ARPAM Routing Protocol Vulnerabilities in Aeronautical Mobile Ad Hoc Networks

Michael Iordanakis, Georgios Dilintas

Technological Educational Institute of Piraeus, Computer Systems Engineering Department, Athens, Greece
{mdi, dili}@oslab.teipir.gr

ABSTRACT

The development of routing protocols has already reached a satisfying level in ensuring the communication channels among the mobile nodes. The need for increased security in ad hoc networks has recently emerged though. In the aeronautical environment, security plays a very important role due to the critical nature of the data exchanged between the aircraft. Adversaries may compromise network functionality by attacking the network layer; routing protocols can turn to Achilles' heel for the network viability and security. In this paper, we attempt to categorize and review the most important routing protocol vulnerabilities that affect the ARPAM routing protocol. We've chosen ARPAM because it is an innovative routing protocol specifically designed for the needs of aeronautical applications and therefore a suitable routing candidate for aeronautical mobile ad hoc networks (Aeronautical MANET).

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is an autonomous system that consists of a variety of mobile hosts forming a network without any fixed infrastructure. In a MANET, all the nodes collaborate to form their own collaborative infrastructure. All the nodes as well as the routers move freely and thus the network topology is highly dynamic.

Use of MANET has been proposed for future networks in avionics. Although not truly ad-hoc in nature, the proposed Aeronautical MANET may utilize existing infrastructure, while attempting to extend the connectivity of aircraft, especially in areas where current infrastructure is insufficient, like over the oceans.

2. THREATS

Due to the nature of wireless communication, communication channels are highly insecure. In addition to that, lack of fixed topology requires the routing protocols to be highly sophisticated. Providing security in such environments, where the presence of hostile nodes is to be anticipated, presents a great challenge for any routing protocol.

I. Denial of Service

A Denial of Service (DoS) attack, as its name implies, makes network resources unavailable. An attacker has several ways at his disposal in order to achieve a DoS attack; in its simplest form an attacker may flood the network with injected packets with the intent of depleting the resources of a network node. In a less passive approach, an attacker may choose to inject malformed routing packets into the network with the intent of causing a crash to any network node, or a network break-up resulting in node isolation. In case the attacker is already part of the network, he could also choose to drop routing packets in order to isolate a specific node or a set of nodes (a subnet perhaps). Alternatively, he may attempt to prevent route set up or he may simply delay routing packets in order to slow down route set up process or to modify routing table.

II. Eavesdropping

Eavesdropping is defined as the unauthorized interception of a data transmission; information itself remains intact but its privacy is compromised. Eavesdropping of routing packets is usually done under two different approaches: an attacker may eavesdrop header information of routing packets, such as the MAC and/or IP addresses of the communicating parties or he may eavesdrop routing packets in order to obtain access to the information contained in them, such as routing data or location data (geographical information).

III. Man-in-the-middle

An attacker may choose to actively invade a route in order to intercept communications between legitimate nodes of the network. There exist quite a few ways to achieve that. For instance, the attacker may choose to reorder routing packets in order to modify routing table appropriately. An attacker may also redirect routing packets, changing either the destination or source address of a packet or he may even replay routing packets in order to invade a specific route.

IV. Impersonation

Impersonation is an act whereby one entity assumes the identity and privileges of another entity without restrictions and without any indication visible to the recipients of the impersonator's calls that delegation has taken place. Therefore, an attacker may gain access to the network with the intention of impersonation. This may occur when the attacker impersonates another authorized user in order to access services for which it is

not authorized or the attacker may even choose to impersonate an entirely fictitious user in order to access reserved data. Besides fictitious user impersonation, the attacker may choose to impersonate a whole (sub)network, as this occurs in sybil attacks. Specifically, in a sybil attack, a malicious node can present multiple identities, thus can control a substantial fraction of the system, thereby undermining the redundancy employed by the network.

3. MESSAGE TAMPERING

Routing messages tampering may result in disruption of the routing process. It can also cause discrepancies between the nodes' routing tables or a complete breakdown at worst. Considering ARPAM, there are four different categories of routing message tampering, each for every different category of routing messages: route request, route reply, route reply acknowledgment and route error.

I . Route Request (RREQ)

When a source node needs a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in their routing tables.

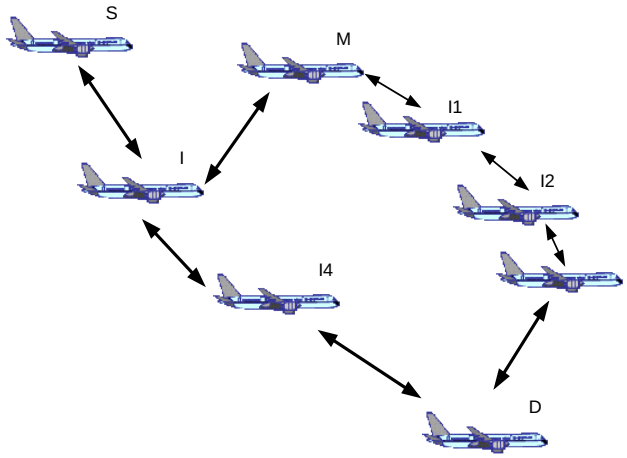

Fig 1. Reduction of hop count field

In addition to the source node's IP address, the RREQ message contains the lifespan of the message, the broadcast ID and the most recent sequence number for the destination of which the source node is aware, which serves as a unique ID. The attacker may choose to impersonate the intended source node so the message seems originating from someone else. Besides that the attacker may arbitrarily reduce the hop count field or increase the sequence number in order to increase the chances of being in the route path so the malicious node may more easily analyze the communication between them.

II. Route reply (RREP)

A route reply message is a node's reply back to the host that emitted the route request message. For example, we assume that node A, wishes to communicate to node Z, but does not know the route, therefore node A sends a RREQ to its neighbors. When node A's neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to node A, otherwise they will broadcast the RREQ they received to their set of neighbors.

The message keeps getting rebroadcast until its lifespan is up. If node A does not receive a reply in a predefined amount of time, it will broadcast the request again, but this time the RREQ message will have a longer lifespan and a new ID number. To ensure whether or not they will rebroadcast a RREQ message, all the involved nodes utilize the "sequence number" field found in the route request message itself.

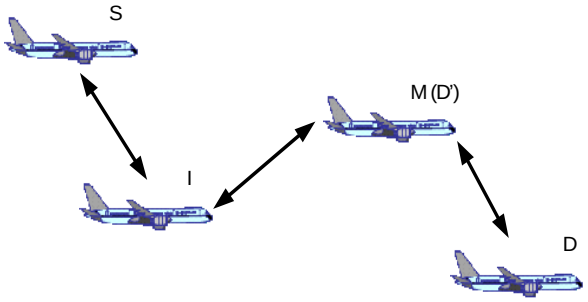

Fig 2. Source node impersonation

The attacker may choose to impersonate the intended destination node by forging a message with its address as a target address. Another trick is the reduction of the hop count field or the increase of the sequence number field, which make the other nodes believe that this is a fresher route. That leads to an increase of the chances that the malicious node is in the route path between the source and the destination nodes so the attacker may analyze the communication between them.

III. Route Reply Acknowledgment (RREP ACK)

The route reply acknowledgment (RREP-ACK) message is used in order to acknowledge the receipt of a route reply message over an unreliable link. The RREP-ACK message must be sent in response to a RREP message with the 'A' bit set. Typically, this is done when there is danger of unidirectional links preventing the completion of a routing discovery process. It is possible that the transmission of a RREP may fail, although this shouldn't be a usual phenomenon. If no other RREP reaches the node which originated the RREP message (a RREP generated from the same route discovery attempt), then a new route discovery process would be initiated after a predefined timeout by the originator. The whole sequence may be repeated again and again without any improvement, unless a corrective action is taken. This correction is achieved through RREP acknowledgement messages, which even though they are quite simple in nature, an attacker still has chances to misuse them in order to disrupt a route.

For example, we assume the existence of a unidirectional link from node S to node D. When node D sends a RREP message with "A flag" to node S, the latter cannot receive the RREP message due to the

unidirectional link, thus it will not send a RREP acknowledgment packet back to D. Normally, node D will realize that the link is broken, but if a malicious node overhears that RREP message from D, he may impersonate node S in order to send a route reply acknowledgement back to node D. If that happens, node D will fail to detect the unidirectional link between node S and itself, causing routing problems. When compared to the tampering attacks concerning RREQ and RREP messages, the misuse of RREP acknowledgment messages has a fairly limited impact and its importance security-wise is therefore considered minimal.

IV. Route Error (RERR)

Using the Route Error Messages (RERR), ARPAM can update routes when the nodes move around. Specifically, whenever a node receives a RERR packet, it looks at the routing table and removes all the routes that contain the invalid nodes.

The RERR message contains a sequence number field which is used in order to uniquely identify each particular message. Tampering RRER messages practically implies the modification of that sequence number field. Let's assume, for instance, a malicious node M which forges a RERR message pretending it is the node S and sends it to its neighbor D. The RERR message has a very high destination sequence number (HDSN) for one of the unreachable destinations (UD). This might cause node D to update the destination sequence number corresponding to UD with the value HDSN. Therefore, future route discoveries performed by node D to obtain a route to node UD will fail (because UD's destination sequence number will be much smaller than the one stored in node D's routing table.

Routing message	Tampering type
Route Request (RREQ)	Source node impersonation Reduction of hop count field Deceptive incrementing of sequence number
Route Reply (RREP)	Destination node impersonation Reduction of hop count field Increase of sequence number
Route Reply Acknowledgment (RREP-ACK)	Whole message forged for impersonation
Route Error (RERR)	Modification of sequence number field

Fig 3. Routing message tampering vulnerabilities

4. ROUTING OF MESSAGES

Another category of vulnerabilities is focused on the disruption of the routing process by ignoring and / or altering the routing rules. This primarily occurs by not forwarding routing messages – either at all or selectively – to the other nodes. On top of that, there are various schemes that attempt to trick the legitimate nodes into believing that a specific route is fresher, shorter and / or better than another, causing traffic to flow to that fraudulent link. Such a link is set up by malicious nodes with the purpose to disrupt the network, overhear and usually control the flow of information.

I. Selective forwarding

When it comes to selective forwarding, a malicious node can selectively drop only certain routing packets; something that may cause great discrepancies to the network as a whole. This behavior may not necessarily be malicious though: a faulty node may as well fail to follow the routing protocol rules and be unable to provide proper acknowledgment and replies. Even though nodes in aeronautical networks are expected to be highly error-proof, still malfunctions do occur sometimes. A node failure may cause a complete drop of packets; that is the node itself may be unable to forward packets on behalf of others, not with a malicious intend, but due to internal inability. A permanent failure would lead to loss of all packets, while an intermittent problem would cause only partial disability in packet forwarding, which in turn might cause an even greater "fuss" to the routing protocol while attempting to drop dead routes only to find them again in short time.

The behavior of selective packet forwarding is especially effective as an attack if combined with another attack that gathers much traffic via the faulty node, such as the sinkhole attack or acknowledgement spoofing. In a sinkhole attack, an adversary attempts to lure all traffic from a particular area through a malicious node, and it is achieved by spoofing high quality route advertisements. It has to be noted that if all packets are dropped, the attack is called a "black hole", and if partially dropped it is called a "gray hole".

II. RREQ Flooding

Flooding is the type of incident involving insertion of a large volume of data resulting in denial of service. For instance, when a node S wishes to communicate with another node D, but lacks the proper routing information, it broadcasts a RREQ packet. This is done in an incremental way, which is bounded by the Time-To-Live (TTL) value in the IP header, in order to reduce flooding overhead. If node S fails to receive any information then it increments the broadcast diameter by a predefined value and the process continues until a valid route is discovered.

A route request ID (RREQ_ID) and a sequence number (SN) is maintained by every node in order to avoid the replaying of the packets. The higher the sequence number the fresher is the information concerning the particular destination. An attacker may easily record the RREQ packet and circulate it to another area, though if that other area is already up-to-date, no problems occur as the offending packet is simply discarded. But if the information in that other area is not up-to-date it will cause extra unnecessary processing of packets which in excess of packets, can lead to a denial of service attack.

III. Wormhole Attack

Let's assume that a source node S wishes to communicate with another node D, but S does not have the route, so it broadcasts a RREQ packet to its neighboring nodes. This process continues until an intermediate node that has a fresh route to node D is found or node D itself is found. In order to prevent the

unnecessary processing of the same RREQ

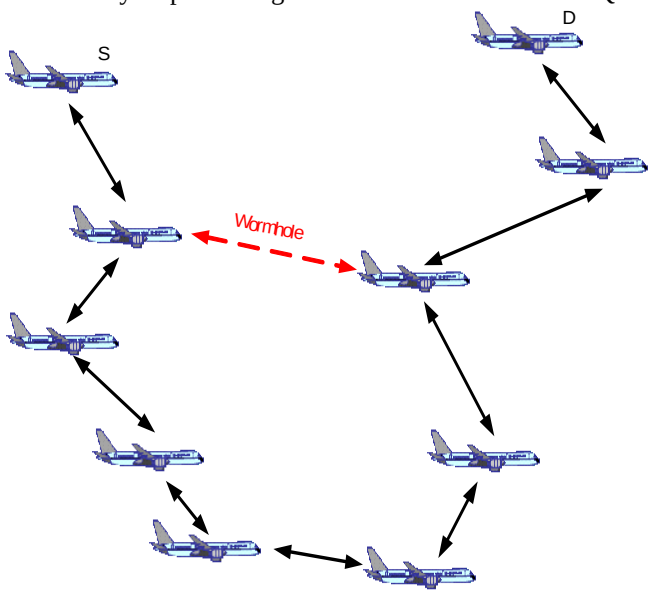

Fig 4. Wormhole attack scenario

packet from different neighbors, every node involved processes the RREQ message that arrives first, ignoring the packets it receives later. The second property is the fact that a direct link (in form of a tunnel) is faster than a general hop-by-hop propagation. The denial of service attack, usually involves two malicious nodes: one residing near the source node S while the other near the destination node D. When node S broadcasts a RREQ packet, the first malicious node records it and transmits it to the second malicious node directly through the tunnel. Any node that neighbors node D that receives the RREQ from the second malicious node processes it in a normal manner. In the meantime though, the original RREQ message is received by hop-by-hop propagation and is quickly discarded because the node believes that it is a copy and it has already received all information necessary. As a result, strategically placed nodes or an excess of malicious nodes may seriously hinder network performance and pose a serious security threat to the whole network.

IV. Byzantine attack

In a Byzantine attack, a compromised intermediate node (or a set of compromised intermediate nodes) works in collusion and carries out attacks such as creating routing loops, forwarding routing packets on non-optimal paths and selectively dropping packets. This type of attack may be considered as some sort of combination of the selective forwarding attack and the wormhole attack. Even though the importance of this attack is high considering the damage it can do to the network, it is quite hard to detect, as the network would seem to be operating normally in the viewpoint of the individual nodes, even though it may actually be exhibiting Byzantine behavior.

5. GEOGRAPHIC INFORMATION

ARPAM is unique compared to other MANET routing protocols due to its inherent support for aeronautical applications. ARPAM packets encapsulate geographical information which is used for the routing procedure, in order to make the most appropriate decisions based on the location of the involved nodes. ARPAM takes advantage of the Automatic Dependent Surveillance - Broadcast (ADS-B) application which exploits the existing Global Positioning System (GPS) and takes into consideration the future introduction of the Galileo system in order to acquire the precise position of the aircraft.

This geographic information is utilized for the computation of coordinates, time and velocity of the neighbor aircrafts. By utilizing the geographic information available from the ADS-B and by assuming that the neighboring nodes are within ADS-B data-link range, ARPAM completes its routing table with information about the neighboring aircraft. Geolocalization information is passed through plain routing protocol messages yet it deserves a special mention considering its role in network stability and security.

Tampering of the geographic data, which –as already mentioned- is a feature specific to ARPAM, may cause erroneous routing decisions (attempts to create invalid routes, premature losses of valid routes, mistaken estimates of current position within the network, etc.) and therefore threaten the integrity of the routing process. In a “normal” network, probably comprised of PDAs and / or laptops or in a sensor network which comprises of a pleiad of nodes, routing errors although important, may not pose an extreme threat compared to networks formed in avionics.

Aeronautical networks, consist of multi-million dollar nodes (airplanes, HAPs and airports), some of which contain or carry human beings. Losing a node due to routing process errors could mean a plane crash disaster which translates not only to high financial loss, but to the loss of many lives as well. Aviation industry and air-line companies can not overlook the security of any component when the stakes at loss are so high. Even if for a moment we rule out the possibility of a plane crash (perhaps using backup flight systems), invalid routing options may lengthen the trip of a plane by a serious factor, inflicting profits of the company due to delays in scheduled trips, increased fuel usage (cost inflated by high oil prices), etc.

Last, but not least, the data link selection mechanism which is used in these aeronautical nodes, relies to the geographic information in order to select and appropriately move their directional antenna. Incorrect information would result in erroneous selection and use of directional antennae, and most probably a partial or even total failure of network connectivity.

6. CONCLUSIONS AND FUTURE WORK

Routing security in wireless networks appears to be a nontrivial problem that cannot easily be solved. More so, it is obvious that ARPAM has its shortcomings as far as security is concerned. Although ARPAM is successful in dealing with replay type of attacks due to its nature, it is highly prone to other failures as there are quite a few

vulnerabilities which can cause great trouble to any network using ARPAM. We've put these vulnerabilities into two distinct categories: message tampering and routing vulnerabilities. As it seems, strategically placed malicious nodes and carefully planned attacks by a single or multiple adversaries can cause network disabilities or a complete network break down.

ARPAM, as it is, is unable to deal with the corruption of its own messages. It is also vulnerable to attack techniques that affect the routing process as a whole, like selective forwarding or complete lack of packet forwarding. Wormholes and byzantine attacks also belong to the latter category and may cause an even greater mess as the malicious nodes attempt to gain complete control of the traffic flow within the network.

In order to deal with these issues, we are actively working on a proposal of secure extensions for the ARPAM routing protocol. These secure extensions will have to deal with the tampering issue at first. It seems appropriate to investigate the possibility of authentication and encryption in order to deal with that aspect of trouble. For the message routing issues though, encryption is pretty much useless. Strong authentication would ensure that adversaries will not be part of the network. This, along with the encryption would elevate the network's ability to protect itself from adversaries that attempt to apply any of the attacks described in this article.

7. REFERENCES

[1] M. Iordanakis, D. Yannis, K. Karras, G. Bogdos, G. Dilintas, M. Amirfeiz, G. Colangelo, S. Baiotti, "Ad-hoc Routing Protocol for Aeronautical Mobile Ad-hoc Networks (ARPAM)", Communication Systems, Networks, and Digital Signal Processing international symposium (CSNDSP 2006), Patras, July 2006

[2] S. Basgani, M. Conti, S. Giordano, and I. Stojmenoviv, "Mobile ad hoc networking", IEEE Press, 2004

[3] J. Nilsson, "VHF Datalinks and ADS-B", Swedish Civil Aviation Administration, August 2000

[4] D. Grace et al., "An Overview of the CAPANINA Project and its Proposed Radio Regulatory Strategy for Aerial Platforms", CAPANINA Consortium, 2005

[5] Jean-Pierre Hubaux et al., "The Quest for Security in Mobile Ad Hoc Network", Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing, 2001

[6] Sonja Buchegger and Jean-Yves Le Boudec, "The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks", IBM Research Report RR 3354, May 2001

[7] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of the ACM Workshop on Wireless Security 2002, pp. 21-30, September 2002.

[8] John R. Douceur, "The sybil attack", In proceedings of the 1st International Workshop on Peer-to-Peer Systems, Cambridge, MA (USA), March 2002.