Security Extensions to MMARP Through Cryptographically Generated Addresses

Francisco J. Galera, Pedro M. Ruiz,* Antonio F. Gomez-Skarmeta, Andreas Kassler

{fran, pedrom, skarmeta}@dif.um.es, andreas.kassler@kau.se

Abstract: The MMARP protocol provides multicast routing in hybrid environments in which an ad hoc network is connected to the Internet. As many other routing protocols it was initially designed without taking into account security concerns. In this paper we propose some extensions to protect the protocol against spoofing and forging attacks. Our solution, based on cryptographically generated addresses and digital signatures, has proven to be effective without the presence of a centralized certification authority.

1 Introduction

Routing protocols proposed for ad hoc networks are designed to deal with dynamically changing topologies, but they are not generally prepared to respond against malicious attacks. On the other hand, many of the mechanisms used in fixed network to provide secure routing are not suitable for ad hoc networks. The reason is that these mechanisms are based on centralized entities or they introduce a very high overhead for an ad hoc network. In their paper of securing ad hoc routing protocols[GA02], Guerrero and Asokan describe a solution for the unicast routing protocol AODV[PRD03] and depict a solution for other ad hoc routing protocols.

Typical security attributes are *availability, confidentiality, integrity, authentication* and *non-repudiation*. To achieve availability, routing protocols should be robust against both changing topologies and malicious attacks. While establishing routes, topology information does not need confidentiality and non repudiation protection. We will then focus our effort in providing availability, authentication and integrity. To achieve them, we use digital signatures and cryptographically generated addresses (CGA[Aur04]).

In this paper, we propose the security extensions for the multicast routing protocol MMARP [RGSG03], which is a multicast routing protocol for hybrid ad hoc networks connected to Internet. Nevertheless, this solution can be applied to any ad hoc routing protocol.

The remainder of the paper is organized as follows: section 2 presents the MMARP protocol and its security issues. Section 3 explains our solution to these problems and an example of its operation. Finally, section 4 gives some conclusions and future directions.

*Part of this work has been funded by the Spanish MCYT by means of the "Ramon y Cajal" workprogramme, the SAM (TIC2002-04531-C04-04) project and the DAIDALOS (IST-2002-506997) project.

2 The MMARP Protocol

2.1 Overview

The MMARP[RGSG03] protocol is designed for mobile ad hoc networks (MANETs). It is fully compatible with the standard IP Multicast model and it allows standard IPv6 nodes to take part in multicast communications without requiring any change. Key to this is that MMARP supports the MLD[DFH04] protocol as a means to interoperate both with access routers and standard IPv6 nodes. The interoperation with access routers is performed by Multicast Internet Gateways (MIGs) which are ad hoc nodes located just one hop away from access routers. Every MMARP node may become a MIG at any time. The MIG is responsible for notifying the access routers about the group memberships within the ad hoc fringe. This mechanism allows MMARP to interwork with any IPv6 multicast routing protocol in the access network.

MMARP uses a hybrid approach to build a distribution mesh. Routes among ad hoc nodes are established on-demand, whereas routes towards nodes in the fixed network are maintained proactively.

The reactive part consists of a request and reply phase. When an ad hoc node has new data to send, it periodically broadcasts a MMARP_SOURCE message which is flooded within the entire ad hoc network to update the state of intermediate nodes as well as the multicast routes. When one of these messages arrives at a receiver, or at a neighbor of a standard IPv6 receiver, it broadcasts a MMARP_JOIN message including the IP address of the selected previous hop towards the source. When an ad hoc node detects its IP address in a MMARP_JOIN message, it recognizes that it is in the path between a source and a destination. It then activates its MF_FLAG (Multicast Forwarder Flag) for the group and rebroadcast a MMARP_JOIN message back to the source.

The proactive part of the protocol is simply based on the periodic advertisement of the MIGs as default multicast gateways to the fixed network broadcasting a MMARP_DFL_GW message. The reception of an MLD Query can be used by ad hoc nodes to detect that they are MIGs. The process of creating the path towards the MIG is similar to the one decribed before. When the MIG receives the MMARP_JOIN message, it then sends an MLD Report which creates forwarding state in the multicast router towards the ad hoc network.

Once the mesh is established, data packets addressed to a certain multicast group are only propagated by ad hoc nodes which have their MF_FLAG active for that group.

2.2 MMARP security flaws

The MMARP protocol was initially designed without considering security. We analyse below which are the security flaws of the protocol:

1. Impersonalization of a node by forging MMARP_SOURCE or MMARP_JOIN messages. The problem worsens if the impersonated node is a MIG.

2. The payload of any MMARP message may be forged when forwarded. For example, decrementing the TTL field of the MMARP_SOURCE or MMARP_DFL_GW messages to increase the chances of being in the route path between the source and the destinations or to affect the election of the selected MIG for other nodes.

3. Selective dropping of certain MMARP or data messages. This attack is very hard to detect because it has the same result that the congestion at that node.

Hence, in this paper we focus in the first two problems. The solutions proposed are based in cryptographically generated addresses and digital signatures. Obviously, a node may generate any number of identities and change it at any time, but this behaviour would not compromise the route discovery process.

3 Security-enhanced MMARP

Two mechanisms are used to secure the MMARP operation: digital signatures to prevent the forging of messages, and cryptographically generated addresses to prevent address spoofing. Both solutions are based in asymmetric cryptography, so that each node needs a public/private key pair. Since in a MANET we can not assume that a node will be always reachable by all the other nodes, the use of Certification Authorities (CAs) is not feasible. In our solution no third parties are needed. Each node can generate its own key pair.

3.1 Digital signatures

Digital signatures are used to protect the integrity of both non-mutable and mutable fields of MMARP messages. In SAODV, hash chains are used to authenticate the hop count, which is the only mutable field, so that, digital signatures protect only the non-mutable fields. This approach is not suitable for MMARP because there are several mutable fields. In addition, hash chains only verify that the hop count has not been decremented by an attacker. However, the attack can consist on transmitting the message without incrementing the hop count or even incrementing it in more than one.

Each MMARP message extension has two digital signatures. The first one is calculated by the originator of the message and protects the integrity of the non-mutable fields. The other signature is computed by each node that forwards the message. Thus, when one message is generated, both signatures are calculated by the originator of the message, but when the message is forwarded by any node, it signs the mutable fields regenerating the correspondent signature in the message. Each signature is generated using the private key of the node, and the public key is included in the message to allow receivers verify that signature without the need of a centralized CA. But, this mechanism alone, can not avoid that an attacker could eventually sign messages containing somebody else's address and its own public/private key pair. Using cryptographically generated addresses we solve this problem binding public keys to nodes.

3.2 Generation of the IPv6 address

The approach we use for the generation of IPv6 addresses is based on CGA[Aur04]. This approach removes the security weakness of previous techniques. Cryptographically generated addresses (CGA) are IPv6 addresses where part of the address, usually the 64-bit interface identifier, is created from a hash of the public key of each node.

The process of generating a new CGA takes three inputs: the 64-bit subnet prefix, the public key of the address owner and a security parameter (Sec), which is a 3-bit unsigned integer that determine the level of security. CGA verification takes as input an IPv6 address (subnet prefix + interface identifier), the associated public key, the modifier and the collision count. The last two parameters are calculated during the process of generation.

This mechanism can work in an isolated ad hoc network, but it also fits well with the protocols capable of providing Internet connectivity for ad hoc networks. We have combined CGA with the Jelger's protocol[JNF04]. This protocol allows nodes in an ad-hoc network to discover a gateway/prefix pair which is used in order to build an IPv6 global address and, when necessary, to maintain a default route towards the Internet. Thus, ad hoc nodes build their IPv6 addresses using the prefix announced by Jelger's protocol and the interface identifier is generated using CGA. Figure 1 shows this process.

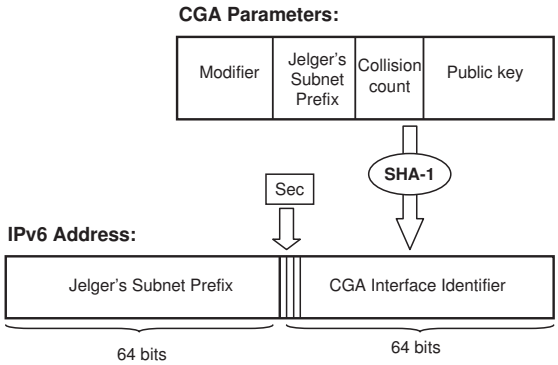
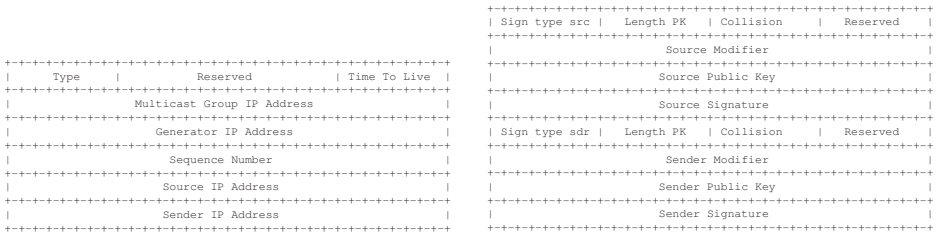


Figure 1: IPv6 address generation based on Jelger and CGA

Figure 2 shows the application of the proposed solution to one of the MMARP messages: the MMARP_SOURCE message. For the rest of MMARP messages a similar approach can be followed.

It is important to note that the signatures are calculated using the private key of the nodes, and the CGA is generated using the public key of the nodes. If an attacker wants to take a CGA created by someone else and send signed messages that appear to come from the owner of that address, it needs to know the private key of the owner of the address. Thus, the authentication of the node and the integrity of the messages are guaranteed.



(a) MMARP_Source message (b) MMARP_Source security extension

Figure 2: Security extension added to the MMARP_SOURCE message

4 Conclusions

We have described an approach to provide security enhancements to the MMARP protocol, but the same idea can be applied to other ad hoc protocols, either multicast or unicast. CGAs have shown to be very useful in MANETs because they do not rely on any public key infrastructure or third trusted party. However, in these environments, nodes tend to have limited capacities (CPU, battery, bandwidth) and the mechanisms proposed make extensive use of signatures, which are costly operations. The use of elliptic curve cryptography (ECC)[Kob87] could be very helpful in order to reduce the size of the keys and signatures.

References

[Aur04] Aura, T.: Cryptographically Generated Addresses (CGA). *IETF Internet-Draft: draft-ietf-send-cga-06, work in progress*. April 2004.

[DFH04] Deering, S., Fenner, W., and Haberman, B.: Multicast Listener Discovery (MLD) for IPv6. *IETF Request For Comments, RFC 2710*. October 1999.

[GA02] Guerrero, M. and Asokan, N.: Securing Ad hoc Routing Protocols. In: *Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002)* S. 1–10. September 2002.

[JNF04] Jelger, C., Noel, T., and Frey, A.: Gateway and address autoconfiguration for IPv6 adhoc networks. *IETF Internet-Draft: draft-jelger-manet-gateway-autoconf-v6-02*. April 2004.

[Kob87] Koblitz, N.: Elliptic Curve Cryptosystems. In: *Mathematics of Computation, 48*. S. 203–209. 1987.

[PRD03] Perkins, C.E., Royer, E.M. and Das, S.R.: Ad hoc On-demand Distance Vector (AODV) Routing. *IETF Request For Comments, RFC 3561*. July 2003.

[RGSG03] Ruiz, P.-M., Gomez-Skarmeta, A., and Groves, I.: The MMARP Protocol for Efficient Support of Standard IP Multicast Communications in Mobile Ad Hoc Access Networks. In: *Proceedings of the IST Mobile and Wireless Comms. Summit*. S. 75–81. June 2003.