IEEE P802.11
Wireless LANs

|  |
| --- |
| Fast Initial Authentication PAR and 5C |
| Date: 2010-05-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Marc Emmelmann | TU Berlin | Einsteinufer 25 | +49 30 314 24580 | emmelmann@ieee.org |
| 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 | 5488 Marvell LaneSanta Clara, CA 95054 | +1-408-222-8341 | paul@marvell.com |
| 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.comcas@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 |

Abstract

Fast Initial Authentication PAR & 5C.

Revisions:

R00 Initial draft for May 2010 meeting in Beijing

R01 Incorporates revisions of the PAR section as agreed to during the Tuesday, 18. May 2010, AM1 session, regarding the PAR section.

R02 Deleted fields which are no longer required by the most recent online form of the PAR; incorporated feedback received up to the Wednesday, May 19, PM1 session.

R03 Reflecting changes as introduced during Wednesday, May 19, PM1 session.

R04 Reflecting changes introduces during Thursday, May 20, AM1 session.

R05 Added last sentence to paragraph (5.1) in Secton 8.1.

Top of Form

      



|  |
| --- |
| **Draft PAR Confirmation Number**  |
| **Submittal Email:**     |
| **Type of Project:** PAR for an amendment to existing Standard 802.11-2007 |
| **1.1 Project Number:** P802.11  |
| **1.2 Type of Document:** Standard for |
| **1.3 Life Cycle:** Full |

|  |
| --- |
| **2.1 Title of Standard:** IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment: Fast Initial Secure Authentication |

|  |
| --- |
| **3.1 Name of Working Group:** Wireless LAN Working Group(C/LM/WG802.11)   **Contact information for Working Group Chair** Bruce Kraemer517 La Costa Court Melbourne, FL 32940USbkraemer@marvell.com **Working Group Vice Chair:** Jon Rosdahl10871 N 5750 West Highland, UT 84003US, **Email:** jrosdahl@ieee.org |
| **3.2 Sponsoring Society and Committee:** IEEE Computer Society/Local and Metropolitan Area Networks(C/LM) **Contact information for Sponsor Chair:** Paul Nikolich18 Bishops Lane Lynnfield, MA 01940USp.nikolich@ieee.org**Contact information for Standards Representative:** |
| **4.1 Type of Ballot:** Individual  |
| **4.2 Expected Date of Submission for Initial Sponsor Ballot:** <<12/2012>> |
| **4.3 Projected Completion Date for Submittal to RevCom:** <<02/2014>> |
| **5.1 Approximate number of people expected to work on this project:** <<30>>  |

|  |  |
| --- | --- |
| **5.2 Scope of Proposed Standard:** Having selected an AP within a new ESS this amendment defines modifications to the IEEE 802.11 Medium Access Control Layer (MAC), to enable a fast initial authentication of 802.11 stations (STAs).  | **Old Scope:**  |

|  |
| --- |
| **5.3 Is the completion of this standard is dependent upon the completion of another standard:** No **If yes, please explain:**  |

|  |  |
| --- | --- |
| **5.4 Purpose of Proposed Standard:** Having selected an AP within a new ESS this amendment provides IEEE 802.11 wireless networks with a fast initial authentication mechanism. | **Old Purpose:**  |

|  |
| --- |
| **5.5 Need for the Project:** The number of mobile devices incorporating IEEE 802.11 is steadily growing. Applications that are continuously running on those devices benefit from the high data rates of the IEEE 802.11 interface. The primary need comes from an environment where mobile users are constantly entering and leaving the coverage area of an AP within an existing extended service set (ESS). For each ESS, the mobile device has to do an initial authentication to establish network connectivity. This requires an efficient mechanism that (a) scales with a high number of users simultaneously entering a ESS (b) supports a very small dwell time in coverage area of a ESS,(c) securely provides initial authentication.The current IEEE 802.11 specification does not meet these requirements.  |
| **5.6 Stakeholders for the Standard:** Manufacturers and users of mobile devices, personal computer, enterprise networking devices, consumer electronic devices. |
| **Intellectual Property****6.1.a.** Is the Sponsor aware of any copyright permissions needed for this project? NoIf yes, please explain: **6.1.b.** Is the Sponsor aware of possible registration activity related to this project? NoIf yes, please explain:  |
| **7.1 Are there other standards or projects with a similar scope?** No |
| **7.2 International Standards Activities** **a. Adoptions**  Is there potential for this standard to be adopted by another organization? **Do not know at this time** Organization:  Technical Committee Name:  Technical Committee Number:  Contact person Name:  Contact Phone:  Contact Email: **b. Joint Development**  Is it the intent to develop this document jointly with another organization? No Organization:  Technical Committee Name:  Technical Committee Number:  Contact person Name:  Contact Phone:  Contact Email: **c. Harmonization**  Are you aware of another organization that may be interested in portions of this document in their standardization development efforts? No Organization:  Technical Committee Name:  Technical Committee Number:  Contact person Name:  Contact Phone:  Contact Email:  |
| **8.1 Additional Explanatory Notes: (Item Number and Explanation)** Ad 5.2)The project intends to amend the MAC only, thereby supporting fast initial authentication for all IEEE 802.11 PHYs. The project does not intend to remove IEEE 802.11i but to add additional mechanisms for fast initial authentication. The fast initial authentication mechanism reduces time of authentication and key management without reducing the security provided by IEEE 802.11iAd 5.5)The protocol sequence for secure link establishment (IEEE 802.11i PEAP/EAP-MSCHAPv2) needs 14 round trip frame exchanges which accumulates to 48.4ms airtime consumed per STA to connect to an AP [1]. During rush hour at a train station, more than 1500 people pass through the coverage area of an AP in less than 1 minute not leaving enough time for all mobile devices to authenticate to the AP; no airtime is furthermore left for data communication.  |

Bottom of Form

Contact the NesCom Administrator

# Five Criteria

1. **17.5.1 Broad Market Potential**

**A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:**

**a) Broad sets of applicability.**

The number of mobile devices with an IEEE 802.11 interface is continuously increasing.

Examples of those devices include smart phones and tablet PCs, and IEEE 802.11 equipment installed in cars or trains. According to Juniper Research, just the number of IEEE 802.11 enabled dual mode handsets will dominate the market by 2012 generating more than $68bn revenues [3]. This expectation is supported by announcements of WiFi Alliance expecting that the “user affinity to [WiFi will] drive annual shipments [of smart phones] to 300 million in 2011 … and 520 million by 2014” [4, 5].

The high data rate offered by IEEE 802.11 is a key driver for dual mode functionality in handsets.

Hence, it is essential that those devices fully exploit the capacity gains offered by IEEE 802.11 whenever possible. The current specification of IEEE 802.11 limits this for devices experiencing only a short dwell time within the coverage area of an ESS or for a high number of users closely entering the coverage area of an AP within an existing ESS for the first time due to the overhead and long time spent in the authentication phase.

Application scenarios limited by the current specification of IEEE 802.11 include, for example:

* a bulk of pedestrians entering / leaving a train station during rush hour, entering for the first time (and passing through) the coverage area of an AP within an existing ESS which is a typical deployment e.g. at a Starbucks shop
* IEEE 802.11 devices on-board a vehicle travelling at lower speeds which initially enters and passes through the limited coverage of an AP within an ESS deployed along the road or railway

where applications (i.e. bulk file transfer, notification, push/pop services) benefit from high data rates offered by IEEE 802.11 even for only a short period of time [1]. The advantage of fully exploiting those short opportunities to exchange data at a high data rate are appealing for network operators and users, as it reduces the load on the bandwidth-limited cellular network and increases the user experience by a larger number of applications available on their mobile devices and the increased bandwidth available to them.

**b) Multiple vendors and numerous users.**

WiFi alliance expects the number of IEEE 802.11-enabled smart phones to surpass 520 million by 2014 [5]. In additon, automotive industry is striving towards equipping their vehicles with IEEE 802.11 devices. In summary, considering estimations of Juniper Research, this will create an expected revenue of hundreds of billion USD. Network operators are supplementing the capacity of their cellular network infrastructure with IEEE 802.11-based connections. Users benefit from an increase in data rates and will favor devices featuring fast initial authentication. Accordingly, manufactures are likely to add the feature in their products.

**c) Balanced costs (LAN versus attached stations).**

The changes to provide fast initial authentication are not expected to significantly affect the cost of the base station or the client, as the hardware (PHY) component are expected to be left unchanged and only changes to the software part are expected. Given a fixed cost for the initial development and testing of the software, and seeing the number of stations benefitting from fast initial authentication (520 million plus), a balance of cost vs. number of affected stations is given.

1. **17.5.2 Compatibility**

**IEEE 802 defines a family of standards. All standards shall be in conformance with the IEEE 802.1 Architecture, Management, and Interworking documents as follows: 802. Overview and Architecture, 802.1D, 802.1Q, and parts of 802.1f. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with 802.**

**Each standard in the IEEE 802 family of standards shall include a definition of managed objects that are compatible with systems management standards.**

Compatibility with IEEE 802 requirements will result from keeping the MAC SAP interface the same as for the existing 802.11 standard. The proposed amendment shall introduce no 802.1 architectural changes. This includes compatibility with 802.1X. The MAC SAP definition shall not be altered, ensuring that all LLC and MAC interfaces are compatible to and in conformance with the IEEE 802.1 Architecture, Management and Internetworking standards. New managed objects shall be defined as necessary in a format and structure consistent with existing 802.11 managed objects.

1. **17.5.3 Distinct Identity**

**Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:**

**a) Substantially different from other IEEE 802 standards.**

The proposed amendment is an amendment to IEEE 802.11.

There are no other approved IEEE 802 projects specifically addressing fast initial authentication for WLAN personal/portable devices, which complete the authentication process for an IEEE 802.11 device in less time as with the current IEEE 802.11 specification.

**b) One unique solution per problem (not two solutions to a problem).**

There is no other approved project providing fast initial authentication for personal/portable WLAN devices.

**c) Easy for the document reader to select the relevant specification.**

The Project will produce an amendment to the IEEE 802.11 specification.

1. **17.5.4 Technical Feasibility**

**For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:**

**a) Demonstrated system feasibility.**

Hardware components, i.e. IEEE 802.11 network cards, are available today and modifications to the existing IEEE 802.11 MAC can be easily introduced today by modifying driver software for the network card given the code of the driver is in the public domain.

The envisioned functionality has been demonstrated to be technically feasible by a proof-of-concept implementaton using OS NetBSD 5.0.1, NetBSD’s net80211 driver, and a network card with the Atheros Communications AR5212 chip set. Required modifications are in the order of 200 lines of code. A presentation on this proof-of-concept demonstrator showing technical feasibility has been given to IEEE 802.11 WNG SC [2].

 **b) Proven technology, reasonable testing.** The main components of the technology and signalling are in use today. Seeing the limited modifications required by the proof-of-concept implementation [2], the involved testing overhead associated with a commercial development undertaken by manufacturers is reasonable.

**c) Confidence in reliability.** Analysis of current WLAN products and proposal for potential candidate approaches provides confidence in the reliability of the proposed solutions. The Working Group envisions that the proposed amendment will result in similar or improved reliability over current levels.

**17.5.4.1 Coexistence of 802 wireless standards specifying devices for unlicensed operation**

**A working group proposing a wireless project is required to demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable. The Working Group will create a CA document as part of the WG balloting process. If the Working Group elects not to create a CA document, it will explain to the EC the reason the CA document is not applicable**.

1. The working group will create a CA document as part of the WG balloting process.
2. **17.5.5 Economic Feasibility**

**For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated) for its intended applications. At a minimum, the proposed project shall show:**

**a) Known cost factors, reliable data.** Support of the proposed standard will require manufactures to modify the MAC of their products. The cost factor involved with such a modification are well known and the data for this is well understood.

**b) Reasonable cost for performance.**

The new amendment will provide manufacturers with means of supporting fast initial authentication. In general, the cost factor changes needed to implement the extenstion envisioned by the study group are within the capabilities of exing technology and competition between manufacturers will ensure that costs remain reasonable.

**c) Consideration of installation costs**. For some configurations and use cases, installed devices will benefit from offering fast initial authentication. Costs for adding fast initial authentication to an existing, deployed device are comparable to the cost of updating the firmware. The cost factors for such transition are known and well understood.

**References:**

[1] H. Mano, H. Morioka, P. Lambert, M. Emmelmann, H. Nakano, and M. Takai. [Fast Initial Authentication](http://www.emmelmann.org/Library/Papers_Reports/docs/11-10-0371-03.pdf). 802.11 Working Group. Doc. 10/0371r3. IEEE 802.11 Plenary, Orlando, FL, USA, March 15--19, 2010. Available online: <https://mentor.ieee.org/802.11/dcn/10/11-10-0371-03-0000-fast-initial-authentication.ppt>

[2] H. Nakano, H. Morioka, and H. Mano: An Example Protocol for FastAKM. 802.11 WNG SC Doc. 10/0059r4. IEEE 802.11 Interim, L.A., CA, USA, January 2010. Available online: <https://mentor.ieee.org/802.11/dcn/10/11-10-0059-03-0wng-an-example-protocol-for-fastakm.ppt>

[3] Juniper Research: Dual Mode (Cellular/ VoIP over Wi-Fi) Mobile Handsets to Drive $82bn VoIP over Wi-Fi Equipment market by 2012. Available online: <http://www.juniperresearch.com/viewpressrelease.php?pr=47>, last accessed May 19, 2010.

[4] WiFi Aliance: Wi-Fi is now a must-have for mobile phones; User affinity to drive annual shipments to 300 million in 2011. WiFi Alliance press release, April 1 2009, available online: <http://www.wi-fi.org/news_articles.php?f=media_news&news_id=795>, last accessed May 19, 2010.

[5] WiFi Aliance: Thirsty for bandwidth, consumers and carriers embrace Wi-Fi® phones. WiFi Alliance press release, March 30 2010, available online: <http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969>, last accessed May 19, 2010.