IEEE International Symposium on Networks, Computers and Communications, May 2017

A Comparison of Migration and Multihoming Support in IPv6 and XIA

Nandi Zhang, Marvin A. Sirbu, Jon M. Peha
Department of Engineering and Public Policy
Carnegie Mellon University
nandiz@cmu.edu, sirbu@cmu.edu, peha@cmu.edu

Abstract— **Mobility and multihoming have become the norm in Internet access, e.g. smartphones with Wi-Fi and LTE, and connected vehicles with LTE and DSRC links that change rapidly. Mobility creates challenges for active session continuity when provider-aggregatable locators are used, while multihoming brings opportunities for improving resiliency and allocative efficiency. This paper proposes a novel migration protocol, in the context of the eXpressive Internet Architecture (XIA), the XIA Migration Protocol. We compare it with Mobile IPv6, with respect to handoff latency and overhead, flow migration support, and defense against spoofing and replay of protocol messages. Handoff latencies of the XIA Migration Protocol and Mobile IPv6 Enhanced Route Optimization are comparable and neither protocol opens up avenues for spoofing or replay attacks. However, XIA requires no mobility anchor point to support client mobility while Mobile IPv6 always depends on a home agent. We show that XIA has significant advantage over IPv6 for multihomed hosts and networks in terms of resiliency, scalability, load balancing and allocative efficiency. IPv6 multihoming solutions either forgo scalability (BGP-based) or sacrifice resiliency (NAT-based), while XIA's fallback-based multihoming provides fault tolerance without a heavy-weight protocol. XIA also allows fine-grained incoming load-balancing and QoS-matching by supporting flow migration. Flow migration is not possible using Mobile IPv6 when a single IPv6 address is associated with multiple flows. From a protocol design and architectural perspective, the key enablers of these benefits are flow-level migration, XIA's DAG-based locators and self-certifying identifiers.**

Keywords—mobility; multihoming; XIA; Mobile IPv6

I. INTRODUCTION

Mobile devices are an integral part of our everyday lives. By 2020, 80% of the adult population will own a smartphone [1]. A similar momentum is seen in mobile networks, such as Internet-connected cars, airplanes offering in-flight Wi-Fi, etc. By 2020, 75% of all cars shipped are predicted to have Internet access [2]. Mobile devices and networks are often equipped with multiple network interfaces, meaning that they can multihome. For example, a car may transmit to a roadside unit (RSU) using the Dedicated Short Range Communications (DSRC) protocol while simultaneously transmitting to a cellular base station.

Mobility and multihoming bring the need for a migration protocol. A mobile host may attach to different access networks as it moves, and typically receives a different Internet locator in each access network. A change in the locator can disrupt ongoing communications between a mobile host and its correspondents if the mobile host is no longer reachable at the previous locator while the correspondents do not recognize the new locator. A protocol is needed that migrates ongoing communications from using one access network to using another. Such a migration protocol would allow multihomed devices and networks to balance load by moving different application traffic to different access networks. Migration may also be warranted if a newly available network provides better QoS and/or lower cost for an ongoing session.

Migration can be performed at different granularities, namely flow-level, host-level, and network-level. Flow migration involves a change in the locators associated with an individual *flow*, which is useful when one would like to migrate some flows but not others. Host migration changes the locator associated with a *host*, which in turn can change the locators of all flows afforded by the host, making it possible to migrate all flows at once. One can also perform migration on a *network* level by changing the network locator, e.g. network prefix.

Today's state-of-the-art Internet architecture, TCP/IPv6, supports migration poorly. Flow migration support is limited to Multi-path TCP (MPTCP) [3]. The Mobile IPv6 (MIPv6) [4] host migration protocol is complex and depends on a fixed mobility anchor point. Network migration in the form of the Network Mobility (NEMO) Basic Support Protocol (BSP) [5] suffers from long packet propagation delays.

The eXpressive Internet Architecture (XIA) is a next-generation Internet architecture that features expressiveness, intrinsic security, and the use of directed acyclic graphs (DAGs) as locators. XIA allows users to express their "intent" to the network, so the ultimate endpoint of a communication is explicit. Intrinsic security ties an identifier to the public key of the corresponding entity, which facilitates authentication of migration signaling messages. DAG addressing creates flexibility for the network in fulfilling an intent, and provides redundancy for multihomed devices and networks. Exploiting these features, we have designed in the context of XIA a novel migration protocol that has the following properties:

- Allows fast migration for environments where connectivity changes frequently.
- Supports flow-level migration. Flow migration allows fine-grained load balancing for multihomed devices and networks, and allows an application to always use its preferred access network.

This research is supported by the National Science Foundation under awards CNS-1040757, CNS-1040800, and CNS-1040801.

978-1-5090-4260-9/17/$31.00 ©2017 IEEE

- A successful migration results in data traffic taking a direct path between the endpoints without routing through an off-path intermediary.
- Provides resiliency for multihomed devices and networks, with low overhead.

This paper is structured as follows. Section II reviews migration support in IPv6. Section III – V are the main contributions of this paper. Section III introduces XIA and the XIA Migration Protocol. Section IV presents a comparative evaluation of the XIA Migration Protocol and its IPv6 counterparts with respect to handoff performance and security. Section V discusses multihoming. We conclude in Section VI.

II. Migration Support in IPv6

Protocols used for migration in TCP/IPv6 include Mobile IPv6, Network Mobility Basic Support Protocol, Multipath TCP and the Stream Control Transmission Protocol.

A. MIPv6 and NEMO BSP

TCP/IPv6 features three sets of protocols for migration, each at a different granularity: MIPv6 [4] for host migration, NEMO BSP [5] for network migration and MPTCP [3] for flow migration. MIPv6 uses a special router called a home agent to maintain the mapping between a mobile host's "Home Address" and its current IP address acquired from a visited network. This allows a mobile host to appear to retain the same IP address as it changes point of attachment to the Internet, and thereby preserves continuity with correspondents. One major weakness of basic MIPv6 is triangular routing, where all traffic to and from a mobile host traverses the home agent that might be topologically far from the actual endpoints. An enhancement scheme, called Route Optimization [4], is introduced to circumvent triangular routing. However, Route Optimization brings with it additional signaling overhead and handoff latency. A further enhancement [6], Enhanced Route Optimization, makes use of cryptographically generated addresses (CGAs) [7]. The additional security provided by CGAs simplifies the authentication of signaling messages between a mobile host and its correspondent, and thereby reduces the signaling overhead introduced by Route Optimization. Route optimization for NEMO has not been standardized by the IETF, although there have been a number of proposals [8].

B. MPTCP and SCTP

MPTCP is an experimental TCP extension that allows one end-to-end connection to make use of multiple paths. MPTCP introduces a shim layer between the TCP layer and application layer, and is designed to be transparent to both layers. To an application, MPTCP presents a standard TCP interface [9]. To the network layer, a MPTCP connection looks like multiple independent, standard TCP flows.

MPTCP thus offers a complete mobility solution at the transport layer, and permits both soft and hard migration modes [10]. However, it requires both endpoints to support MPTCP, and does not work with non-TCP communications.

The Stream Control Transmission Protocol (SCTP) [11] is an IETF Standards Track reliable data transfer protocol and a complement to TCP at the transport layer. It natively supports multihoming, as a SCTP port can be associated with multiple IP addresses. Standard SCTP supports static multihoming, while a later extension enables dynamic address reconfiguration [12], which can be used to manage mobility [13]. However, similar to MPTCP, SCTP is not a general-purpose migration solution.

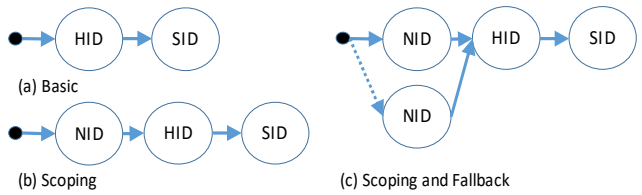

Fig. 1. Examples of DAGs

III. Migration in XIA

We propose the XIA Migration Protocol for migration of mobile clients with active sessions. In this section, we start with a review of XIA core concepts, followed by detailed protocol operation and message formats. Whenever applicable, we use the same terminologies as in MIPv6 and NEMO BSP to describe the protocol. Lastly, we briefly discuss a rendezvous service for migration of mobile servers.

A. XIA Backgrounds

XIA refers to communicating entities as principals, and names them with eXpressive identifiers (XIDs) [14]. Four main XID types are host XID (HID), service XID (SID), content XID (CID) and network XID (NID). XIDs are cryptographically derived to achieve intrinsic security. HID, SID and NID are hashes of the public keys of the corresponding host, service and network, respectively. A CID is the hash of the content itself.

XIA separates identifier (XID) and locator (DAG), which facilitates mobility [15]. An XIA locator is a DAG of XIDs, as shown in Fig. 1. The dot represents a conceptual source of the packet. The terminating XID represents the intent, or the end principal of a locator. We believe that mobile networks will be sufficiently numerous so that flat routing, where each mobile network is represented separately in the global routing table, is infeasible due to excessive burden on router hardware. Therefore, we assume that the locator for a mobile network uses "scoping" [14], as shown in Fig. 1b. That is, an application running on Host A attached to a mobile network served by Internet service provider (ISP) #1 will include ISP1 in its locator, e.g. $\cdot \rightarrow NID_{ISP1} \rightarrow NID_{mobile} \rightarrow HID_A \rightarrow SID$, as opposed to $\cdot \rightarrow NID_{mobile} \rightarrow HID_A \rightarrow SID$. Continuing with this example, if the upstream access network becomes ISP2, the locator should be updated to $\cdot \rightarrow NID_{ISP2} \rightarrow NID_{mobile} \rightarrow HID_A \rightarrow SID$.

Another feature of DAGs is fallbacks. Fallbacks are alternative routes to reach the intent, as shown by the dashed edge in Fig. 1c. DAG-based addressing in XIA brings immediate benefit for multihomed devices and networks because fallbacks can be used to expose the availability of multiple upstream access networks. XIA allows multihomed hosts and networks to build redundancy through DAG-based addressing, without burdening routing tables or adding middleboxes such as NAT [16].

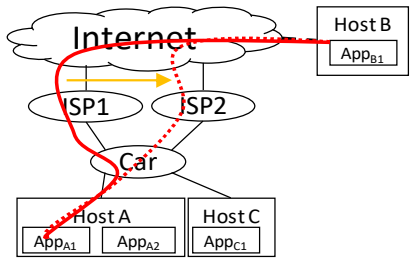

Fig. 2. Example Topology for Protocol Discussion

B. XIA Migration Protocol

1) The Need for a Migration Protocol

Hierarchical DAGs (*network_prefix:endpoint_id)* resemble the format of IP addresses. An endpoint thus has different DAGs when attached to different access networks. An endpoint may need to update its DAG over the course of a conversation with its corresponding endpoint, either because of mobility, *i.e.* when a device moves to a different access network, or for traffic engineering purposes, *e.g.* a multihomed device prioritizing one access network and not the other. A change in the DAG may disrupt ongoing communications, which is typically identified by source and destination identifier and locators. Along these lines, a migration protocol is needed to provide two functions: to certify the migrating endpoint's identity and to ensure that traffic can be rerouted to the new Internet location.

XIA inherently separates identifier and locator, allowing an endpoint to maintain the same identifier during a migration. MIPv6 achieves the same goal with two IP addresses, using home address as the identifier and care-of address as the locator. MIPv6 essentially manages the mapping between the two.

To ensure that the migrating endpoint can still receive packets from the ongoing conversation, MIPv6 either uses indirection (Bidirectional Tunneling mode) or sends the new locator directly to a correspondent (Route Optimization mode). The XIA Migration Protocol adopts a philosophy similar to Route Optimization mode and allows an endpoint to communicate its new DAG directly to its correspondent.

2) Message Formats

The design of the XIA Migration Protocol is fundamentally similar to the approach by Snoeren and Balakrishnan [17]. We will use a mobile vehicular network in Fig. 2 as an example to describe the protocol. The protocol consists of two messages, MIGRATE and MGRTACK (**migrate** **ack**nowledgement). Assume that the endpoint wants to migrate from ISP1 to ISP2. The MIGRATE message is sent from Application A1 (SID_{A1}) to its correspondent Application B1 (SID_{B1}). The MGRTACK message is the response to a valid MIGRATE message, confirming a successful migration.

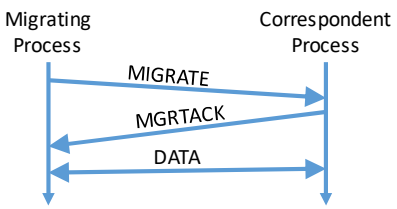

Fig. 3. Time Sequence Diagram of XIA Migration Protocol

TABLE I. DEFINITION OF MIGRATE MESSAGE

Destination	$\mathrm{DAG_{B1}}$
Source	$\cdot\rightarrow \mathrm{NID_{ISP2}} \rightarrow \mathrm{NID_{car}} \rightarrow \mathrm{HID_A} \rightarrow \mathrm{SID_{A1}}$
Body	$\{DAG_{A1,old}, \mathrm{DAG_{A1,new}}, SEQ, K_{SID_{A1}}\}^{K^{-1}_{SID_{A1}}}$
Example	$\left\{\begin{matrix}\cdot\rightarrow \mathrm{NID_{ISP1}} \rightarrow \mathrm{NID_{car}} \rightarrow \mathrm{HID_A} \rightarrow \mathrm{SID_{A1}},\\ \cdot\rightarrow \mathrm{NID_{ISP2}} \rightarrow \mathrm{NID_{car}} \rightarrow \mathrm{HID_A} \rightarrow \mathrm{SID_{A1}},\\ seq,\\ key\end{matrix}\right\}^{K^{-1}_{SID_{A1}}}$

TABLE II. DEFINITION OF MGRTACK MESSAGE

Destination	$\cdot\rightarrow \mathrm{NID_{ISP2}} \rightarrow \mathrm{NID_{car}} \rightarrow \mathrm{HID_A} \rightarrow \mathrm{SID_{A1}}$
Source	$\mathrm{DAG_{B1}}$
Body	$\{\mathrm{MGRTACK\ flag, SEQ, K_{SID_{B1}}}\}^{K^{-1}_{SID_{B1}}}$
Example	$\{\mathrm{MGRTACK\ flag, seq, key}\}^{K^{-1}_{SID_{B1}}}$

a) MIGRATE message

Note that the XIA Migration Protocol is a flow migration protocol. It lets an application notify its correspondent of a change in its locator. The MIGRATE message contains the old and new locator of Application A1, a sequence number (or, alternatively, a timestamp) and Application A1's public key.

Upon receipt of a MIGRATE message, Application B first checks the sequence number to see if this is a replayed MIGRATE message. If the MIGRATE message is fresh, it then verifies the signature on the MIGRATE message. If the signature is correct, Application B1 sends back a MGRTACK message. If any of these checks fails, Application B1 should discard the MIGRATE message in question.

b) MGRTACK message

The MGRTACK message contains the Migration Acknowledgement flag indicating this is a confirmation of receipt of a MIGRATE message, an echo of the sequence number, and the Application B1's public key.

The protocol is designed to be robust against accidental loss of protocol messages and during overlapping migration. After sending a MIGRATE message, Application A1 starts the MGRTACK timer. If Application A1 does not receive a MGRTACK message at its new locator before timeout, it should assume that the MIGRATE message is lost and resend the MIGRATE message. The number of migration retries is up to the implementation.

It might occur that a MIGRATE message from an earlier handover arrives later than the MIGRATE message of a current handover. The sequence number in MIGRATE and MGRTACK messages enables endpoints to identify stale messages. The sequence number and signature also serve to defend against spoofing and replay attacks, which we discuss in Section IV.

3) Interaction with X-Host Configuration Protocol

The XIA Migration Protocol provides a method for resuming a flow after migration to a new access network. There must be a complementary mechanism that notifies applications of the need to migrate in the first place. In XIA, X-Host Configuration Protocol (XHCP) [18] provides this functionality. An XHCP

Server broadcasts a periodic beacon containing the default router DAG along with other configuration information for bootstrapping a newly-joined host. Additionally, an XHCP Server broadcasts a BEACON whenever there is a change in upstream connectivity to notify hosts of the need for a migration.

It is assumed that, within a router, there is a mechanism that notifies the XHCP Server process when the router detects a new DAG on any of its WAN-side interfaces. When that happens, the router XHCP Server broadcasts an XHCP BEACON with the new router DAG(s), regardless of its position in the default broadcast cycle. In the case of a mobile router, the mobile router acts as an XHCP Client to the XHCP Server in the upstream access network and as an XHCP Server to hosts within its own network.

An XHCP BEACON also contains a CONFIG_CHANGED flag. A router sets CONFIG_CHANGED = 0(1) if none (any) of the network configuration information has changed since the last BEACON. XHCP Servers are required to cache a copy of the most recently-sent BEACON. Before issuing a new BEACON, an XHCP Server compares the network configuration information in the current BEACON against that in the previous BEACON. If they are the same, the CONFIG_CHANGED flag in the outgoing BEACON should be set to 0. If they are different, the CONFIG_CHANGED flag in the outing BEACON should be set to 1. If an XHCP Server has just booted up and does not have a copy of BEACON, it should always set the flag.

An XHCP BEACON contains the router DAG of the router sending the BEACON. For a multihomed network, i.e. when a router has multiple WAN-side interfaces, a router DAG may include fallbacks through different NIDs. The default router DAG is determined by the network's own policies in terms of performance, cost or other criteria.

The CONFIG_CHANGED flag is intended to be a quick indicator for XHCP Clients to tell whether they need to process the BEACON further due to a network configuration change. It saves a compare operation of potentially hundreds if not thousands of bits (each XID in a DAG is 160 bits). If CONFIG_CHANGED=0, XHCP Clients can discard the BEACON. If CONFIG_CHANGED=1, XHCP Clients should continue to examine the rest of the BEACON and process it as appropriate.

4) Supporting Mobile Services

The above solution allows a mobile *client* to maintain a connection. In order for a mobile *server* to be reachable for incoming connections, XIA uses a rendezvous service to track the current locator of a mobile server [19].

Conceptually, a rendezvous service may appear similar to an MIPv6 home agent. Whereas an MIPv6 home agent is required for both mobile clients and mobile servers, in XIA, a rendezvous service is optional for mobile clients, which means less infrastructure is needed to support client mobility.

5) Implementation

The XIA Migration Protocol has been implemented [20]. Active session migration for mobile clients and rendezvous services for mobile servers both perform as expected. A demonstration of migrating a video stream in a moving vehicle is available [21].

IV. Comparing Migration in IPv6 with XIA Migration Protocol

This section presents a comparison between migration support in IPv6 and in XIA. We start with a performance evaluation followed by a discussion on the security design of the migration protocols. The related issue of multihoming support is discussed separately in the next section.

A. Performance Comparison

We compare the handoff latency of each protocol, defined as the time period during which a packet sent by a correspondent host cannot be delivered to the migrating endpoint. This time period can be further divided into two phases. Assume that a mobile host does not multihome and that migration signaling is performed after a mobile host has associated with the new access network. Immediately after the mobile host disconnects from its previous upstream access network, there is a period when the mobile node is connected to no network before physical and link layer association with the new access network can be completed. The first phase contributes equally to the overall handoff latency regardless of the migration protocol being used, so it will not change the relative standing when we compare the handoff latency of each migration protocol. Of greater interest is the time period after the mobile host has associated with its new network, when the migrating endpoint executes the migration protocol. The time to complete migration signaling is protocol-specific, and thus affects handoff latency differently. More specifically, the contribution to handoff latency from running a migration protocol is the time it takes for a correspondent node/home agent to be informed of a migrating endpoint's new locator after the migrating endpoint gets the new locator.

We will compare performance in three scenarios corresponding to three levels of migration: flow migration, host migration, and network migration. We assume that there are f flows talking to c correspondent hosts per migrating host, h migrating hosts per mobile network.

In each scenario, we ask the following quantitative questions:

- What is handoff latency?
- What is the signaling overhead? i.e. what is total number of migration signaling messages?

We also ask the following qualitative questions protocol:

- Does data traffic take a direct path between the endpoints, or is it routed through an intermediary? In other words, is it route-optimized?
- Will a mobile service continue to be reachable after performing a migration using the protocol in question?
- Does the protocol support flow migration?

Starting with the qualitative comparison, among the five migration protocols, MIPv6 Bidirectional Tunneling mode and NEMO Basic Support Protocol are not route-optimized. All five protocols allow a mobile service to remain reachable using the

same identifier before and after migration. The rendezvous service in XIA can be viewed as the equivalent of a home agent in MIPv6 in this regard. Among the five migration protocols, only the XIA Migration Protocol supports flow migration. Flow migration allows fine-grained and flexible management of an application's access network usage, giving XIA a clear advantage over MIPv6 and NEMO BSP in the ability to improve allocative efficiency in multihomed environments. The XIA Migration Protocol holds a clear advantage over its IPv6 counterparts in our qualitative comparison.

Quantitatively, in terms of handoff latency, all protocols except MIPv6 Route Optimization are comparable. They can notify a correspondent node (in the case of XIA Migration Protocol and MIPv6 Enhanced Route Optimization) or a home agent (in the case of MIPv6 Bidirectional Tunneling and NEMO BSP) of a migrating endpoint's new locator with one one-way message, hence the $0.5RTT_{MNCN}/0.5RTT_{MNHA}$. MIPv6 Route Optimization is significantly slower due to its complex protocol message set.

In terms of the number of signaling messages consumed to perform a migration, MIPv6 Bidirectional Tunneling and NEMO Basic Support Protocol are clear winners for a host migration and a network migration, respectively. MIPv6 Route Optimization consumes the most signaling messages among the three MIPv6 variants. There is no clear winner between MIPv6 Enhanced Route Optimization and the XIA Migration Protocol. For MIPv6 Enhanced Route Optimization to consume fewer messages than the XIA Migration Protocol, it must be that $2+3c<2+2f$, or $f>1.5c$. That is, when there are more than 1.5 flows per correspondent node on average, the XIA Migration Protocol will use more messages than MIPv6 Enhanced Route Optimization does in migrating a host or a mobile network.

MIPv6 Bidirectional Tunneling and NEMO Basic Support Protocol both have a simple message set and low handoff latency, but they incur higher packet propagation delay due to the absence of Route Optimization.

In summary, we conclude that the XIA Migration Protocol and MIPv6 Enhanced Route Optimization are the better migration protocols among the five candidates, for their low handoff latency and route efficiency. The XIA Migration Protocol has the additional advantage of supporting flow migration, although it might come at the expense of higher signaling overhead when there are many flows to the same correspondent host, also referred to as "Signaling Storm" [22].

B. Security Comparison

To compare the security of migration protocols, we assess their respective abilities to withstand all possible attacks that involve either forging or replaying any of the messages in a migration protocol. Migration protocols provide a mechanism to redirect packets from one destination locator to a new destination locator. An attacker may exploit this capability in an attempt to disrupt a normal packet flow, causing denial-of-service, data breach and/or falsified information. Section IV.B.1 discusses the spoofed or replayed Binding Update (BU)/MIGRATE messages, since they would be the most harmful ones within the protocol message set. Section IV.B.2 discusses all other spoofed/replayed protocol messages.

1) Spoofed/Replayed BU/MIGRATE Messages

a) Threats and Consequences

Spoofed and replayed BU/MIGRATE messages present the biggest concern. Availability, confidentiality and message integrity would be at risk if BU/MIGRATE messages are not authenticated.

Availability. An attacker may forge a BU/MIGRATE message with the "migrate-to" locator set to any locator other than the victim's true locator. If a home agent or correspondent node accepts such a BU/MIGRATE, it would stop sending packets to the victim's true locator.

Confidentiality. An attacker may forge a BU/MIGRATE message with the "migrate-to" locator set to its own locator. If a home agent or correspondent node accepts such a BU/MIGRATE message, it would send packets destined to the victim to the attacker instead, potentially exposing the content of the message. An attacker could even spoof BU/MIGRATE messages to both endpoints of a session and stage a man-in-the-middle attack.

Message integrity. A man-in-the-middle could also modify the content of the packets received before forwarding them to the actual recipients. There are other mechanisms to defend against confidentiality and message integrity attacks, such as

TABLE III. SUMMARY OF MIPV6, NEMO AND XIA MIGRATION PROTOCOL

	MIPv6 Bidirectional Tunneling	MIPv6 Route Optimization	MIPv6 Enhanced RO	NEMO Basic Support	XIA
Protocol Message Set	BU, BA	BU, BA, HoTI*2, HoT *2, CoTI, CoT, BU, (BA)	BU, BA, Early BU+CoTI, Early BA+CoT, BU, (BA)	BU, BA	MIGRATE, MGRTACK
Route-optimized?	No	Yes	Yes	No	Yes
Flow migration?	No	No	No	No	Yes
# of messages Host migration:	2	$2+7c$	$2+3c$	n/a	$2+2f$
# of messages Network migration:	$2h$	$(2+7c)h$	$(2+3c)h$	2	$(2+2f)h$
Latency Host migration:	$0.5RTT_{MNHA}$	$1RTT_{MNHA}+1RTT_{MNHA}+1RTT_{HACN}+0.5RTT_{MNCN}$	$0.5RTT_{MNCN}$	n/a	$0.5RTT_{MNCN}$
Latency Network migration:	$0.5RTT_{MNHA}$	$1RTT_{MNHA}+1RTT_{MNHA}+1RTT_{HACN}+0.5RTT_{MNCN}$	$0.5RTT_{MNCN}$	$0.5RTT_{MRHA}$	$0.5RTT_{MNCN}$

encryption. Those methods are separate from the migration protocols themselves.

b) Defenses in Mobile IPv6

The primary defense mechanism against spoofing attacks in MIPv6 Route Optimization is the return routability procedure. The return routability procedure tests the reachability of the sender of a BU message at both the claimed home address and care-of address. It does not defend against attackers who are able to receive both the Home Test message and Care-of Test message, but practically limits the location of attackers to the path between a correspondent node and the home agent [23]. Attackers may attempt to replay a BU message to get around the return routability procedure, but a stale BU message would be identified by the correspondent node using the sequence number.

MIPv6 Enhanced Route Optimization builds upon the same reachability-probing principle, and adds an extra layer of protection through the use of CGAs. Because the home keygen token is transmitted encrypted, assuming that the mobile node's private key is not compromised, an attacker cannot steal the token to forge a BU message even if he is able to eavesdrop on the path between the correspondent node and the home agent, and receive the Home Test message.

c) Defenses in XIA Migration Protocol

Aside from provider-independent addresses [24], an IPv6 address is typically network-dependent. Successful completion of a return routability procedure in MIPv6 is a strong indication that a mobile node is entitled to use the claimed IPv6 addresses, including both the interface identifier and the subnet prefix. The XIA Migration Protocol, on the other hand, examines a network-independent field, typically an SID, when authenticating MIGRATE messages. The "subnet prefix" in the XIA locator is not authenticated. Therefore, when assessing the XIA Migration Protocol, we consider two types of spoofed locators separately, locators with spoofed intent XID and locators with spoofed intermediate XID(s).

The first type, spoofed intent (XID), is easy to spot. In the XIA Migration Protocol, a MIGRATE message must be signed with the sender's private key that is in turn tied to the sender's intent XID, similar to the use of CGA in MIPv6 Enhanced Route Optimization. Without the corresponding private key, a spoofed MIGRATE message will fail the signature check at the receiver and therefore will not be accepted. A replay of a MIGRATE message will be identified by the correspondent node from the sequence number.

The other type of spoofed locator is to use a legitimate intent XID but spoofed intermediate XIDs. Such attacks are harder to protect against. XIA Migration Protocol by default only authenticates the intent XID (typically the SID of the migrating process), even though each XID in the locator might be cryptographically generated. This makes the protocol vulnerable to malicious locators. For example, an attacker may initiate a flow with "$NID_{attacker}$: $HID_{attacker}$: $SID_{attacker}$", and then use "NID_{victim}: $HID_{attacker}$: $SID_{attacker}$" as the new locator in a MIGRATE message. The MIGRATE message would look legitimate to a correspondent node because the attacker can correctly sign it. However, when packets are sent to the new locator, they will be forwarded to the victim network, which becomes a model for a flooding attack against NID_{victim}.

Due to the use of DAGs in the XIA architecture, this kind of attack can occur with XIA that would be stopped in IPv6. However, such an attack can occur in any architecture using DAGs as locators, with or without a migration protocol, so it is not specifically a limitation of the XIA Migration Protocol itself. DAGs were adopted in XIA despite this known limitation, because DAGs have other advantages such as flexibility in packet forwarding [14]. DAGs also provide an inexpensive way for multihomed hosts and networks to build redundancy, which will be further discussed in Section V.

In summary, MIPv6 Enhanced Route Optimization is less vulnerable to spoofed BU/MIGRATE message attacks than the XIA Migration Protocol as a result of the thorough verification of both interface identifier as well as subnet prefix in MIPv6. Both protocols can defend against replay attacks, although they use different mechanisms to do so. MIPv6 Enhanced Route Optimization avoids public-key cryptography for every migration by design due to performance concerns. Increasing computational power in end devices will make universal adoption of public-key cryptography less of an issue.

2) Spoofing/Replaying Other Protocol Messages

Section IV.B.1 reviewed how MIPv6 and XIA Migration Protocol cope with spoofed or replayed BU/MIGRATE messages. This section will go over the remaining messages types in each protocol and show that spoofing or replaying those messages is not harmful.

a) Mobile IPv6 Enhanced Route Optimization

Spoofed or replayed HoTI and CoTI messages. Such messages will trigger the correspondent node to send HoT and CoT messages containing the tokens needed for authenticating a BU message. By themselves they are not harmful.

Spoofed or replayed HoT and CoT messages. Upon receiving a HoT or CoT message, a mobile node will extract the contained token from such messages and proceed to send a BU message, if the mobile node has a corresponding entry in its Binding Update List. If the mobile node has not previously sent a HoTI or CoTI message, it would not find the corresponding entry in that list, and would simply ignore the HoT and CoT messages.

Spoofed BA message. Such a message becomes an issue if the correspondent node has not received the BU message. It would indicate to the mobile node a successful registration that did not actually happen. However, the probability of such an event is small.

Replayed BA message. Such messages will be identified through a stale sequence number by the mobile node.

b) XIA Migration Protocol

Spoofed MGRTACK message. In a MGRTACK message, a correspondent node is required to sign the MGRTACK. An attacker needs to compromise the correspondent node's private key in order to forge a MGRTACK.

Replayed MGRTACK message. Such messages will be identified by the mobile node via the stale sequence number.

In summary, spoofing or replaying protocol messages other than the BU/MIGRATE message does not pose a major threat.

V. Comparing Multihoming Support in IP and XIA

Today's mobile devices are often equipped with multiple network interfaces. They frequently multihome and possess multiple Internet locators, a classic example being a smartphone connected to both a LTE network and a Wi-Fi network. Primary use cases of multihoming include increased redundancy, load balancing, and QoS matching.

This section highlights the role of migration protocols in multihomed environments. IPv6 and XIA differ greatly in terms of how hosts and networks can make use of multihoming. Migration is closely related to multihoming in XIA, while the two are largely independent under IPv6.

A. Using Multihoming to Improve Resiliency

One common incentive to multihome is to improve resiliency in case of upstream link failure. Hosts and networks that value uninterrupted connectivity can utilize multihoming because multiple link failures at the same time are less likely than a single link failure. In the event of a link failure, in-flight packets may be lost if they are forwarded onto the downed link. End users would like to shorten the reaction time to link failure, which we define as the time period during which in-flight packets cannot be delivered to the recipient after a link failure.

For network multihoming, the IP architecture has BGP-based and NAT-based solutions [24]. NAT-based solutions cannot preserve session continuity in the event of a link failure. For BGP-based, the reaction time depends on how quickly BGP converges when a link becomes unavailable. Reducing convergence time of dynamic routing protocols has proved difficult, and current solutions to do so come at the expense of router overhead and protocol complexity [25].

XIA provides a complementary failure-handling mechanism that would improve reaction time to link failure thanks to the fallback feature of DAGs. In XIA, applications have the option to construct their DAGs with fallbacks to expose multiple access networks. When a router makes a forwarding decision on a packet whose destination DAG contains fallback(s), if the link to the primary XID is unavailable, the router can simply switch to the appropriate fallback XID as the forwarding destination. As long as the router before the downed link is aware of the link failure and incoming packets contain usable fallbacks, those packets will be redirected to their final destination via an alternative route when the primary path has failed. In other words, a network multihomed with BGP relies solely on the routing system to provide fault tolerance. With XIA, every packet can carry failover information in the form of fallbacks.

This benefit of fallbacks extends to multihomed hosts as well, such as cell phones with both Wi-Fi and LTE connections. While a large network might afford running BGP, the same does not apply for smaller networks such as in-vehicle networks. For multihomed hosts, BGP-based multihoming is not an option.

B. Using Multihoming to Improve Allocative Efficiency

Access networks often provide different QoS's and/or charge different prices. For example, cellular networks are usually expensive in terms of cost per unit of data transmitted, but relatively reliable as long as one is in the coverage area. Vehicle-to-vehicle and vehicle-to-infrastructure communications using the DSRC protocol are relatively cheap, but their availability might be limited. On the other hand, applications' QoS requirements and willingness to pay vary.

The set of available access networks of a multihomed mobile host or network, and thus the available QoS's and prices, may change as the device moves. Applications with ongoing flows need to perform a migration, during which they choose which access network to migrate to. Because of diverse QoS requirements and willingness to pay, the preferred access network varies across flows. In order to satisfy all flows, it must be that individual flows can migrate to different access networks if they wish to. Therefore, our criterion for assessing Internet architectures in terms of ability to utilize multihoming is:

- Does the architecture support flow-level migration?

The MIPv6 protocol family performs migration typically at the host level, as flows on the same host usually share a single IP address in current implementations. NEMO BSP works at the network level. Only the XIA Migration Protocol can perform flow-level migration, making XIA particularly desirable for reaping multihoming benefits.

C. Load Balancing for Multihomed Hosts and Networks

Lastly, a multihomed host or network may wish to balance incoming load across all of its links to avoid congestion on one particular link. Assigning traffic to a particular link (corresponding to a particular locator) during flow initiation stage is well-understood [26]. To shift an existing flow between access networks, a flow migration protocol is needed. Granular flow-level migration protocols, including the XIA Migration Protocol, have a natural advantage over host-level solutions.

VI. Conclusions

In this paper, we briefly reviewed the Mobile IPv6, Network Mobility Basic Support Protocol and Multipath TCP. We presented the XIA Migration Protocol in the context of eXpressive Internet Architecture and compared it with the IPv6 mobility solutions. We then discussed the related issue of multihoming and presented a comparison between XIA and IP with respect to three multihoming use cases.

From a migration support perspective, both IPv6 and XIA provide acceptable solutions. The handoff latency of XIA Migration Protocol and Mobile IPv6 Enhanced Route Optimization are expected to be comparable, consuming one one-way message propagation time. In both cases, data traffic will take direct paths between the endpoints after a migration. Neither protocol creates significant vulnerability to spoofing or replay attacks. However, the two protocols differ slightly in terms of the infrastructure needed to support mobility. Home agents are required in MIPv6, regardless of whether the mobile node is a client or a server. A mobile node must establish a trust relationship with one or more home agents a priori, which represents higher overhead to engage in mobility, and the mobile node is dependent on the home agent when migration occurs. In contrast, a rendezvous service is optional in XIA if a mobile node only engages in client activities.

From a multihoming perspective, XIA has advantages over IP for two reasons. Regarding fault tolerance, existing IP solutions either forgo scalability or sacrifice resiliency. BGP-based multihoming is only suitable for larger networks, and mobile hosts and smaller networks like vehicular networks may not afford BGP. NAT-based multihoming works for hosts and networks of all sizes, but it does not preserve session continuity when a link fails. XIA's fallback-based multihoming achieves resiliency while remaining scalable as it does not rely on a heavy-weight protocol like BGP, or a middle box like NAT that breaks session continuity. Moreover, the reaction time to link failure is shorter in XIA due to DAG-based locators; in an XIA network with DAGs, packets can be rerouted to a fallback path after a failure on the preferred path long before new routes could be established using a distributed algorithm like BGP. Regarding load-balancing and allocative efficiency, XIA's flow-level migration allows fine-grained incoming load-balancing and QoS-matching, whereas in a typical IP network one IP address is associated with many flows and flow migration relies on specialty protocols such as MPTCP. In a world where multihoming is the norm, XIA brings substantial benefits.

The enablers of these benefits are twofold, which brings us to our lessons learned on specific features and design choices. From a protocol design perspective, flow-level migration allows fine-grained load balancing and QoS matching for multihomed devices running heterogeneous applications. However, it implies more signaling messages than host- or network-level migration where there is more than one flow per correspondent host, or more than one host per network. Multipath TCP does allow flow-level migration, but is limited to TCP flows.

From an architectural point of view, DAG-based locators, and fallbacks in particular, allow quick response to link failure and enhances the resiliency of multihomed hosts and networks. Identifier-locator separation plays an important role in mobility management, which is inherent to the XID-DAG setup of XIA and implicit in the HoA-CoA arrangement of MIPv6. However, DAGs are not without drawbacks. An attacker can construct a malicious DAG with XIDs that he is not entitled to use. Additional mechanisms are required to mitigate such threats. Lastly, cryptographically generated addresses, or self-certifying identifiers in general, facilitate authentication of migration signaling messages, which helps reduce the round trips consumed by authentication and thus handoff latency. They are a fundamental building block in both MIPv6 Enhanced Route Optimization and XIA. Internet architects may want to consider flow-level migration, DAG-based locators and/or self-certifying identifiers when designing the future Internet.

REFERENCES

[1] The Economist, "Planet of the phones; Smartphones," *The Economist*, vol. 414, no. 8927, p. 9, 2015.

[2] J. Greenough, "The 'connected car' is creating a massive new business opportunity for auto, tech, and telecom companies," *Business Insider Inc.*, 2015. [Online]. Available: http://www.businessinsider.com/connected-car-statistics-manufacturers-2015-2.

[3] M. Handley, O. Bonaventure, C. Raiciu, and A. Ford, "TCP Extensions for Multipath Operation with Multiple Addresses," *IETF*, 2013. [Online]. Available: https://tools.ietf.org/html/rfc6824.

[4] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *IETF*, 2011. [Online]. Available: http://tools.ietf.org/html/rfc6275.

[5] A. Petrescu, R. Wakikawa, P. Thubert, and V. Devarapalli, "Network Mobility (NEMO) Basic Support Protocol," *IETF*, 2005. [Online]. Available: https://tools.ietf.org/html/rfc3963.

[6] J. Arkko, W. Haddad, and C. Vogt, "Enhanced Route Optimization for Mobile IPv6," *IETF*, 2007. [Online]. Available: https://tools.ietf.org/html/rfc4866.

[7] T. Aura, "Cryptographically Generated Addresses (CGA)," *IETF*, 2005. [Online]. Available: https://tools.ietf.org/html/rfc3972.

[8] [A. Z. M. Shahriar, M. Atiquzzaman, and W. Ivancic, "Route optimization in network mobility: Solutions, classification, comparison, and future research directions," *IEEE Commun. Surv. Tutorials*, vol. 12, no. 1, pp. 24–38, 2010.

[9] UCLouvain, "MultiPath TCP - Linux Kernel implementation," 2015. [Online]. Available: http://www.multipath-tcp.org/.

[10] C. Raiciu, D. Niculescu, M. Bagnulo, and M. J. Handley, "Opportunistic mobility with multipath TCP," in *Proceedings of the sixth international workshop on MobiArch - MobiArch '11*, 2011, p. 7.

[11] R. Stewart, "Stream Control Transmission Protocol," *IETF*, 2007. [Online]. Available: https://tools.ietf.org/html/rfc4960.

[12] R. Stewart, X. Q., M. Tuexen, S. Maruyama, and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration," *IETF*, 2007. [Online]. Available: https://tools.ietf.org/html/rfc5061.

[13] S. Zeadally and F. Siddiqui, "An Empirical Analysis of Handoff Performance for SIP, Mobile IP, and SCTP Protocols," *Wirel. Pers. Commun.*, vol. 43, no. 2, pp. 589–603, Oct. 2007.

[14] D. Naylor *et al.*, "XIA," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 50–57, Jul. 2014.

[15] J. Pan, S. Paul, R. Jain, and M. Bowman, "MILSA: A Mobility and Multihoming Supporting Identifier Locator Split Architecture for Naming in the Next Generation Internet," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, 2008, pp. 1–6.

[16] X. Liu and L. Xiao, "A Survey of Multihoming Technology in Stub Networks: Current Research and Open Issues," *IEEE Netw.*, vol. 21, no. 3, pp. 32–40, May 2007.

[17] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," in *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00*, 2000, pp. 155–166.

[18] D. Barrett, "XIA Prototype Overview," *GitHub*, 2017. [Online]. Available: https://github.com/XIA-Project/xia-core/wiki/XIA-Prototype-Overview.

[19] N. Gupta, "XIA Mobility and Intrinsic Security," *GitHub*, 2017. [Online]. Available: https://github.com/XIA-Project/xia-core/wiki/XIA-Mobility-and-Intrinsic-Security.

[20] Carnegie Mellon University, "eXpressive Internet Architecture Project," *GitHub*, 2016. [Online]. Available: https://github.com/XIA-Project/xia-core.

[21] R. Meireles, "XIA Vehicular Video Demo," *YouTube*, 2016. [Online]. Available: https://youtu.be/msLZnPcNp2o.

[22] M. Watari, C.-W. Ng, F. Zhao, and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis," *IETF*, 2007. [Online]. Available: https://tools.ietf.org/html/rfc4889.

[23] J. Arkko, T. Aura, G. Montenegro, E. Nordmark, and P. Nikander, "Mobile IP Version 6 Route Optimization Security Design Background," *IETF*, 2005. [Online]. Available: https://tools.ietf.org/html/rfc4225.

[24] V. Gill, J. Abley, E. B. Davies, K. E. Lindqvist, and B. Black, "IPv4 Multihoming Practices and Limitations," *IETF*, 2005. [Online]. Available: https://tools.ietf.org/html/rfc4116.

[25] M. Caesar, M. Casado, T. Koponen, J. Rexford, and S. Shenker, "Dynamic route recomputation considered harmful," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 2, p. 66, Apr. 2010.

[26] Fanglu Guo, Jiawu Chen, Wei Li, and Tzi-cker Chiueh, "Experiences in building a multihoming load balancing system," in *IEEE INFOCOM 2004*, vol. 2, pp. 1241–1251.