Early Binding Updates for Mobile IPv6

Christian Vogt, Roland Bless, Mark Doll, Tobias Kuefner
Institute of Telematics, University of Karlsruhe, Germany
Email: {chvogt | bless | doll | kuefner}@tm.uka.de

***Abstract*— The long latency associated with Mobile IPv6's home-address and care-of-address tests can significantly impact delay-sensitive applications. This paper presents an optimization to Mobile IPv6 correspondent registrations that evades the latency of both address tests. An optimized correspondent registration eliminates 50%, or more, of the additional delay that a standard correspondent registration adds to the network stack's overall latency. The optimization is realized as an optional, and fully backward-compatible, extension to Mobile IPv6.**

I. Introduction

The introduction of mobility support to the Internet heralds a diversity of promising, new IP-based services. Examples range from ubiquitous Web access and media streaming to audio or video real-time communications. Migrating to a mobile Internet, however, is less straightforward than it might seem: Traditionally, the network prefix of an IP address locates a node's point of network attachment. It is used by routers to forward IP packets towards the correct destination. A mobile node hence needs to configure a new IP address whenever it moves from one access network to another. At the same time, existing transport-layer protocols and applications use the IP address as a node identifier. This naturally rules out mobility: When a mobile node moves, it configures a new IP address with the prefix of the new access network. The new ”identity” causes transport-layer protocols and applications to abort.

The Mobile IPv6 mobility-management protocol [1] was developed to facilitate the continued use of traditional transport-layer protocols and applications in spite of mobility. Mobile IPv6 uses two IP addresses per mobile node in an attempt to separate localization semantics from identification semantics: a transient *care-of address* is used for the purpose of routing. It is reconfigured whenever the mobile node moves to a new access network. A static *home address* serves as an identifier for transport-layer protocols and applications. It doesn't change when the mobile node moves.

The beauty of Mobile IPv6 is that data packets can be directly relayed between the mobile node and its correspondent node. This mode is called *route optimization*. Mobile IPv6 defaults to route optimization. It falls back to non-optimized mode only when the correspondent node does not support route optimization. If the correspondent node does not support route optimization, the mobile node's care-of address must be concealed from the correspondent node. For this, all packets to and from the mobile node are routed through the mobile node's home address. The mobile node has a proxy in its home network, a *home agent*, which relays all packets between the mobile node and the correspondent node when these packets traverse the home address.

If route optimization is used, a new care-of address is communicated to the mobile node's home agent and to the correspondent node. This is called a *home registration* and a *correspondent registration*, respectively. Without route optimization, the correspondent registration is omitted. Registrations must be refreshed after a certain lifetime.

Home registrations consist of a Binding Update (BU) message and a Binding Acknowledgement (BA) message being exchanged between the mobile node and the home agent (cf. Figure 1). Mobile IPv6 requires that these messages be secured through IPsec. Since no IPsec security association can be presupposed to exist between the mobile node and the correspondent node, correspondent registrations imply significant security issues [2]. Empowering a node—not necessarily a mobile one—to redirect packets from one IP address to another poses two questions:

- When the correspondent node receives a command to redirect a mobile node's packets, how can the correspondent node be sure that it is the legitimate mobile node, rather than a malicious third node, which has send this command?
- How can the correspondent node rely on the mobile node actually being present at the IP address to which packets are to be redirected?

The first question identifies the need for a mobile node to authenticate itself during a correspondent registration. Without such authentication, a malicious node could interfere with a packet flow of another node, redirecting the flow to its own location for inspection purposes, or redirecting it to a random IP address for the purpose of denial of service against the legitimate recipient. The second question refers to spoofed care-of addresses: Probing a mobile node's presence at a care-of address is important to rule out flooding attacks against other nodes (cf. section IV).

Mobile IPv6's answer to both of the above questions is the *return-routability procedure*. It is part of a correspondent registration and consists of two tests (cf. Figure 1). During the *home-address test*, the mobile node sends a Home Test Init (HoTI) message to the home agent. The home agent forwards the HoTI to the correspondent node. The correspondent node sends in response a Home Test (HoT) message containing a secret *Home Keygen Token*. The HoT is addressed to the mobile node's home address, and it is forwarded by the home agent to the mobile node's current care-of address. During the *care-of-address test*, the mobile node sends a Care-of Test Init (CoTI) message to the correspondent node, and the correspondent node returns a Care-of Test (CoT) message containing a secret *Care-of Keygen Token*. The CoTI and CoT are routed between the mobile node and the correspondent node directly. They do not pass the home agent.

The mobile node needs both the Home Keygen Token and the Care-of Keygen Token to validate the correspondent registration: The former proves the mobile node to be the legitimate owner of its home address. The latter shows that the mobile node is actually present at the new care-of address. The mobile node signals the care-of address to the correspondent node with a Binding Update (BU) message, and it may ask for a Binding Acknowledgement (BA) message to be returned for confirmation.

A correspondent registration consumes, at a minimum, two round-trip times between a mobile node and its correspondent node. The latency can be higher than two round-tip times due to the HoTI and HoT being relayed through the home network. Most of the latency is, unfortunately, part of the *critical phase* (cf. section V-A) during which the mobile node cannot communicate. This can be unsuitable for interactive real-time applications. As an example, two round-trip times may easily exceed 200 milliseconds in a transatlantic call.

This said, it becomes obvious that an optimization to reduce the latency of correspondent registrations would be of true benefit. One such approach, Early Binding Updates for Mobile IPv6 [3], is proposed in this paper. Early Binding Updates are an optional and fully backward-compatible enhancement to Mobile IPv6. Using them eliminates 50%, or more, of the additional delay that a standard correspondent registration adds to the network stack's overall latency. Early Binding Updates go hand in hand with Credit-Based Authorization [4], a security mechanism which gives Early Binding Updates a security level equivalent to that of standard Mobile IPv6. Credit-Based Authorization can be implemented such that it operates locally at the correspondent node and transparently to the mobile node. (An advanced version of Credit-Based Authorization [4] requires support from the mobile node, but is not presented in here.)

This paper is structured as follows. Section II presents related research efforts for Mobile IPv6 optimization. Early Binding Updates and Credit-Based Authorization are explained in sections III and IV, respectively. An analytic performance comparison between standard Mobile IPv6 and the proposed optimization is provided in section V. The paper concludes in section VI.

II. Related Work

Mobile IPv6 optimization projects are still in their early stages. However, it can be expected that research efforts in this area will accelerate now that Mobile IPv6 has been internationally standardized [1].

Part of a home-address test's purpose is to ensure that packets can only be redirected by the legitimate recipient. The legitimate recipient is identified through the home address, and only the legitimate recipient is expected to receive the Home Keygen Token sent to the home address.

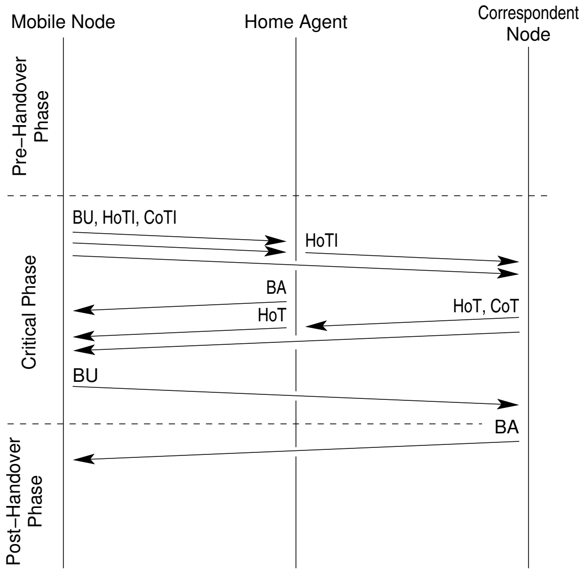

Fig. 1. Standard Correspondent Registration

Cryptographically Generated Addresses (CGAs) [5] can provide the same functionality without sending a packet to the home address. A node that uses a CGA at a certain time can prove at a later time that it is still the same node when it uses this CGA again. But instead of relying on a routing property, as with the home-address test, this proof can be drawn from the CGA's special interface identifier. The interface identifier is a hash on the CGA owner's public key plus some auxiliary parameters. The CGA owner signs important packets with its private key and includes its public key along with the auxiliary data in these packets. Since it is computationally hard to produce another public/private-key pair that hashes to the same CGA, the recipient of the signed message can verify, by recomputing the hash and comparing it with the CGA's interface identifier, that the sender must be the legitimate owner of this CGA.

[6] applies CGAs to Mobile IPv6. A mobile node uses a CGA as its home address, and it signs BUs with its private key. The correspondent node can thus verify that the BU is from the same mobile node that used this home address before.

However, different than a home-address test, [6] does not ensure that a mobile node can indeed receive packets at the home address it claims to own. This property can be misused for a flooding attack against the home network. The following scenario illustrates this threat: An attacker registers with a correspondent node its current care-of address and a forged home address. The interface identifier of the home address is cryptographically generated, but the network prefix is from a victim network that the attacker intends to flood with unwanted data. Shortly before the registration expires, the attacker requests the correspondent node to send to it a large file. Then, upon expiry, data packets are automatically redirected to the spoofed home address, i.e., towards the victim network. [6] also does not ensure that the mobile node is present at its care-of address. An attacker could misuse this property for a flooding attack against an arbitrary care-of address.

[7] attends to these problems by combining CGAs with home- and care-of-address tests. A home-address test is performed at first contact between a mobile node and a correspondent node. This test verifies that the mobile node is the legitimate owner of the home address. Since the home address is cryptographically generated, the correspondent node will recognize the mobile node as the owner of this home address during subsequent registrations without having to do the home-address test again. On the other hand, as care-of addresses are not cryptographically protected, [7] demands a care-of-address test whenever packets are to be redirected.

A disadvantage with CGAs in general is that they involve computationally expensive algorithms. This *may* be an issue for small mobile devices with low processing power. It *is* an issue for correspondent nodes that simultaneously communicate with a large number of mobile nodes, such as publicly accessible servers. Let alone the computational overhead required for legitimate mobile nodes, a correspondent node will have to protect itself against potential denial-of-service attempts from attackers by limiting the amount of resources it spends on CGA verification.

[8] proposes statically configured authentication keys for peers that have a pre-existing trust relationship. This approach does not depend on the return-routability procedure or CGAs. It is thus very efficient. Since communicating peers must be configured with the same authentication key at some time before the communication takes place, the scope of this approach is rather limited, though.

Other research efforts focus on reducing the signaling load posed upon mobile nodes. [9] uses a credit-based approach to gradually increase the lifetime for home and correspondent registrations. Thus, fewer refreshes are required from a mobile node that does not move for a while.

III. Early Binding Updates

A disadvantage of the return-routability procedure is that a mobile node must wait for both address tests to conclude before it can register a new care-of address. Early Binding Updates move these tests to a time when they do not hurt: A *proactive home-address test* takes place when the mobile node can still use its old care-of address. A *concurrent care-of-address test* runs in parallel with data transfer to and from the new care-of address.

Early Binding Updates do not rely on CGAs or statically configured authentication keys, and they reduce the additional delay that a standard correspondent registration adds to the network stack's overall latency by at least 50%. Early Binding Updates are an optional and fully backward-compatible enhancement to Mobile IPv6. They use two new messages, an Early Binding Update (EBU) message and an Early Binding Acknowledgement (EBA) message (cf. Figure 2). Both messages have no effect if either communication end-point does not support them. All standard Mobile IPv6 messages remain unchanged and retain their original meaning.

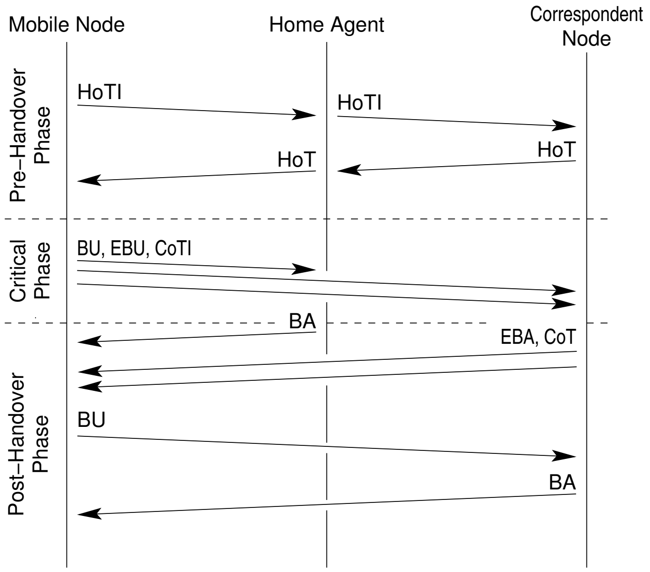

Fig. 2. Optimized Correspondent Registration Using Early Binding Updates

A proactive home-address test is technically the same as a standard home-address test. It delivers to the mobile node a Home Keygen Token proving that the mobile node is the legitimate owner of the home address. The Home Keygen Token has a lifetime of 3.5 minutes. Hence, if the mobile node seeks to have available a fresh Home Keygen Token at all times, it needs to send a HoTI, and receive a HoT, at least every 3.5 minutes. Alternatively, the mobile node may be able to receive a trigger from its local link layer indicating that a handover is imminent. In this case, the mobile node can initiate the home-address test just before the old link breaks.

When the mobile node detects that it has moved to a different access network, it configures a new care-of address. The mobile node then initiates a home registration, and it sends to the correspondent node an EBU for *tentative* care-of-address registration. The mobile node authenticates the EBU with the Home Keygen Token received during the proactive home-address test. (Note that the authentication does not include a Care-of Keygen Token at this time.)

By now, the correspondent node knows the mobile node's new care-of address, and it knows, due to the authenticator in the EBU, that the mobile node is the legitimate owner of the home address. The correspondent node hence starts using the new care-of address. It needs to be wary, though, because the mobile node has not yet proven that it is really present at this care-of address. A security mechanism that the correspondent node should apply is described in section IV. The mobile node may ask the correspondent node to return an EBA for confirmation.

The mobile node initiates a concurrent care-of-address test as soon as it has sent the EBU. A concurrent care-of-address test is technically the same as a standard care-of-address test. It delivers to the mobile node a Care-of Keygen Token that the mobile node can use to show its presence at the new care-of address. When the concurrent care-of-address test concludes, the mobile node sends a BU to the correspondent node. The mobile node authenticates the BU with both the Home and the Care-of Keygen Token.

When the correspondent node receives the BU, it knows that the mobile node is the legitimate owner of the home address, and it knows that the mobile node is actually present at the new care-of address. The mobile node may ask the correspondent node to return a BA for confirmation. At this point, the correspondent registration concludes.

IV. Credit-Based Authorization

A correspondent node learns from an EBU a mobile node's new care-of address, but it cannot see whether the mobile node is actually present at this care-of address until it receives a BU from the mobile node. The care-of address is said to be *unconfirmed* during this period of incertitude, and it is called *confirmed* otherwise. In order to avoid the introduction of new security hazards by Early Binding Updates, there is a strong need to prevent malicious use of unconfirmed care-of addresses. An attacker could otherwise adopt a victim's IP address as its own care-of address and flood the victim with redirected packets while the care-of address is unconfirmed.

One may argue that many types of flooding attacks are already possible in today's Internet, even without mobility support. (Indeed, one may not hesitate to say that such attacks are a common disease.) However, it is important that the introduction of mobility support—and thus the ability to redirect packets—can, if carelessly applied, result in a serious flooding *amplification*. To understand this, the reader may consider the following scenario: An attacker accomplishes a TCP handshake for downloading a huge file from a server. The attacker then redirects the download to the IP address of its victim, claiming that this IP address be its own care-of address. From the handshake, the attacker knows the initial TCP sequence number, and it can easily spoof TCP acknowledgements to keep the data flow going, or even accelerate it. The ratio between the data volume of the correspondent node's data packets, which are routed towards the victim, and the data volume of the attacker's acknowledgements constitutes the amplification factor for this flooding attack.

Credit-Based Authorization is a simple approach that prevents misuse of unconfirmed care-of addresses for amplified flooding attacks. Credit-Based Authorization comes in two variants: A correspondent node monitors the packets it either sends to a confirmed care-of address, or receives from a confirmed or unconfirmed care-of address of a mobile node. The mobile node either receives or sends these packets, respectively. In both cases, it will have to spend resources for these packets in terms of bandwidth, processing power, and memory. The correspondent node acknowledges this effort by granting the mobile node credit for it. How much credit the mobile node gets depends on the size of the monitored packets. When the mobile node switches to a new, unconfirmed care-of address, subsequent packets will consume the credit that the mobile node has collected up to then. This ensures that the data volume brought on way to a mobile node's unconfirmed care-of address does not exceed the data volume that was earlier sent to or received from a confirmed care-of address of the same mobile node. A protocol-configuration parameter specifies how much faster the credit shrinks than it grows while the mobile node uses an unconfirmed or confirmed care-of address, respectively. Provided that this parameter is sufficiently big, even non-amplified flooding attacks can be discouraged.

V. Performance Evaluation

A handover from one point of network attachment to another causes signaling delays at multiple layers of the stack. It requires a mobile node to perform link-layer signaling, authentication and access-control signaling, router and neighbor discovery, IPv6 address configuration, and Mobile IPv6 home and correspondent registrations. In order to keep a perspective on the gross improvement that an optimization for one of these tasks can bring, one should therefore evaluate the complete stack. Surely, this would be cumbersome and distracting. It would also go beyond the scope of this paper. For this reason, delays other than those caused by Mobile IPv6 are ignored in the following performance evaluation.

Section V-A makes some preparatory considerations that will be helpful for the calculations to come. Section V-B evaluates the current performance of Mobile IPv6; an analysis of Early Binding Updates follows in section V-C.

A. Preparatory Considerations

Three conceptual movement phases will be used throughout the performance evaluation:

- Pre-handover phase
- Critical phase
- Post-handover phase

The mobile node still uses its old care-of address during the *pre-handover phase*. The mobile node may have sensed a new access point with a better S/N ratio, but link-layer signaling for inter-access-point switching has not yet been initiated.

During the *critical phase*, the mobile node switches from its old point of network attachment to the new. The mobile node accomplishes handover tasks at different layers of the stack, like authentication, access control, router discovery, and neighbor discovery. The mobile node also configures a new care-of address. Once this is done, the mobile node communicates its new care-of address to the correspondent node—be it through a BU in case standard correspondent registrations are used, or through an EBU in case Early Binding Updates are used. The mobile node cannot use its new care-of address during the critical phase.

After the mobile node has communicated its care-of address to the correspondent node, the *post-handover phase* begins. As of then, the mobile node can fully use its new care-of address. The new care-of address may be unconfirmed for a while if Early Binding Updates are used, but this has no delaying impact on packet transmission. If Early Binding Updates are used, the mobile node also needs to run a concurrent care-of-address test, and it must send to the correspondent node a BU in order to confirm its new care-of address.

A home-address test is intended to prove a mobile node's ownership of its home address. For this reason, the home-address test must be performed before the new care-of address is registered with the correspondent node, i.e., either during the pre-handover phase or during the critical phase. It cannot be performed during the post-handover phase. Most Mobile IPv6 implementations do the home-address test during the critical phase. Technically, however, there is nothing that prevents a mobile node from proactively initiating the home-address test during the pre-handover phase [1].

A care-of-address test is intended to prove that the mobile node is present at its new care-of address. Since the new care-of address is configured during the critical phase, it obviously cannot be tested during the pre-handover phase. Mobile IPv6 specifies that the care-of-address test is to be accomplished during the critical phase. Early Binding Updates, however, perform the care-of-address test during the post-handover phase. Credit-Based Authorization prevents misuse of the new care-of addresses while it is unconfirmed.

B. Standard Correspondent Registrations

This sub-section evaluates the performance of correspondent registrations as they are defined in [1].

When the mobile node detects that it has moved to a different network, it configures a new care-of address. Mobile IPv6 specifies that a mobile node must do the following steps before it can use the new care-of address: First, the mobile node must accomplish a home registration. Then, as part of the correspondent registration, a home-address test and a care-of-address test must be executed. Finally, the mobile node must register the new care-of address with its correspondent node.

The home registration is a two-way message exchange between the mobile node and the home agent. It consists of a BU and a BA. Let RTT_{HA} be the required round-trip time. The subscript ”HA” denotes ”home agent”.

The home-address test is a two-way message exchange between the mobile node and the correspondent node. It consists of a HoTI and a HoT, both of which are routed through the mobile node's home address. Let the round-trip time for this exchange be $RTT_{\wedge}$, the subscript ”$\wedge$” indicating the redirection at the home network.

The care-of-address test is a two-way message exchange between the mobile node and the correspondent node. It consists of a CoTI and a CoT. These messages are relayed on the direct path between the mobile node and the correspondent node. They do not pass the home network. Let the round-trip time for the CoTI and the CoT be RTT_{CN}, where the subscript ”CN” stands for ”correspondent node”.

The mobile node may send the HoTI and the CoTI at any time after having sent the BU to its home agent. The mobile node may thus send out all three messages virtually in parallel. The time it takes until the mobile node receives the BA, the HoT, and the CoT is, respectively, RTT_{HA}, $RTT_{\wedge}$, and RTT_{CN}. The mobile node must wait for all three messages before it can register the new care-of address with its correspondent node.

Registering the new care-of address with the correspondent node is achieved by sending a BU to the correspondent node. In most Mobile IPv6 implementations, the mobile node uses a new care-of address as soon as it has sent the BU to the correspondent node without requesting a BA for confirmation. Hence, a standard correspondent registration's total latency with respect to sending data from a new care-of address can be approximated by

$$L_{std}^{send} = \max(RTT_{HA}, RTT_{\wedge}, RTT_{CN})$$

The latency may be higher in case the mobile node waits for a BA to be returned from the correspondent node.

Whether or not the mobile node waits for the returning BA, the correspondent node starts using the mobile node's new care-of address upon receiving the BU. The BU takes $0.5 \cdot RTT_{CN}$ until it reaches the correspondent node. When the correspondent node switches to the new care-of address, it takes another $0.5 \cdot RTT_{CN}$ until the first data packets arrive at the mobile node's new care-of address. Thus, a standard correspondent registration's total latency with respect to receiving data at a new care-of address can be approximated by

$$L_{std}^{recv} = \max(RTT_{HA}, RTT_{\wedge}, RTT_{CN}) + RTT_{CN}$$

According to [1], a mobile node may reuse its previously acquired Home Keygen Token without running another home-address test if it has recently changed its point of network attachment before. In this situation, $RTT_{\wedge}$ reduces to zero, and $\max(RTT_{HA}, RTT_{\wedge}, RTT_{CN}) = \max(RTT_{HA}, RTT_{CN})$.

C. Optimized Correspondent Registrations

This sub-section evaluates the performance of correspondent registrations that use Early Binding Updates for optimization.

With Early Binding Updates, the home-address test is moved to the pre-handover phase, and the care-of-address test is moved to the post-handover phase. The proactive home-address test does no longer delay the correspondent registration, because it runs while the mobile node still uses the old care-of address, which is functioning and fully confirmed. The concurrent care-of-address test does no longer delay the correspondent registration either, because it runs while the mobile node uses the new, unconfirmed care-of address.

Note that, when standard Mobile IPv6 is used, the mobile node registers its care-of address with the correspondent node during the critical phase (by sending the correspondent node a BU). With Early Binding Updates, the critical phase ends when the mobile node has tentatively registered its new care-of address with the correspondent node (by sending the correspondent node an EBU), and sending the BU is part of the post-handover phase. Thus, only two tasks are left to be done during the critical phase: First, the mobile node must register the new care-of address with its home agent. Second, the mobile node must tentatively register the new care-of address with the correspondent node.

The home registration is a two-way message exchange between the mobile node and the mobile node's home agent. It consists of a BU and a BA. RTT_{HA} denotes the round-trip time for these messages. Tentatively registering the new care-of address with the correspondent node is achieved by sending an EBU to the correspondent node. (An EBA may be requested for confirmation, but this is mainly to query the correspondent node whether it supports Early Binding Updates.) The mobile node sends the EBU virtually in parallel with sending the BU to the home agent, and it can start using its new care-of address immediately thereafter.

All things considered, the total latency of an optimized correspondent registration with respect to sending data from a new care-of address is zero:

$$L_{opt}^{send} = 0$$

The correspondent node starts using the mobile node's new care-of address upon receiving the EBU. The EBU takes $0.5 \cdot RTT_{CN}$ until it reaches the correspondent node. When the correspondent node switches to the new care-of address, it takes another $0.5 \cdot RTT_{CN}$ until the first data packets arrive at the mobile node's new care-of address. Thus, an optimized correspondent registration's total latency with respect to receiving data can be approximated by

$$L_{opt}^{recv} = RTT_{CN}$$

This evaluation shows that an optimized correspondent registration using Early Binding Updates is about one round-trip time, or 50%, faster than a standard correspondent registration. This is true even when a standard correspondent registration can be expedited by reusing a previously acquired Home Keygen Token without running another home-address test. The performance gain is even higher when $RTT_{\wedge}$ is longer than RTT_{HA} or RTT_{CN}, which is expected to be the case in many common scenarios.

VI. Conclusion and Outlook

Mobile IPv6 defines two address tests that must be performed during a correspondent registration: a home-address test and a care-of-address test. The long latency associated with these tests makes it difficult for delay-sensitive applications to hold up service quality during a handover.

This paper makes two contributions. Early Binding Updates are a strategy to move both address test to a handover phase where they no longer have an impact on handover latency: A proactive home-address test is performed before the handover, and a concurrent care-of-address test is done after the handover. In order to compensate the new risk that comes along with a delayed care-of-address test, this paper describes Credit-Based Authorization, a security mechanism that can be implemented such that it operates locally at the correspondent node and transparently to the mobile node. Credit-Based Authorization gives Early Binding Updates a security level equivalent to that of standard Mobile IPv6.

The proposed optimization is realized as an optional and fully backward-compatible enhancement to Mobile IPv6. An analytic performance evaluation shows that an optimized correspondent registration using Early Binding Updates eliminates 50%, or more, of the additional delay that a standard correspondent registration adds to the network stack's overall latency.

There is, however, a price to pay for the reduced latency. First, Early Binding Updates require one or two additional messages to be transmitted during a handover: an EBU and, optionally, an EBA for confirmation. Second, the mobile node must do the home-address test periodically unless the test can be more efficiently scheduled through link-layer events. This generally increases the signaling overhead as well. Third, the correspondent node must implement Credit-Based Authorization to prevent misuse of unconfirmed care-of addresses. This implies an increased complexity at the correspondent node. The authors believe, however, that the additional overhead is worth being spent in exchange for the expected performance gain. To gather more insight in this regard, Early Binding Updates and Credit-Based Authorization are currently being implemented based on the Kame-Shisa source code [10]. These efforts will be continued. Future work will also be expended into practical performance evaluations to supplement the analytical results shown in this paper.

Acknowledgment

Early Binding Updates for Mobile IPv6 were first presented at the 59th IETF meeting in early 2004, and there has been a fruitful discussion on the MIP6 and MOBOPTS mailing lists. For their valuable comments and feedback, the authors of this paper express their gratitude to the MIP6 and MOBOPTS communities, in particular to Jari Arkko, Francis Dupont, James Kempf, Pekka Nikander, Erik Nordmark, Charles Perkins, Oliver Stanze, Kilian Weniger, and Jidong Wu.

References

[1] D. Johnson, C. E. Perkins, and J. Arkko. (2004, June) Mobility Support in IPv6. RFC 3775.

[2] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark. (2004, July) Mobile IP version 6 Route Optimization Security Design Background. Internet Draft draft-ietf-mip6-ro-sec.

[3] C. Vogt, R. Bless, M. Doll, and T. Kuefner. (2004, February) Early Binding Updates for Mobile IPv6. Internet Draft draft-vogt-mip6-early-binding-updates.

[4] C. Vogt, J. Arkko, R. Bless, M. Doll, and T. Kuefner. (2004, May) Credit-Based Authorization for Mobile IPv6 Early Binding Updates. Internet Draft draft-vogt-mipv6-credit-based-authorization.

[5] T. Aura. (2004, April) Cryptographically Generated Addresses (CGA). Internet Draft draft-ietf-send-cga.

[6] G. O'Shea and M. Roe, "Child-Proof Authentication for MIPv6 (CAM)," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 2, pp. 4–8, 2001.

[7] W. Haddad, L. Madour, J. Arkko, and F. Dupont. (2004, June) Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6). Internet Draft draft-haddad-mip6-cga-omipv6.

[8] C. E. Perkins. (2004, April) Preconfigured Binding Management Keys for Mobile IPv6. Internet Draft draft-ietf-mip6-precfgKbm.

[9] J. Arkko and C. Vogt. (2004, May) Credit-Based Authorization for Binding Lifetime Extension. Internet Draft draft-arkko-mipv6-binding-lifetime-extension.

[10] "Kame-Shisa Mobile IPv6 Implementation." [Online]. Available: http://www.mobileip.jp/