NFC-triggered IMS Flow Mobility across Different Devices

Vassilis Zafeiris*
Department of Informatics
Athens University of Economics and Business
Patission 76
Athens, Greece

Petros Belsis† Christos Skourlas‡
Department of Informatics
Technological Educational Institute of Athens
Ag. Spyridonos 12
Athens, Greece

ABSTRACT

Smartphones are gradually providing support for advanced user applications with high computation and network bandwidth requirements. However, their usually restricted size raises usability issues. A need is emerging for utilization and collaboration with devices in the user's reach that provide advanced capabilities. The 3GPP IP Multimedia Subsystem (IMS) is making an important contribution toward this direction, through specifications for distribution and replication of a multimedia session's media components to multiple devices that either belong to the same or different subscriptions. The IMS Service Continuity capability enables the transfer of one or more media components of an IMS session across different user devices. Although IMS can handle the media flow transfer, the user is still required to be engaged in a tedious device discovery and configuration process. We propose an out-of-band signaling mechanism, based on Near Field Communication (NFC) connectivity for fast and effortless initialization of a collaborative multimedia session between devices in close proximity that may involve the transfer of one or more media flows among them. We specify the utilization of an intuitive NFC touch interface for (a) user and device discovery and (b) negotiation of media stream properties (e.g. encoding, transport protocol) during the transfer of a media flow among different devices.

Categories and Subject Descriptors

C.2.2 [**Network Protocols**]: Applications; J.m [**Computer Applications**]: Miscellaneous

General Terms

Reliability, Design

*bzafiris@aueb.gr

†pbelsis@cs.teiath.gr

‡cskourlas@teiath.gr

Keywords

IMS, NFC, service continuity, flow mobility, inter-device media transfer

1. INTRODUCTION

Smart-phones are progressively evolving to platforms that provide access to the user's personal, recreation and business application environment. They combine secure identification with high processing power capabilities, as well as, access to increased bandwidth and coverage through multiple radio access technologies. 3GPP network architecture contributes toward this direction through (a) the packet-switched core network architecture, Evolved Packet Core, that enables the integration of different technology access networks, and (b) the IP Multimedia Subsystem (IMS) that enables access-independent delivery of services by application and content providers. Despite smart-phones' increasing access to processing power and connectivity resources, their usually restricted size raises usability issues. A need is emerging for utilization and collaboration with advanced capabilities' devices in the user's environment. This will shift a smart-phone's role toward a coordinator and integrator of the capabilities offered by the user's computing environment. 3GPP IMS is making an internet standard's compliant contribution toward this direction through specifications for distribution and replication of a multimedia session's media components to multiple devices that either belong to the same or different subscriptions [5, 3].

Some of the capabilities provided by IMS for session continuity and distribution across different devices are highlighted through a case study scenario. Assume a doctor that provides medical support in the place of an accident situated in an urban area. The doctor utilizes her smart-phone to engage in a multimedia telephony session with a specialist in the hospital that provides instructions and information on the patient's medical record. However, the restricted dimensions and density of her smart-phone's display do not allow a detailed view to visualizations and instructions provided by the specialist. In order to overcome her device's constraints, the doctor borrows and employs the advanced multimedia capabilities of a passer-by's tablet for rendering the video component of the multimedia session, while still talking to the hospital specialist through her own phone.

Although IMS can handle the transfer of a media flow across different devices, the user is still required to provide IMS-related identification information regarding the target device and its subscriber. Thus, the user must be engaged in a tedious device discovery and configuration process that complicates the ad-hoc collaboration of close-by devices or the utilization of public multimedia infrastructure (e.g., IMS capable video or audio reproduction equipment).

In this work we propose an out-of-band signaling mechanism, based on Near Field Communication (NFC) connectivity, for fast and effortless initialization of a collaborative multimedia session between devices in close proximity that may involve the transfer of one or more media flows among them. The rest of the paper is structured as following: Section 2 presents work relevant to the use of NFC for ad-hoc collaboration of user devices, Section 3 makes an introduction to the IMS Service Continuity capability and its enhancements for inter-device media transfer, Section 4 describes the proposed solution for triggering inter-device media transfer through NFC. The paper is concluded in Section 5 with future extensions to this work.

2. RELATED WORK

Mobile payments and access control represent common application areas for NFC. In [7] a mobile payment system is specified that employs NFC for interaction with existing Point of Sale systems. A generic access control scheme for NFC-enabled smartphones is presented in [8]. The proposed solution is token-based and can be applied for controlled access to both digital objects, e.g. electronic documents, and restricted physical areas. NFC enables the delegation of access tokens and, thus, of access rights among users without contacting a central token issuer.

A number of scenarios of peer-to-peer interactions between devices through NFC are presented in [9]. These interactions are referred to as micro-interactions and may involve peer devices of different persons (e.g. smart-phones) or devices of a single person (e.g. smart-phone to TV or PC). Moreover, it introduces a framework for utilization of micro-interactions without pre-configuration from a large class of user applications.

Fast configuration of device connectivity is proposed by NFC Forum as a basic capability that can be provided through NFC [2]. Suggested application areas involve the pairing of Bluetooth-enabled devices or the configuration of a device for WiFi access, through contact of the device to another device or tag. As concerning Bluetooth device pairing, NFC Forum provides recommendations for execution of the *Secure Simple Pairing* mechanism through an out-of-band signaling channel conveyed through NFC [15].

3. IMS SERVICE CONTINUITY

The IP Multimedia Subsystem (IMS) constitutes part of the 3GPP core network architecture and focuses on the delivery of multimedia services. It enables the delivery of various types of multimedia services to end-users by leveraging standard internet protocols, principally specified by IETF. IP connectivity is a basic requirement for access to IMS services, regardless of the type of access network technology (fixed or wireless) that provides IP access. Although the deployment of IMS in a 3GPP system does not require the presence of Circuit Switched (CS) core network elements, the IMS architecture supports the delivery of its services through CS connectivity [6]. IMS Centralized Services (ICS) architecture has a key role toward this direction, as it enables access to all services and service control exclusively through IMS mechanisms and enablers [4]. Moreover, IMS Centralized Services support the transfer of IMS sessions among the Circuit Switched and Packet Switched (PS) domains of a 3GPP system or across different IP-based access networks, regardless of the support of network layer mobility or not. This capability is referred to in the IMS terminology as IMS Service Continuity [5].

IMS Service Continuity (IMS SC) refers to continuity of multimedia sessions while the User Equipment (UE) is moving from the Packet Switched (PS) to the Circuit Switched (CS) domain, and vice versa, or is roaming across different access networks that provide IP connectivity. Moreover, IMS SC enables the transfer of an IMS session (or a subset of its media flows) among the radio interfaces of a user device or across different user devices. As concerning the latter, it is supported by the Inter-User Equipment Transfer (IUT) enhancements to IMS SC [3, 5] that allows a multimedia session to be shared among user devices that belong to the same user subscription or different subscriptions under the same operator.

A core part of the IMS Centralized Services architecture and a basic functional element of IMS Service Continuity is the Service Centralization and Continuity Application Server (SCC AS). The SCC AS is introduced in the signaling path between the ICS-enhanced user device and the remote party. It is configured as the first and last Application Server (AS) that processes session signaling for originating or terminating sessions respectively. The role of the SCC AS is to establish and control IMS sessions on behalf of the user device, in cases that it uses the Circuit Switched domain for session signaling or media transfer. Moreover, it makes decisions (based on user device configuration, session media components, subscription, operator policies etc.) on the termination of incoming IMS sessions by assigning the delivery of media traffic to (a) either the PS, CS domain or both and (b) one or more user devices that are authorized to serve session traffic [4].

3.1 Inter-UE Transfer enhancements

Inter-UE Transfer (IUT) enhancements specify the support of advanced scenarios of IMS SC, where session control, session traffic or individual media flows, that constitute part of a session (e.g. the video stream of a multimedia telephony session), are distributed across different user devices that belong to the same or different user subscriptions of a single domain [3]. Session distribution refers to (a) capability of addition, removal, modification or replication of media flows across different user devices and (b) participation of multiple devices in session control. An IMS session that engages multiple devices in session control, either in the origination or termination side, is referred to as Collaborative Session [3]. Among the participants of a Collaborative Session, a single user device has the role of the *Controller UE*, while the rest of them have the role of the *Controllee UE*. The service profile of the Controller UE determines the services that will be established with the remote party. Moreover, the Controller UE authorizes all IUT related actions.

The SCC AS has a key role in IUT since it constitutes an anchor point for IMS signaling for all devices that a specific user needs to engage in a Collaborative Session. Specifically, it terminates the session control signaling paths (*access legs* in IMS terminology) of all IUT-enhanced devices participating in a session. On the other hand, it originates a single session control signaling path (*remote leg*) toward the re-

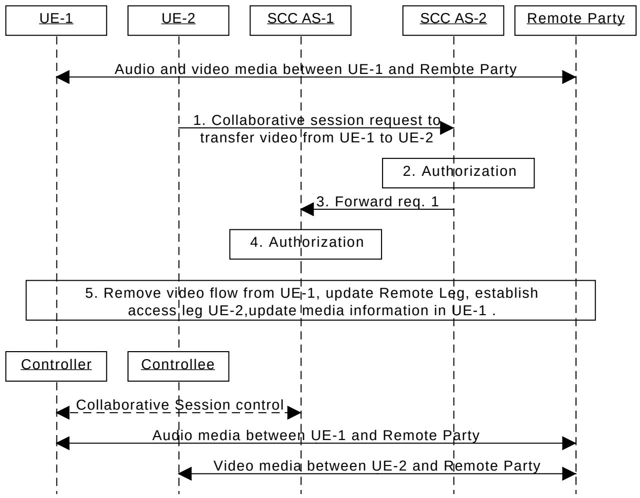

Figure 1: IUT between devices belonging to different subscriptions [3].

mote party by combining, if required, two or more access legs. A Collaborative Session is, thus, characterized by the presence of multiple access paths toward the SCC AS, originating from different radio interfaces of the same device or from different user devices. Note that, the establishment of a Collaborative Session is not mandatory for making use of IUT capabilities. However, in the absence of a Collaborative Session, IUT results to transfer of the entire session (control and media traffic) among the source and target devices.

Figure 1 illustrates the interaction of two user devices, that belong to different subscriptions, with the SCC AS during the execution of an IUT operation. The operation affects a multimedia telephony session that is established between user device UE_1 and a remote party. Specifically, it involves the participation of user device UE_2 in the ongoing session of UE_1, through the transfer of the video media component to UE_2. The scenario is documented in IUT enhancements 3GPP specification [3], while a similar scenario of IUT initiated by the source UE (UE_1) is documented in the base IMS Service Continuity specification [5]. The figure does not include the Serving-Call Session Control Function (S-CSCF) servers of each subscriber that provide user registration and route IMS signaling to and from the respective SCC AS elements.

The IUT target, UE_2, initiates the interaction through an IUT request for participation in a Collaborative Session controlled by UE_1, where the video flow will be transferred to and served by UE_2 (step 1). The request must include sufficient information for the network to (a) identify the media flow to be transferred and the session that contains it, as well as the source and target UEs, and (b) give control of the Collaborative Session to UE_1. The request is authorized and forwarded toward UE_1 from SCC AS_2 that serves UE_2 (steps 2). However, prior to reaching UE_1, the request is routed to SCC AS_1 that will subsequently control the Collaborative Session (step 3). SCC AS_1 authorizes the request for flow transfer on the basis of user preferences or through signaling exchange with UE_1 (step 4). Finally, SCC AS_1 establishes an access leg with UE_2 and updates the remote leg with the new device that will serve the video flow (step 5).

Besides signaling exchange, the execution of a media flow transfer between devices belonging to different subscriptions requires active user involvement for its successful completion. As regards the initial IUT request from UE_2 (step 1), it must include information that identifies UE_1 and its user, as well as the multimedia session and the media flow to be transferred. Although IMS specifies an information flow for session discovery [5], the user of UE_2 still needs to provide the user and device identification for the session discovery request to SCC AS. The same information, concerning UE_2, must be provided by the user of UE_1, during a UE_1-initiated media flow transfer toward UE_2.

Such user involvement, complicates the spontaneous collaboration of close-by user devices or the utilization of public infrastructure (e.g. IMS capable audiovisual equipment). In order to relieve the user from a tedious device discovery and configuration process, we propose an out-of-band signaling mechanism, based on Near Field Communication (NFC) connectivity, for enhancing IUT operations. Specifically, we specify the utilization of an intuitive NFC touch interface for (a) user and device discovery and (b) negotiation of media stream properties (e.g. encoding, transport protocol) during IUT flow transfer between devices of different IMS subscribers.

4. NFC-TRIGGERED IUT

Near Field Communication (NFC) is a RFID-compatible technology that enables data exchange in close proximity ($<$ 20cm) between pairs of devices. Connection establishment is automatic, once NFC devices are close enough, without requiring pairing. Unlike RFID, where one device has the role of the reader and the other of a passive transponder, NFC enables peer-to-peer communication between devices with continuous interchange of the sender/receiver roles in both parties [10].

NFC Forum highlights the potential of NFC as a technology enabler, as it introduces a new interface to existing devices through touch interaction [2]. Among the proposed applications is the pairing of Bluetooth-enabled devices or the configuration of a device for WiFi access, through contact of a device to another device or tag. Toward this direction, NFC Forum, in cooperation with the Bluetooth SIG, provides recommendations for enhancing user experience in applications that use Bluetooth through NFC [15]. These enhancements are related to device discovery, pairing and application launching. As concerning device pairing, it specifies the execution of the *Secure Simple Pairing* mechanism through an out-of-band signaling channel conveyed through NFC.

In this work, we propose the use of NFC for enhancing the establishment of an IMS collaborative session and the transfer of media flows among IUT-capable devices of different subscribers. The focus is on the discovery of the IUT target and the negotiation of the media flow to be transferred to the device. Since minimal user involvement is a basic requirement, the interaction for inter-device media transfer will be triggered by simple contact between the source and target devices. A basic requirement for NFC-triggered IUT is the presence, in both the source and target devices, of appropriate software infrastructure that can be deployed as

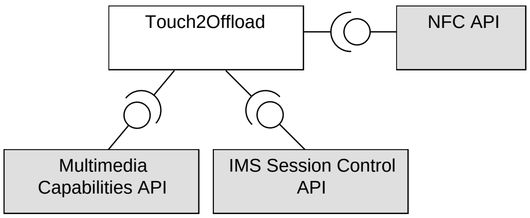

Figure 2: Touch2Offload mobile application architecture

a mobile or desktop application. This application will be, henceforth, referred to as *Touch2Offload*, since it enables, through a touch event, the offloading of media traffic to another device.

4.1 Touch2Offload application architecture

Touch2Offload delivers its functionality based on APIs provided by the operating system and device's communication frameworks. Figure 2 presents API dependencies of the application that comprise:

- Multimedia Capabilities API for access to device configuration information including (a) supported audio and video codecs and (b) multimedia capture and playback capabilities,
- IMS Session Control API for discovery and control of ongoing IMS sessions,
- NFC API for device discovery and communication through NFC.

The application needs to be pre-installed in a user device in order to initialize NFC-triggered flow transfers. On the other hand, target devices may download the application from a software repository once a touch from a Touch2Offload peer is perceived. This capability is currently supported in Android (from version 4.0/API Level 14) through the Android Application Record (AAR) information element of an NFC message. The AAR identifies the application that should be activated in order to handle the NFC message conveyed through the touch interaction. If the application is not available in the target device, Android launches the Google Play application for its download [1].

4.2 NFC Information flow

This section presents the interaction between user devices during the establishment of an IMS Collaborative Session for IUT media transfer. The interaction is based on message exchange through NFC and is coordinated by *Touch2Offload* application instances executing on the source and target devices. Message exchange between NFC devices operating in peer mode is based on the Simple NDEF Exchange Protocol (SNEP) [14]. SNEP is a request/response, application-level protocol that carries in the payload of each protocol data unit a single NDEF (NFC Data Exchange Format) message or a fragment of it. NDEF is a basic message construct for information exchange between NFC applications that contains one or more NDEF records. NDEF records encapsulate the application data transferred between the NFC devices [13].

A device submitting a SNEP request has the role of the SNEP client, while the recipient device acts as a SNEP server. Each SNEP request encapsulates an NDEF message and is characterized by a request code denoting the type of the request, e.g. GET for retrieval of a specific NDEF message from the server, PUT for requesting the server to accept the transmitted message etc. A SNEP response indicates the status of the server's request processing and may include an NDEF result message.

Figure 3 presents the interaction of user devices through NFC for the initialization of an inter-device media transfer. The message exchange enables the device UE_2, of the IUT scenario introduced in Figure 1, to successfully request its participation in a Collaborative Session with UE_1. Then, the session's bidirectional video stream component will be transferred and served by UE_2.

The interaction is triggered by getting the devices close enough for NFC communication. The source device, UE_1, initiates the IUT flow transfer negotiation with a SNEP GET request for the retrieval of target device IMS identification, as well as of information that verifies its capability to participate in the IUT procedure (*message 1*). The latter comprises the network domain that UE_2 is registered to and the IUT capabilities that UE_2 supports. Note that IUT operations can take place among devices that belong to the same or different subscriptions under the same operator. Device identification is performed with the Temporary Globally Routable User Agent URI (T-GRUU), a URI that uniquely identifies in IMS the availability of a subscriber to a specific device [6]. IMS specifies both Public and Temporary GRUUs, each one representing a unique combination of Public User Identity and device. Unlike a Public GRUU, a T-GRUU is not long-lived and does not include a reference to the subscriber's Public User Identity. Thus, the anonymity of both parties is protected after IMS session completion.

Each SNEP message includes an identification of the *Touch2Offload* application in order to ensure its proper processing. Android employs the Android Application Record for this purpose [1]. In case that *Touch2Offload* is not available in the target device, AAR enables its discovery and retrieval from a software repository upon user approval (*message 2*). *Touch2Offload* generates a SNEP SUCCESS response with all required information (*message 3*) in case that user preferences and device capabilities allow the engagement in an IUT session.

Once the target device succesfully responds to the initial SNEP request, UE_1 proceeds with negotiation of the codecs that will be used by the target device while serving the video flow. Negotiation begins with a SNEP GET request encapsulating a Service Description Protocol offer [11] (*message 4*). The SDP offer lists the codecs that the remote party supports for the media flow under transfer. This information was provided and cached to UE_1 during IMS session establishment. Depending on its multimedia capabilities, UE_2 responds with an appropriate SDP response (*message 5*). The latter will also be forwarded to the remote party during IUT execution. However, NFC negotiation of SDP parameters limits the UE_2's interaction with the remote party to a single message exchange.

Media negotiation is followed by a SNEP PUT request with all information that is required by UE_2 for identification to SCC AS_1 of the video flow to be transferred. Specifically, the request includes the following data elements: (a)

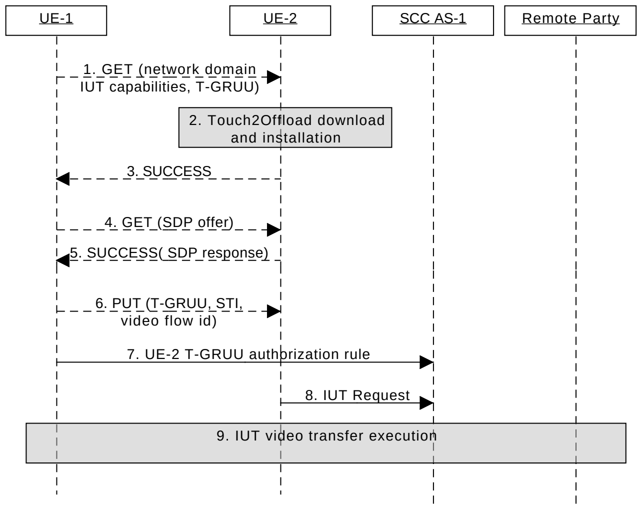

Figure 3: Interaction through NFC (dashed lines) and IMS for media flow tranfser.

T-GRUU of the source device, (b) Session Transfer Identifier that identifies the session that the flow is part of and (c) SDP label that identifies the video flow within the IMS session [12]. The interaction continues with configuration of an appropriate rule to SCC-AS_1 by UE_1, for automatic authorization of UE_2 participation in the collaborative session (*message 7*). Finally, UE_2 submits an IUT request for initiation of the video flow transfer (*message 8*).

5. CONCLUSIONS AND FUTURE WORK

We have proposed an out-of-band signaling mechanism, based on Near Field Communication (NFC) connectivity, for triggering and fast configuration of inter-device transfers of media flows belonging to an ongoing IP Multimedia Subsystem (IMS) session. The mechanism will be deployed to user devices in the form of a desktop or mobile application called *Touch2Offload*. We specify the requirements for *Touch2Offload* in terms of (a) the NFC message exchange that needs to take place between application instances for triggering inter-device flow transfer, and (b) IMS-relevant content of each NFC message. Our future work will involve a prototype implementation of the proposed capability.

6. ACKNOWLEDGMENTS

This research has been co-funded by the European Union (Social Fund) and Greek national resources under the framework of the "Archimedes III: Funding of Research Groups in TEI of Athens" project of the "Education and Lifelong Learning" Operational Programme.

7. REFERENCES

[1] Android NFC Basics. http://developer.android.com /guide/topics/connectivity/nfc/nfc.html.
[2] NFC Forum. http://www.nfc-forum.org.
[3] 3GPP. IP Multimedia Subsystem (IMS) Service Continuity; Inter-UE Transfer enhancements; Stage 2 (Release 10). Technical Report TS 23.831 v10.0.0, 2010.
[4] 3GPP. IP Multimedia Subsystem (IMS) centralized services; Stage 2 (Release 12). Technical Report TS 23.292 v12.0.0, 2012.
[5] 3GPP. IP Multimedia Subsystem (IMS) Service Continuity; Stage 2 (Release 12). Technical Report TS 23.237 v12.1.0, 2012.
[6] 3GPP. IP Multimedia Subsystem (IMS); Stage 2 (Release 11). Technical Report TS 23.228 v11.7.0, 2012.
[7] W. Chen, G. P. Hancke, K. E. Mayes, Y. Lien, and J. H. Chiu. Nfc mobile transactions and authentication based on gsm network. In *Second International Workshop on Near Field Communication (NFC)*, pages 83–89, 2010.
[8] A. Dmitrienko, A.-R. Sadeghi, S. Tamrakar, and C. Wachsmann. Smarttokens: Delegable access control with nfc-enabled smartphones. In S. Katzenbeisser, E. Weippl, L. Camp, M. Volkamer, M. Reiter, and X. Zhang, editors, *Trust and Trustworthy Computing*, volume 7344 of *Lecture Notes in Computer Science*, pages 219–238. Springer Berlin Heidelberg, 2012.
[9] B. Dodson and M. S. Lam. Micro-interactions with NFC-Enabled Mobile Phones. In J. Zhang, J. Wilkiewicz, and A. Nahapetian, editors, *Mobile Computing, Applications, and Services*, pages 118–136. Springer Berlin Heidelberg, 2012.
[10] K. Finkenzeller. *RFID Handbook, 3rd Edition*. Wiley, 2010.
[11] IETF Network Working Group. SDP: Session Description Protocol. Proposed Standard RFC 4566, 2006.
[12] IETF Network Working Group. The Session Description Protocol (SDP) Label Attribute. Proposed Standard RFC 4574, 2006.
[13] NFC Forum. NFC Data Exchange Format. Technical Specification NFCForum-TS-NDEF 1.0, 2006.
[14] NFC Forum. Simple NDEF Exchange Protocol. Technical Specification NFCForum-TS-SNEP 1.0, 2011.
[15] NFC Forum, Bluetooth SIG. Bluetooth Secure Simple Pairing Using NFC. Application Document NFCForum-AD-BTSSP 1.0, 2011.