A Secure Approach for Global Home Agent Dynamic Discovery based on Peer-to-Peer

Rubén Cuevas[1], Angel Cuevas[1], Manuel Urueña[1], Carmen Guerrero[1], and Jose M. Gutiérrez[2]

[1] Department of Telematics Engineering, Universidad Carlos III de Madrid*
Av. Universidad, 30. Edif. Torres Quevedo. E-28911 (Leganés), Spain
{rcuevas,acuevas,muruenya,guerrero}@it.uc3m.es
[2] Department of Electronic and Electrical Systems. Aalborg University
Niels Jernes Vej 12, 9220 Aalborg Ø, Denmark
jgl@kom.aau.dk

Abstract. The Peer to Peer Home Agent Network is a novel overlay that allows to the Mobile Devices to discover a close HA among a set of them geographically distributed. The use of a close HA permits to reduce the delay in the communications between the Mobile Device and its Correspondent Nodes in Internet. This paper defines the main mechanism to make the Peer to Peer Home Agent Network secure. This mechanism is named Secure Join Procedure.

1 Introduction

Mobile IP [1] [2] and Network Mobility [3] [4] are the IETF proposals to obtain mobility. However, both of them have routing limitations, due to the presence of an entity (Home Agent) in the communication path. Those problems have been tried to be solved in different ways. A family of solutions tries to improve the routing by locating closer Home Agents making shorter the communication path. These techniques require a method to discover a close Home Agent from the Mobile Device. For this purpose the Peer to Peer Home Agent Network (P2PHAN) [5] was proposed. This is a novel overlay network that allows to the Mobile Device to discover a close Home Agent among those geographically distributed.

This paper focuses on the security of the P2PHAN. Security issues can be solved because of the specific features of this architecture, as verifiable data based on Border Gateway Protocol (BGP) information [6] and a reduced number of peers in comparison with the file sharing p2p networks. In addition, a mechanism that secures the communications between the Mobile Device -MD- and the Home Agent -HA- (i.e. to guarantee the trust between the HA and the MD) must be

* This work was supported by the European Commission through NoE CONTENT FP6-CONTENT-038423, the Spanish government through the Project IMPROVISA TSI2005-07384-C03-027 and the Madrid regional government through the Project BIOGRIDNET CAM-S-0505/TIC-0101.

used. This is IKEv2 [7] and its application to the mobile environment can be done as it is proposed in [8]. All this guarantees a practical high security level for the P2PHAN approach.

The paper describes the main mechanism to guarantee the security on the P2PHAN: *The Secure Join Procedure*. This is based on the use of a central bootstrapping server. The bootstrapping nodes are commonly used in commercial p2p networks since they are an efficient method for the peers to join the network and find other peers (e.g. Emule [9]). The Secure Join Procedure defines a secure Peer-ID assignment where the node receives a random Peer-ID from the network. This solves the main cause of possible attacks in the structured DHT p2p networks which is that peers can choose its own Peer-ID. Furthermore, the Secure Join Procedure performs other tests in order to check the good behaviour of the new HA.

2 The Secure Join Procedure

In order to define the *Secure Join Procedure* (SJP) in the proposed scenario the re-use of a Bootstrapping Server as security point is proposed. The main security function of this Bootstrapping Server is to assign a random identifier to the new HA which wants to become a member within the P2PHAN. However, this bootstrapping server cannot guarantee the Secure Join Procedure itself. Therefore, the next method will be applied in order to get a secure access to the P2P network.

First of all, if an organisation managing an AS wants to introduce HAs in the P2PHAN, it has to create a pair public key-private key (*AS_pu_key*, *AS_pr_key*). Therefore, if a HA wants to register itself within the P2PHAN, it must own the *AS_pr_key* to be able to register its information within the P2PHAN. The list of HAs of a given AS is stored by a peer within the P2PHAN (which is another HA). This node is called *Responsible HA*. When a HA tries to register its information, its *Responsible HA* will use the *AS_pu_key* as it will be described later to check that the new HA trying to join the P2PHAN knows the *AS_pr_key*. This implies that the new HA is an authorised node of that AS. The *Responsible HA* can obtain the *AS_pu_key* from a repository or it could be included in the registration message of the first HA of an AS which is registered within the P2PHAN. Following the SJP is described.

A new HA which wants to join the P2PHAN sends a *Join Request* to the Bootstrapping Server (See step 1 in fig. 1) with its IP address, the AS number and a checksum of all this information ciphered with the private key (*AS_pr_key*) of the AS where it is located, that is, its signature.

After that, the Bootstrapping Server generates a random Peer-ID for the new HA and launches a search in the p2p network to find the HA which has the most similar ID to the Peer-ID generated, which is the *Responsible HA* (See step 2 in fig. 1). Then, the bootstrapping server forwards the message received from the new HA adding the Peer-ID generated to the *Responsible HA* (See step 3 in fig. 1). The function of this *Responsible HA* is to make several tests in order to

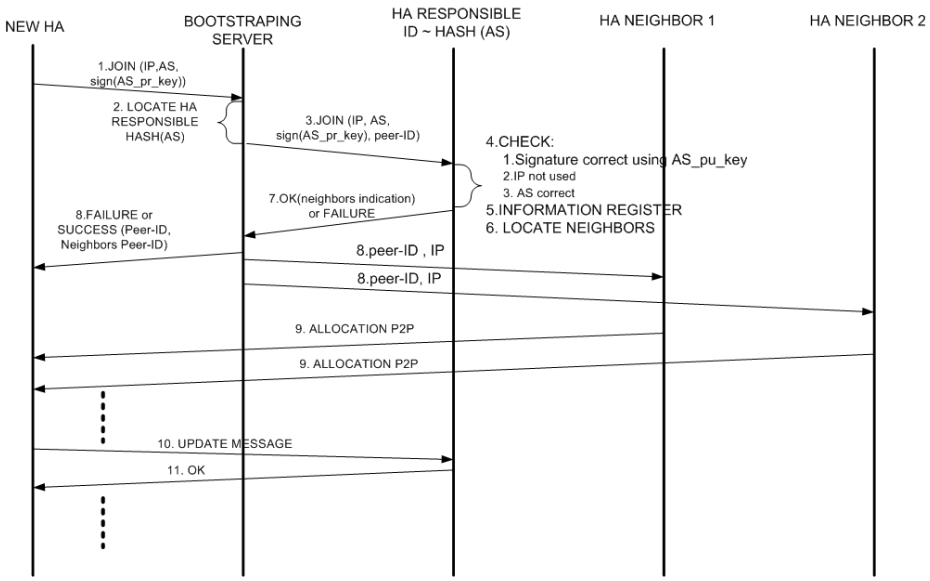

Fig. 1. Secure Join Procedure Message Exchange

check if the new HA is a malicious node. If one of these tests is not successful the *Responsible HA* returns a *Check Failure* to the Bootstrapping Server. Otherwise, the information of the new HA is stored by the *Responsible HA*. The following three tests are executed (See step 4 in fig. 1):

1. The *Responsible HA* uses the *AS_pu_key* which has stored in order to check if the checksum obtained is the same than the checksum ciphered with the *AS_pr_key* for the new HA. If it is not, it returns a *Check Failure*, otherwise it runs the second test.
2. The *Responsible HA* checks whether it has information stored for the IP which appears in the *Check Request* or not. If it has information stored for that IP, it returns a *Check Failure*, otherwise it runs the third test.
3. The *Responsible HA* checks if the IP within the *Check Request* belongs to the AS present in the request. In order to get this information the *Responsible HA* obtains the AS path for the IP address using BGP. Then, it checks if the AS number given in the *Check Request* matches with the last AS number returned in the AS path.

If any of these tests are not successful the *Responsible HA* returns a *Check Failure*. Otherwise, since all the tests were successful it registers the new HA information (See step 5 in fig. 1) and sends a query to the P2PHAN in order to find the neighbors for the new HA, i.e. the two nodes with the closest higher and the closest lower Peer-ID (See step 6 in fig. 1). After locating the neighbors, the *Responsible HA* sends to the Bootstrapping Server a *Check Success* adding

the neighbors IP addresses and Peer-IDs (See step 7 in fig. 1). Next, the Bootstrapping Server sends the neighbors Peer-IDs and the random Peer-ID to the new HA. In parallel the Bootstrapping server sends the Peer-ID and the IP of the new HA to the neighbors (See step 8 in fig. 1). When the neighbors receive the message from the Bootstrapping Server, they allocate the new HA using standard P2P techniques (See step 9 in fig. 1).

From this moment, the new HA will send periodically update messages in order to indicate that it is alive to the *Responsible HA*. If the *Responsible HA* does not receive these update messages during a pre-configured time out, it removes the entry for that HA (See steps 10 and 11 in fig.1). It must be noticed that a P2PHAN member has to sign the update messages sent to the *Responsible HA* with its *AS_pr_key*.

3 Conclusion

This paper has introduced the Secure Join Procedure. This is a mechanism which improves the security of the P2PHAN. However, the Secure Join Procedure is not enough to provide the whole security to the P2PHAN. Other mechanisms as redundancy and parallel queries must be considered. The description of the security threats of the P2PHAN and their solution based on the Secure Join Procedure and other techniques as redundancy and parallel queries are presented in [10]. Finally, it must be studied the application of the Secure Join Procedure to other scenarios where Overlay Networks are involved in.

References

1. C. Perkins: Mobility Support for IPv4. RFC 3344, August 2002.
2. D. Johnson, C. Perkins, J. Arkko: Mobility Support in IPv6. RFC 3775. June 2004.
3. V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert. Network Mobility (NEMO) Basic Support Protocol. RFC 3963, January 2005.
4. K. Leung, G. Dommety, V. Narayanan, A. Petrescu. IPv4 Network Mobility (NEMO) Basic Support Protocol. IETF Draft, June 2006.
5. R. Cuevas, C. Guerrero, A. Cuevas, M. Calderón, C.J. Bernardos: P2P Based Architecture for Global Home Agent Dynamic Discovery in IP Mobility. In Proceedings of the IEEE 65th Vehicular Technology Conference. April 2007.
6. Y. Rekhter, T. Li, S. Hares: A Border Gateway Protocol 4 (BGP-4). RFC 4271, January 2006.
7. C. Kaufman: Internet Key Exchange (IKEv2) Protocol. RFC 4306, December 2005.
8. V. Devarapalli, F. Dupont: Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture. IETF Draft. December 2006.
9. Emule: [Online]. Available: http://www.emule-project.net
10. A. Cuevas, R. Cuevas, M. Urueña, C Guerrero: A Novel Overlay Network for a Secure Global Home Agent Dynamic Discovery. 1st International Workshop on Peer to Peer Networks (PPN'07). November 2007. Accepted for publication.