Introducing Mobile Home Agents into the Distributed Authentication Protocol to Achieve Location Privacy in Mobile IPv6

Andrew Georgiades, Dr Yuan Luo, Dr Aboubaker Lasebae, Prof. Richard Comley

***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.

***Keywords*—**Mobile Home Agent, MIPv6, Distributed Authentication Protocol, 4G, Location Privacy.

I. Introduction

Mobile IPv6 is the next step in the evolution of networking. The most widely used internet protocols are ones currently based on IPv4 networks which are restricted to 32 bit addresses. This provides a finite number of IP addresses which, over time, has become 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 3.4×1038 addresses 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 [1].

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 [2].

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 [3] and the distributed authentication protocol [4]. 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.

Manuscript received February, 2009: This work is sponsored by Middlesex University, London, England and is part of the research undertaken by the PhD candidate Andrew Georgiades which goes towards achieving his doctorate.

Andrew Georgiades, PhD candidate, Middlesex University, and Production Innovation Coordinator, BBC, Television Centre, London, England. He works for the Innovation department of the British Broadcasting Corporation, Providing support to and introducing new and innovative technologies into the BBC's top Entertainment, Comedy and Event productions. (Andrew_georgiades@yahoo.co.uk).

Dr Yuan Luo, Senior Lecturer and Program leader of BEng Computer Communications and Networks, Middlesex University, London, England. (y.luo@mdx.ac.uk)

Dr Abubaker Lasebae, Principle Lecturer and Director of post graduate programs (Computer Communications), Program leader MSc Computer and Network Security, Middlesex University, London, England. (a.lasebae@mdx.ac.uk)

Professor Richard Comley, Associate Dean – Research, Professor of Computer Communications, Middlesex University, London, England. (r.comley@mdx.ac.uk)

II. Problem Definition

Before a security solution can be designed for a future telecommunication network, it is wise and vital to take a look at the emerging technologies and economical factors, which may impact the very core of the telecommunications industry, as we know it. This paper will present some predictions of which technologies will be incorporated into the Forth Generation of mobile telecommunications, technologies, which may have such a fundamental impact, that it will create a paradigm shift in the way the service is run. Only then can the network architecture be understood and a security solution crafted to adequately take advantage of its environment. This paper attempts to find a solution to prevent binding updates in Mobile Ipv6 from being susceptible to masquerading, impersonation attacks and provide location privacy to the mobile and correspondent nodes.

Mobile IP has primarily been designed for the ease of mobility of communicating devices. It is the underlining architecture for the fourth generation of mobile phones. Due to the nature of TCP/IP, only static IP addresses are permitted to be used within the network. This causes problems for mobile nodes, which wish to migrate to a new location yet still remain connected to the network. This is because physically moving to another location results in a new attachment to a wireless network node and as a result the IP address would change. Mobile IP solves this issue by employing two addresses [5].

The First address belongs to the home agent, which acts as a proxy for the mobile node and ensures the mobile node remains reachable by having a static address.

The mobile node itself has a dynamic address and this changes every time the node is associated with another point of attachment. Each time the mobile node migrates to a new location, it is assigned a new IP address and the home agent is informed of that new address. A node wishing to contact the mobile node must contact the home agent, which will tunnel the data packets to the current address of the mobile node. Correspondent nodes communicate by sending packets to the mobile nodes static address, which are then forwarded to the mobile node. This is called triangle routing and can have an impact on communication latency. To avoid latency issues binding updates were introduced to allow the mobile node to communicate directly with the correspondent node by bypassing the home agent, with the use of a binding update. This keeps the home agent and the correspondent node aware of the mobile nodes' current location and allows for direct communication. Binding updates however are susceptible to security attacks such as interception and impersonation. This can be used by an attacker to mount man in the middle, redirection and denial of service attacks [6]. The distributed authentication protocol [4] has been designed to prevent or at least limit this attack from taking place. However, no matter the security in place within the network infrastructure, if the address of the mobile node is known, it is easily susceptible to direct attacks such as D.o.S from malicious sources. Can looking at current and future technologies and solutions, which may be implemented and incorporated into 4G technology, allow for improvements in the security design?

III. Emerging Technology

Second generation telecommunications, utilise the circuit switched GSM network to provide a dedicated line for the duration of the call. With the intermediate generational leap to 2.5G, bandwidth speeds have not necessarily increased but support for packet switching of data has been implemented with the use of GPRS. The Third generation systems have been initially designed to provide both circuit switched and packet switched domains for voice and data respectively. However an alternate access network, from 2G systems, needs to be used such as UMTS or CDMA 2000 [7].

Unlike 3G, Fourth Generation systems are based on packet switching only. The method of transmission of voice calls is done with the use of Voice over IP, (VoIP) [8]. This splits voice into data packets, which are sent across the Internet, which are reassembled at the destination address. The advantage is that there is no dedicated line created for the call as packets can take any path they choose, however during some network conditions voice calls can suffer a loss of quality.

4G Mobile devices will use Mobile Ipv6 addresses to identify themselves. This of course does not mean telephone numbers will become obsolete as then can be resolved in the same way a web page address is found in a look up table giving its IP address. This does mean however that mobile phones will operate in a similar way to the infrastructure of broadband Internet in the home. This could possible mean that telecommunication companies in effect become Internet service providers, and as such, instead of paying for a telephone subscription we may have an ISP subscription instead [9].

Even if companies try to keep the lucrative business models, which they currently enjoy, consumers may find cheaper alternatives such as the Skype service [10], [11] which provides free PC-to-PC calls. As time moves on its highly likely that mobile devices will become comparable in processing power of a PDA or even a low end computer. This means that applications such as Skype will find its way to mobile devices and telecom (ISP) companies will find themselves losing revenue.

ISPs will change their business plan to a more service orientated market and try to generate revenue from killer applications such as premium content music, videos and live streaming television IPTV.

Payments for these services would of course need to be secure, combining a range of technologies such as encryption and authentication to prevent sensitive payment details from falling into the wrong hands. Of course if an attacker is unaware of the location of a potential victim this makes it very difficult for an attack to take place. This is where location privacy comes in and this paper introduces a way of achieving this through the use of mobile agents which are autonomous software agents. These will prevent interception of data within the network however an attacker can still intercept data between the signal sent from the mobile device and the point of attachment.

As 4G devices will operate at much high bandwidth speeds modern GSM and 3G radio frequencies would not be able to cope with the demand put on it so it is most likely that 4G will operate on high speed frequencies most likely based on WI-FI. Of course the drawback then is that WI-FI has a limited range in comparison to GSM. The most likely method of wireless transmission is WiMAX, which can cover a large metropolitan area [12]. However it is more likely that this will be used as a backbone for last mile delivery of high-speed broadband to the home. Fortunately it is interoperable with other wireless standards allowing for WI-FI enabled phones/nodes to communicate with each other by interconnecting them.

The WiMax standard utilises a scheduling MAC, which allocates a time slot to the base station as opposed to Wi-Fi's contention access where all nodes are competing for the base stations attention randomly. This makes WiMax more stable for the purpose of mobile communications. WiMAX also has the potential for mesh networking allowing users to connect to each other by bypassing the infrastructure or allowing nodes to become part of the infrastructure that would otherwise be out of range.

IV. Current Solutions

Mobile IPv6 Binding updates are vulnerable to attacks such as interception and impersonation. Numerous security solutions have been proposed to protect mobile IPv6 networks and each has their advantages and disadvantages. The two main types of security are encryption and authentication. Encryption protects the confidentiality of the data and authentication allows users to verify that they are communicating with validated participants. Different authentication systems exist, such as Kerberos [13] that perform authentication by referring to a central authentication database to compare users credentials.

Other security components include hashes [14], digital signatures [15], address based keys [16] and cryptographically generated addresses [17].

More elaborate systems such as IPSEC [18] and RADIUS [19] based on AAA Authentication, authorization and accounting [20], require the utilization of a central authentication authority. These techniques may not be practical for a mobile environment, and could effectively reduce the users quality of service.

Security protocols, which have been specifically designed for the protection of binding updates such as, Bake/2 [21] and CAM [3] are good but have flaws. The Trinity protocol [22] introduced a third node to aid in authentication but the addition of new hardware proved to be impractical. However, the two main techniques, which have practically become standardised for binding update security, are: Cryptographically generated addresses and return routability.

A. CGA

Cryptographically generated addresses [17] are IPv6 addresses, which are generated by hashing the owner's public key. The address owner uses the corresponding private key to assert address ownership and to sign messages from that address without PKI or some other security infrastructure. 62 bits of the interface identifier can be used to store a cryptographic hash of the public key.

$$\text{Host ID} = \text{HASH62}(\text{public key}) \quad (1)$$

The CGA binds a users 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 [23]. A major problem, which should be understood is that, an attacker can always create its own CGA address but will not be able to spoof someone else's address since the message needs to be signed with the corresponding private key, which is only known only by the legitimate owner.

The aim of CGA is to prevent stealing and spoofing of existing IPv6 addresses. 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 [23]. As a result, CGA needs to be used together with a reachability test such as return routability, where redirection denial-of-service attacks are a concern.

B. Return routability

Return routability tests whether packets addressed to the two claimed addresses are routed to the mobile node. The Return Routability Procedure gives the correspondent node some reasonable assurance that the mobile node is addressable at its claimed care-of address and its home address. Only with this assurance is the correspondent node able to accept Binding Updates from the mobile node [2]. The return routability test is the most effective way to limit bombing attacks of the mobile's new address. The correspondent only accepts the binding update if the mobile is able to return the hash of a secret value sent in a packet to the new location. This proves that the mobile can receive packets at the address where it claims to be [5].

Some malicious entities on the correspondent's local network may be able to capture a test packet but the number of potential attackers is dramatically reduced. The return routability test is complementary to CGA-based BU authentication, which does not prevent bombing of the home network [5].

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:

C. 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 [24].

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.

D. Authorised Anonymous ID

To address the issue of location privacy, [25] 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 [25] that a distributed architecture would be more appropriate as a centralized architecture has drawbacks.

E. Temporal Mobile Identifier (TMI)

Various ways are suggested in [26] 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.

F. Hierarchical Mobile IPv6

The hierarchical mobile IP management model [26] 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) [27]. 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.

V. 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 [28].

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

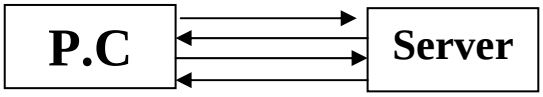

Fig. 1 Client Server Model

They perform a continuous dialogue until the task is complete. Mobile agents work in a different way [29]. 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).

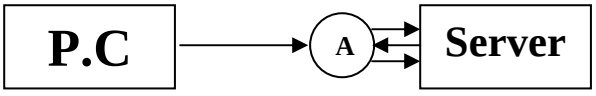

Fig. 2 Agent communication with server

The benefit of this is that it reduces the network load and frees up bandwidth, it also allows for faster communication [30].

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.

VI. 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.

A. 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.

A new component in a Mipv6 architecture may introduce new security threats but work has already been done to protect the security of mobile agents themselves limiting the risk of their utilization [31].

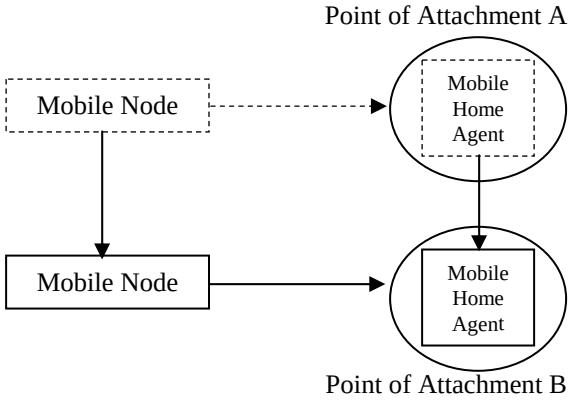

Fig 3. Mobile node and mobile home agent migrating to a new point of attachment.

B. 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 [17]:

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

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+.
All the messages exchanged can be seen in fig 4.

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 Kcn only known to the correspondent. A nonce index is also included to allow the CN to find the appropriate nonce easily.

$$\text{Home token} = \text{hash}(K_{cn} \mid \text{source address} \mid \text{nonce} \mid 0)$$

This is then sent to the home agent.

$$\text{CN} \longrightarrow \text{HA: HoT.}$$

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.

$$\text{HA} \longrightarrow \text{MN: HoT.}$$

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.

$$\text{Care-of token} = \text{hash}(K_{cn} \mid \text{source address} \mid \text{nonce} \mid 1)$$

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.

$$\text{CN} \longrightarrow \text{MHA: CoT.}$$

Message 5.
The mobile home agent tunnels the care of test to the mobile node.

$$\text{MHA} \longrightarrow \text{MN: CoT.}$$

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

$$K_{bm} = \text{hash}(\text{home token} \mid \text{care-of token})$$

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 Kbm.

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

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).

$$\text{CN} \longrightarrow \text{MHA: RAD}$$

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

$$\text{MHA} \longrightarrow \text{MN: RAD}$$

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 Kbm.

$$\text{MN} \longrightarrow \text{CN: } K_{bm}$$
(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.

$$\text{CN} \longrightarrow \text{HA: RAD}$$

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.

$$\text{HA} \longrightarrow \text{CN: Hash}$$
(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 ⟶ 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 ⟶ 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 [9] and has support for mobile correspondent nodes which can also have their location privacy by implementing their own mobile correspondent home agent.

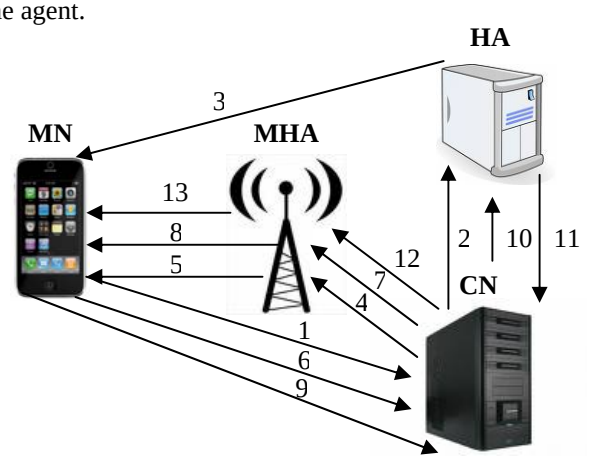

Fig 4. Mobile Home Agent message exchange in mobile to static communication.

C. Mobile Home Agent used in a Mobile to Mobile Node Communication.

In this scenario we will assume that the correspondent node is mobile and so requires a mobile home agent.

Message 1.
The mobile node MN attempts to contact the correspondent node CN. The correspondent node however is not directly contactable because it is mobile and it too has a Mobile Home Agent. The Mobile node will have to contact the correspondent's traditional home agent first which will then forward the messages to the correspondent node. The mobile node's public key MNK+, care of address CoA and home address HoA are sent to the HA2 Home Agent of the CN the correspondent node. Message flows are shown in Fig.5. 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 3 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+.
All the messages exchanged can be seen in fig 5.

MN ⟶ HA2: MHAK+, MHA, HoA.

Message 2.
The Correspondent Node's Home Agent received the message from the Mobile Node and forwards it to the correspondent node.

HA2 ⟶ CN: MHAK+, MHA, HoA.

Message 3.
The correspondent 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 Kcn only known to the correspondent. A nonce index is also included to allow the CN to find the appropriate nonce easily.

$$\text{Home token} = \text{hash}(K_{cn} \mid \text{source address} \mid \text{nonce} \mid 0)$$

This is then sent to the home agent.

CN ⟶ HA: HoT.

Message 4.
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 5.
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.

$$\text{Care-of token} = \text{hash}(K_{cn} \mid \text{source address} \mid \text{nonce} \mid 1)$$

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 6.
The mobile home agent tunnels the care of test to the mobile node.

MHA ⟶ MN: CoT.

Message 7.
The mobile node receives both tokens from both the test packets sent. It then creates a binding key Kbm 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, via the correspondents home agent, which is protected with the binding key Kbm.

MN ⟶ HA2: K_{bm}(BU)

Message 8.
The Correspondents home agent forwards the binding update request to the correspondent node.

HA2 ⟶ CN: K_{bm}(BU)

Message 9.
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 ⟶ MHA: RAD

Message 10.
The mobile home agent tunnels the request for authentication data (RAD) to the mobile node.

MHA ⟶ MN: RAD

Message 11.
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 is sent to the CN, via HA2, encrypted with the binding key Kbm.

MN ⟶ HA2: K_{bm}
(MHA, Sim No, IMEI, Phone No., Biometric)

Message 12.
The correspondent's mobile home agent, HA2, forwards the encrypted authentication data to the correspondent.

HA2 ⟶ CN: K_{bm}
(MHA, Sim No, IMEI, Phone No., Biometric)

Message 13.
Simultaneously to message 9, the correspondent sends a request for authentication data message to the home agent.

CN ⟶ HA: RAD

Message 14.
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 via it's home agent.

HA ⟶ HA2: Hash
(MHA, Sim No, IMEI, Phone No., Biometric)

Message 15.
The correspondents home agent forwards the authentication data to the home agent.

HA2 ⟶ CN: Hash
(MHA, Sim No, IMEI, Phone No., Biometric)

Message 16.
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 via it's mobile home agent, which speeds up the communication and still maintains location privacy.

CN ⟶ MHA: BA

Message 17,
The mobile home agent passes the binding acknowledgement to the mobile node to let it know that the process has been successful.

MHA ⟶ 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 [9]. The above message exchange allows for mobile correspondent nodes to also have their location privacy

by implementing their own mobile correspondent home agents which communicate directly with the mobile nodes mobile home agent, acting as a secure proxy with negligible communication latency.

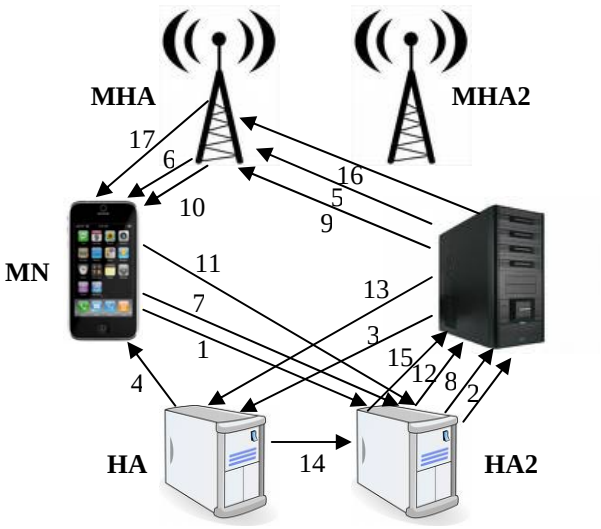

Fig 5. Mobile Home Agent message exchange in mobile to mobile communication.

Once the protocol has completed authentication of the mobile and correspondent nodes and the binding update has been exchanged, then direct route optimized communication can take place between the communicating nodes via the Mobile Home Agents on the points of attachment shown in Fig 6. This provides low latency communication with the benefit of a non processor intensive location privacy security solution due to the mobile agent software not running on the mobile device itself but running on the points of attachment.

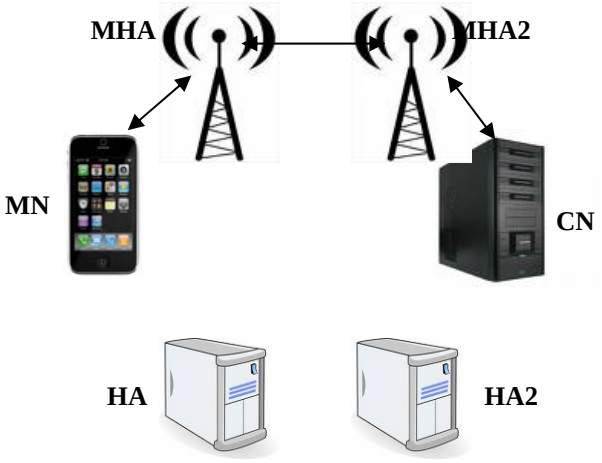

Fig. 6, Communication between mobile to mobile nodes via mobile home agents on points of attachment

VII. 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 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, making it a very cost effective option. 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.

The proposed solution will be tested with the network simulation software Opnet. The results will be gathered and compared to other security solutions in terms of effectiveness and impact on latency and resources. It is believed that this proposal will provide a robust and unique security solution.

References:

[1] Mohammad Ali Badamchizadeh, Ali Akbari Chianeh, Security in IPv6, Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 27-29, 2006 (pp249-254)

[2] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, RFC 3775, http://www.faqs.org/rfcs/rfc3775.html, June 2004

[3] Greg O'Shea and Michael Roe, Child-proof authentication for MIPv6 (CAM), ACM Computer Communications Review, 31(2), April 2001.

[4] A. Georgiades, Y. Luo, A. Lasebae, R. Comley.

"Binding Update Security for Mobile Ipv6 using the Distributed Authentication Protocol ". WSEAS Transactions on Communications, Issue 9, volume 4, September 2005, ISSN 1109-2742
[5] Tuomas Aura, Michael Roe, and Jari Arkko. Security of internet location management. In Proc. 18th Annual Computer Security Applications Conference, pages 78-87, Las Vegas, NV USA, December 2002. IEEE Press.
[6] Pekka Nikander, Tuomas Aura, Jari Arkko and Gabriel Montenegro, "Mobile IP version 6 (MIPv6) Route Optimization Security Design, In Proc. IEEE Vehicular Technology Conference Fall 2003, Orlando, FL USA, October 2003. IEEE Press.
[7] Alan Clapton, *Future mobile networks: 3G and beyond*, BT Exact technologies, IEE, 2001.
[8] T. J. Kostas, M. S. Borella, I. Sidhu, G. M. Schuster, J. Grabiec, and J. Mahler. Real-time voice over packet switched networks. IEEE Network, 12(1):18--27, Jan/Feb 1998.
[9] A. Georgiades, Y. Luo, A. Lasebae, R. Comley. "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.
[10] S. Baset and H. Schulzrinne. *An analysis of the skype peer-to-peer internet telephony protocol*, Computer Science Department, Columbia University, New York, NY, Sep 2004.
[11] Skype: The whole world can talk for free http://www.skype.com
[12] Michael Richardson, Patrick Ryan, *WiMAX: Opportunity or Hype?,* Advances in Telecom: Proceedings of the Fourth Annual ITERA Conference, ITERA 2006
[13] J. Kohl and C. Neuman, The Kerberos Network Authentication Service, RFC 1510, http://www.faqs.org/rfcs/rfc1510.html, September 1993
[14] J. Arkko, P. Nikander, and G. Montenegro. Selection of MIPv6 Security Level Using a Hashed Address Internet Draft draft-arkko-mIPv6-select-hash-00.txt. Work In Progress, IETF, June 2002.
[15] A.S Tanenbaum and M.V Steen, Distributed systems – Principle and paradigms, prentice hall, new jersey, 2002.
[16] James Kempf, Craig Gentry, "Securing IPv6 Neighbor Discovery Using Address Based Keys (ABKs)." (IETF, May 6, 2003)
[17] 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.
[18] J. Arkko, V. Devarapalli, F. Dupont. Using IPSec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. RFC 3776, IETF, June 2004.
[19] C. Rigney, S. Willens, A. Rubens, W. Simpson. Remote Authentication Dial In User Service (RADIUS, http://www.faqs.org/rfcs/rfc2865.html, RFC 2865, June 2000.
[20] J. Arkko, P. Calhoun, E. Guttman, D. Nelson, and B. Wolff. AAA Solutions. Internet Draft draft-ietf-aaa-solutions-01.txt. Work In Progress, IETF, November, 2000.
[21] M. Roe, G. O'Shea, T. Aura, J. Arkko. Authentication of Mobile IPv6 Binding Updates and Acknowledgments, Internet Draft draft-roe-mobileip-updateauth-02.txt. IETF, February 2002.
[22] A.Georgiades, Y. Luo, A. Lasebae, R. Comley. Trinity Protocol for the authentication of binding updates in mobile IPv6, WSEAS Transactions on communications, Issue 3, Volume 3, July 2004.
[23] W. Haddad, L. Madour, J. Arkko, F. Dupont. Applying Cryptographically Generated Addresses to Optimize MIPv6, http://www.ietf.org/internet-drafts/draft-haddad-mip6-cga-omipv6-03.txt, October 2004
[24] J. Ylitalo and Pekka Nikander. "BLIND: A Complete Identity Protection Framework for End-points", to appear in Security Protocols, Twelfth International Workshop, Cambridge, 2004.
[25] Qi He, Dapeng Wu, Pradeep Khosla. The quest for personal control over mobile location privacy, IEEE communications magazine, Vol. 4, No.2, May, 2004.
[26] A. Escudero, Location Privacy in IPv6: 'Tracking binding updates'. Tutorial at Interactive Distributed Multimedia Systems (IDMS2001). Lancaster, UK. September 2001.
[27] Sangheon Pack; Xuemin Shen; Mark, J.W. Adaptive Route Optimization in Hierarchical Mobile IPv6 Networks, IEEE Transactions on Mobile Computing, pp. 903-914, August 2007
[28] Aneiba, A., Rees, J.S., Mobile Agent Technology and Mobility, 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, PGNet 2004, Liverpool.
[29] William R. Cockayne and Michael Zyda. Mobile Agents, Manning, Greenwich (1998).
[30] Danny Lange, Mitsuru Oshima. 'Mobile Agents with Java: The Aglet API' in mobility processes, Computers and Agents, Addison-Wesley, Reading Massachussets (2000).
[31] Magdy Saeb, Meer Hamza, Ashraf Soliman. Protecting Mobile Agents against Malicious Host Attacks Using Threat Diagnostic AND/OR Tree, 5th WSEAS International Conference on Signal Processing, Istanbul, 2006

Abbreviations and Acronyms

MN	Mobile node
CN	Correspondent node
HA	Home agent
HA2	Correspondents' Home agent
H(m)	A hash of message m
K^+	Public Key
K-	Private Key
MNK^+	Mobile nodes' public key
MHAK+	Mobile Home Agent Public Key
HoA	Home Agent Address
CoA	Care of Address
HoT	Home Keygen Token
CoT	Care of Keygen Token
Kbm	Binding Key
BU	Binding Update
BA	Binding Acknowledgement
RAD	Request for Authentication Data