Fast Initial Authentication

Authors:

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

New location and presence
Updated new twitters and messages
Get new handbills

No need stop! Just pass through!
Prospect of use case 2

RF Tag application
Automatic Electrical Cash Register
Security Gate

Digital Signage + Info Stand
Distribute information

ID Exchange

No need stop! Just pass through!
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

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: IEEE802.11i (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: IEEE802.11r 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.

Upper Layer Aspects
→ Out of scope for .11
11r and 11r do not address the problem of initial authentication

.11i is used for Initial authentication

Intra-Network fast authentication is supported by .11r
Protocol Sequence between AP and STA on
IEEE802.11i (PEAP/EAP-MSCHAPv2)

STA

AP

Probe (1 round trip)
Authentication (1 round trip)
Association (1 round trip)
EAP-Identity (1 round trip)
Establishing TLS tunnel for PEAP
(3 round trip)
PEAP
EAP-MSCHAPv2
(4 round trip)
EAP-Success
EAPOL-Key
(2 round trip)

Total: 14 round trip
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.

<table>
<thead>
<tr>
<th>Frame</th>
<th>ACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>aSlotTime:</td>
<td>20us</td>
</tr>
<tr>
<td>aSIFSTime:</td>
<td>10us</td>
</tr>
<tr>
<td>aPreambleLength:</td>
<td>144us</td>
</tr>
<tr>
<td>aPLCPHeaderLength:</td>
<td>48bits</td>
</tr>
<tr>
<td>aCWmin:</td>
<td>31</td>
</tr>
<tr>
<td>aCWmax:</td>
<td>1023</td>
</tr>
<tr>
<td>DIFS:</td>
<td>50us</td>
</tr>
<tr>
<td>CW:</td>
<td>620us</td>
</tr>
<tr>
<td>ACKRate:</td>
<td>1Mbps</td>
</tr>
<tr>
<td>ACKLength:</td>
<td>14Bytes</td>
</tr>
</tbody>
</table>

- 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

Questions & Comments
Motion

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