

A Byzantine Resilient Distributed Position Service

Josh Olsen David Zage Cristina Nita-Rotaru
Department of Computer Science and CERIAS, Purdue University
250 N. University St., West Lafayette, IN 47907 USA
{jolsen,zagedj,crisn}@cs.purdue.edu

I. Introduction

On-demand routing and position-based routing protocols were proposed to address the problem of routing in wireless ad hoc networks. Such protocols are more appropriate for wireless networks than traditional proactive routing because they converge quickly and save energy by building routes only when needed. In particular, position-based routing protocols forward packets based on the geographical position of the destination node. These protocols provide increased scalability since nodes are not required to maintain explicit routes. Instead, the approach requires a mechanism that allows a node to obtain current positions of other nodes in the network. A distributed position service provides a scalable infrastructure to store and retrieve positions of all nodes in the network [1]. Every node in the network stores its position with some subset of position servers and periodically updates its current position. Any node can then obtain the position of any other node by querying any of the servers members of the position service. One mechanism for creating a distributed position service system for mobile ad hoc networks is based on a node's virtual home region (VHR) [2].

The transmission in the open medium and the reliance on untrusted entities for routing make wireless ad hoc networks extremely vulnerable to attacks. For example, an attacker can forge, modify, drop, or replay routing packets, which can lead to discovering non-optimal or adversarial-controlled routes. In addition to attacks against routing, position-based routing protocols are also vulnerable to attacks targeting the position service. Previous work has focused on protecting the position service from passive adversaries and malicious clients [3]. While a malicious client can perform arbitrary actions, the consequences are localized to operations on their own node and position. An attacker can create much more damage by compromising a position server. With one position server compromised and no protection against malicious server behavior, the security of the whole network is at risk.

In this work, we propose a Byzantine resilient VHR-based distributed position service that can tolerate up to b position servers exhibiting arbitrary (possibly malicious) behavior. Through the use of node-disjoint paths and threshold cryptography we mask malicious behavior and provide clients with the correct position of other correct clients. We present our system model in Section II, our protocol in Section III, and our findings in Sections IV.

II. Models

A. System Model

The wireless network consists of a set of loosely synchronized mobile nodes and a set of position servers which are a subset of the network nodes. Each node is able to determine its own position through the use of GPS receivers or protocols such as [4]. Nodes are linked to one or more geographical regions (VHRs) through a globally known static mapping of node identifiers to region identifiers. A node's VHR is responsible for correctly maintaining each member node's position.

We assume that the basic mechanisms for providing encryption, integrity, and data authentication are available for use on the wireless network. We employ a $(b+1, n)$ -threshold signature scheme [5] to allow nodes in a VHR to generate signatures in a collaborative manner. In this scheme, n partial shares of the private key are securely distributed to the nodes in the system and any subset of $b+1$ nodes is able to generate a valid signature.

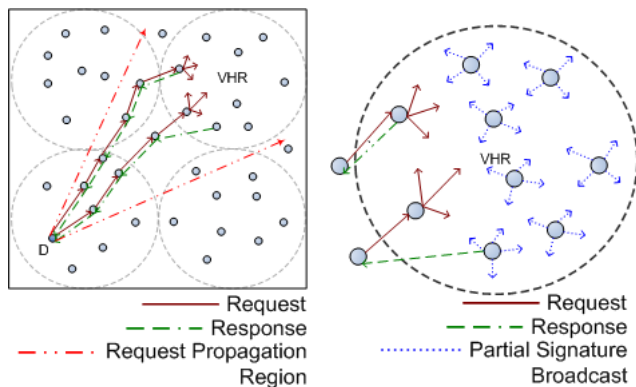
We assume each VHR has a minimum of $2b+1$ nodes during the operation of the position service. This can be achieved by locating VHRs at high traffic hotspots where nodes will congregate, such as an internet cafe. We assume that the system can tolerate an attacker corrupting up to b nodes in the network.

B. Attacker Model

A single, mobile attacker is able to eavesdrop on the communication channel, receive all packets within its transmission range, drop any packet, and forge or alter all non-cryptographically protected packets. An attacker can move within the network and compromise any server within its transmission range. Attackers are computationally bounded and cannot break the cryptographic primitives used in the protocols. Once a server has been compromised, the attacker has access to all data (including cryptographic keys) contained on the server and can collude with any other compromised server(s). An attacker has control of a compromised server's speed and direction if the server is mobile. While an attacker can consume the transmission medium in a denial-of-service type attack, such attacks are beyond the scope of this research.

III. Protocol Description

Our position service has three main components: a position request protocol, a position update protocol, and intra-VHR protocols for storing and replying to node requests. In previous



(a) The request and reply travel along the same node-disjoint paths within the general direction of the VHR. The angle is the smallest that contains enough nodes in range.

(b) Flooding takes place within the VHR for maximum redundancy to mask forwarding attacks. When forming replies, nodes randomly act as combiners for the threshold signature.

Fig. 1. System Operation

work [6], once any server in a VHR received a request, it could respond with the correct value since position servers were non-malicious. We introduce intra-VHR protocols in order to tolerate malicious servers by generating a number of responses signed by a correct majority of nodes in a VHR. Node-disjoint paths are used to propagate messages in order to guarantee at least one correct messages is delivered to and from the desired VHR. Once a message reaches the VHR, it is flooded to and processed by all the nodes currently residing in the VHR. When a reply is required from the VHR, threshold signatures are used to create a single response, which is then forwarded back along the node-disjoint paths that the request used.

Let D denote a correct node that initiates a read request and C be a correct node that has received a previously unseen read request message. The read request protocol operates as follows:

- 1) D creates and signs a position request containing its ID, its current position, and the ID of the requested node.
- 2) D then propagates the position request to at least $b + 1$ neighbors. If there are less than $b + 1$ neighbors, it forwards to all neighbors.
- 3) C appends its own ID, its current position, and the current hop count. It then signs and forwards the message to $O(p^{-1})$ (where p is the current path length, in order to curb flooding as paths grow in length) nodes according to the direction scheme described in Figure 1(a).
- 4) If C is within the destination VHR, it creates a partial signature for the reply and floods it within the VHR as shown in Figure 1(b). Each node in the VHR performs this step.
- 5) If C previously issued a partial signature, upon collecting $b + 1$ unique partial signatures, it will act as a threshold signature combiner with a probability inversely proportional to the number of nodes within range. It will then forward the reply along the node-disjoint paths discovered during the read request propagation. Note

that if there are not enough eligible nodes in the VHR to meet the threshold, then less trusted individual responses with each nodes signature are sent back to the client.

A mobile node runs the update protocol when it has moved a predetermined distance away from its previous location. The update protocol operates in a similar fashion, with an initial node forming a signed message consisting of its own ID and current position. The propagation of the message is identical to that of the position request protocol. When a node in the VHR receives an update message from outside of the VHR from the first time, it will flood the message to the VHR. We note that the VHR is a small portion of the entire network and thus the cost of flooding is not prohibitive.

IV. Correctness

In this section we provide the intuition behind our solution and a proof sketch for its correctness.

When a mobile node updates or requests a position from a VHR, the message is propagated through a set of $b + 1$ disjoint paths. As a consequence of the disjoint paths, up to $b + 1$ different nodes from the VHR will be contacted, ensuring at least one valid message is received by a correct node in the VHR. The correct node(s) will flood the VHR, causing all correct nodes to receive and process the message.

When a position request is processed, a correct node will broadcast the request and a partial signature of the response. Since there are at least $2b + 1$ nodes in the VHR, a majority of nodes will have the correct position and be able to produce a valid signature from $b + 1$ partial signatures. The reply and valid signature are sent back along the disjoint paths as demonstrated in Figure 1(a). Therefore, any correct client requesting a position will receive the correct position held by the VHR.

V. Conclusion

We proposed a Byzantine resilient VHR-based distributed position services which tolerates b failures and provides correct functionality to correct clients.

We plan to perform further theoretical analysis of our protocol to more accurately analyze the message complexity and correctness guarantees it provides. We will incorporate and evaluate further probabilistic techniques into our protocol to increase system performance and decrease the network load.

REFERENCES

- [1] M. Mauve, J. Widmer, and H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad-Hoc Networks," 2001.
- [2] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. Hubaux, and J. L. Boudec, "Self-Organization in Mobile Ad-Hoc Networks: The Approach of Terminodes," 2001.
- [3] X. Wu and C. Nita-Rotaru, "On the Security of Distributed Position Services," in *IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm) 2005*, 2005.
- [4] S. Capkun, M. Hamdi, and J.-P. Hubaux, "GPS-Free Positioning in Mobile ad-hoc Networks," in *HICSS*, 2001.
- [5] V. Shoup, "Practical Threshold Signatures," *Lecture Notes in Computer Science*, vol. 1807, pp. 207–220, 2000.
- [6] X. Wu, "VPDS: Virtual home region based distributed position service in mobile ad hoc networks," in *25th International Conference on Distributed Computing Systems*, 2005.