Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Handheld Authenticator for WLAN Access using WFDS and NFC

Mir Khizer Ali
I&CT, MIT
India

Santhosh Kamath
I&CT, MIT
India

Vinoth Sampath
Broadcom Corporation
India

Abstract- Existing authentication services on Session Layers or using Service Providers (webpage) based are cumbersome to extend for mass usage. This paper proposes a new authenticator Protocol to be used indifference with the Service Provider and by using the available WLAN based Protocols and NFC methods that are mass spread /available.

Keywords— Wi-Fi Direct, WFDS, Authentication, NFC, WLAN

I. INTRODUCTION

Need for the time is to enhance and extend the internet availability for public places or in personal (home) locations.Existing public schemes are based on SIM authentication [1] or use web based session authentication [2]. In SIM based authentication the user is required to send SMS and web based authentication involves filling up of lengthy user information forms which make it cumbersome for the user.

The current personal (home) authentication schemes for Wi-Fi networks involves home network administrator sharing the pass phrase of the Wi-Fi network to the new visitor/guest there by compromising with the home network security. There is always a risk of the visitor leaking the pass phrase/key of the home network to a third party. As there is a conflict of interest home owner cannot help but to share his network's key to guest's visiting his home.

In this paper we introduce the authentication service that lets the home network owner to allow the guest's to access his Wi-Fi network without sharing the passphrase of the home Wi-Fi network to any new user. The authentication is done by a hand held Wi-Fi direct services (WFDS)/Near Field Communications (NFC) enabled device that is running the Authentication Service on it.

WFDS is a standard specification defined by the Wi-Fi alliance, which is built on current standard Wi-Fi direct. The content of this specification is designed to address the solution requirement areas identified in SRD as:

1. Send service
2. Play service
3. Print service
4. Display service
5. Enable APIs
6. Application Service Platform.

WFDS specification defines an architecture, protocols and functionality for interoperability of Wi-Fi Direct Services (WFDS). Application Service Platform (ASP) is a software service or library that implements the common functions needed by all applications and services conforming to the Wi-Fi Direct Services specification. ASP enables or creates a session which is a logical link between two ASP enabled peers to enabled streamlined and structured communication between them. The WFDS enabled system can have multiple ASP-sessions between two or more devices needing the WFDS functionalities. Wi-Fi Direct Services framework has defined components that interact to provide services to capable WFD devices. ASP component is the logical entity to implement the common functions across all the services.ASP Adaptation layer is an interface layer between the Service and ASP, which services should invoke to access the ASP Functionality.

At its core, all NFC is doing is identifying us, and our bank account, to a computer. The technology is simple. It's a short-range, low power wireless link evolved from radio-frequency identification (RFID) tech that can transfer small amounts of data between two devices held a few centimeters from each other. Unlike Bluetooth, no pairing code is needed, and because it's very low power, no battery in the device being read. By tapping your phone on a contactless payment terminal in a shop, train station or coffee shop is able to identify your account (and even your personal preferences, shopping habits and even your most frequently travelled route home) and takes payment through an app on your phone. Passive NFC 'tags' on posters, in shops and on trains could contain a web address, a discount voucher, a map or a bus timetable that passers-by could touch their phones on to receive - or to instantly pay for absolutely anything.

II. WI-FI DIRECT SERVICES OPERATIONS

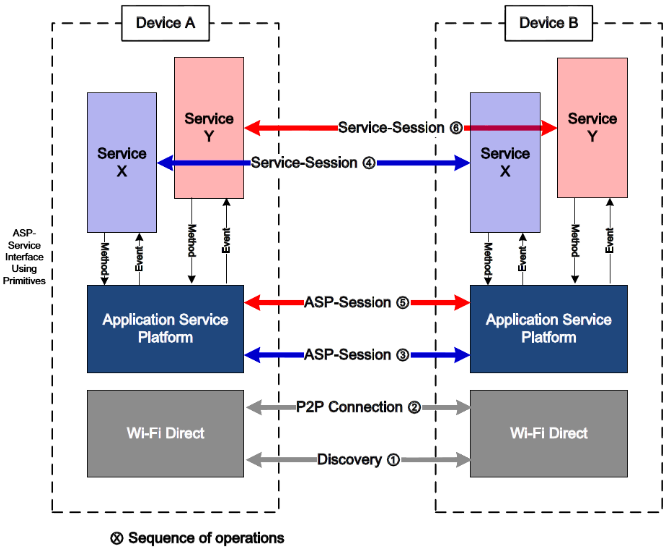

Fig. 1 Wi-Fi Direct Services operations

Fig. 1 describes the overall flow of operations between two peer devices. Application Service Platform (ASP) is a logical entity that implements the common functions needed by services, for example Send service. These functions include but are not limited to Device & Service Discovery, ASP-Session management, connection topology management, and security.

ASP-Session is a logical link between the ASP on one device and the ASP on another device. A P2P connection between peer devices is required to start an ASP-Session. An ASP can setup multiple ASP-Sessions between two devices. Each ASP-Session is identified by a session identifier assigned by ASP requesting the ASP-Session.

Service is a logical entity that utilizes ASP to provide use case specific functionalities to other services or applications. Service on one device communicates with the corresponding service on one or more devices using a service-specific protocol defined by the service specification and the ASP protocol.

When a user wishes to use service X between Device A and Device B, ASPs on each of the devices will create an ASP-Session between the devices which is exclusive to service X. If the user subsequently wants to use service Y another ASP-Session will be established for that service.

Overall above exemplary procedure follows following steps as illustrated in Fig. 1

1. Discovery procedure.
2. P2P connection procedure.
3. ASP-Session setup for service X.
4. Service X service session setup.
5. ASP-Session setup for service Y.
6. Service Y service session setup.

III. IMPLEMENTATION

Consider the scenario shown in Fig. 2. Device 1 and Device 2 are two WFDS enabled devices. The Device 2 is controlled by the home network administrator or simply the home owner. The Device 1 is controlled by a visitor/guest who intends to connect to the home Wi-Fi network (WLAN) in order to access the internet. The message flow for the Authentication service is shown in Fig. 2.

The two devices exchange a sequence of messages to establish a WFDS connection. All messages after this are exchanged over WFDS. After the WFDS connection is established the Authentication Service (AS) is started on Device 2. Device 1 sends a Request to Device 2 to grant access to the wireless router. In response Device 2 sends a message to Device 1 requesting its SIM number. Upon receiving the SIM number (SIM_NUM) the Device 2 validates the user of Device 1 against a pre-existing data base of trusted users made by Device 2's user. The data base in the message flow is taken to be as a simple friends list on Face Book (FB) or WhatsApp (WA). Alternately this data base could be on a sever setup by the home owner which can be accessed only by him. If Device 1 is found to be a trusted user then a copy of Device 1's SIM number is stored in Device 2 for future transactions. If Device 1 is not a trusted user then the home owner can manually add Device 1's user to the list of trusted users if he is intending to grant Device 1 an access to the Wi-Fi network. This can be done by adding Device 1's user to home owner's friends list in FB/WA or alternately updating the data base server to include Device 1's user in the trusted users list.

The Device 2 further gets the IMEI of validated Device 1 and stores a copy of it against the corresponding SIM number. Device 2 then gets the MAC address from Device 1 and sends it to the wireless router for including it in the list of know hosts that are allowed to access the router. It is important to note here that since Device 2 is the home network administrator he knows the pass phrase for the Wi-Fi router. The router adds the MAC address of Device 1 to the required list and starts a session control timer and sends a time stamp (TIME_STAMP) specifying the duration for which the session will remain active from the point the timer was started. With this the Device 1 has an access to the internet via the wireless router.

When the timer in the router times out it sends a Session logout message to Device 1 and deletes the MAC address entry of Device 1. If the Device 1 intends to connect to the router once more the above process is partially repeated again. Since Device 2 has a copy of Device 1's SIM number Device 2 does not have to revalidate Device 1 from the beginning and only needs to compare it with a stored copy of SIM number in its memory. As a result the process of validation is much faster compared to the validation in the first attempt by Device 1.

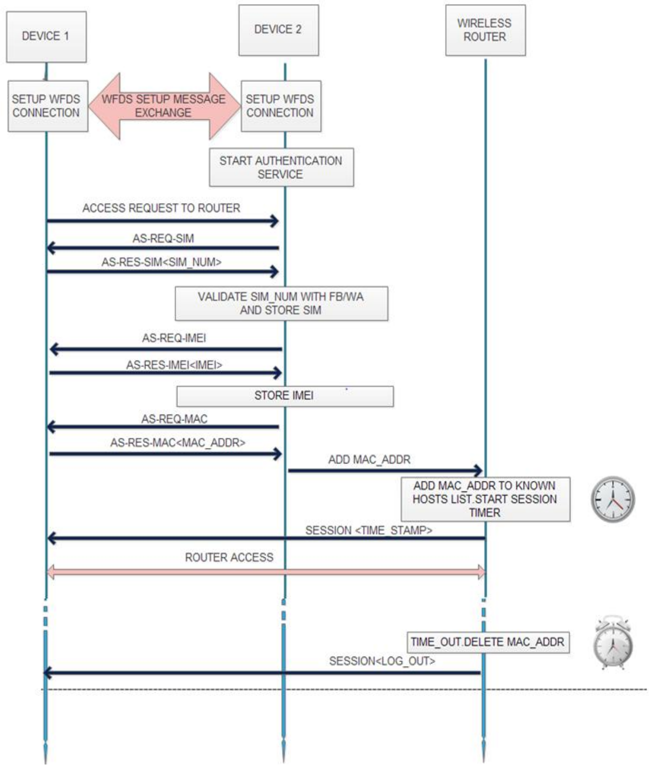

Fig. 2 Authentication service message exchange flow in WFDS

IV. USE CASE

The Authentication Service can be extended to NFC enabled hand held devices. The two devices exchange a sequence of messages to establish a NFC connection. All messages after this are exchanged over NFC. The message flow is shown in Fig. 3

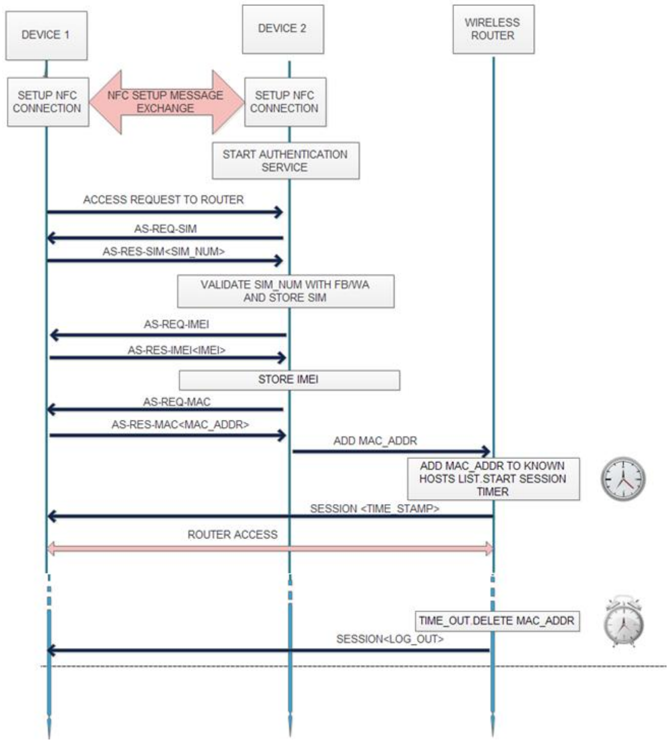

Fig. 3 Authentication service message exchange flow in NFC

V. CONCLUSION

Authentication of the device user for an access to any network plays a crucial role in the security of that network. In this paper we were introduced to Authentication Service that runs over Wi-Fi direct/NFC. With this service the administrator of a home/Public Wi-Fi network is able to authenticate a new user and provide access to the network without sharing the pass phrase to the user.

ACKNOWLEDGMENT

I thank Mr. Neeraj Garg and Mr. Vinoth Sampath of Broadcom Corporation for giving me an opportunity to come with this paper. Special thanks to Mr. Vinoth Sampath for his suggestions and comments which helped me to improve the quality of the paper. I am very thankful to Mr. Santhosh Kamath for his constant motivation and guidance throughout the course of the paper.

REFERENCES

[1] “Analysis and design of a SIM based authentication solution for WLAN”, Anja Feldmann, 2004

[2] “Use of SIM Card Authentication in the Open Web Platform”, John Mattsson, pp.1-3, *Ericsson Research*

[3] Wi-Fi Direct Services Technical Specification Version 0.1.

[4] Wi-Fi Peer-to-Peer (P2P) Technical Specification Version 0.1.