International Journal of Mobile Device Engineering
Vol. 3, No. 1 (2019), pp.7-12
http://dx.doi.org/10.21742/ijmde.2019.3.1.02

A Simplified FT protocol over Software-Defined WLAN

Hyeon-Ki Yun[1], Taeyoon Kim[2], Sung-Gi Min[3*], Pill-Won Park[4]

[1,2,3] Korea University, Korea*
[4]Dongguk University, Korea
[1]shicnova@korea.ac.kr, [2]taeyoon0929@gmail.com, [3]sgmin@korea.ac.kr,*
[4]pillwon79@gmail.com

Abstract

The fast BSS transition (FT) is defined to support intra-ESS mobility at the IEEE 802.11 network. In the FT protocol, authentication and reassociation messages piggyback the parameters for a new session key generation. When a station changes its point of attachment from the current access point(AP) to the target AP, the supplicant key holders of the station and associator key holders in the current AP and the target AP interact to simplify the authentication and a new session key generation processes. We propose a simplified FT protocol to achieve a faster FT for the IEEE 802.11 network over SDN. In SDN, associator key holders can locate at the centralized SDN controller, so an integrated key holder can replace associator key holders of APs. As a result, the simplified FT protocol re-associates the station and the target AP with a single message exchange (two messages) instead of two message exchanges (four messages).

Keywords: *FT; IEEE 802.11; WLAN; Authentication; SDN*

1. Introduction

Professor Jerry Kaplan of Stanford University, an expert in artificial intelligence,"The development of AI will destroy most of the current human work,""We can not avoid mass unemployment."错误!未找到引用源。. The Korea Employment Information Service analyzed the job replacement pr The Wireless Local Area Network (WLAN) defined by IEEE 802.11-1999 [1]is a wireless communication technology for nomadic stations to be connected to the Internet. But the user experience of the mobility service in the Plain Land Mobile Network (PLMN) force the inclusion of the mobility service in WLAM. Therefore, IEEE 802.11-2016[2] supports the intra-Extended Service Set (ESS) mobility service, called the Fast Basic Service Set (BSS) Transition (FT) [3].

The FT introduces the three-tier key hierarchy and the two-tier key holder concepts. When a station (STA) changes its point of attachment from current Access Point (AP) to new target AP, the STA has to re-associate and generate a new session key with the new AP. To speed up those processes, the FT protocol integrates these two processes by piggybacking parameters used for generating a new session key into the messages exchanged during the re-association process.

The Software Defined Network (SDN) concept is a network architectural concept to separate the control plane and the data plane of a network node. In the SDN, a centralized SDN controller

Article history:
Received (June 3, 2019), Review Result (July 15, 2019), Accepted (August 10, 2019)

Print ISSN: 2207-5992, eISSN: 2207-600X IJMDE

can manage several underlying network nodes. Therefore, the control functions of AP nodes deployed over the SDN can be centralized onto a control application running over the SDN controller.

In this paper, we propose a simplified FT protocol for a software-defined WLAN network (SDWN). In the proposed scheme, all associator key holders (R0KHs/R1KHs) located in APs in the SDWN are moved onto the corresponding integrated R0KH (iR0KH) and the integrated R1KH (iR1KH) over the SDN controller. The iR0KH and the iR1KH are parts of the Integrated System Management Entity (iSME), which runs over the SDN controller.

2. The fast BSS transition

The standard FT protocol consists of two processes. The first process describes the FT initial mobility domain association. It is used when an STA tries to make an association with an AP in an ESS for the first time. The second process, which is called the FT protocol, is used when the STA changes its point of attachment to new AP within the ESS.

2.1. FT Initial Mobility Domain Association

When an STA tries to attach to an AP in an ESS at first, it performs the FT initial mobility domain association process. The overall process is the same as the normal association process without FT capability. For FT, messages include a few new parameters. Figure 1 shows the sequence diagram of the FT initial mobility association process.

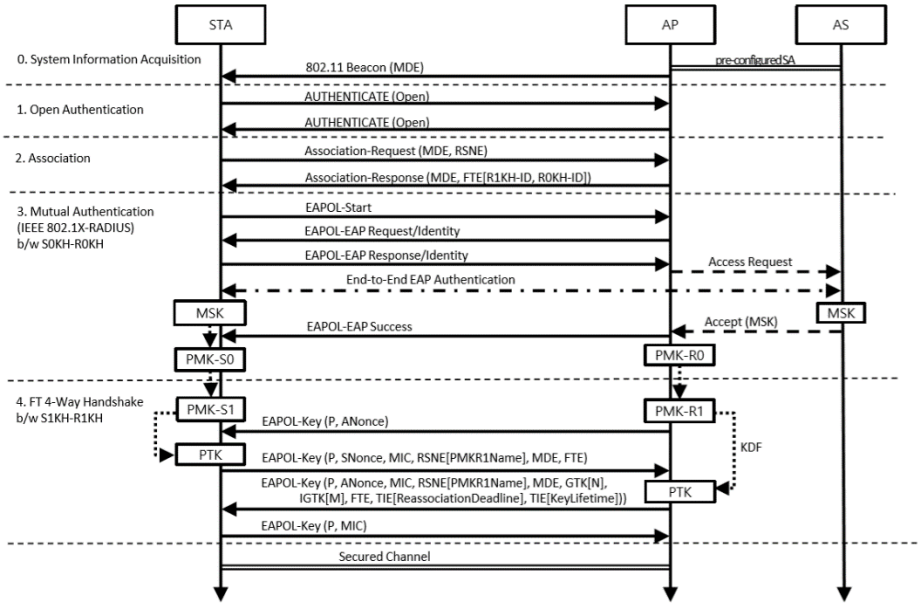

Figure 1. The FT initial mobility domain association with IEEE 802.1X[4].

2.2. FT Protocol

The FT protocol is used to make a fast reassociation between an STA and a target AP when the STA changes its point of attachment from the current AP to the target AP.

The FT protocol does not use the FT 4-way handshake. It piggybacks the key information for a new session key into reassociation message instead of the EAPOL-KEY frame used in the

IEEE 802.11 4-way handshake. The key information is carried by the FTE element. All messages used by the FT protocol include MDE and RSNE [PMKR0Name].

The FT protocol support two modes of fast reassociation. When the STA and new target AP can communicate directly, they use the over-the-air authentication. If the STA wants to prepare the session keys for new AP before the STA handovers, it uses the over-the-DS authentication. Figure 3 shows the sequence diagram of the FT protocol.

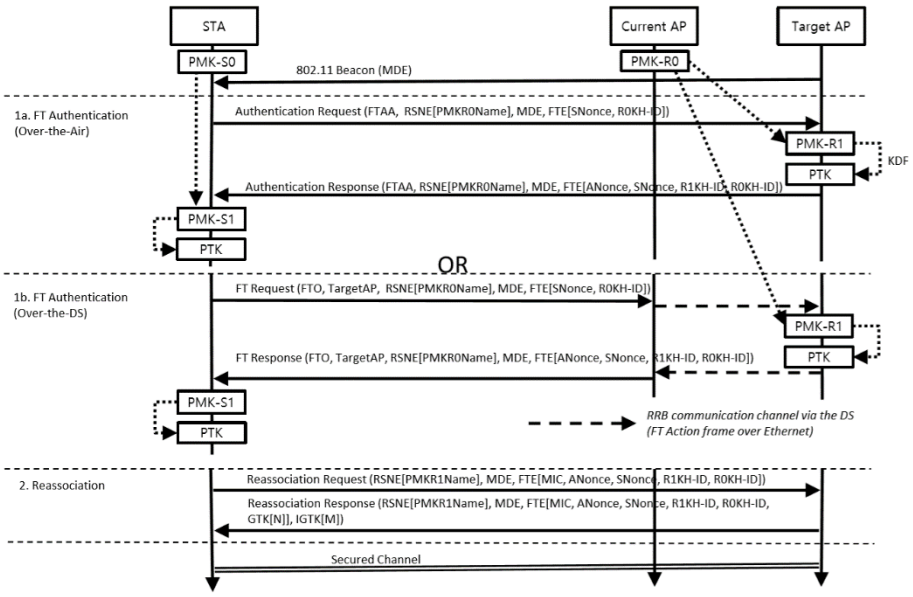

Figure 3. Over-the-Air/Over-the-DS FT Protocol

3. Simplified FT protocol: Over-the-SDN FT Protocol

3.1. Simplified FT System Architecture

In the simplified FT system architecture, an integrated SME (iSME) control application for an ESS runs over the SDN controller[5]. The iSME control application contains the integrated R0KH (iR0KH) and the integrated R1KH (iR1KH). When an AP receives an association related frame, it forwards the frame to the iSME via the SDN controller. The AP and the iSME communicate via the secure SDN control channel.

To distinguish the WLAN deployment over the SDN, the "fast BSS transition over the SDN" bit is defined at the MDE element to indicate the ability of the Over-the-SDN FT protocol. The bit is always set whenever the AP supports the proposed FT protocol.

If an STA supports the Over-the-SDN FT protocol, it sets the "fast BSS transition over SDN" field of the MDE in all FT messages it sends. When the iSME receives an FT message, which the "fast BSS transition over SDN" field of the MDE is set, it handles the FT messages according to the Over-the-SDN FT mode.

The simplified FT also defines a new sub-element of the FTE element, referred as ANonce [NHCounter]. The sub-element conveys the next hop AP Nonce (NHANonce) and the next hop counter (NHCounter). It is encrypted by the iR1KH with the KEK of the iR1KH and it is decrypted by the S1KH with the KEK of the S1KH.

3.2. FT Initial Mobility Domain Association for Over-the-SDN FT Protocol

The FT initial mobility domain association for the Over-the-SDN FT protocol uses the same message sequence, messages, IEs used at the standard FT initial mobility domain association. The "fast BSS transition over SDN" field of the MDE, which is included all FT messages, must be set to indicate that the AP supports the Over-the-SDN FT protocol.

In the Over-the-SDN FT protocol, the S0KH and the iR0KH use the iR0KH-ID instead of R0KH-ID to derive the PMK-R1. The iR0KH-ID is a string name for the iR0KH. The iR1KH uses the R1KH-ID of the AP to generate the PMK-R1.

Furthermore, the FTE element of the third message of the FT-4-way handshake at the FT Initial Mobility Domain Association conveys the NHANonce [NHCounter] sub-element. The lifetime of the NHANonce[NHCounter] is bound to the PTK lifetime indicated by TIE [KeyLifetime] in the same message.

3.3. Over-the-SDN FT Protocol

The Over-the-SDN FT protocol is used when the STA re-associate with another AP in the ESS after its FT initial mobility domain association with an AP in the ESS over the SDWN.

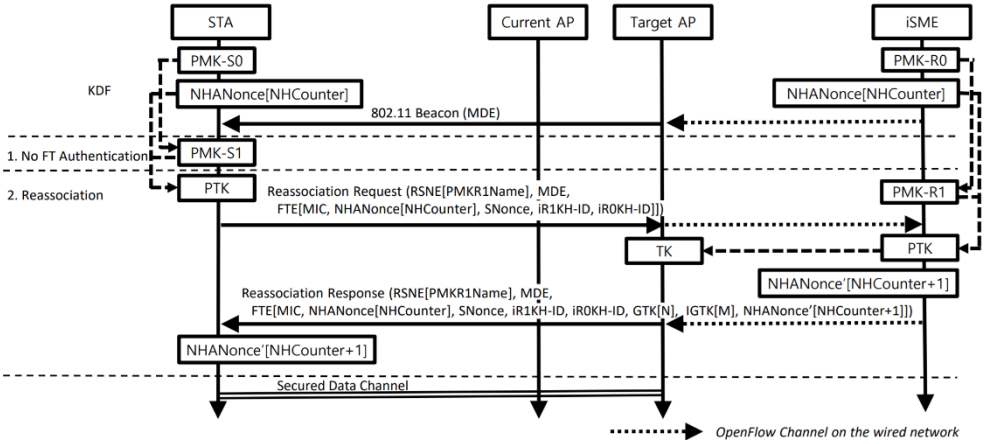

Figure 3. Proposed Over-the-SDN FT Protocol

Step 0 : When the STA changes its point of attachment, it receives beacons from the surrounding APs. Then it detects APs which support the FT. If it supports the over-the-SDN, it selects an AP which advertises the MDE with "fast BSS transition over SDN" bit is set. Then the S0KH at the STA generates new PMK-R1 for new AP. It notifies its S1KH with new PMK-R1

Step 1: The Over-the-SDN FT protocol omits this step because the S0KH of the STA and the R0KH of the iSME are not changed even if the STA changes its point of attachment to another AP in the ESS. They have authenticated each other already.

Step 2.1: The S1KH generates a new nonce (SNonce) and derives new PTK from the PMK-R1 with the SNonce and the NHANonce[NHCounter]. The NHANonce[NHCounter] has been obtained during the "FT Initial Mobility Domain Association" or by the latest Over-the-SDN FT protocol.

Step 2.2: The S1KH sends the reassociation request to the target AP. The AP forwards it to the iR1KH at the iSME. The reassociation request includes RSNE[PMKR1Name], MDE and the FTE[MIC, ANonce[NHCounter], SNonce, R1KH-ID, iR0KH-ID].

Step 2.3: The iR1KH asks new PMK-R1 to the iR0KH. The iR1KH supplies the R1KH-ID included in the reassociation message. The iR0KH notifies the new PMK-R1 to the iR1KH. The iR1KH derives new PTK with NHANonce[NHCounter] which stores for the STA. With new KCK, it compares the MIC in the message with the calculated MIC by the iR1KH. If they match, the reassociation request is accepted. It installs the TK in the target AP.

Step 2.4: The iR1KH generates new ANonce and increase the NHCounter by one. Then it sends the reassociation response to the STA. The FTE element contains them in the NH ANonce and Next Hop Counter fields in newly defined FTE element optional parameter, NHANonce[NHCounter]. These values are encrypted by new KEK. They are also stored with S1KH-ID at the iR1KH.

When the S1KH receives this message, it verifies the message and stores the NHANonce[NHCounter].

4. Security Evaluation

In this section, we provide details of the security analysis of the simplified FT. The proposed simplified FT uses the same FT initial mobility domain association, except adding a few parameters in the MDE and FTE elements. It also supports the standard over-the-air and over-the-DS FT protocol if the "fast BSS transition over SDN" field of the MDE is not set. Therefore, the simplified FT protocol, except over-the-SDN FT protocol, is expected to have the same security capabilities provided by the standard FT.

For these reasons, we mainly focus on the over-the-SDN FT protocol messages that are exchanged between the SME of the STA and the iSME over the SDN controller to analyze their protection capabilities against major attacks. We assume that the SDN control channel is secure.

5. Conclusion

We propose a simplified FT protocol used at the WLAN deployed over the SDN. In the SDN, associator key holders of APs are combined into a centralized key holder (iR0KH/iR1KH) over the SDN controller. They are not changed even if the STA changes its point of attachment to another AP in the ESS. The proposed FT protocol exploits the situation to speed up the reassociation process. Firstly, the supplicant key holders and the integrated key holders maintain their states until the STA moves out of ESS service area. Therefore, we can omit the authentication of both devices. By pre-loading the AP nonce, the proposed scheme reduces the number of messages by two instead of four. The proposed FT protocol compatible with the standard FT protocol, and the experiment shows both protocols work together.

Acknowledgements

Funding: This research was supported by the Korean MSIT (Ministry of Science and ICT), under the National Program for Excellence in SW (2015-0-00936), supervised by the IITP (Institute of Information & communications Technology Planning & Evaluation)

References

[1] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE Standard 802.11-1999, **(1999)**.

[2] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. IEEE Standard 802.11-2016, **(2016)**.

[3] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition. IEEE 802.11r-2008, **(2008)**.

[4] IEEE Standard for Port-Based Network Access Control. IEEE Standard 802.1X-2010, **(2010)**. DOI: 10.1109/IEEESTD.2001.92774

[5] P. Berde, M. Gerola, J. Hart, and Y. Higuchi. "ONOS: Towards an open, distributed SDN OS," in Proc. 3rd Workshop Hot Topics Software Defined Networking, Chicago, Illinois, USA, pp.1-6, **(2014)**. DOI: 10.1145/2620728.2620744

Authors

Hyeon-Ki Yun
He received B.S. degrees in Computer Engineering from Kyunghee University, Korea in 2016. He is currently working toward M.S. degree in Computer Science and Engineering at Korea University, Seoul, Korea. His interests in research include Internet of things, security, wireless network.

Taeyoon Kim
He received B.S. degrees in Computer Science from Korea University, Korea in 2017. He received his M.S. degree in Computer Science and Engineering from Korea University in 2019. He is currently working at Tmax, Seongnam, Korea. His interests in research include mobile network, cloud network, mobility.

Sung-Gi Min
He received his B.S. degree in Computer Science from Korea University, Seoul, Korea, in 1988. He received his M.S. and Ph.D. degrees in Computer Science from University of London in 1989 and 1993, respectively. From 1 January 1994 to 28 February 2000, he worked in LG Information and Communication Research Center, and from 2 March 2000 to 28 February 2001, he was a Professor in the Department of Computer Engineering at Dongeui University, Busan, Korea. Since 2 March 2001, he has been a Professor in the Department of Computer Science and Engineering at Korea University, Seoul, Korea. His research is focused to wired/wireless communication networks, especially heterogeneous network environment, and he is interested in mobility protocols such as MIP, SIP, and SCTP, network architectures, QoS, and mobility management in future network.

Pill-Won Park
He received his B.S. degree in Computer Science from Chungnam National University, Daejeon, Korea, in 2008. He received his M.S. and Ph.D. degrees in Computer Science from Korea University, Seoul, Korea in 2010 and 2017, respectively. His research is focused to wired/wireless communication networks, and he is interested in mobility protocols such as MIP, network architectures, QoS, and mobility management in future network.