ Out of scope for .11

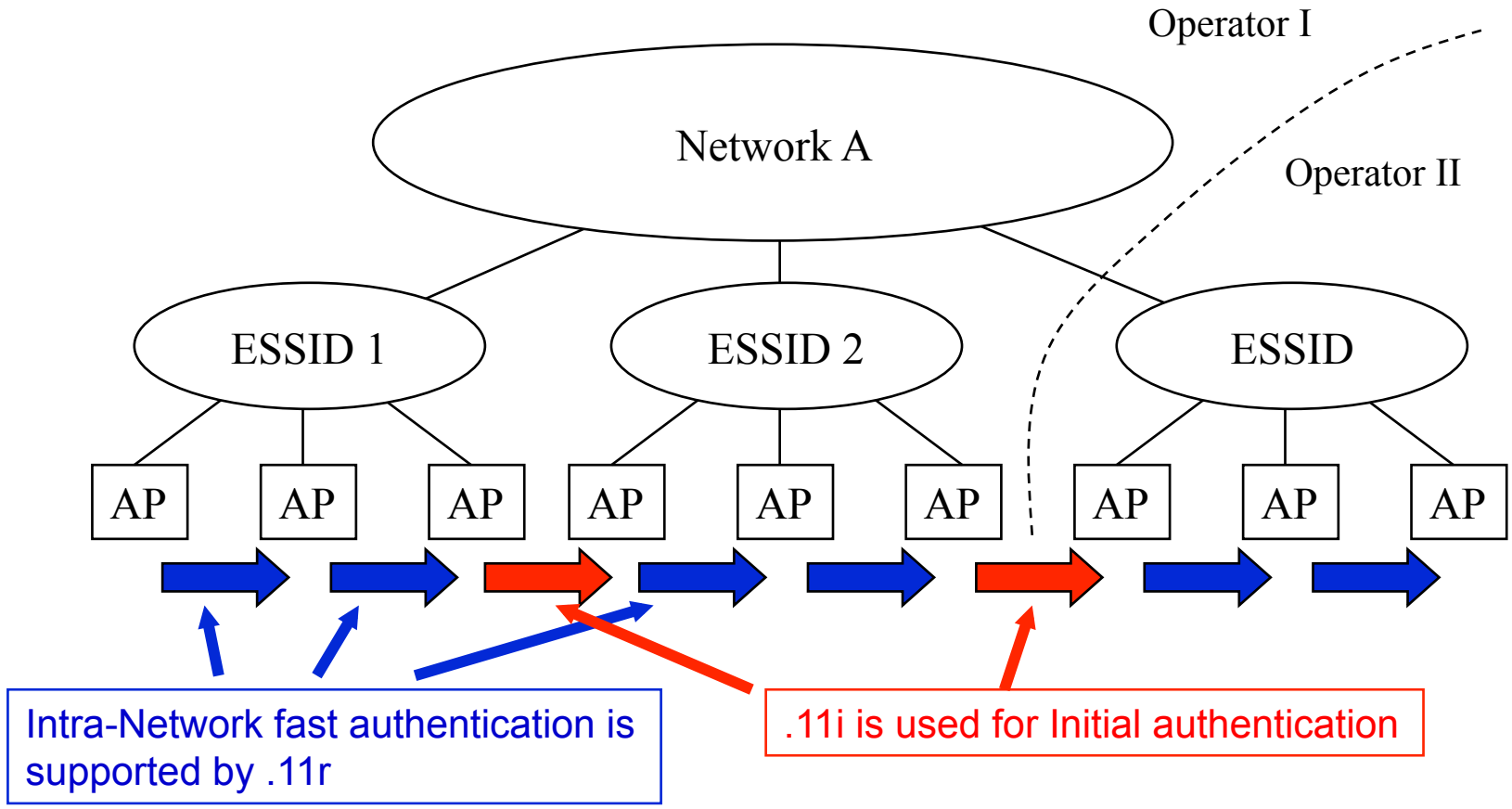
Link layer (re-) establishment ✗

= **Authentication, Association (+ security)**

- **No Security**: Open Authentication & Association @ 1 Mbps = 2.8 ms mean value + time for required synchronization of TSF (2 ms mean) → **Total of 4.8 ms**
- **Adding Security**: IEEE**802.11i** (PEAP/EAP-MSCHAPv2) increases delay to at least **48ms**, large number of simultaneous initial authentication cause a tremendous network load due to the large number of message exchanges → **does not scale**
- **Optimized:** IEEE**802.11r** can reduce delay BUT 11r and 11i do not address the problem of intial authentication

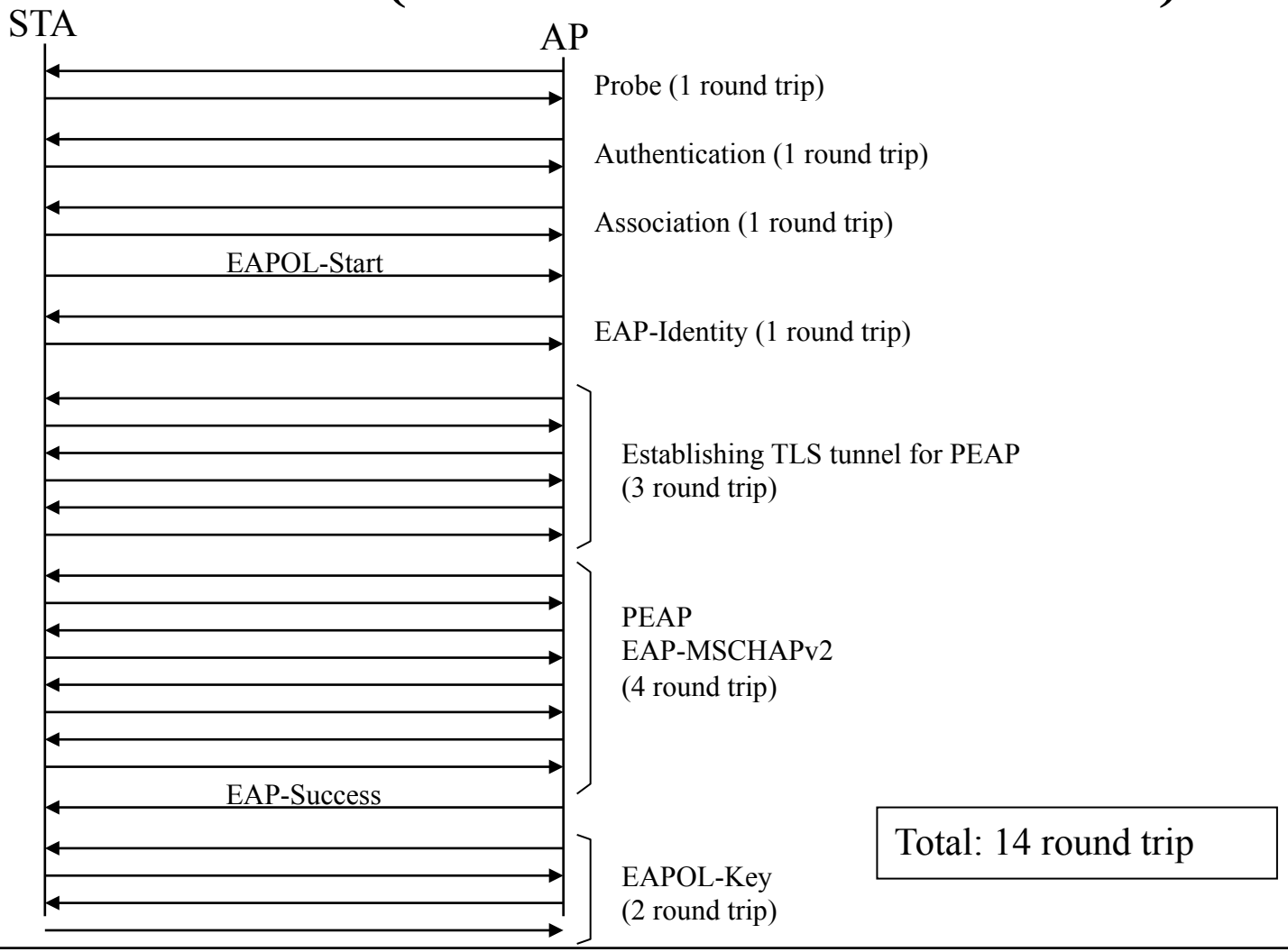
Most of time consumption in initial authentication process is used for AKM.

Scope of .11r and .11i



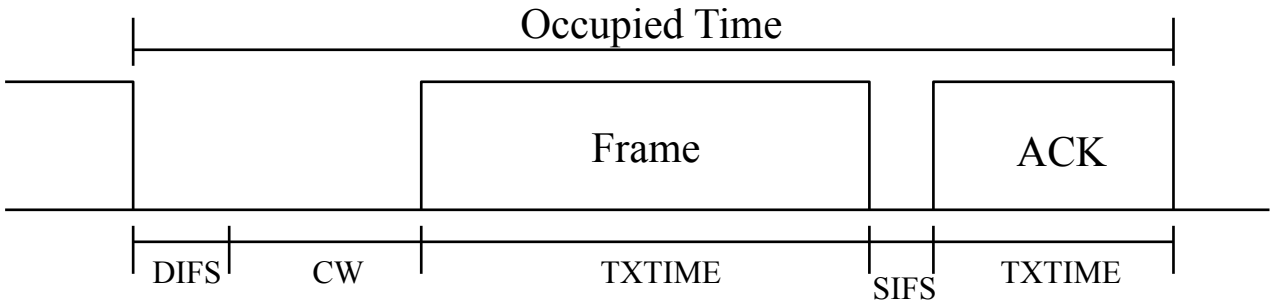
11r and 11r do not address the problem of initial authentication

Protocol Sequence between AP and STA on IEEE802.11i (PEAP/EAP-MSCHAPv2)



Airtime consumption for every single authentication process

- **We observed an STA connecting to an AP with PEAP/MS-CHAPv2 by IEEE802.11g.**
- **All management frames were transmitted in 1Mbps mode.**
- **Required airtime for one unicast frame is defined as described below.**



- aSlotTime: 20us
- aSIFSTime: 10us
- aPreambleLength: 144us
- aPLCPHeaderLength: 48bits
- aCWmin: 31
- aCWmax: 1023

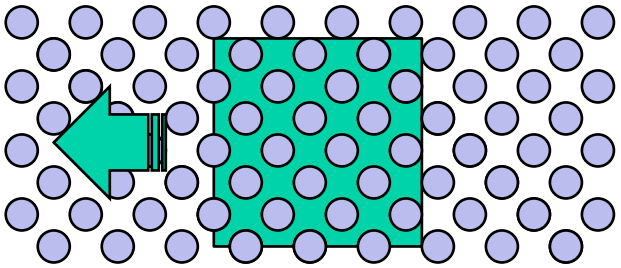
- DIFS: 50us
- CW: 620us

- ACKRate: 1Mbps
- ACKLength: 14Bytes

- PEAP/EAP-MSCHAPv2 needs 14 round trip frame exchanges.
- From our observation result, total frame length without PLCP header is 4390 byte.
- An STA needs 48.4ms airtime connecting to an AP.

Simulation

- **Assumption**
  - Place: Train Station
  - Time: Rush Hour
  - Walking Speed: 4.8km/h=80m/min
  - AP cover area: 80m*80m square
  - Occupied Space by 1 Person: 2m*2m square
  - All persons have a cellular phone which supports WLAN.
  - All persons are walking same direction.



- **1,600 STAs are passing through the AP's cover area in 1 minutes.**
- **this means 1,600 authentication process should be proceeded during every 1 minutes.**
- **Every authentication process needs 48.4ms airtime to connect to the AP.**
- **Only 1,238 authentication process can be proceeded .**
- **There is no time space to data communication.**
- **Furthermore, AP transmits beacons, STA needs DHCP…**

Current 802.11 initial authentication process does not meet the requirements for mobility.

Summary: Problem with existing standard

- **Speed of moving devices is limited by the authentication process**
- **Authentication and Key Management time can be much larger than data exchange (for short status or location updates)**
- **Initial secure authentication and association process is very inefficient**
- **Long Authentication and Key Management time loosing scalability**
- **Limited number of simultaneous access of initial authentications**

Currently, we do not have a secure, fast initial authentication that
a) is suitable for users experiencing a small dwell time in a cell
(due to high mobility or small cell sizes users)
b) scales for large number of simultaneously occurring
initial authentications

Moving forward: Call For Interest in creating a study group

- **The audience of 802.11 WNG SC requested to explore the need for "mobile communication" / fast initial secure authentication to the entire working group. (Straw poll in Jan. session: Yes - 18; No – 1)**

- **Technical presentation given in WNG SC and today have elaborated on the commercial interest in applications scenarios requiring fast and secure initial authentication**

- **There have also been presentations showing the technical feasibility of approaches incorporating fast and secure initial authentication in 802.11**

- **Next step: have in a study group drafting a PAR and 5C to enable fast and secure initial authentication**
  - → very narrow limited scope in order to
  - → Complete amendment in due time

References

- [1] H. Morioka, H. Mano, M. Ohmori, M. Ohta, "MIS Protocol for Secure Connection and Fast Handover on Wireless LAN", No.454, The IEEE 20th International Conference on Advanced Information Networking and Applications, Austria, Apr.18-20, 2006
- [2] H. Morioka, H. Mano, M. Ohmori, M. Ohta, M. Hirabaru, M. Hasegawa, M. Inoue, "Seamless Handover with Wireless LAN, Mobile IP, MISP and PDMA", The 9th International Symposium on Wireless Personal Multimedia Communications, 2006
- [3] H. Morioka, H. Mano, "Broadband V2I Access for High Speed Transportation", 09/0111r3
- [4] H. Mano, H. Morioka, "IEEE802.11 for High Speed Mobility", 09/1000r6
- [5] H. Nakano, H. Morioka, H. Mano, "An Exsample Protocol for FastAKM", 10/0059r3
- [6] H. Nakano, H. Morioka, H. Mano, "Fast Initial Authentication", 10/0361r0
- [7] M. Emmelmann. System Design and Proof-of-Concept Implementation of Seamless Handover Support for Communication-Based Train Control. In M. Emmelmann, B. Bochow, and C. Kellum, editors, Vehicular Networking -- Automotive Applications and Beyond. John Wiley & Sons, 2010, ISBN: 9780470741542.
- [8] M. Emmelmann, S. Wiethölter, and H.-T. Lim. Continuous network discovery using Opportunistic Scanning. 802.11 WNG SC Wireless Next Generation Standing Committee. Doc. 09/1207r1. IEEE 802.11 Plenary, Atlanta, GA, USA, November 16 -- 20, 2009.
- [9] M. Emmelmann, S. Wiethölter, and H.-T. Lim. Opportunistic Scanning: Interruption-Free Network Topology Discovery for Wireless Mesh Networks. In Porc. of International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM), Kos, Greece, June 15-19, 2009.

Questions & Comments

Motion

Motion:

Request approval by IEEE 802 LMSC to form an 802.11Study Group to address fast initial authentication with the intent of creating a PAR and five criteria.