Network Working Group
Internet-Draft
Expires: December 25, 2006

J. Arkko
Ericsson Research NomadicLab
C. Vogt
Universitaet Karlsruhe (TH)
W. Haddad
Ericsson Research
June 23, 2006

Applying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6
draft-arkko-mipshop-cga-cba-04.txt

Status of this Memo

Copyright Notice

Abstract

This document proposes an enhanced security mechanism for Mobile IPv6 route optimization, providing lower handoff delays, increased security, and reduced signaling overhead.

Table of Contents

1. Introduction

Mobile IPv6 [1] includes a mode for route optimization that allows nodes to communicate with reduced latency via a direct routing path. Route optimization is protected through a "return routability procedure", which serves essentially two purposes:

- A correspondent node can (weakly) authenticate a mobile node based on a verification of the mobile node's reachability at its home address.

- A correspondent node can verify that the mobile node is reachable at the claimed care-of address.

While authentication prevents impersonation threats, the reachability verification for the care-of address protects against "redirection-based flooding attacks" [8].

Standard route optimization is limited by the capabilities of the return routability procedure. For one thing, the procedure does not protect against an impersonator on the path between the mobile node's home agent and the correspondent node. This vulnerability may oftentimes be acceptable, given that it already exists in the non-mobile Internet of today. But scenarios with higher security needs are also conceivable. Second, the return routability procedure consumes a significant of the overall handoff delay. Since route optimization was orignally developed with an intent to improve support for interactive real-time applications, it is exactly those applications that suffer from prolonged handoff delays.

This document amends the Mobile IPv6 base specification by two optional, interrelated, yet orthogonal optimizations to the return routability procedure. The first optimization enables unidirectional or mutual authentication based on a cryptographically generated home address [9]. This replaces the weaker authentication through pure reachability verification at a home address. The second optimization allows a correspondent node to securely verify a mobile node's reachability at a new care-of address while it already sends data packets to that care-of address [10]. The two optimizations can be applied separately or, preferably, in conjunction.

2. Objectives

The design of Mobile IPv6 route optimization is in may ways conservative, leaving room to optimize handoff delay, security, and signaling overhead. The protocol defined in this document tackles

these issues and thus constitutes a more progressive variant of the base mobility protocol.

In spite of any improvements in the mobility protocol, it is important to take into account that other mobility-related activities in the protocol stack may have their own impact, in particular on handoff delay. E.g., attachment procedures, access control, and authentication at the link layer contribute their own delay. So do IPv6 tasks such as router discovery, neighbor discovery, movement detection, and address configuration. These other delays are in many cases significantly larger than the handoff delay of Mobile IPv6 route optimization. The protocol defined in this document concentrates on making the mobility signaling as efficient as possible, ignoring mobility-related functions elsewhere in the protocol stack. The improvements that the protocol facilitates hence ought to be seen in view of the entire protocol stack.

2.1 Handoff Latency

The typical handoff delay in Mobile IPv6 route optimization is 1 round-trip time between the mobile node and the home agent for the home registration, 1 round-trip time between the mobile node and the home agent plus 1 round-trip time between the home agent and the correspondent node for the return routability procedure, and 1 one-way time from the mobile node to the correspondent node for the propagation of the Binding Update message. (The assumption here is that the latency of the return routability procedure is dominated by the home-address test.) The first packet sent to the new care-of address requires 1 additional one-way time to propagate from the correspondent node to the mobile node. The mobile node can resume transmissions right after it has dispatched the Binding Update message. But if it requests a Binding Acknowledgment message from the correspondent node, communications are usually delayed until this is received.

Handoff delays in Mobile IPv6 route optimization are additive to other delays at IP layer or link layer. They can cause perceptible quality degradations for interactive and real-time applications. TCP bulk-data transfers are likewise affected since long handoff latencies may lead to successive retransmission timeouts and degraded throughput [11]. This protocol eliminates the additional handoff delay induced by Mobile IPv6 route optimization for packets that a mobile node sends, and it reduces the delay to 1 round-trip time between the mobile node and the correspondent node for packets that the mobile node receives.

2.2 Security

Given that mobile and correspondent nodes with support for Mobile IPv6 route optimization form a true subset of all Internet nodes, the security design of the mobility protocol cannot make the Internet any safer than it is without the mobility protocol. The return routability procedure was therefore designed with the objective to provide a level of security which compares to that of today's non-mobile Internet [8]. As such, it protects against impersonation and denial of service that an insecure mobility protocol may be vulnerable to. In particular, the return routability procedure satisfies the following key requirements for mobility protocols:

- An attacker should not be able to redirect a third node's communication flow to itself or to another IP address, at least not beyond what is already possible in plain IPv6. This requirement applies both to ongoing and future communication flows.

- An attacker should not be able to redirect its own communication flows to a third party, flooding the victim with unrequested packets. Such redirection-based flooding attack would provide substantial amplification that is today only possible through a network of compromised nodes [12]. E.g., an attacker could accomplish the initial TCP handshake for a voluminous file download through its own address (or home address, for that matter), and then redirect the flow to the address of its victim. The attacker could spoof acknowledgments on behalf of the victim based on the sequence numbers it learned from the initial handshake, but those would be small compared to the full-sized segments that the correspondent node generates.

- Attackers should not be able to cause denial-of-service through potentially expensive computations involved in the mobility protocol.

Applications that require a higher security level than the return routability procedure can provide are generally advised to use end-to-end protection such as IPsec or TLS. But even then are they vulnerable to denial of service. Furthermore, these mechanisms either require end nodes to be preconfigured with credentials for mutual authentication, or they depend on a public-key infrastructure. Either approache impedes [13] wide deployment of Mobile IPv6 route optimization. The protocol defined in this document permits end nodes to authenticate each other by means of a cryptographic property of their home addresses. It neither depends on preconfiguration nor on a public-key infrastructure, and yet it conforms to the key requirements listed above.

2.3 Signaling Overhead

A complete correspondent registration involves 6 message transmissions at the mobile node, totaling about 376 bytes (cf. [14]). This signaling overhead may be acceptable if movements are infrequent. E.g., a mobile node that moves once every 30 minutes generates an average of 1.7 bits/second of signaling traffic. Higher mobility causes more serious overhead, however. A cell size of 100 meters and a speed of 120 km/h yields 1 movement every 3 seconds and about 1,000 bits/second of signaling traffic. This compares to a highly compressed voice stream with a typical data rate of 10,000 to 30,000 bits/second. The protocol defined in this document introduces a new message exchange between mobile and correspondent nodes in order to accomplish the desired improvements in handoff delay. The implied new signaling overhead is compensated for by verifying reachability of the care-of address in-band, sparing a separate message exchange.

Standard Mobile IPv6 requires mobile nodes to renew a binding at a correspondent node at least every 7 minutes. The signaling overhead amounts to 7.16 bits per second if the mobile node communicates with a stationary node [14]. It doubles if both peers are mobile. This overhead may be negligible when the nodes communicate, but it can be an issue for mobile nodes that are inactive and stay at the same location for a while. These nodes typically prefer to go to standby mode to conserve battery power. Also, the periodic refreshments consume a fraction of the wireless bandwidth that one could use more efficiently. The protocol defined in this document allows correspondent nodes to specify a binding lifetime much larger than 7 minutes. It thereby reduces the signaling overhead generated by mobile nodes that do not change their care-of address for a while.

3. Protocol Design

The protocol defined in this document applies a set of techniques in order to meet the objectives discussed in Section 2. These are summarized in the following:

Cryptographically generated home addresses

A Mobile IPv6 binding is conceptually a packet redirection from a home address to a care-of address. The home address is the source of the redirection, whereas the care-of address is the destination. The packets to be redirected can hence be identified based on the home address. This motivates a strong, cryptographic ownership proof for the home address. The protocol defined in

this document features this through the application of cryptographically generated home addresses [15][16]. In general, a cryptographically generated address [9] provides a strong, cryptographic binding between the interface identifier of the address and the address owner's public key. This enables other nodes to securely authenticate the owner as such, modulo the correctness of the address prefix. Cryptographically generated home addresses can supersede home address tests with the exeption of an initial test for validating the home address prefix. This facilitates lower handoff delays as well as longer binding lifetimes and, consequently, reduced signaling overhead for nodes which temporarily do not move.

Non-cryptographic care-of addresses

In contrast to a home address, a care-of address does not have identifying functionality. There is hence little benefit in a cryptographic ownership proof of a care-of address. Given that the care-of address is the destination of a packet redirection, it is rather the mobile node's reachability at the care-of address which matters. The protocol defined in this document uses care-of address tests for this purpose, but allows correspondent nodes to send packets to a new care-of address already before the mobile node has been found to be reachable at the address.

Semi-permanent security associations

Cryptographically generated addresses involve public-key cryptography and are computationally inefficient to validate. Further, the technique requires a significant amount of supplementary data to be piggybacked onto protected messages. The protocol defined in this document therefore leverages the cryptographic property of home addresses to securely exchange a secret shared key between a mobile node and a correspondent node [17]. This key is used to authenticate subsequent signaling messages efficiently.

Initial home address tests

An initial home address test is necessary in order to prevent redirection-based flooding attacks against an alleged home network. Specifically, in the absence of a home address test, a malicious node can cryptographically generate a home address with the prefix of a targeted victim network, and register a binding between this spoofed home address and its own IP address at a correspondent node. The attacker proceeds to request the correspondent node, which may be a public server, to send a stream of packets to its current location. The attacker then de-

registers the binding, or lets it expire, with the consequence of having the correspondent node redirect the packet stream "back" to the victim network. The result is a flooding attack against the victim network. To avoid such misuse, the initial home address test is executed at the same time as the semi-permanent security association is being established [17]. The test does not need to be repeated upon subsequent movements, however.

Concurrent care-of address tests

The protocol defined in this document allows a correspondent node to send packets to a new care-of address already before a proof of reachability at that address has been received from the mobile node. Specifically, when the mobile node moves to a different link, it first registers its new care-of address without providing a proof of reachability. The correspondent node registers the unverified care-of address on a tentative basis and sends a token to the mobile node based on which the latter can follow up with a proof of reachability. This completes the binding update.

Credit-Based Authorization

Concurrent care-of address tests without additional protection would enable an attacker to temporarily redirect its own communication flows to a spoofed, unverified care-of address. This introduces a vulnerability to redirection-based flooding attacks and is hence in conflict with the security requirements defined in Section 2.2. Recall that the appeal of redirection-based flooding attacks is the potential for significant amplification. Credit-Based Authorization [10] guarantees that malicious packet redirection cannot generate amplification. This defeats the purpose of redirection-based flooding: Any attacker could more effectively flood its victim by sending bogus packets directly.

Reduced reachability verification

A cryptographically generated home address does not tell whether its prefix is correct, so there is still need for a home address test. Reachability verification is also required for care-of addresses since those are not cryptographically protected. The protocol defined in this document executes a home address test during the initial key establishment procedure and a care-of address test upon each handoff. However, due to the strong, cryptographic address ownership authentication of the home address, binding lifetimes can be much longer than in standard Mobile IPv6 route optimization, and reachability tests may occur on a less frequent basis.

4. Protocol Operation

The protocol defined in this document features a variety of possible message exchanges. These are described below, packaged by the type of message processing operation.

4.1 Sending Binding Update messages

A mobile node may initiate a correspondent registration for any of the following reasons:

- To establish a new binding at a correspondent node so that further packets can be route-optimized and do no longer need to be routed through the mobile node's home agent.
- To update an existing binding at the correspondent node while moving from one point of IP attachment to another.
- To follow up an early Binding Update message with a complete Binding Update message after receiving a Binding Acknowledgment message with a Care-of Test option.
- To refresh an existing binding at the correspondent node without changing its point of IP attachment.
- To request the correspondent node to renew an existing permanent home keygen token shared between the mobile node and the correspondent node (cf. Section 4.7).

In any of these cases, the mobile node sends a Binding Update message to the correspondent node. The Binding Update message MUST be authenticated either through the CGA property of the mobile node's home address, or through a proof of reachability at the home address. The appropriate authentication method is selected as follows:

- If the mobile node's home address is a CGA, and the mobile node has a permanent home keygen token in its Binding Update List entry for the correspondent node, the mobile node MUST authenticate the Binding Update message with the CGA property of its home address.
- If the mobile node's home address is a CGA, but the mobile node does not have a permanent home keygen token in its Binding Update List entry for the correspondent node, the mobile node MUST authenticate the Binding Update message with a proof of reachability at its home address.

- If the mobile node's home address is not a CGA, the mobile node MUST authenticate the Binding Update message with a proof of reachability at its home address.

The mobile node SHOULD request the correspondent node to accept its CGA parameters for future CGA-based authentication if its home addess is a CGA, but it does not yet have a permanent home keygen token from the correspondent node. The mobile node then includes its CGA parameters in the Binding Update message by adding one or more CGA Parameters options (cf. Section 5.1) followed by a Signature option (cf. Section 5.3). Once a permanent home keygen token has been obtained from the correspondent node, the mobile node MUST authenticate all subsequent Binding Update messages with the CGA property of its home address until either the binding lifetime expires, or the mobile node explicitly de-registers from the correspondent node. The mobile node MAY choose to ignore the CGA property of its home address and continue authenticating Binding Update messages through a proof of reachability at the home address, but this behavior is NOT RECOMMENDED.

The mobile node also includes its CGA parameters in the Binding Update message if it intends to renew an existing permanent home keygen token shared with the correspondent node (cf. Section 4.7). This is accomplished, as before, by adding to the message one or more CGA Parameters options and a Signature option.

The authenticator for the Binding Update message is calculated based on a permanent or temporary home keygen token. Which type of home keygen token the mobile node uses in calculating the authenticator depends on the authentication method:

- If the Binding Update message is to be authenticated through the CGA property of the mobile node's home address, the mobile node MUST use the permanent home keygen token that is has in its Binding Update List entry for the correspondent node.

- If the Binding Update message is to be authenticated through a proof of reachability at the home address, the mobile node MUST use a temporary home keygen token from the correspondent node. The mobile node may already have a valid temporary home keygen token in its Binding Update List entry for the correspondent node, or it may retrieve one through the exchange of a Home Test Init message and a Home Test message as defined in [1].

The authenticator for the Binding Update message is further calculated based on a care-of keygen token. The care-of keygen token to be used is selected as follows:

- If the mobile node has a valid care-of keygen token in its Binding Update List entry for the correspondent node, the mobile node MUST use this in calculating the authenticator for the Binding Update message. The Binding Update message is in this case "complete".

- If the mobile node does not have a valid care-of keygen token in its Binding Update List entry for the correspondent node, the mobile node SHOULD define the care-of keygen token to be zero and use this in calculating the authenticator for the Binding Update message. The Binding Update message is in this case "early".

- If the mobile node does not have a valid care-of keygen token in its Binding Update List entry for the correspondent node, the mobile node MAY choose to retrieve a care-of keygen token through the exchange of a Care-of Test Init message and a Care-of Test message, as defined in [1], without sending an early Binding Update message. In this case, the mobile node waits for receipt of the Care-of Test message and uses the care-of keygen token contained therein in calculating the authenticator for a complete Binding Update message. This approach is NOT RECOMMENDED, however.

If the Binding Update message is early, the mobile node MUST add a Care-of Test Init option to the message, requesting the correspondent node to return a new care-of keygen token. Once a responding Binding Acknowledgment message with a Care-of Test option is received, the mobile node MUST use the care-of keygen token contained therein in calculating the authenticator for a complete Binding Update message and send this message to the correspondent node.

The mobile node includes the nonce indices associated with the selected home and care-of keygen tokens in the Binding Update message using a Nonce Indices option [1]. These nonce indices are determined as follows:

- The home nonce index is defined to be zero if the Binding Update message is to be authenticated through the CGA property of the mobile node's home address. (In this case, the mobile node uses a permanent home keygen token to calculate the authenticator for the Binding Update message.)

- If the Binding Update message is to be authenticated through a proof of reachability at the home address, the mobile node uses a temporary home keygen token to calculate the authenticator for the Binding Update message, and the associated home nonce index is taken from the Home Test message with which the home keygen token was obtained.

- The care-of nonce index is zero if the Binding Update message is early.

- If the Binding Update message is complete, the associated nonce index is taken from the Care-of Test message with which the care-of keygen token was obtained.

The Nonce Indices options follows the CGA Parameters and Signature options, if any.

The mobile node finally calculates an authenticator for the Binding Update message based on the selected home and care-of keygen tokens, following the rules described in [1]. The authenticator is placed into a Binding Authorization Data option [1], which the mobile node adds to the Binding Update message as the last option.

4.2 Receiving Binding Update messages

When the correspondent node receives a Binding Update message, it must first verify whether the sending mobile node is the legitimate owner of the home address specified in the message. This is accomplished either through the CGA property of the home address, or through verification of the mobile node's reachability at the home address. The correspondent node selects the authentication method based on the home nonce index given in the Nonce Indices option of the Binding Update message:

- If the home nonce index is zero, the correspondent node MUST authenticate the Binding Update message through the CGA property of the home address.

- If the home nonce index is set to a non-null value, the correspondent node MUST authenticate the Binding Update message through verification of the mobile node's reachability at the home address.

The authenticator for the Binding Update message is calculated based on a permanent or temporary home keygen token. Which type of home keygen token the correspondent node uses in validating the authenticator, and how to retrieve or recompute the home keygen token, depends on the authentication method:

- If the Binding Update message is to be authenticated through the CGA property of the mobile node's home address, the correspondent node should have a permanent home keygen token in its Binding Cache entry for the mobile node. If so, the correspondent node MUST use this permanent home keygen token in validating the

authenticator of the Binding Update message. If the correspondent node does not have a permanent home keygen token for the mobile node in its Binding Cache, the correspondent node MUST reject the Binding Update message.

- If the Binding Update message is to be authenticated through verification of the mobile node's reachability at the home address, the correspondent node MUST verify that it does not have a permanent home keygen token in its Binding Cache entry for the mobile node. Provided that no permanent home keygen token is found, the correspondent node MUST recompute the temporary home keygen token defined by the (non-null) home nonce index in the Nonce Indices option of the Binding Update message, and it MUST use this recomputed token in validating the authenticator of the message. In case the correspondent node does have a permanent home keygen token in its Binding Cache entry for the mobile node, it MUST reject the Binding Update message. This is necessary to ensure that an attacker cannot bid down the authentication method to hijack a mobile node's legitimate binding.

The authenticator for the Binding Update message is further calculated based on a care-of keygen token. Which care-of keygen token the correspondent node uses in validating the authenticator depends on whether the Binding Update message is complete or early:

- If the care-of nonce index in the Nonce Indices option of the Binding Update message is set to a non-null value, the Binding Update message is complete. In this case, the correspondent node MUST recompute the care-of keygen token defined by the index, and it MUST use this recomputed token in validating the authenticator of the message.

- If the care-of nonce index is zero, the Binding Update message is early. In this case, the correspondent node uses a value of zero in validating the authenticator of the Binding Update message.

The correspondent node finally validates the authenticator in the Binding Update message based on the selected home and care-of keygen tokens, following the rules described in [1].

If the validation fails, the correspondent node MUST discard the Binding Update message. The correspondent node may have to send a Binding Acknowledgment message with a negative status code as described in [1].

Provided that the validation of the authenticator in the Binding Update message succeeds, the correspondent node registers the mobile node's new care-of address, either updating an existing Binding Cache

entry, if one exists, or creating a new Binding Cache entry. The state of the new care-of address depends on whether the Binding Update message is complete or early:

- If the Binding Update message is complete, the new care-of address is set to VERIFIED state. The correspondent node may then immediately send packets to the new care-of address without restrictions.

- If the Binding Update message is early, the new care-of address is set to UNVERIFIED state. The correspondent node MUST then follow the rules defined in section 5.4 for sending packets to this care-of address until the care-of address is set in VERIFIED state.

If the Binding Update message contains a CGA Parameters option, the mobile node is requesting the correspondent node to accept the included CGA parameters either for establishing a new, or for renewing an existing permanent home keygen token shared between the mobile node and the correspondent node. The correspondent node MUST in this case check if the CGA Parameters option is directly followed by a Signature option and, if so, validate the signature included in the latter. This is done as described in Section 4.6.

If the CGA Parameters option is not directly followed by a Signature option, or the validation of the signature included in the Signature option fails, the correspondent node MUST discard the Binding Update message.

Provided that the signature included in the Signature option is correct, the correspondent node generates a permanent home keygen token to be shared with the mobile node and stores it in its Binding Cache entry for the mobile node. The permanent home keygen token is sent to the mobile node within a Binding Acknowledgment message as described in Section 4.3.

4.3 Sending Binding Acknowledgment messages

Upon receipt of a valid Binding Update message, the correspondent node returns to the mobile node a Binding Acknowledgment message in any of the following cases:

- The Acknowledge flag in the Binding Update message is set.

- The Binding Update message is early and includes a Care-of Test Init option.

- The Binding Update message contains a CGA Parameters option followed by a Signature option, and the signature included in the latter was determined to be correct.

If the Binding Update message is early, the Binding Acknowledgment message MUST contain a Care-of Test option with a pseudo-random value in the Care-of Keygen Token field.

If the Binding Update message contains a CGA Parameters option followed by a Signature option, and the signature included in the latter was determined to be correct, the Binding Acknowledgment message MUST include a Permanent Home Keygen Token option with the permanent home keygen token stored in the correspondent node's Binding Cache entry for the mobile node.

4.4 Receiving Binding Acknowledgment messages

A mobile node verifies a received Binding Acknowledgment message according to the rules specified in [1].

If the Binding Acknowledgment message contains a Care-of Test option, the mobile node extracts the care-of keygen token included in this option, stores this token in the appropriate entry of its Binding Update List, and sends the correspondent node a complete Binding Update message as defined in section Section 4.1.

If the Binding Acknowledgment message contains a Permanent Home Keygen Token option, the mobile node extracts the permanent home keygen token included in this option and stores it in the appropriate entry of its Binding Update List. Future Binding Update messages will then be authenticated based on the CGA property of the mobile node's home address.

4.5 Sending CGA Parameters

TBD.

4.6 Receiving CGA Parameters

TBD.

4.7 Renewing a Permanent Home Keygen Token

A mobile node MAY request a correspondent node to renew an existing

permanent home kegen token at any time, but it MUST do so in the imminent event of a sequence number rollover, or when the lifetime of the binding at the correspondent node is about to expire.

4.8 Handling Payload Packets

A correspondent node maintains a "credit counter" for each mobile nodes with which it uses the protocol specified in this document. Whenever a packet arrives from one of these mobile nodes, the correspondent node SHOULD increase that mobile node's credit counter by the size of the received packet. When the correspondent node has a packet to be sent to the mobile node, if the mobile node's care-of address is labeled UNVERIFIED, the correspondent node checks whether it can send the packet to the UNVERIFIED care-of address: The packet SHOULD be sent if the value of the credit counter is higher than the size of the outbound packet. If the credit counter is too low, the packet MUST be discarded or buffered until address verification succeeds. When a packet is sent to a mobile node at an UNVERIFIED care-of address, the mobile node's credit counter MUST be reduced by the size of the packet. The mobile node's credit counter is not affected by packets that the host sends to a VERIFIED care-of address of that mobile node.

Figure 1 depicts the actions taken by the correspondent node when a packet is received. Figure 2 shows the decision chain in the event a packet is sent.

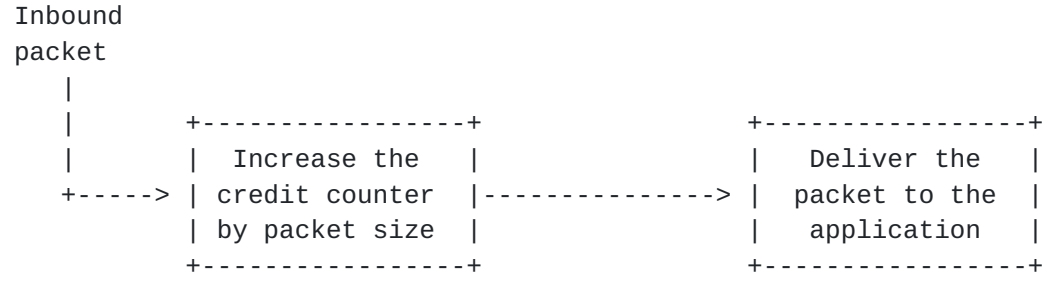


Figure 1: Receiving Packets with Credit-Based Authorization

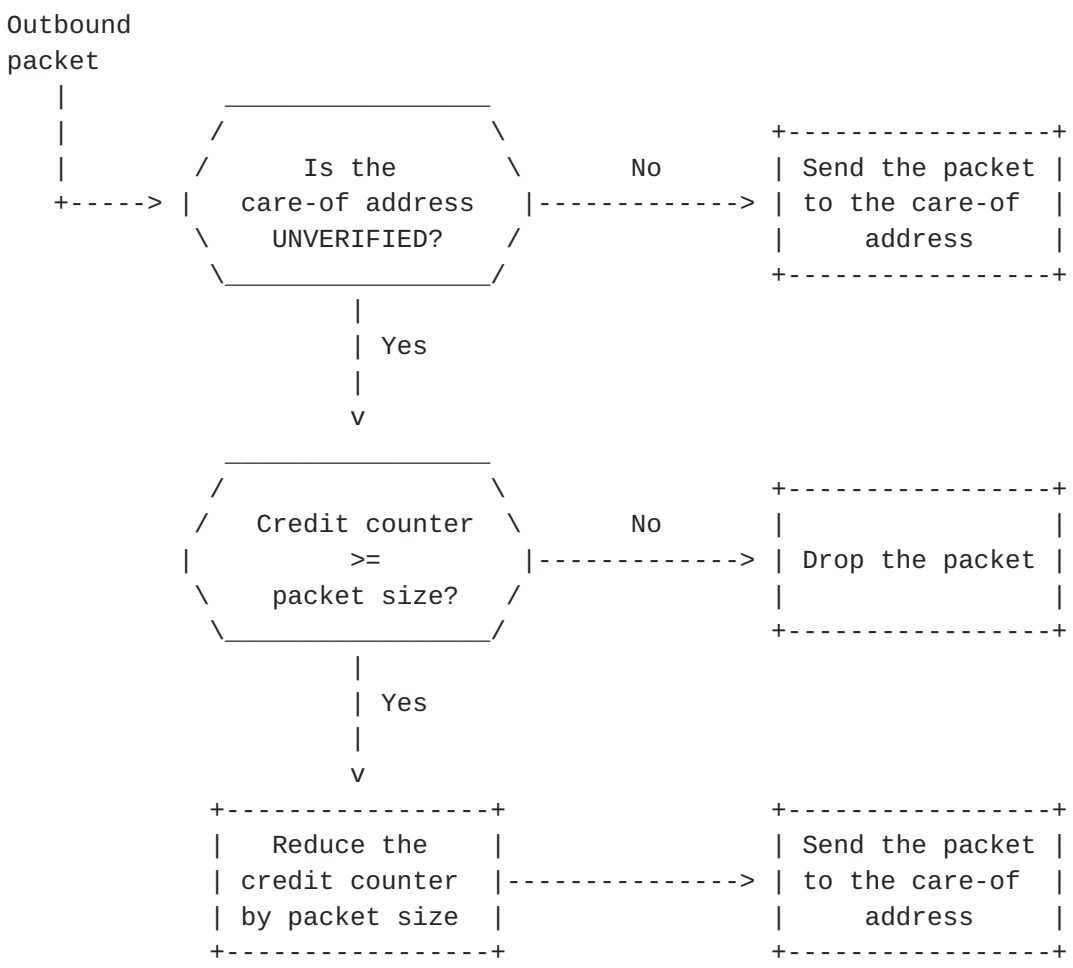


Figure 2: Sending Packets with Credit-Based Authorization

4.9 Credit Aging

A correspondent node ensures that the credit counters it maintains for its mobile nodes gradually decrease over time. Such "credit aging" prevents a malicious node from building up credit at a very slow speed and using this, all at once, for a severe burst of redirected packets.

Credit aging SHOULD be implemented by multiplying credit counters with a factor, CreditAgingFactor, less than one in fixed time intervals of CreditAgingInterval length. Choosing appropriate values for CreditAgingFactor and CreditAgingInterval is important to ensure that the correspondent node can send packets to an address in state UNVERIFIED even when the mobile node sends at a lower rate than the correspondent node itself. When CreditAgingFactor or

CreditAgingInterval are too small, the mobile node's credit counter might be too low to continue sending packets until address verification concludes.

The following values are used for the credit-aging parameters defined in this document:

CreditAgingFactor	7/8
CreditAgingInterval	5 seconds

Note: These parameter values work well when the correspondent node transfers a file to the mobile node via a TCP connection and the end-to-end round-trip time does not exeed 500 milliseconds.

4.10 Cryptographic Calculations

The Signature option is calculated with the mobile node's private key over the following sequence of octets:

```
Mobility Data = care-of address | correspondent | MH Data
```

Where | denotes concatenation and "correspondent" is the correspondent node's IPv6 address. Note that in case the correspondent node is mobile, correspondent refers to the correspondent node's home address.

MH Data is the content of the mobility message including the MH header. The Authenticator within the Binding Authorization Data option is zeroed for purposes of calculating the signature.

The RSA signature is generated by using the RSASSA-PKCS1-v1_5 [2] signature algorithm with the SHA-1 hash algorithm.

When the SKey option is used, the correspondent node MUST encrypt the Kbm with the MN's public key using the RSAES-PKCS1-v1_5 format [2].

4.11 Simultaneous Movements

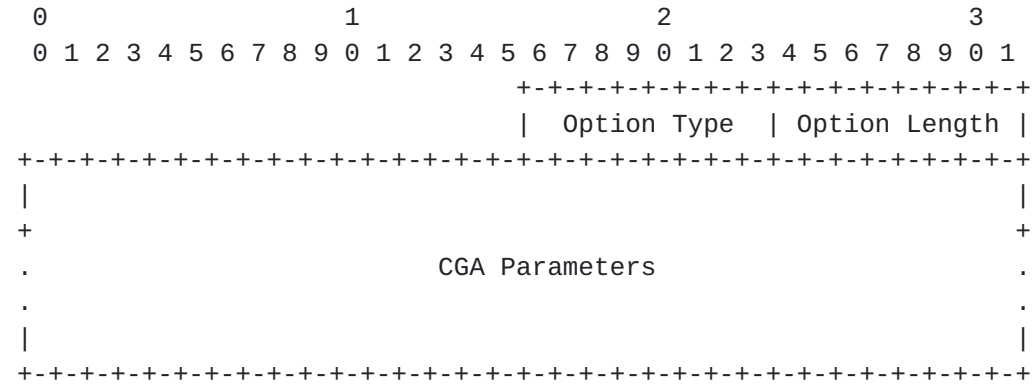
As specified in RFC 3775 [1], Mobility Header messages are generally sent via the mobile node's home agent and to the peer's home address, if it is also mobile. This makes it possible for two mobile nodes to communicate even if they are moving simultaneously.

5. Option Formats and Status Codes

5.1 CGA Parameters Option

Options of this type are used to carry the mobile node's public key and the CGA parameters needed by the correspondent node to check the validity of the mobile node's CGA. RFC 3775 [1] limits Mobility Header options to a maximum length of 255 bytes, excluding the Option Type and Option Length fields. For this reason, multiple options of this type are used to carry the entire CGA information, which is likely to exceed the limit specified in RFC 3775.

The format of the option is the following:



Option Type

<To Be Assigned By IANA>.

Option Length

Length of the option.

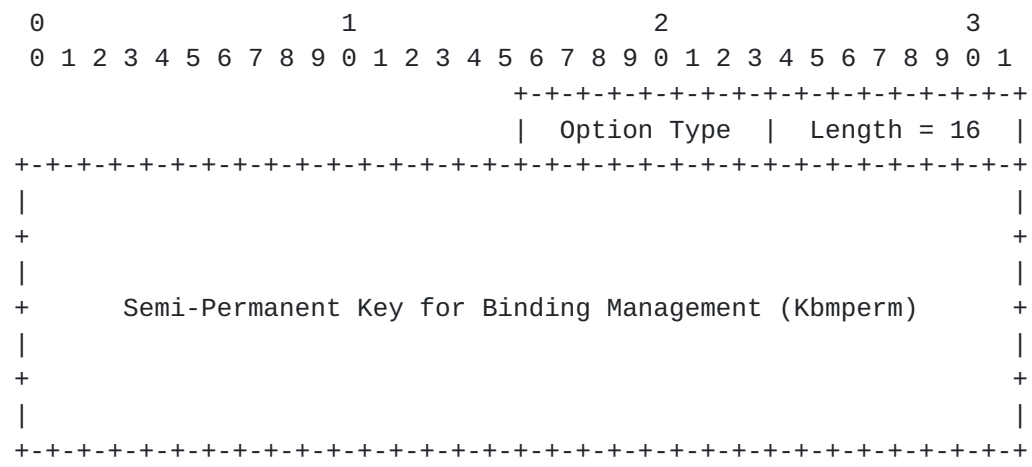
Option Data

This field contains up to 255 bytes of the string holding the mobile node's CGA public key and other CGA parameters in the format defined in [18]. The concatenation of all options of this type in the order they appear in the Binding Update message MUST result in the string defined in [18]. All options of this type carried in the Binding Update message except the last one MUST contain exactly 255 bytes in the Option Data field, and the Option Length field MUST be set to 255 accordingly. All options of this type MUST appear one after another, i.e., an option of a different type MUST NOT be placed in between two options of this type.

5.2 Permanent Home Keygen Token Option

As it has been mentioned above, the correspondent node MUST send a new Kbm each time it receives a Binding Update message containing the CGA Parameter option. For this purpose, this proposal uses a new option called SKey option, which MUST be inserted in the Binding Acknowledgment message.

The format of the option is as follows:



Option Type

<To Be Assigned By IANA>.

Option Length

Length of the option.

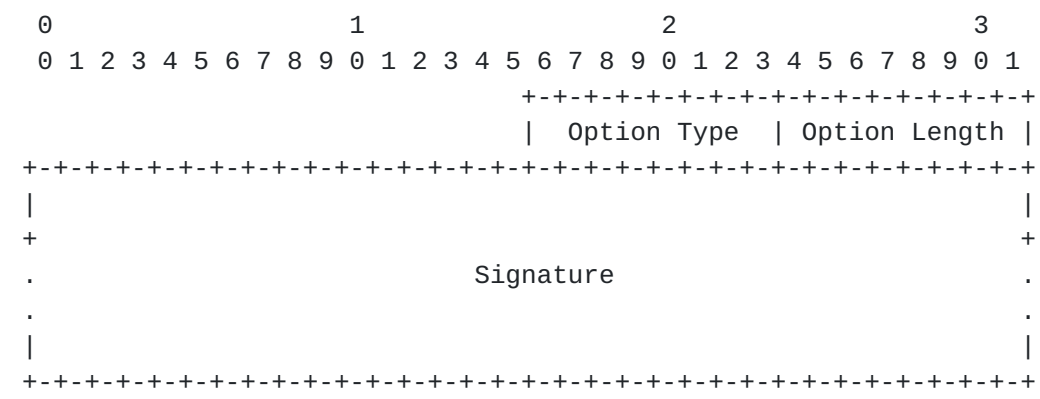
Option Data

This field contains the Kbmperm value. Note that the content of this field MUST be encrypted with the mobile node's public key as defined in Section 4.10. The length of Kbmperm value is 20 octets (before encryption or padding possibly involved [2]).

5.3 Signature Option

When the mobile node signs the Binding Update message with its CGA private key, it MUST insert the signature in the SIG option. Such scenario occurs when the mobile node sends its first Binding Update message to the correspondent node and if the mobile node reboots during an ongoing session.

The option format is as follows:



Option Type

<To Be Assigned By IANA>.

Option Length

Length of the option.

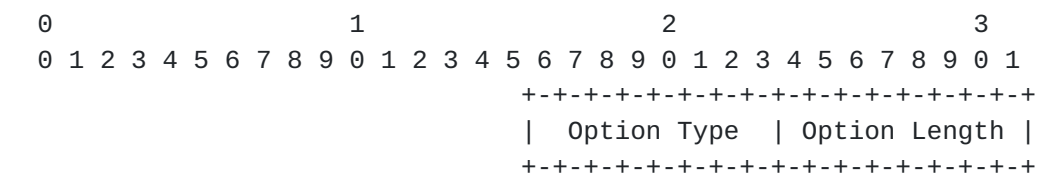
Option Data

This field contains the signature of the MH message it is contained within.

5.4 Care-of Test Init Option

A mobile node that wishes to employ the care-of address test optimization MAY employ this option in Binding Update message sent to a correspondent node in which it has previously established a Binding Cache entry. When received by such a correspondent node, it SHOULD return a Care-of Keygen Token option in the Binding Acknowledgement message.

The option format is as follows:



Option Type

<To Be Assigned By IANA>.

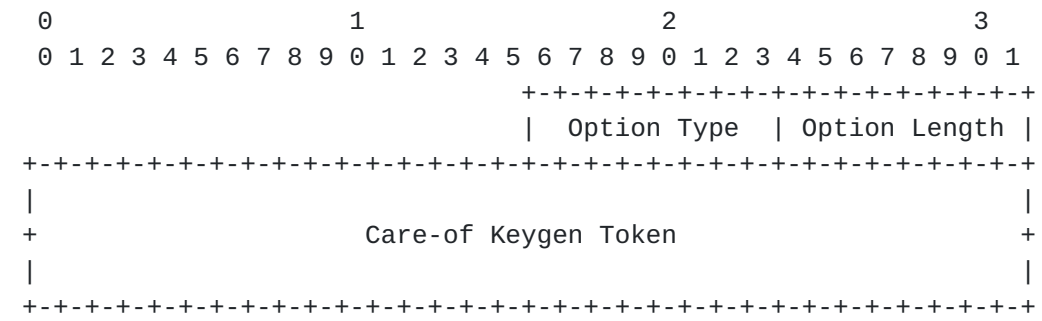
Option Length

Length of the option = 0.

5.5 Care-of Test Option

This option is returned by a correspondent node upon seeing a Care-of Test Init option in a Binding Update.

The option format is as follows:



Option Type

<To Be Assigned By IANA>.

Option Length

Length of the option = 8.

Care-of Keygen Token

A care-of keygen token, calculated as in RFC 3775.

5.6 Status Codes

The following new Status codes are allocated:

Lost Kbmperm State (<To Be Allocated By IANA>)

This code is returned when the correspondent node does not have a Binding Cache Entry, Kbmperm, or has an invalid Binding Authorization Data option. The code MUST only be used in to respond to Binding Updates that contain one of the mobility options defined in this document.

6. Security Considerations

This draft describes a method to exploit the CGA features in order to authenticate route optimization signaling. In fact, the CGA replaces the authentication by providing a proof of ownership while the RR procedure replaces the authentication by a routing property.

This proof of ownership ensures that only the mobile node will be able to change the routing of packets destined to it, modulo exhaustive attacks on the CGA mechanism itself. The feasibility of such attacks and the defenses against them have been discussed in [18].

Note that, as specified, the proof of ownership protection applies only to the correspondent node believing the statements made by the mobile node. There is no guarantee that the answers from the correspondent node truly come from that correspondent node and not from someone who was on the path to the correspondent node during the initial contact phase. This is because we do not require correspondent nodes to have CGAs, and as a result, they can not make any statements that are authenticated in the strong sense. We chose not to protect against this, because this attack is something that already exists in plain IPv6, as is explained in the following. Lets assume that the correspondent node does not care about the IP address of the peers contacting it and that it does not protect its payload packets cryptographically. Then, a man-in-the-middle can always use its own address when communicating to the correspondent node, and the correspondent node's address when communicating to the mobile node. Philosophically, one can also argue that since the problem we attempt to solve here is routing modifications for the mobile node's address, it is sufficient to ensure that these modifications are protected.

It should be mentioned that while the CGA can provide a protection against unauthenticated Binding Update messages, it can expose the involved nodes to denial-of-service attacks since it is computationally expensive. The draft limits the use of CGA to only the first registration and if/when re-keying is needed. In addition,

it is RECOMMENDED that nodes track the amount of resources spent to the CGA processing, and disable the processing of new requests when these resources exceed a predefined limit.

The protocol specified in this document relies on standard 16-bit Mobile IPv6 sequence numbers and periodic rekeying to avoid replay attacks. Nodes rekey at least once every 24 hours. Nodes also rekey whenever a rollover in the available sequence-number space becomes imminent. Rekeying allows the nodes to reuse sequence numbers without exposing themselves to replay attacks.

This protocol is secure against flooding attacks due to the use of care-of-address tests, Credit-Based Authorization, and the use of an initial home address test.

7. Performance Considerations

Performance of our protocol depends on whether we look at the initial or subsequent runs. The number of messages in the initial run is one less as in base Mobile IPv6, but the size of the messages is increased somewhat.

On a mobile node that does not move that often, there is a significant signaling reduction, as the lifetimes can be set higher than in return routability. For instance, a mobile node that stays in the same address for a day will get a 99.52% signaling reduction. Such long lifetimes can be achieved immediately, as opposed to methods like [14] that grow them gradually.

On a mobile node that moves fast, the per-movement signaling is reduced by 33%.

Latency on the initial run is not affected, but on the subsequent movements there's a significant impact. This is because the home address test is eliminated. The exact effect depends on network topology, but if the home agent is far away and the correspondent node is on the same link, latency is almost completely eliminated.

Additional latency and signaling improvements could be achieved through mechanisms that optimize the care-of address tests in some way. This is outside the scope of this document, however.

8. IANA Considerations

This document defines a new CGA Message Type name space for use as type tags in messages that may be signed using CGA signatures. The values in this name space are 128-bit unsigned integers. Values in this name space are allocated on a First Come First Served basis [3]. IANA assigns new 128-bit values directly without a review.

CGA Message Type values for private use MAY be generated with a strong random-number generator without IANA allocation.

This document defines a new 128-bit value under the CGA Message Type [18] namespace, 0x5F27 0586 8D6C 4C56 A246 9EBB 9B2A 2E13.

This document defines a set of new mobility options, which must be assigned Option Type values within the mobility option numbering space of [1]. This document also allocates a new Status code value.

9. References

9.1 Normative References

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

[2] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[3] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[4] International Telecommunications Union, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, July 2002.

[5] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

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

[7] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

9.2 Informative References

[8] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", IETF Request for Comments 4225, December 2005.

[9] Aura, T., "Cryptographically Generated Addresses (CGA)", IETF Request for Comments 3972, March 2005.

[10] Vogt, C., "Credit-Based Authorization for Mobile IPv6 Early Binding Updates", draft-vogt-mipv6-credit-based-authorization-00 (work in progress), May 2004.

[11] Vogt, C. and M. Doll, "Efficient End-to-End Mobility Support in IPv6", Proceedings of the IEEE Wireless Communications and Networking Conference, IEEE, April 2006.

[12] Mirkovic, J. and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Vol. 34, No. 2, ACM Press, April 2004.

[13] Vogt, C. and J. Arkko, "Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization", IETF Internet Draft draft-irtf-mobopts-ro-enhancements-08.txt (work in progress), May 2006.

[14] Arkko, J. and C. Vogt, "Credit-Based Authorization for Binding Lifetime Extension", draft-arkko-mipv6-binding-lifetime-extension-00 (work in progress), May 2004.

[15] O'Shea, G. and M. Roe, "Child-Proof Authentication for MIPv6 (CAM)", ACM SIGCOMM Computer Communication Review, ACM Press, Vol. 31, No. 2, April 2001.

[16] Nikander, P., "Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World", Revised papers from the International Workshop on Security Protocols, Springer-Verlag, April 2002.

[17] Haddad, W. and S. Krishnan, "Optimizing Mobile IPv6 (OMIPv6)", draft-haddad-mipv6-omipv6-01 (work in progress), February 2004.

[18] Aura, T., "Cryptographically Generated Addresses (CGA)", draft-ietf-send-cga-06 (work in progress), April 2004.

[19] Roe, M., "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", draft-roe-mobileip-updateauth-02 (work in progress), March 2002.

[20] Haddad, W., "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)", draft-haddad-mip6-cga-omipv6-04 (work in progress), May 2005.

[21] Vogt, C., "Early Binding Updates for Mobile IPv6", draft-vogt-mip6-early-binding-updates-00 (work in progress), February 2004.

[22] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[23] Nikander, P., "Mobile IP version 6 Route Optimization Security Design Background", draft-ietf-mip6-ro-sec-03 (work in progress), May 2005.

[24] Dupont, F. and J. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes", draft-dupont-mipv6-cn-ipsec-01 (work in progress), June 2004.

[25] Perkins, C., "Preconfigured Binding Management Keys for Mobile IPv6", draft-ietf-mip6-precfgKbm-00 (work in progress), April 2004.

Authors' Addresses

Jari Arkko
Ericsson Research NomadicLab
FI-02420 Jorvas
Finland

Email: jari.arkko@ericsson.com

Christian Vogt
Institute of Telematics
Universitaet Karlsruhe (TH)
P.O. Box 6980
76128 Karlsruhe
Germany

Email: chvogt@tm.uka.de

Wassim Haddad
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2, Canada

Email: wassim.haddad@ericsson.com

Appendix A. Acknowledgment

The authors would like to thank Pekka Nikander, Tuomas Aura, Greg O'Shea, Mike Roe, Gabriel Montenegro, Vesa Torvinen for interesting discussions around cryptographically generated addresses.

The authors would also like to thank Greg Daley, Samita Chakrabarti, Marcelo Bagnulo, Suresh Krishnan, Mohan Parthasarathy, Lila Madour, Francis Dupont, Roland Bless, Mark Doll, and Tobias Kuefner for their review and comments on the predecessors of this document.

Finally, the authors would also like to emphasize that [19] pioneered the use of cryptographically generated addresses in the context of Mobile IPv6 route optimization, and that this document consists largely of material from [20], [21], and [10] and the contributions of their authors.

Appendix B. Overview of CGA

As described in [18], a Cryptographically Generated Address (CGA) is an IPv6 address, which contains a set of bits generated by hashing the IPv6 address owner's public key. Such feature allows the user to provide a "proof of ownership" of its IPv6 address.

The CGA offers three main advantages: it makes the spoofing attack against the IPv6 address much harder and allows to sign messages with the owner's private key. CGA does not require any upgrade or modification in the infrastructure.

The CGA offers a method for binding a public key to an IPv6 address. The binding between the public key and the address can be verified by re-computing and comparing the hash value of the public key and other parameters sent in the specific message with the interface identifier in the IPv6 address belonging to the owner. Note that an attacker can always create its own CGA address but he will not be able to spoof someone else's address since he needs to sign the message with

the corresponding private key, which is supposed to be known only by the real owner.

CGA assures that the interface identifier part of the address is correct, but does little to ensure that the node is actually reachable at that identifier and prefix. As a result, CGA needs to be employed together with a reachability test where redirection denial-of-service attacks are a concern.

Each CGA is associated with a public key and auxiliary parameters. In this protocol, the public key MUST be formatted as a DER-encoded [4] ASN.1 structure of the type SubjectPublicKeyInfo defined in the Internet X.509 certificate profile [5].

The CGA verification takes as input an IPv6 address and auxiliary parameters. These parameters are the following:

- a 128-bit modifier, which can be any value,
- a 64-bit subnet prefix, which is equal to the subnet prefix of the CGA,
- an 8-bit collision count, which can have values 0, 1 and 2.

If the verification succeeds, the verifier knows that the public key in the CGA parameters is the authentic public key of the address owner. In order to sign a message, a node needs the CGA, the associated CGA parameters, the message and the private cryptographic key that corresponds to the public key in the CGA parameters. The node needs to use a 128 bit type tag for the message from the CGA Message Type name space. The type tag is an IANA-allocated 128 bit integer.

To sign a message, a node performs the following two steps:

1. Concatenate the 128 bit type tag (in the network byte order) and message with the type tag to the left and message to the right. The concatenation is the message to be signed in the next step.
2. Generate the RSA signature. The inputs to the generation procedure are the private key and the concatenation created in a).

Appendix C. Overview of Credit-Based Authorization

To prevent redirection-based flooding attacks, the easiest way would be not to use a new care-of address until it has been verified. This could proceed unnoticed when the mobile node can meanwhile communicate through a second interface. However, many situations are conceivable in which mobile nodes have a single interface only. The care-of-address test would increase signaling delays by one round-trip time in such cases. To avoid this additional delay, a new care-of address is used as soon as possible, and the correspondent node verifies the mobile node's reachability at that care-of address concurrently. Credit-Based Authorization for concurrent care-of-address tests prevents illegitimate packet redirection until the validity of the address has been established. This is accomplished based on the following three hypotheses:

1. A flooding attacker typically seeks to somehow multiply the packets it generates itself for the purpose of its attack because bandwidth is an ample resource for many attractive victims.

2. An attacker can always cause unamplified flooding by sending packets to its victim directly.

3. Consequently, the additional effort required to set up a redirection-based flooding attack would pay off for the attacker only if amplification could be obtained this way.

On this basis, rather than eliminating malicious packet redirection in the first place, Credit-Based Authorization prevents any amplification that can be reached through it. This is accomplished by limiting the data a correspondent node can send to an unverified care-of address of a mobile node by the data recently received from that mobile node. Redirection-based flooding attacks thus become less attractive than, e.g., pure direct flooding, where the attacker itself sends bogus packets to the victim.

Figure 10 illustrates Credit-Based Authorization: The correspondent node measures the bytes received from the mobile node. When the mobile node changes to a new care-of address, the correspondent node labels this address UNVERIFIED and sends packets there as long as the sum of the packet sizes does not exceed the measured, received data volume. The mobile node's reachability at the new care-of address meanwhile gets verified When the care-of-address test completes with success, the correspondent node relabels the care-of address from UNVERIFIED to VERIFIED. As of then, packets can be sent to the new care-of address without restrictions. When insufficient credit is left while the care-of address is still UNVERIFIED, the correspondent node stops sending further packets until address verification

completes.

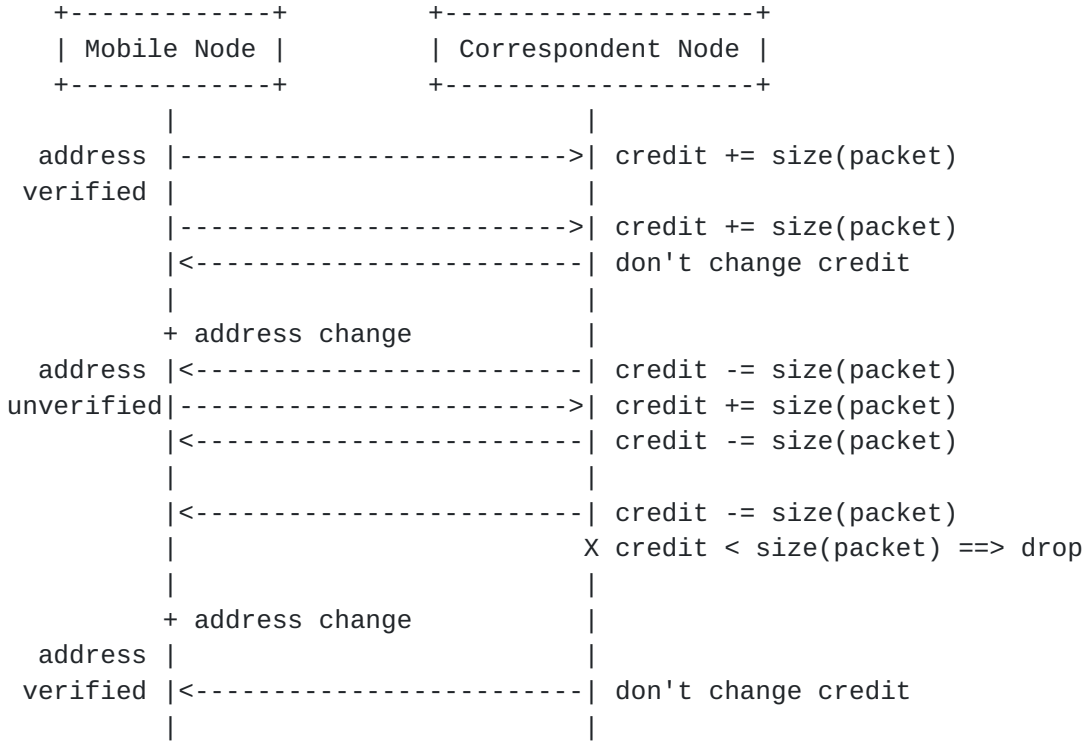


Figure 10: Credit-Based Authorization

The correspondent node ensures that the mobile node's acquired credit gradually decrease over time. Such "credit aging" prevents a malicious node from building up credit at a very slow speed and using this, all at once, for a severe burst of redirected packets.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.