Network Working Group
Request for Comments: 5677
Category: Standards Track

T. Melia, Ed.
Alcatel-Lucent
G. Bajko
Nokia
S. Das
Telcordia Technologies Inc.
N. Golmie
NIST
JC. Zuniga
InterDigital Communications, LLC

December 2009

IEEE 802.21 Mobility Services Framework Design (MSFD)

Abstract

This document describes a mobility services framework design (MSFD) for the IEEE 802.21 Media Independent Handover (MIH) protocol that addresses identified issues associated with the transport of MIH messages. The document also describes mechanisms for Mobility Services (MoS) discovery and transport-layer mechanisms for the reliable delivery of MIH messages. This document does not provide mechanisms for securing the communication between a mobile node (MN) and the Mobility Server. Instead, it is assumed that either lower-layer (e.g., link-layer) security mechanisms or overall system-specific proprietary security solutions are used.

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

IESG Note

As described later in this specification, this protocol does not provide security mechanisms. In some deployment situations lower-layer security services may be sufficient. Other situations require proprietary mechanisms or as yet incomplete standard mechanisms, such as the ones currently considered by IEEE. For these reasons, the specification recommends careful analysis before considering any deployment.

The IESG emphasizes the importance of these recommendations. The IESG also notes that this specification deviates from the traditional IETF requirement that support for security in the open Internet environment is a mandatory part of any Standards Track protocol specification. An exception has been made for this specification, but this should not be taken to mean that other future specifications are free from this requirement.

Copyright Notice

Table of Contents

1. Introduction

This document proposes a solution to the issues identified in the problem statement document [RFC5164] for the layer 3 transport of IEEE 802.21 MIH protocols.

The MIH Layer 3 transport problem is divided into two main parts: the discovery of a node that supports specific Mobility Services (MoS) and the transport of the information between a mobile node (MN) and the discovered node. The discovery process is required for the MN to obtain the information needed for MIH protocol communication with a peer node. The information includes the transport address (e.g., the IP address) of the peer node and the types of MoS provided by the peer node.

This document lists the major MoS deployment scenarios. It describes the solution architecture, including the MSFD reference model and MIHF identifiers. MoS discovery procedures explain how the MN discovers Mobility Servers in its home network, in a visited network or in a third-party network. The remainder of this document describes the MIH transport architecture, example message flows for several signaling scenarios, and security issues.

This document does not provide mechanisms for securing the communication between a mobile node and the Mobility Server. Instead, it is assumed that either lower layer (e.g., link layer) security mechanisms, or overall system-specific proprietary security solutions, are used. The details of such lower layer and/or proprietary mechanisms are beyond the scope of this document. It is RECOMMENDED against using this protocol without careful analysis that these mechanisms meet the desired requirements, and encourages future standardization work in this area. The IEEE 802.21a Task Group has recently started work on MIH security issues that may provide some solution in this area. For further information, please refer to Section 8.

2. Terminology

The following acronyms and terminology are used in this document:

Media Independent Handover (MIH): the handover support architecture defined by the IEEE 802.21 working group that consists of the MIH Function (MIHF), MIH Network Entities, and MIH protocol messages.

Media Independent Handover Function (MIHF): a switching function that provides handover services including the Event Service (ES), Information Service (IS), and Command Service (CS), through service access points (SAPs) defined by the IEEE 802.21 working group [IEEE80221].

MIHF User: An entity that uses the MIH SAPs to access MIHF services, and which is responsible for initiating and terminating MIH signaling.

Media Independent Handover Function Identifier (MIHFID): an identifier required to uniquely identify the MIHF endpoints for delivering mobility services (MoS); it is implemented as either a FQDN or NAI.

Mobility Services (MoS): composed of Information Service, Command Service, and Event Service provided by the network to mobile nodes to facilitate handover preparation and handover decision, as described in [IEEE80221] and [RFC5164].

MoSh: Mobility Services provided by the mobile node's Home Network.

MoSv: Mobility Services provided by the Visited Network.

MoS3: Mobility Services provided by a third-party network, which is a network that is neither the Home Network nor the current Visited Network.

Mobile Node (MN): an Internet device whose location changes, along with its point of connection to the network.

Mobility Services Transport Protocol (MSTP): a protocol that is used to deliver MIH protocol messages from an MIHF to other MIH-aware nodes in a network.

Information Service (IS): a MoS that originates at the lower or upper layers of the protocol stack and sends information to the local or remote upper or lower layers of the protocol stack. The purpose of IS is to exchange information elements (IEs) relating to various neighboring network information.

Event Service (ES): a MoS that originates at a remote MIHF or the lower layers of the local protocol stack and sends information to the local MIHF or local higher layers. The purpose of the ES is to report changes in link status (e.g., Link Going Down messages) and various lower layer events.

Command Service (CS): a MoS that sends commands from the remote MIHF or local upper layers to the remote or local lower layers of the protocol stack to switch links or to get link status.

Fully Qualified Domain Name (FQDN): a complete domain name for a host on the Internet, showing (in reverse order) the full delegation path from the DNS root and top-level domain down to the host name (e.g., myexample.example.org).

Network Access Identifier (NAI): the user ID that a user submits during network access authentication [RFC4282]. For mobile users, the NAI identifies the user and helps to route the authentication request message.

Network Address Translator (NAT): a device that implements the Network Address Translation function described in [RFC3022], in which local or private network layer addresses are mapped to routable (outside the NAT domain) network addresses and port numbers.

Dynamic Host Configuration Protocol (DHCP): protocols described in [RFC2131] and [RFC3315] that allow Internet devices to obtain respectively IPv4 and IPv6 addresses, subnet masks, default gateway addresses, and other IP configuration information from DHCP servers.

Domain Name System (DNS): a protocol described in [RFC1035] that translates domain names to IP addresses.

Authentication, Authorization, and Accounting (AAA): a set of network management services that respectively determine the validity of a user’s ID, determine whether a user is allowed to use network resources, and track users’ use of network resources.

Home AAA (AAAh): an AAA server located on the MN’s home network.

Visited AAA (AAAv): an AAA server located in a visited network that is not the MN’s home network.

MIH Acknowledgement (MIH ACK): an MIH signaling message that an MIHF sends in response to an MIH message from a sending MIHF.

Point of Service (PoS): a network-side MIHF instance that exchanges MIH messages with an MN-based MIHF.

Network Access Server (NAS): a server to which an MN initially connects when it is trying to gain a connection to a network and that determines whether the MN is allowed to connect to the NAS's network.

User Datagram Protocol (UDP): a connectionless transport-layer protocol used to send datagrams between a source and a destination at a given port, defined in RFC 768.

Transmission Control Protocol (TCP): a stream-oriented transport-layer protocol that provides a reliable delivery service with congestion control, defined in RFC 793.

Round-Trip Time (RTT): an estimation of the time required for a segment to travel from a source to a destination and an acknowledgement to return to the source that is used by TCP in connection with timer expirations to determine when a segment is considered lost and should be resent.

Maximum Transmission Unit (MTU): the largest size of an IP packet that can be sent on a network segment without requiring fragmentation [RFC1191].

Path MTU (PMTU): the largest size of an IP packet that can be sent on an end-to-end network path without requiring IP fragmentation.

Transport Layer Security Protocol (TLS): an application layer protocol that primarily assures privacy and data integrity between two communicating network entities [RFC5246].

Sender Maximum Segment Size (SMSS): size of the largest segment that the sender can transmit as per [RFC5681].

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Deployment Scenarios

This section describes the various possible deployment scenarios for the MN and the Mobility Server. The relative positioning of the MN and Mobility Server affects MoS discovery as well as the performance of the MIH signaling service. This document addresses the scenarios listed in [RFC5164] and specifies transport options to carry the MIH protocol over IP.

3.1. Scenario S1: Home Network MoS

In this scenario, the MN and the services are located in the home network. We refer to this set of services as MoSh as shown in Figure 1. The MoSh can be located at the access network the MN uses to connect to the home network, or it can be located elsewhere.

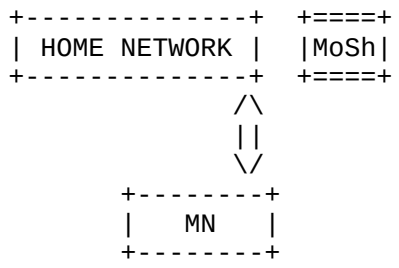

Figure 1: MoS in the Home Network

3.2. Scenario S2: Visited Network MoS

In this scenario, the MN is in the visited network and mobility services are provided by the visited network. We refer to this as MoSv as shown in Figure 2.

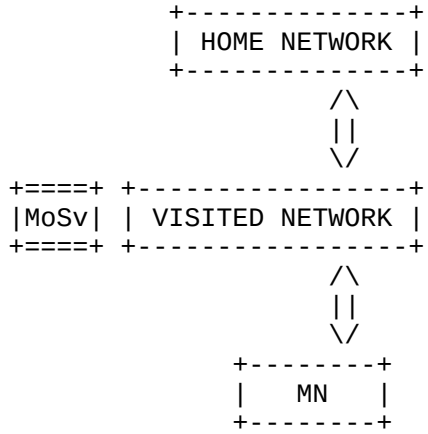

Figure 2: MoSv in the Visited Network

3.3. Scenario S3: Third-Party MoS

In this scenario, the MN is in its home network or in a visited network and services are provided by a third-party network. We refer to this situation as MoS3 as shown in Figure 3. (Note that MoS can exist both in home and in visited networks.)

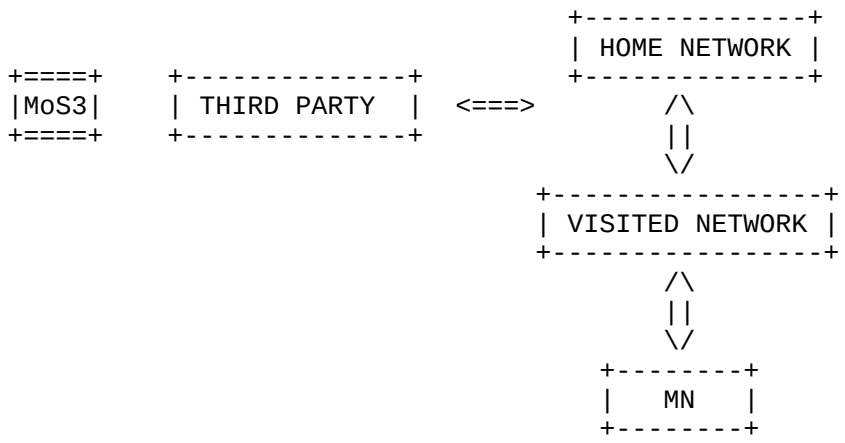

Figure 3: MoS from a Third Party

3.4. Scenario S4: Roaming MoS

In this scenario, the MN is located in the visited network and all MIH services are provided by the home network, as shown in Figure 4.

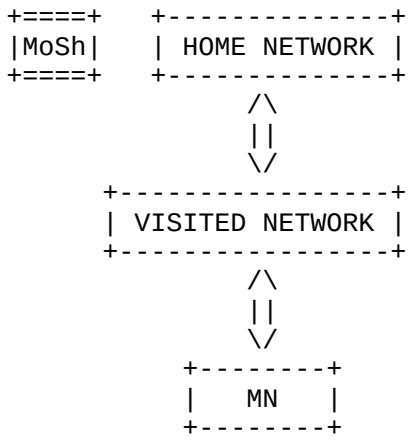

Figure 4: MoS Provided by the Home While in Visited

Different types of MoS can be provided independently of other types and there is no strict relationship between ES, CS, and IS, nor is there a requirement that the entities that provide these services should be co-located. However, while IS tends to involve a large amount of static information, ES and CS are dynamic services and some relationships between them can be expected, e.g., a handover command (CS) could be issued upon reception of a link event (ES). This document does not make any assumption on the location of the MoS (although there might be some preferred configurations), and aims at flexible MSFD to discover different services in different locations to optimize handover performance. MoS discovery is discussed in more detail in Section 5.

4. Solution Overview

As mentioned in Section 1, the solution space is being divided into two functional domains: discovery and transport. The following assumptions have been made:

- The solution is primarily aimed at supporting IEEE 802.21 MIH services -- namely, Information Service (IS), Event Service (ES), and Command Service (CS).
- If the MIHFID is available, FQDN or NAI’s realm is used for mobility service discovery.
- The solutions are chosen to cover all possible deployment scenarios as described in Section 3.
- MoS discovery can be performed during initial network attachment or at any time thereafter.

The MN may know the realm of the Mobility Server to be discovered. The MN may also be pre-configured with the address of the Mobility Server to be used. In case the MN does not know what realm / Mobility Server to query, dynamic assignment methods are described in Section 5.

The discovery of the Mobility Server (and the related configuration at MIHF level) is required to bind two MIHF peers (e.g., MN and Mobility Server) with their respective IP addresses. Discovery MUST be executed in the following conditions:

- Bootstrapping: upon successful Layer 2 network attachment, the MN MAY be required to use DHCP for address configuration. These procedures can carry the required information for MoS configuration in specific DHCP options.

- If the MN does not receive MoS information during network attachment and the MN does not have a pre-configured Mobility Server, it MUST run a discovery procedure upon initial IP address configuration.

- If the MN changes its IP address (e.g., upon handover), it MUST refresh MIHF peer bindings (i.e., MIHF registration process). In case the Mobility Server used is not suitable anymore (e.g., too large RTT experienced), the MN MAY need to perform a new discovery procedure.

- If the MN is a multi-homed device and it communicates with the same Mobility Server via different IP addresses, it MAY run discovery procedures if one of the IP addresses changes.

Once the MIHF peer has been discovered, MIH information can be exchanged between MIH peers over a transport protocol such as UDP or TCP. The usage of transport protocols is described in Section 6 and packing of the MIH messages does not require extra framing since the MIH protocol defined in [IEEE80221] already contains a length field.

4.1. Architecture

Figure 5 depicts the MSFD reference model and its components within a node. The topmost layer is the MIHF user. This set of applications consists of one or more MIH clients that are responsible for operations such as generating query and response, processing Layer 2 triggers as part of the ES, and initiating and carrying out handover operations as part of the CS. Beneath the MIHF user is the MIHF itself. This function is responsible for MoS discovery, as well as creating, maintaining, modifying, and destroying MIH signaling associations with other MIHFs located in MIH peer nodes. Below the MIHF are various transport-layer protocols as well as address discovery functions.

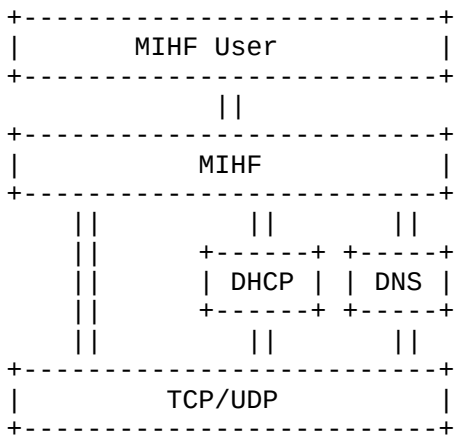

Figure 5: MN Stack

The MIHF relies on the services provided by TCP and UDP for transporting MIH messages, and relies on DHCP and DNS for peer discovery. In cases where the peer MIHF IP address is not pre-configured, the source MIHF needs to discover it either via DHCP or DNS as described in Section 5. Once the peer MIHF is discovered, the MIHF must exchange messages with its peer over either UDP or TCP. Specific recommendations regarding the choice of transport protocols are provided in Section 6.

There are no security features currently defined as part of the MIH protocol level. However, security can be provided either at the transport or IP layer where it is necessary. Section 8 provides guidelines and recommendations for security.

4.2. MIHF Identifiers (FQDN, NAI)

MIHFID is required to uniquely identify the MIHF end points for delivering the mobility services (MoS). Thus an MIHF identifier needs to be unique within a domain where mobility services are provided and independent of the configured IP address(es). An MIHFID MUST be represented either in the form of an FQDN [RFC2181] or NAI [RFC4282]. An MIHFID can be pre-configured or discovered through the discovery methods described in Section 5.

5. MoS Discovery

The MoS discovery method depends on whether the MN attempts to discover a Mobility Server in the home network, in the visited network, or in a third-party remote network that is neither the home network nor the visited network. In the case where the MN already

has a Mobility Server address pre-configured, it is not necessary to run the discovery procedure. If the MN does not have pre-configured Mobility Server, the following procedure applies.

In the case where a Mobility Server is provided locally (scenarios S1 and S2), the discovery techniques described in [RFC5678] and [RFC5679] are both applicable as described in Sections 5.1 and 5.2.

In the case where a Mobility Server is located in the home network while the MN is in the visited network (scenario S4), the DNS-based discovery described in [RFC5679] is applicable.

In the case where a Mobility Server is located in a third-party network that is different from the current visited network (scenario S3), only the DNS-based discovery method described in [RFC5679] is applicable.

It should be noted that authorization of an MN to use a specific Mobility Server is neither in scope of this document nor is currently specified in [IEEE80221]. We further assume all devices can access discovered MoS. In case future deployments will implement authorization policies, the mobile nodes should fall back to other learned MoS if authorization is denied.

5.1. MoS Discovery When MN and MoSh Are in the Home Network (Scenario S1)

To discover a Mobility Server in the home network, the MN SHOULD use the DNS-based MoS discovery method described in [RFC5679]. In order to use that mechanism, the MN MUST have its home domain pre-configured (i.e., subscription is tied to a network). The DNS query option is shown in Figure 6a. Alternatively, the MN MAY use the DHCP options for MoS discovery [RFC5678] as shown in Figure 6b (in some deployments, a DHCP relay may not be present).

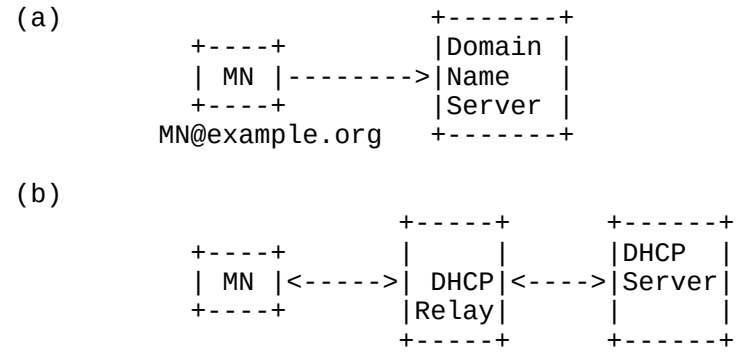

Figure 6: MOS Discovery (a) Using DNS Query, (b) Using DHCP Option

5.2. MoS Discovery When MN and MoSv Both Are in Visited Network (Scenario S2)

To discover a Mobility Server in the visited network, the MN SHOULD attempt to use the DHCP options for MoS discovery [RFC5678] as shown in Figure 7.

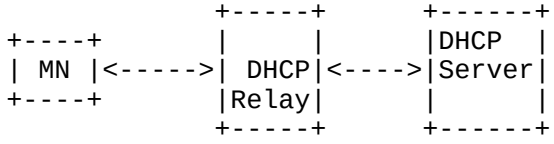

Figure 7: MoS Discovery Using DHCP Options

5.3. MoS Discovery When MIH Services Are in a Third-Party Remote Network (Scenario S3)

To discover a Mobility Server in a remote network other than home network, the MN MUST use the DNS-based MoS discovery method described in [RFC5679]. The MN MUST first learn the domain name of the network containing the MoS it is searching for. The MN can query its current Mobility Server to find out the domain name of a specific network or the domain name of a network at a specific location (as in Figure 8a). IEEE 802.21 defines information elements such as OPERATOR ID and SERVICE PROVIDER ID that can be a domain name. An IS query can provide this information, see [IEEE80221].

Alternatively, the MN MAY query a Mobility Server previously known to learn the domain name of the desired network. Finally, the MN MUST use DNS-based discovery mechanisms to find a Mobility Server in the

remote network as in Figure 8b. It should be noted that step b can only be performed upon obtaining the domain name of the remote network.

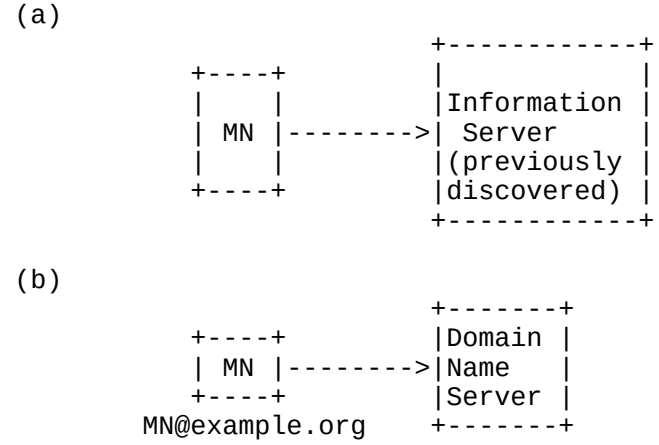

Figure 8: MOS Discovery Using (a) IS Query to a Known IS Server, (b) DNS Query

5.4. MoS Discovery When the MN Is in a Visited Network and Services Are at the Home Network (Scenario S4)

To discover a Mobility Server in the visited network when MIH services are provided by the home network, the DNS-based discovery method described in [RFC5679] is applicable. To discover the Mobility Server at home while in a visited network using DNS, the MN SHOULD use the procedures described in Section 5.1.

6. MIH Transport Options

Once the MoS have been discovered, MIH peers run a capability discovery and subscription procedure as specified in [IEEE80221]. MIH peers MAY exchange information over TCP, UDP, or any other transport supported by both the server and the client. The client MAY use the DNS discovery mechanism to discover which transport protocols are supported by the server in addition to TCP and UDP that are recommended in this document. While either protocol can provide the basic transport functionality required, there are performance trade-offs and unique characteristics associated with each that need to be considered in the context of the MIH services for different network loss and congestion conditions. The objectives of this section are to discuss these trade-offs for different MIH settings such as the MIH message size and rate, and the retransmission parameters. In addition, factors such as NAT traversal are also

discussed. Given the reliability requirements for the MIH transport, it is assumed in this discussion that the MIH ACK mechanism is to be used in conjunction with UDP, while it MUST NOT be used with TCP since TCP includes acknowledgement and retransmission functionality.

6.1. MIH Message Size

Although the MIH message size varies widely from about 30 bytes (for a capability discovery request) to around 65000 bytes (for an IS MIH_Get_Information response primitive), a typical MIH message size for the ES or CS ranges between 50 to 100 bytes [IEEE80221]. Thus, considering the effects of the MIH message size on the performance of the transport protocol brings us to discussing two main issues, related to fragmentation of long messages in the context of UDP and the concatenation of short messages in the context of TCP.

Since transporting long MIH messages may require fragmentation that is not available in UDP, if MIH is using UDP a limit MUST be set on the size of the MIH message based on the path MTU to destination (or the Minimum MTU where PMTU is not implemented). The Minimum MTU depends on the IP version used for transmission, and is the lesser of the first hop MTU, and 576 or 1280 bytes for IPv4 [RFC1122] or for IPv6 [RFC2460], respectively, although applications may reduce these values to guard against the presence of tunnels.

According to [IEEE80221], when an MIH message is sent using an L3 or higher-layer transport, L3 takes care of any fragmentation issue and the MIH protocol does not handle fragmentation in such cases. Thus, MIH layer fragmentation MUST NOT be used together with IP layer fragmentation and MUST not be used when MIH packets are carried over TCP.

The loss of an IP fragment leads to the retransmission of an entire MIH message, which in turn leads to poor end-to-end delay performance in addition to wasted bandwidth. Additional recommendations in [RFC5405] apply for limiting the size of the MIH message when using UDP and assuming IP layer fragmentation. In terms of dealing with short messages, TCP has the capability to concatenate very short messages in order to reduce the overall bandwidth overhead. However, this reduced overhead comes at the cost of additional delay to complete an MIH transaction, which may not be acceptable for CS and ES. Note also that TCP is a stream-oriented protocol and measures data flow in terms of bytes, not messages. Thus, it is possible to split messages across multiple TCP segments if they are long enough. Even short messages can be split across two segments. This can also cause unacceptable delays, especially if the link quality is severely degraded as is likely to happen when the MN is exiting a wireless access coverage area. The use of the TCP_NODELAY option can

alleviate this problem by triggering transmission of a segment less than the SMSS. (It should be noted that [RFC4960] addresses both of these problems, but discussion of SCTP is omitted here, as it is generally not used for the mobility services discussed in this document.)

6.2. MIH Message Rate

The frequency of MIH messages varies according to the MIH service type. It is expected that CS/ES messages arrive at a rate of one in hundreds of milliseconds in order to capture quick changes in the environment and/or process handover commands. On the other hand, IS messages are exchanged mainly every time a new network is visited, which may be in order of hours or days. Therefore, a burst of either short CS/ES messages or long IS message exchanges (in the case where multiple MIH nodes request information) may lead to network congestion. While the built-in rate-limiting controls available in TCP may be well suited for dealing with these congestion conditions, this may result in large transmission delays that may be unacceptable for the timely delivery of ES or CS messages. On the other hand, if UDP is used, a rate-limiting effect similar to the one obtained with TCP SHOULD be obtained by adequately adjusting the parameters of a token bucket regulator as defined in the MIH specifications [IEEE80221]. Recommendations for token bucket parameter settings are as follows:

- If the MIHF knows the RTT (e.g., based on the request/response MIH protocol exchange between two MIH peers), the rate can be based upon this as specified in [IEEE80221].

- If not, then on average it SHOULD NOT send more than one UDP message every 3 seconds.

6.3. Retransmission

For TCP, the retransmission timeout is adjusted according to the measured RTT. However due to the exponential backoff mechanism, the delay associated with retransmission timeouts may increase significantly with increased packet loss.

If UDP is being used to carry MIH messages, MIH MUST use MIH ACKs. An MIH message is retransmitted if its corresponding MIH ACK is not received by the generating node within a timeout interval set by the MIHF. The maximum number of retransmissions is configurable and the value of the retransmission timer is computed according to the algorithm defined in [RFC2988]. The default maximum number of

retransmissions is set to 2 and the initial retransmission timer (TMO) is set to 3s when RTT is not known. The maximum TMO is set to 30s.

6.4. NAT Traversal

There are no known issues for NAT traversal when using TCP. The default connection timeout of 2 hours 4 minutes [RFC5382] (assuming a 2-hour TCP keep-alive) is considered adequate for MIH transport purposes. However, issues with NAT traversal using UDP are documented in [RFC5405]. Communication failures are experienced when middleboxes destroy the per-flow state associated with an application session during periods when the application does not exchange any UDP traffic. Hence, communication between the MN and the Mobility Server SHOULD be able to gracefully handle such failures and implement mechanisms to re-establish their UDP sessions. In addition and in order to avoid such failures, MIH messages MAY be sent periodically, similarly to keep-alive messages, in an attempt to refresh middlebox state. As [RFC4787] requires a minimum state timeout of 2 minutes or more, MIH messages using UDP as transport SHOULD be sent once every 2 minutes. Re-registration or event indication messages as defined in [IEEE80221] MAY be used for this purpose.

6.5. General Guidelines

The ES and CS messages are small in nature and have tight latency requirements. On the other hand, IS messages are more resilient in terms of latency constraints, and some long IS messages could exceed the MTU of the path to the destination. TCP SHOULD be used as the default transport for all messages. However, UDP in combination with MIH acknowledgement SHOULD be used for transporting ES and CS messages that are shorter than or equal to the path MTU as described in Section 6.1.

For both UDP and TCP cases, if a port number is not explicitly assigned (e.g., by the DNS SRV), MIH messages sent over UDP, TCP, or other supported transport MUST use the default port number defined in Section 9 for that particular transport.

A Mobility Server MUST support both UDP and TCP for MIH transport and the MN MUST support TCP. Additionally, the server and MN MAY support additional transport mechanisms. The MN MAY use the procedures defined in [RFC5679] to discover additional transport protocols supported by the server (e.g., SCTP).

7. Operation Flows

Figure 9 gives an example operation flow between MIHF peers when an MIH user requests an IS and both the MN and the Mobility Server are in the MN's home network. DHCP is used for Mobility Services (MoS) discovery, and TCP is used for establishing a transport connection to carry the IS messages. When the Mobility Server is not pre-configured, the MIH user needs to discover the IP address of the Mobility Server to communicate with the remote MIHF. Therefore, the MIH user sends a discovery request message to the local MIHF as defined in [IEEE80221].

In this example (one could draw similar mechanisms with DHCPv6), we assume that MoS discovery is performed before a transport connection is established with the remote MIHF, and the DHCP client process is invoked via some internal APIs. The DHCP client sends a DHCP INFORM message according to standard DHCP and with the MoS option as defined in [RFC5678]. The DHCP server replies via a DHCP ACK message with the IP address of the Mobility Server. The Mobility Server address is then passed to the MIHF locally via some internal APIs. The MIHF generates the discovery response message and passes it on to the corresponding MIH user. The MIH user generates an IS query addressed to the remote Mobility Server. The MIHF invokes the underlying TCP client, which establishes a transport connection with the remote peer. Once the transport connection is established, the MIHF sends the IS query via an MIH protocol REQUEST message. The message and query arrive at the destination MIHF and MIH user, respectively. The Mobility Server MIH user responds to the corresponding IS query and the Mobility Server MIHF sends the IS response via an MIH protocol RESPONSE message. The message arrives at the source MIHF, which passes the IS response on to the corresponding MIH user.

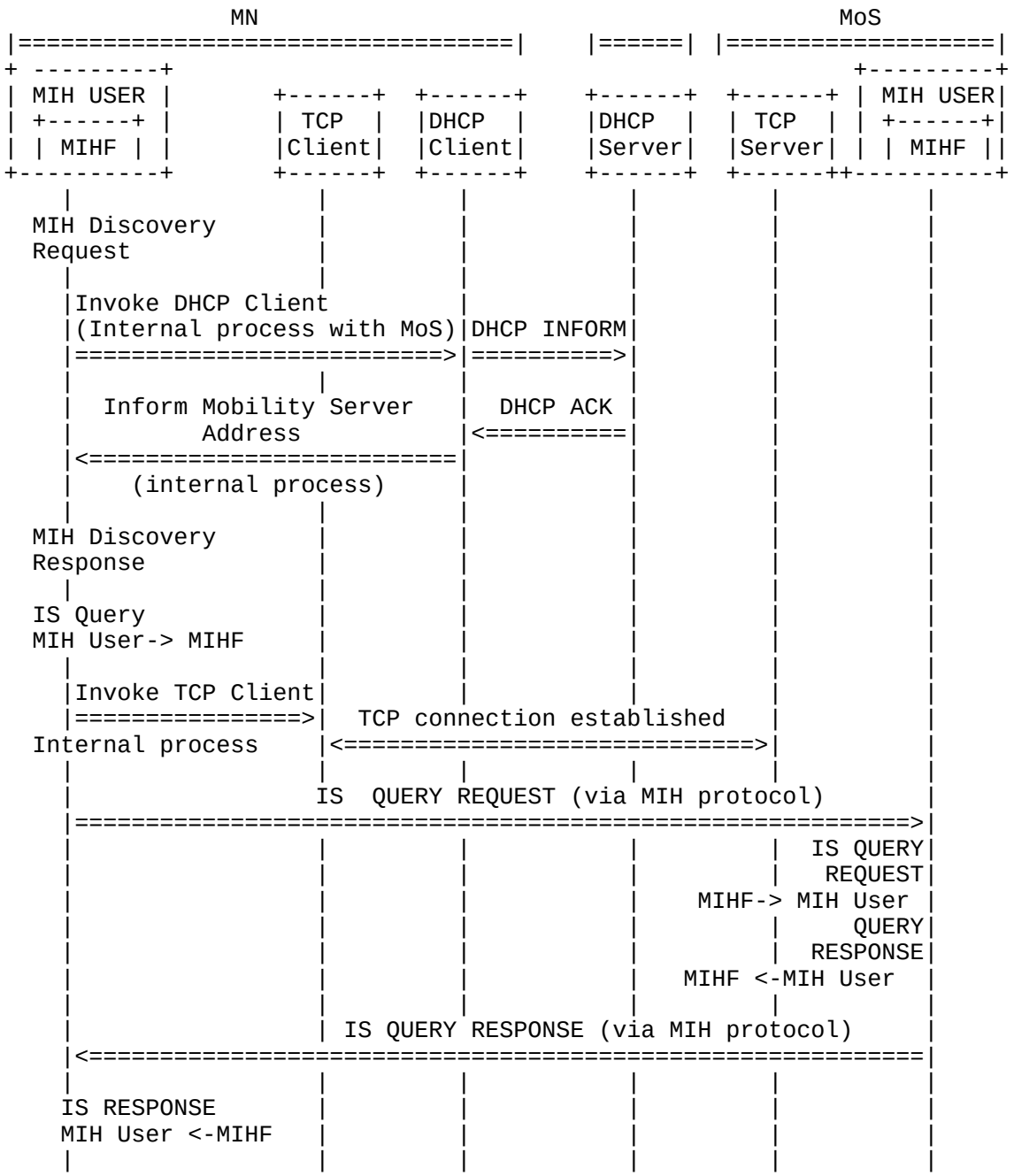

Figure 9: Example Flow of Operation Involving MIH User

8. Security Considerations

There are two components to the security considerations: MoS discovery and MIH transport. For MoS discovery, DHCP and DNS recommendations are hereby provided per IETF guidelines. For MIH transport, we describe the security threats and expect that the system deployment will have means to mitigate such threats when sensitive information is being exchanged between the mobile node and Mobility Server. Since IEEE 802.21 base specification does not provide MIH protocol level security, it is assumed that either lower layer security (e.g., link layer) or overall system-specific (e.g., proprietary) security solutions are available. The present document does not provide any guidelines in this regard. It is stressed that the IEEE 802.21a Task Group has recently started work on MIH security issues that may provide some solution in this area. Finally, authorization of an MN to use a specific Mobility Server, as stated in Section 5, is neither in scope of this document nor is currently specified in [IEEE80221].

8.1. Security Considerations for MoS Discovery

There are a number of security issues that need to be taken into account during node discovery. In the case where DHCP is used for node discovery and authentication of the source and content of DHCP messages is required, network administrators SHOULD use the DHCP authentication option described in [RFC3118], where available, or rely upon link layer security. [RFC3118] provides mechanisms for both entity authentication and message authentication. In the case where the DHCP authentication mechanism is not available, administrators may need to rely upon the underlying link layer security. In such cases, the link between the DHCP client and Layer 2 termination point may be protected, but the DHCP message source and its messages cannot be authenticated or the integrity of the latter checked unless there exits a security binding between link layer and DHCP layer.

In the case where DNS is used for discovering MoS, fake DNS requests and responses may cause denial of service (DoS) and the inability of the MN to perform a proper handover, respectively. Where networks are exposed to such DoS, it is RECOMMENDED that DNS service providers use the Domain Name System Security Extensions (DNSSEC) as described in [RFC4033]. Readers may also refer to [RFC4641] to consider the aspects of DNSSEC operational practices.

8.2. Security Considerations for MIH Transport

The communication between an MN and a Mobility Server is exposed to a number of security threats:

- Mobility Server identity spoofing. A fake Mobility Server could provide the MNs with bogus data and force them to select the wrong network or to make a wrong handover decision.

- Tampering. Tampering with the information provided by a Mobility Server may result in the MN making wrong network selection or handover decisions.

- Replay attack. Since Mobility Services as defined in [IEEE80221] support a 'PUSH model', they can send large amounts of data to the MNs whenever the Mobility Server thinks that the data is relevant for the MN. An attacker may intercept the data sent by the Mobility Server to the MNs and replay it at a later time, causing the MNs to make network selection or handover decisions that are not valid at that point in time.

- Eavesdropping. By snooping the communication between an MN and a Mobility Server, an attacker may be able to trace a user's movement between networks or cells, or predict future movements, by inspecting handover service messages.

There are many deployment-specific system security solutions available, which can be used to countermeasure the above mentioned threats. For example, for the MoSh and MoSv scenarios (including roaming scenarios), link layer security may be sufficient to protect the communication between the MN and Mobility Server. This is a typical mobile operator environment where link layer security provides authentication, data confidentiality, and integrity. In other scenarios, such as the third-party MoS, link layer security solutions may not be sufficient to protect the communication path between the MN and the Mobility Server. The communication channel between MN and Mobility Server needs to be secured by other means.

The present document does not provide any specific guidelines about the way these security solutions should be deployed. However, if in the future the IEEE 802.21 Working Group amends the specification with MIH protocol level security or recommends the deployment scenarios, IETF may revisit the security considerations and recommend specific transport-layer security as appropriate.

9. IANA Considerations

This document registers the following TCP and UDP ports with IANA:

Keyword	Decimal	Description
ieee-mih	4551/tcp	MIH Services
ieee-mih	4551/udp	MIH Services

10. Acknowledgements

The authors would like to thank Yoshihiro Ohba, David Griffith, Kevin Noll, Vijay Devarapalli, Patrick Stupar, and Sam Xia for their valuable comments, reviews, and fruitful discussions.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC3118] Droms, R., Ed., and W. Arbaugh, Ed., "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC5678] Bajko, G. and S. Das, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Services (MoS) Discovery", RFC 5678, December 2009.

[RFC5679] Bajko, G., "Locating IEEE 802.21 Mobility Services Using DNS", RFC 5679, December 2009.

11.2. Informative References

[IEEE80221] "IEEE Standard for Local and Metropolitan Area Networks - Part 21: Media Independent Handover Services", IEEE LAN/MAN Std 802.21-2008, January 2009, http://www.ieee802.org/21/private/Published%20Spec/802.21-2008.pdf (access to the document requires membership).

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2988] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", RFC 2988, November 2000.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, September 2006.

[RFC4787] Audet, F., Ed., and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, September 2007.

[RFC5164] Melia, T., Ed., "Mobility Services Transport: Problem Statement", RFC 5164, March 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5382] Guha, S., Ed., Biswas, K., Ford, B., Sivakumar, S., and P. Srisuresh, "NAT Behavioral Requirements for TCP", BCP 142, RFC 5382, October 2008.

[RFC5405] Eggert, L. and G. Fairhurst, "Unicast UDP Usage Guidelines for Application Designers", BCP 145, RFC 5405, November 2008.

[RFC5681] Allman, M., Paxson, V., and E. Blanton, "TCP Congestion Control", RFC 5681, September 2009.

Authors' Addresses

Telemaco Melia (editor)
Alcatel-Lucent
Route de Villejust
Nozay 91620
France

EMail: telemaco.melia@alcatel-lucent.com

Gabor Bajko
Nokia

EMail: Gabor.Bajko@nokia.com

Subir Das
Telcordia Technologies Inc.

EMail: subir@research.telcordia.com

Nada Golmie
NIST

EMail: nada.golmie@nist.gov

Juan Carlos Zuniga
InterDigital Communications, LLC

EMail: j.c.zuniga@ieee.org