Location Privacy in Mobile IPv6 Distributed Authentication Protocol Using Mobile Home Agents

ANDREW GEORGIADES
YUAN LUO
ABOUBAKER LASEBAE
RICHARD COMLEY
Department of Computer Science
Middlesex University
Hendon Campus, The Burroughs, London, NW4 4BT
UNITED KINGDOM
Andrew_georgiades@yahoo.co.uk http://www.andrewgeorgiades.com

Abstract: - Mobile IPv6 will be the basis for the fourth generation 4G networks which will completely revolutionize the way telecommunication devices operate. This paradigm shift will occur due to the sole use of packed switching networks. Mobile IPv6 utilizes binding updates as a route optimization to reduced triangle routing between the mobile node, the home agent and the correspondent node, allowing direct communication between the mobile node and the correspondent. However, direct communication between the nodes produces a range of security vulnerabilities, which the home agent avoided. This paper attempts to provide the advantages of using the home agent as an intermediary whilst reducing the latency of triangle routing. This can be achieved with the proposed use of a mobile home agent which essentially follows the mobile node as it moves between points of attachment providing location privacy and pseudo-direct communication, which can be incorporated into the distributed authentication protocol or be used as a stand alone solution.

Key-Words: - Mobile Home Agent, MIPv6, Distributed Authentication Protocol, 4G, Location Privacy

1 Introduction

Mobile IPv6 is the next step in the evolution of networking. The most widely used internet protocol are currently networks based on IPv4 which are restricted to 32 bit addresses. This provides a number of IP addresses which, over time, has became limited to the number of devices which need them. Network address translation has helped to delay the need for more address. However a new Internet protocol was inevitably created to solve this issue, IPv6. Ipv6 addresses are 128 bit providing 3.4×10^{38} address which solves the issue of address limitation however as most devices are becoming mobile, IPv6 provides no method for them to migrate to a new location as the IP addresses are static [13].

Mobile IPv6 solves this issue by providing an infrastructure which allows the mobile node to acquire a new address every time it moves to a new point of attachment and yet still remain reachable as it has a home agent which has an IP address which remains static and also keeps track of the mobile node's current location. The home agent is the first point of contact when attempting to contact the mobile node as the home agent acts as a proxy and tunnels messages to the mobile node. This is called triangle routing and the latency of communication between the nodes increases the further away the mobile node travels from the home agent [8].

The introduction of the route optimization protocol allows the mobile node to communicate directly with its correspondents with the use of binding updates. However these are vulnerable to a variety of attacks such as interception, modification, impersonation and redirection. Binding updates are also susceptible to denial of service attacks.

However, several security solutions have been created which attempt to protect the binding updates, such as CAM [11] and the distributed authentication protocol [5]. But non of these address the issue of location privacy, for if the attacker is unable to determine the location of the mobile node, he will not be able to attack it.

This paper will look at the advantages and disadvantages of current location privacy security solutions in Mobile IPv6. It will then look at the new technology of mobile autonomous software agents, which can exist and move independently within heterogeneous networks. The paper will then go on to suggest that mobile agents can be used in a security solution where they will act as mobile home agents providing location privacy without increasing communication latency. This solution can be used as a stand alone solution or be used as part of the distributed authentication protocol.

2 Current Solutions

Several solutions have been created in an attempt to solve the issue of Identity protection in Mobile IPv6. Each have their advantages and disadvantages and are discussed here:

2.1 BLIND

BLIND is a security framework that provides identity protection against active and passive attacks for end-points. A two-round-trip authenticated Diffe-Hellman Key Exchange Protocol that protects the initiator's and responder's identity is presented in [14].

The protocol hides the public key based identifiers from attackers and eavesdroppers by blinding the identifiers. The protocol completes the identity protection by offering location privacy with forwarding agents. An end-point must negotiate a key exchange with its peer via the forwarding agent to obtain location privacy.

The forwarding agent provides location privacy by hiding the real location of the node. The peers are able to see only the virtual address, not the real address of the end-point. A cryptographic hash of the public key end point identifier (EID) is called a fingerprint.

Each party creates scrambled versions of the fingerprints and use each scrambled value only during one protocol run. This makes it impossible to correlate independent protocol runs.

2.2 Authorised Anonymous ID

To address the issue of location privacy, [7] introduces the idea of an authorized anonymous ID based scheme, which eliminates the need for a trusted server or administration.

A cryptographic technique called blind signatures are used to generate an authorized anonymous ID which is used to replay the real ID of the mobile device. To address location privacy issues, an architecture was designed on the Wireless Andrew 802.11 WLAN network which used a centralized location server which stored the location data of registered mobile users.

It is suggested in [7] that a distributed architecture would be more appropriate as a centralized architecture has drawbacks.

2.3 Temporal Mobile Identifier (TMI)

Various ways are suggested in [4] in which to prevent location information leakage. One way to do this is to hide the home address of the mobile node from third parties by using a temporal mobile identifier.

In MIPv6 packets transmitted contain the addresses of the mobile node and home address in clear text in the header. This can allow an eavesdropper to identify packets and track mobile movement. One solution is to use a Temporal Mobile Identifier (TMI) for each mobile node. This is a random 128 bit sequence which can identify the mobile node to other nodes. The TMI replaces the home address in the header of packets and has the effect of hiding the mobile home network identity from the correspondent and eavesdroppers.

An alternative method would be not to use binding updates at all and use bi-directional tunneling. This means the correspondent sends all packets to the home address, which then encapsulates them and forwards them to the care of address.

If route optimization is used then the binding update must contain the TMI in the home address option and the binding update must be encrypted.

2.4 Hierarchical Mobile IPv6

The hierarchical mobile IP management model [4] utilizes a new node called a mobility anchor point (MAP). It provides a central point to assist with hand offs. It can be located at any level in a hierarchical network including the access router (AR).

In the basic mode of Hierarchical mobile IP, the mobile node has two address, a regional care of address (RCoA) and on the MAP’s subnet an on link care of address (LCoA) [12]. The MAP acts as a local home agent that maps the mobile node’s regional care of address to its on link care of address. The mobile node has the option of hiding its on link care of address from the corresponding nodes and its home agent by using its regional care of address in the source field in the packets it sends. However an eavesdropper can still determine the mobile nodes home address by snooping the packets.

3 Mobile Agents

Traditionally programs are executed on one machine; perform a task and end execution on the same machine. The next step in evolution for software is to become mobile. Tasks that have started execution on one machine can now be paused, “jump” to another computer and continue execution there. This is possible with mobile agents and opens up a new dimension in computer programming and usage.

Mobile agents are autonomous applications, which features the behavior of autonomy, social ability, learning and most importantly, mobility. Mobile agents can move from host to host in a heterogeneous network by saving its current state, performing a move to another host via data duplication and then resuming execution from the saved state. This means that they can control their own actions and move to different machines and execute on them at any time regardless of operation or operating system [1].

The traditional client/server model shows that the client sends a message to the server and the server replies (fig 1).

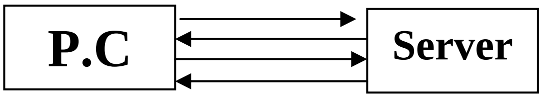

Fig 1. Client Server Model

They perform a continuous dialogue until the task is complete. Mobile agents work in a different way [3]. Their approach is to contain the user’s data and instructions within the agent and dispatch it to a destination computer and there the agent communicates with the server at the server side (fig 2).

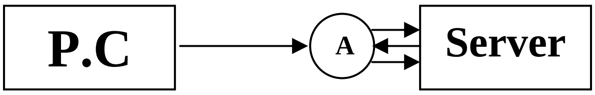

Fig 2. Agent communication with server

The benefit of this is that it reduces the network load and frees up bandwidth, it also allows for faster communication [9,10].

This is a very attractive technology for the purposes of Mobile IP and as you will see in the proposed solution mobile agents can be used to facilities network messages and location privacy.

4 Proposed Solution

Mobile IPv6 provides two methods of communication between the mobile and correspondent node. The first is triangle routing which is when all communication to the mobile node is via the home agent. This is necessary as the home agents’ IP address is static and is the first point of contact for any communication to the mobile node. The disadvantage however is that the further the mobile node travels from the home agent the further data packets will have to travel to reach their destination.

The second method involves the use of a route optimization technique which allows direct communication between the mobile and correspondent node. This is achieved with the use of binding updates. The disadvantage to this method is that the location of the mobile node is revealed to any correspondent in communication with it, which could be a potential security risk.

This paper introduces an alternative method which provides the best of both worlds without the disadvantages.

4.1 Mobile Agents technology introduced in to Mobile IPv6

The concept involves the introduction of mobile agent technology into mobile IPv6 networks.

The way they would be used is as an intermediary between the mobile node and the correspondent effectively becoming triangle routing. However the mobile agent would reside on the IPv6 node which the mobile node is using as its point of attachment. The mobile agent is a piece of software responsible for routing messages from other nodes to the mobile node and at the same time provide location privacy by acting as a proxy and masking the true IP address of the mobile node.

As the mobile agent resides on the mobile nodes point of attachment there is negligible latency in comparison to triangle routing via the home agent. As the mobile agent will effectively resume most of the roles of the home agent we can call it a mobile home agent. But why is it mobile?

As it resides on the mobile nodes point of attachment, if the mobile node travels to a new location it will connect to a new point of attachment which will then be responsible for the mobile node as all communications are handed over to it. However the mobile home agent would not lose communication with the mobile node as the software is autonomous and capable of duplicating itself to the new point of attachment and resuming its role in the network.

Every time the mobile node moves to a new point of attachment the mobile home agent will follow providing constant location privacy with the advantages of low latency communication. This process can be seen in fig 3.

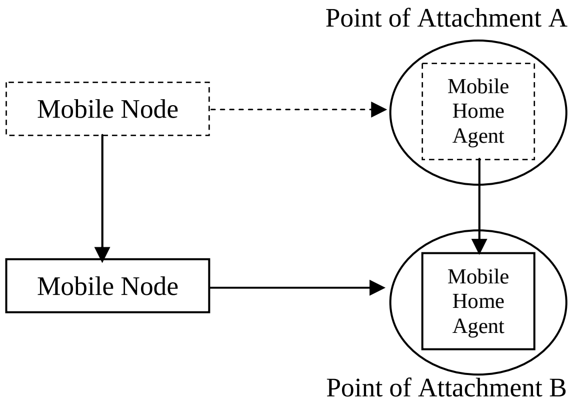

Fig 3. Mobile node and mobile home agent migrating to a new point of attachment.

4.2 Mobile Home Agent used in a Mobile to Static Node Communication.

The introduction of mobile home agents will noticeably increase the speed of node communication and protect the identity of the mobile nodes' current location.

Firstly all nodes should be using cryptographically generated address, which have been previously created by the function discussed in [2]:

$$(2), \text{Host ID} = \text{HASH}_{62}(\text{public key})$$

In this scenario we will assume that the correspondent node is static and so does not require a mobile home agent.

Message 1.

The mobile node MN attempts to contact the correspondent node CN. The mobile node's public key MNK+, care of address CoA and home address HoA are sent to CN the correspondent node. Message flows are shown in Fig.1. However the CoA care of address given is not the mobile nodes true address, it is the address of its Mobile Home Agent. This is to protect the location of the mobile node. Therefore the proxy care of address which is the Mobile Home Agent is represented by MHA.

In message 2 the correspondent will compare the mobile nodes' public key with the supplied care of address. Under the circumstances this test will fail as the mobile home agents care of address will not match the public key of the mobile node. Therefore the mobile node must supply a public key based on the address of the mobile home agent. MHAK+.

MN ⟶ CN: MHAK+, MHA, HoA.

Message 2.

The corresponding node compares the mobile node's public key with that of its claimed CGA address and determines if they match. If they do then return routability and device authentication will proceed, otherwise the connection / binding update request is denied. In this case the public key and CGA address are those of the mobile home agent.

The next step the correspondent will perform the home address check and the care of address check.

The correspondent will send a home test (HoT) packet, which is assumed that the home agent will tunnel to the mobile node. The HoT packet consists of a home keygen token generated by hashing the secret key K_{cn} only known to the correspondent. A nonce index is also included to allow the CN to find the appropriate nonce easily.

Home token = hash (K_{cn} | source address | nonce | 0)

This is then sent to the home agent.

CN ⟶ HA: HoT.

Message 3.

The Home Test packet is then forwarded to the mobile node's care of address. This is sent directly to the mobile node as it is assumed that the home agent is a trusted node and needs to know the location of the mobile node anyway. So sending data via the Mobile home agent would have no benefit.

HA ⟶ MN: HoT.

Message 4.

The correspondent also performs a care of address test (CoT), which is similar to the home address test and takes place at the same time as message 3, however the token generated is slightly different.

Care-of token = hash(K_{cn} |source address|nonce|1)

This is then sent directly to the mobile node within a Care of test (CoT) packet. Or so the correspondent thinks. In actuality the correspondent node sends the Care of test (CoT) packet to the mobile home agent.

CN ⟶ MHA: CoT.

Message 5.

The mobile home agent tunnels the care of test to the mobile node.

MHA ⟶ MN: CoT.

Message 6.
The mobile node receives both tokens from both the test packets sent. It then creates a binding key K_{bm} by hashing the two tokens together.

K_{bm} = hash (home token | care-of token)

The key is used to protect the first and following binding updates. The mobile node then sends a binding update request to the correspondent node, which is protected with the binding key $K_{bm.}$

MN $\longrightarrow$ CN: K_{bm}(BU)

Message 7.
This is where traditionally the correspondent would decrypt the data and accept the binding update, however before this begins it must wait for the result of another authentication protocol to complete. This authentication takes place simultaneously with return routability.
The correspondent node sends a request message to the mobile node for its authentication data (RAD).

CN $\longrightarrow$ MHA: RAD

Message 8.
The mobile home agent tunnels the request for authentication data (RAD) to the mobile node.

MHA $\longrightarrow$ MN: RAD

Message 9.
The mobile node replies to the message by sending its authentication data, which includes the mobile home agents' current address, its sim number, IMEI number, phone number and even and option for user authentication such as biometric data. This sent to the CN encrypted with the binding key $K_{bm.}$

MN $\longrightarrow$ CN: K_{bm}(MHA, Sim No, IMEI, Phone No., Biometric)

Message 10.
Simultaneously to message 7, the correspondent sends a request for authentication data message to the home agent.

CN $\longrightarrow$ HA: RAD

Message 11.
The home agent does not have the binding key so sending the authentication data would be a security risk. Instead the home agent hashes the authentication data together and sends that to the correspondent.

HA $\longrightarrow$ CN: Hash(MHA, Sim No, IMEI, Phone No., Biometric)

Message 12.
Now the correspondent will have both the hash of the authentication data and the authentication data encrypted with the binding key. The correspondent performs the authentication comparison by decrypting the binding key and hashing the authentication data received from the mobile node then comparing this to the hash received by the home agent.

If the result of the authentication is successful then the binding update is accepted and a binding acknowledgement BA is sent to the mobile node allowing it to communicate directly with the correspondent.

CN $\longrightarrow$ MHA: BA

Message 13,
The mobile home agent passes the binding acknowledgement to the mobile node to let it know that the process has been successful.

MHA $\longrightarrow$ MN: BA

The authentication mechanism is optional and is part of the distributed authentication protocol. The use of mobile home agents can be used on their own, with authentication as seen here or it can be used with the full implementation of the distributed authentication protocol which utilizes dual identity return routability [6] and has support for mobile correspondent nodes which can also have their location privacy by implementing their own mobile correspondent home agent.

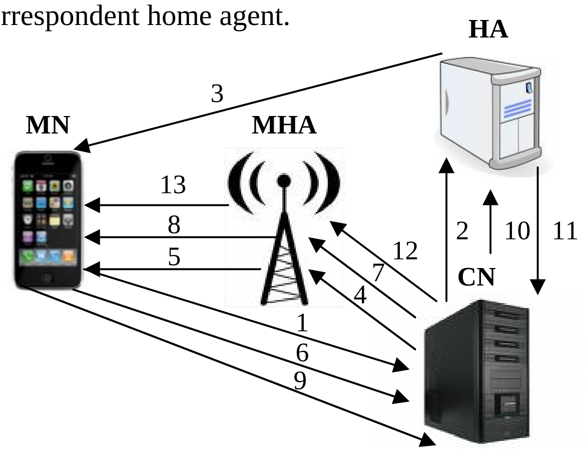

Fig 4. Mobile Home Agent message exchange in mobile to static communication.

All the messages exchanged within the mobile home agent mobile to static communication can be seen in fig 4.

4 Conclusion

This paper has shown that the Mobile IPv6 route optimization protocol is vulnerable to a variety of attacks which attempt to disrupt or hijack communication between the mobile and the correspondent nodes.

This paper investigated several security solutions which were specifically designed to protect location privacy. But the main drawback of these solutions was an increase in latency between communication of the mobile node and the correspondent.

A second technology, mobile agents, were investigated which could potentially change the way networks operate. These are autonomous software based programs which can migrate to another node on the network independently of any other process. They work well in heterogeneous networks and are capable of managing network messages.

This technology was the basis for the proposed security protocol using mobile home agents. Mobile home agents act in some ways as a proxy home agent which follows the mobile node as it moves from point of attachment to point of attachment. The mobile home agent resides on the point of attachment itself therefore even though technically the solution reintroduces triangle routing in some respect, in reality there is a negligible latency increase as the data packet would have to pass via the point of attachment anyway to reach the mobile node.

The mobile home agent preserves the mobile nodes location privacy by acting as a proxy and passing all messages to the mobile node via a secure tunnel.

When the mobile node migrates to a new point of attachment the mobile home agent duplicates itself and is transmitted to the new point of attachment when it continues to act as the proxy for the mobile node. The home agent keeps track of both of these entities to ensure they are reachable.

The advantage of the proposed solution is that it is entirely software based and no new hardware would be needed to be introduced. This makes it a very cheap option also. The location of the mobile node is protected without the cost of increased latency.

The only disadvantages rest with the fact that the mobile home agent is autonomous and so its behavior relies heavily on its robust programming and that every point of attachment may have to be modified to accept mobile agents.

References:

[1] Aneiba, A., Rees, J.S., Mobile Agent Technology and Mobility, *Proceeding of the 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, pp. 14-20, PGNet 2004, Liverpool, ISBN:1-9025-6010-8

[2] Tuomas Aura. Cryptographically Generated Addresses (CGA). *In Proc. 6th Information Security Conference (ISC'03)*, volume 2851 of LNCS, pages 29-43, Bristol, UK, October 2003. Springer.

[3] Cockayne, W.R and Zyda, M., (1998) *Mobile Agents*, Manning, Greenwich.

[4] A. Escudero, Location Privacy in IPv6: 'Tracking binding updates'. *Tutorial at Interactive Distributed Multimedia Systems (IDMS2001)*. Lancaster, UK. September 2001.

[5] A. Georgiades, et al."Binding Update Security for Mobile Ipv6 using the Distributed Authentication Protocol ". *WSEAS Transactions on Communications*, Issue 9, volume 4, September 2005, ISSN 1109-2742

[6] A. Georgiades, et al, “Distributed Authentication protocol Utilizing Dual Identity Return Routability for the Security of Binding Updates within Mobile IPv6”, *WSEAS Transactions on Communications* , Issue 10, Volume 5, October 2006, ISSN 1109-2742.

[7] Qi He et al, The quest for personal control over mobile location privacy, *IEEE communications magazine*, Vol. 4, No.2, May, 2004.

[8] D. Johnson et al, Mobility Support in IPv6, RFC 3775, June 2004.

[9] Lange, D.B. Oshima M. (1998) *Programming and deploying Java Mobile Agents with Aglets*, Addison-Wesley, Reading Massachussets.

[10] Lange, D.B. and Oshima M. (2000) ‘*Mobile Agents with Java: The Aglet API’ in mobility processes, Computers and Agents*, Milojicic D. et al, Addison-Wesley, Reading Massachussets.

[11] Greg O'Shea et al, Child-proof authentication for MIPv6 (CAM), *ACM Computer Communications Review*, 31(2), April 2001.

[12] Sangheon Pack et al, Adaptive Route Optimization in Hierarchical Mobile IPv6 Networks**,** *IEEE Transactions on Mobile Computing*, pp. 903-914, August 2007

[13] IPv6, *Wikipedia*, http://en.wikipedia.org/wiki/ IPv6, November 2008

[14] Jukka Ylitalo et al, "BLIND: A Complete Identity Protection Framework for End-points", to appear in *Security Protocols, Twelfth International Workshop*, Cambridge, 24-28 April, 2004.