"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2013
Brasov, 23-25 May 2013

SECURING ZRP – A HYBRID AD HOC ROUTING PROTOCOL

Ionut CONSTANTIN*, Mihai-Lica PURA*

*Faculty of Military Electronic and Information Systems, Military Technical Academy, Bucharest, Romania

Abstract: *Ad hoc networks are a very promising networking concept. Given the fact that they do not need any infrastructure in order to operate, they are suited for emergency scenarios, as well as in military applications and as backup connections. The operation of such networks is assured by the routing protocol. Ad hoc routing protocols are specially designed so that each of the network's nodes acts like a router and forwards packets for all the other nodes. There are three types of ad hoc routing protocols: proactive, reactive and hybrid. The choice for one of these types is made by considering the scenario in which the network will operate. We take into consideration the scenarios in which the network is very large and the communication characteristics are not the same all over it, but it can be clustered. The best type of ad hoc routing protocols in this case would be a hybrid one. From the security point of view, research had addressed proactive and reactive ad hoc routing protocols, but very little the hybrid ones. Our aim was to research how such a protocol can be secured. For this we have chosen a very popular hybrid routing protocol, namely ZRP. Starting from an ns2 implementation of this protocol, we have secured it using asymmetric cryptography. Our new implementation provides authentication, confidentiality and non-repudiation for all the messages exchanged through the protocol regarding routing information and data also.*

Keywords: *security, ns2, ad hoc networks, hybrid routing, ZRP*

1. INTRODUCTION

The society of the present day is based on information technology in such a degree that one can say that it cannot exist without it. But information technology, in order to accomplish what is expected from it, is dependent on communication. Ubiquitous computing (all the devices that now operate independently will work together to make our life easier and safer and more joyful) takes this dependency a step further. It also depends on a way to assure communication between these devices. Distributed transient network paradigm suits very well the paradigm of ubiquitous computing. A network that can operate without any infrastructure and that is still capable of assuring communication between a very large number of nodes is perfect for what ubiquity needs. Ad hoc networks are an implementation of this paradigm that manages to assure all its characteristics.

The operation of an ad hoc network is assured by the ad hoc routing protocol that is run by each of the nodes in the network. The protocol is responsible for finding the route data must travel on in order to reach destination, and to transmit it. Finding the routes in such a network can be done in a reactive or a proactive way. For large networks and for networks that can be clustered in such a way that much of the communication is done inside the cluster, but very little between clusters, a hybrid approach must be used.

Security is also an important aspect in communication. Authenticating the nodes that

communicate routing information and data, and also assuring confidentiality and non-repudiation of the transmitted data are mandatory for any communication system. In the case of reactive and proactive routing protocols, there are many proposed secure routing protocols. But in case of hybrid routing, there are not.

Our aim was to develop a secure hybrid routing protocol for ad hoc networks. We have started from a very popular hybrid routing protocol named ZRP and we had proposed to secure it making it possible to assure authentication, confidentiality and non-repudiation. We made the implementation in Network Simulator 2 (ns2), starting from a classical non-secured ZRP implementation ([8]).

The rest of the paper is organized as follows: section 2 describes the concept of ad hoc networks and presents ad hoc routing protocols. In section 3 the ZRP hybrid routing protocol is presented. Section 4 describes the way we have secured ZRP. Section 5 presents the implementation in ns2 of our secured version of ZRP. Section 6 contains some conclusions and future research directions.

2. AD HOC ROUTING

2.1 Ad hoc networks. The term “ad hoc“ refers to a way of connecting wireless devices that is characterized by the following traits. The formed network is temporary because the connections between the nodes are established only for the duration of a single session. These connections do not require a main station, but each of the nodes search in its discovery area for other devices witch which to form the network ([2]). The nodes can search for devices that are beyond their discovery area by using broadcast packets that are retransmitted by all the nodes they reach. All the connections are established by multiple nodes, thus such networks are called multi hop networks ([6]). After the connections are established, the routing protocol maintains them even if the nodes move. So the nodes can enter or leave the network arbitrary, which makes the topology of the network very dynamic ([2]). The nodes communicate directly only on very small distances, so the vast majority of the data paths use intermediate nodes that route the packets towards destination. In fact, all the nodes of such networks act as routers and are equivalent with each other, all performing the same task: they route packets for all the other nodes. Such networks are highly heterogeneous, the devices that formed them being very different from the point of view of the storage, computational, communication and energy capabilities.

The advantage of such network is the fact that they do not need any infrastructure in order to operate. Rather the nodes are themselves an infrastructure of routers that assure the routing of the packets through the special routing protocols they use, named ad hoc routing protocols.

2.2 Ad hoc routing protocols. Because of the special characteristics of the ad hoc networks, classical routing protocols cannot be used ([1]). So special ad hoc routing protocols were designed that can auto-start and auto-organize them in order to offer the requested multi hop paths to the destinations. Also these protocols are scalable for very large networks and can dynamically maintain the topology of the network. And above all these, the overhead of the data transmission is very low and the memory and band wide resources consumed are fewer than in a classic routing protocol ([12]).

Based on these requests, three categories of ad hoc routing protocols were designed: proactive, reactive and hybrid. The proactive protocols establish the data paths towards all the other nodes in the network prior to any data communication. They are suited for small size ad hoc networks in which the nodes communicate with the majority of the other nodes and in which the overhead of data transmission must be very low. The best known proactive protocol is OLSR ([10]).

Reactive routing protocols are characterized by the fact that they search for that the data path for a node only when it is needed. They are suited especially for large ad hoc networks in which a node communicates only with a small number of the other nodes and in which the small delay of computing the path prior to the actual transmission is

unimportant. The best known reactive protocols are TORA ([3]), DSR ([11]) and AODV ([9]).

Hybrid ad hoc routing protocols combine the reactive technique with the proactive one in order to take full benefit of the advantages of each one of them, and also to minimize their disadvantages. The ad hoc network is split in sub networks called zones so that a hierarchical routing can be used: for communicating between the nodes inside the same zone the protocol uses a proactive approach, and for communicating between nodes from different zones it is used a reactive approach. This type of operation for hybrid routing makes it the best choice for large networks like the one that ubiquitous computing and military applications use. That is the reason for our focus on them. The best known hybrid protocols are ZRP ([4]), and CBRP ([5]).

3. ZONE ROUTING PROTOCOL

ZRP is, as we mentioned above, a hybrid ad hoc routing protocol. It splits the ad hoc network in which it operates in several routing zones and uses two different routing protocols ([4,7]): one inside each of the zones (IARP – Intrazone Routing Protocol), and the other between the zones (IERP – Interzone Routing Protocol). Also, it uses a third routing protocol (NDP – Neighbor Discovery Protocol) which is responsible for finding the neighbors for a node that belong to the same routing zone, and for finding and maintaining the topology of the routing zone to which a node belongs. We will further present each of these three routing protocols.

3.1 Neighbor Discovery Protocol. NDP is the part of ZRP responsible for finding the nodes from the same routing zone. A routing zone is defined based on the number of hopes between the nodes. If this number is bigger that a given value, then the nodes belong to different zones. Otherwise, they belong to the same zone.

NDP operates by broadcasting "Hello" beacon messages at regular time intervals. When receiving such a message, each node updates its routing table either by adding a new neighbor, if the "Hello" message is received for the first time from a certain node, either by updating the current information about that node. If after a certain period of time no "Hello" messages are received from a node, it is deleted from the routing table.

3.2 Intrazone Routing Protocol. IARP is a proactive routing protocol and operates only inside a zone. Each of the nodes maintains a routing table for its routing zone in which it has a priori stored the routes to all the nodes from the same zone.

3.3 Interzone Routing Protocol. IERP is the reactive component of ZRP and it is used when a nodes needs to communicate with another node that belongs to a different routing zone. By using bordercasting, the nodes from the border of each zone initiate an IERP path finding when they conclude that the destination node is outside of their zone.

For more details about the routing process using the three components of ZRP, please see [7].

4. SECURING ZRP

In order to create a secure implementation of ZRP, we proposed to provide the following security goals: authentication, confidentiality and non-repudiation for all the routing process - regarding the type of messages exchanged by

each component. And for this we have implemented a PKI.

The three components of the ZRP require sending some packets that contain routing information. Our implementation of secure ZRP supposes securing each component by signing the routing information for each packet sent between the nodes ([8]).

The secured routing process can be detailed as follows. Each time a new node is accepted as trusted and is granted access to the secured network, it is assigned a pair of public RSA keys. The public key is later integrated in a security certificate which is sent to the CA in order to be signed by the authority. When a node has to send a packet that contains routing information, it will sign the routing information from that packet using its own private key and it will attach the certificate to the signed message. The recipient node first validates the sender's certificate using the CA's public key and then it validates the signature of the routing information using the public key of the sender from the validated certificate. Judging the result of these validations, the recipient decides whether to act according to the routing information or not.

Given the fact that ZRP contains three different routing components (NDP, IARP and IERP), each having its own type of packets and routing technique, each of these routing components had to be secured as an individual routing protocol.

5. SECURE ZRP IMPLEMENTATION

Implementing our secure version of ZRP required the installation of the ns2 network simulator. The second step consisted of downloading the actual ZRP implementation from the Internet ([8]). After successfully simulating a routing process over an arbitrary ad hoc network using the traditional ZRP, we had to integrate the simulator with the chosen cryptographic library, namely openssl.

With the simulation environment fully configured, we started to modify the traditional implementation by altering the zrp.h and zrp.cc files that describe the routing procedure. We created the CA and Cert classes for the implementation of the CA and the used certificates, and then we altered the ZRPAgent class and hdr_zrp data structure in order to include all of the objects involved in the digital signature algorithm. Given the fact that each node receives a pair of keys and a certificate, the ZRPAgent class had to be altered accordingly, by adding the proper fields and methods to it.

In order to attach to the packets the digital signature for the routing information exchanged by the nodes, the hdr_zrp data structure also had to be completed with the proper fields.

The Cert class implements the security certificate used in our implementation in order to grant the connection between a node's public key and its identity.

The CA class represents our implementation of the Certification Authority. The main responsibility of this central authority is to store and sign the security certificate of every node so that when a node receives a signed message, it can first validate the certificate's authenticity.

For the signing and the validation processes, we decided to use the RSA algorithm. We used the C++ implementation of the methods from the openssl cryptographic library.

For the signature process, each time a new node is created, it receives a private and a public key, both encoded using the DER format so that the private key of the node can be stored and used properly when the node has to sign the routing information.

On the other side, the validation of the signature implies the following operations: first, the security certificate has to be extracted from the message. After the certificate is extracted, two validations have to be made: whether the certificate expiration date and time was not reached and whether the certificate is indeed signed by the CA. Judging upon these two validations, we can use the public key from the security certificate in order to check the signature of the routing information from the message.

Each of the three components of ZRP has its own type of packets. In order to completely secure our implementation of ZRP, we had to secure each of these types of routing packets by signing the routing information as follows.

For the NDP component, we had to secure the NDP BEACON and NDP BEACON ACK packet types by signing the source address, destination address and packet type. For the IARP component, the only packet type that contained routing information was the IARP UPDATE packet type. For this type of message, the source address, destination address, packet type and TTL were signed and validated in the corresponding methods. For the IERP component, we had three types of packets to secure: IERP REPLY, IERP REQUEST and IERP ROUTE ERROR. For each of these packets, the source address, destination address and packet type were signed and validated in the corresponding methods.

After recompiling the whole ns2 simulator with the new version of ZRP, we created a simulation scenario that would use all of the ZRP components in order to test that each type of message is correctly signed by the sender and that the signature is correctly validated.

6. CONCLUSIONS & ACKNOWLEDGMENT

In this paper we presented how we secured the ZRP hybrid ad hoc routing protocol in order to assure authentication, confidentiality and non-repudiation: authentication and non-repudiation for the routing information, and authentication, non-repudiation and confidentiality for data. We started from an ns2 implementation of ZRP and modified it by using a PKI-like infrastructure with a central CA and each of the nodes having a public-private key pair. Then the packet exchange between the nodes was modified by signing/encrypting the contents of the packets so that the security objectives are achieved. The manipulation of the packets at the moment of receive was also modified, by adding validations for the computed signatures.

ZRP is the most popular hybrid routing protocol and we expect that a secure version of it will have a high impact on research. We have proposed to make our secure implementation accessible on the Internet as soon as we complete our research. We are in the process of conducting quantitative measurements over our secured implementation and over the classical one. We want to establish what is the overhead added by our implementation and thus to compare it to the classical one. Our aim is to perform this evaluation both in a simulated environment (ns2), and in a real implementation.

REFERENCES

1. Abolhasan, M., Wysocki, T., *Highly Scalable Routing Strategies: DZTR Routing Protocol*, *Advanced Wired and Wireless Networks*, Springer (2005).
2. Bhaskar, R., *Cryptographic Protocols for Mobile Ad Hoc Networks*, PhD thesis, Doctoral School of L'Ecole Politechnique (2006).
3. TORA, online. Available: http://tools.ietf.org/html/draft-ietf-manet-tora-spec-00 (February 2013).
4. ZRP, online. Available: http://tools.ietf.org/html/draft-ietf-manet-zone-zrp-00 (February 2013).
5. CBRP, online. Available: http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01 (February 2013).
6. Gordon, R. L., *Trust Establishment in Mobile Ad Hoc Networks*, *Mobile Ad-Hoc Networks: Applications*, online. Available: http://www.intechopen.com/books/mobile-

ad-hoc-networks-applications/trust-establishment-in-mobile-ad-hoc-networks-key-management (February 2013).

7. Haas, Z. J., Pearlman, M. R., *The Performance of Query Control Schemes for the Zone Routing Protocol, IEEE/ACM Transactions on Networking*, vol. 9, issue 4 (2001).
8. Patel Brijesh, ZRP Agent for NS2, online. Available: http://magnet.daiict.ac.in/magnet_members/MTech/2007/PatelBrijesh/Thesis_files/MyZRP/ZRPManual.pdf
9. RFC 3561, online. Available: http://tools.ietf.org/html/9 (February 2013).
10. RFC 3626, online. Available: http://hipercom.inria.fr/olsr/ (February 2013).
11. RFC 4728, online. Available: http://www.ietf.org/rfc/rfc4728.txt (February 2013).
12. RTO Technical Report, *Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies*, online. Available: https://www.cso.nato.int/pubs/rdp.asp?RDP=RTO-TR-IST-035 (February 2013).