Context-based Mutual Authorization of a Service in Mobile Ad hoc Networks

Sanjay Madria, Department of Computer Science, Missouri University of Science and Technology, Rolla, MO 65401
And
Mark Linderman, Air Force Research Lab, Rome, NY

1. Problem Statement

In mobile peer-to-peer networks many s*ervice discovery* protocols have been proposed. In these methods, the participating peers must provide their identities, during the service discovery process, to be authorized to utilize a service (service could be a request for a data). However, a peer might not be willing to reveal its identity until it identifies the service providing peer due to privacy and security reasons. Even though both the user and service provider peers are legitimate, neither of them wants to reveal their details before the other does, thus can cause a deadlock situation, similar to a chicken-and-egg problem. In addition, some peers may be only entitled to situational-aware and context-based information dissemination based on their roles though these peers may have been authenticated by the network, but not all the peers are authorized to take/provide a particular service. For example, a coalition force node may be authorized into the network, but only allowed some limited access to some information which may not have all the details. Thus, a peer should authorize each other only if that service can be provided by the peer who is authenticating. The solution also requires validating each others' authentication as a two way process rather than one usual one way authentication only (independent of content) and authorization (based on the content entitled to). Moreover, since many peers may be moving sometimes at a higher speed and therefore, the connection available may be very fragile because existing data links don't have large bandwidth to share and can cause a denial of service. Thus, a solution has to have state remembrance/checkpoints so that the process does not need to restart again and again.

Context-based authorization is needed in many military environments where due to security and privacy reasons peers do not want reveal their identities, or share secret keys. For example, some fighters (JSF, F-22) do not want to transmit their identities and secure keys etc because they don't want to be detected. Similarly, a UAV (Unmanned Aerial Vehicle) may be looking for some content based on the current situation from another UAV in the vicinity or soldiers on the ground are looking for some services, but they would like to discover them without revealing their identities or sharing keys for data authorization due to security restrictions or communication timeout. Therefore, some privacy-preserving techniques with stored states can be used to establish the content authorization.

In this proposal, we propose a privacy-preserving authorization model based on challenged/response idea to discover the services available in the mobile peer-to-peer network even when the moving user and the service provider are at a single or multi-hop distance away.

2. Architecture, Service Discovery Process, General Methodology and Procedure

We propose a protocol to solve the chicken-and-egg problem among the peers participating in the service discovery protocol. A Mobile P2P network has an arbitrary topology and lacks a centralized system. The participating peers can be in the vicinity of one another or can be at a multi-hop distance away. In order to maintain the service details of all the peers and to utilize the network features (services) efficiently, we divide the network into a group of *clusters*. Each *cluster* is a collection of peers. All the peers in a cluster can communicate among themselves. Every cluster will have a special peer node called *Broker* which acts as the cluster-head. Cluster-head is selected, based on the reliability and the transmission features, among the peers in the

cluster. Broker calculates the ranking information of each peer present in the cluster and the rank is increased after each successful service request. Multicasting the service request to highly ranked peers is carried out to reduce the network traffic and improve latency, unlike flooding the service request.

A user initiates the service discovery process by broadcasting an encrypted service request. All the peers who receive this request will try to decrypt the message. If none of them succeeds in doing so, the user will send the request to its broker. When a service request is arrived at the broker, it sends the request to all the peers in the same cluster. If there is no reply from the peers, then broker sends the request to the highest ranked peer set. If the service is not yet found, then broker resends the request to the next highest ranking peer set. This process is done until the service is found. Brokers will send the request to the highest ranking nodes by finding the routes (between user and the service provider). When a peer (service provider) is able to decrypt the service request, it starts playing a game with the user by sending a reply to the service request in order to authenticate and authorize them before revealing their private details. The game consists of various message transfers between the user and service provider and their validation. Each message consists of encrypted masked information about user/service provider identity and the service request. The game will be continued until both of them are authorized or when at least one of them recognizes that the other node cannot be authorized. Even when a mismatch occur, since all the messages are masked and encrypted, privacy details of the participating nodes will not be revealed.

Handling Route Failures and Peers Transparency: Peers in the mobile ad hoc network move randomly causing the wireless connections, between the intermediate peers (peers present on the route between user and the service provider), to be disconnected. So there is a probability of route failure between the user and the service provider, during the authentication process (i.e., while the peers exchange the masked identities). When a route failure occurs during the authentication process, the Broker peer of the user will find a new route between the user and the service provider, using the routing protocol and keeps the route failure transparent to the participating peers by resending the last packet with the current masked identities. By doing so, the peers can still continue the game and this keeps the route failure transparent to the user and the service provider.

References

1. F. Zhu, W. Zhu, M. W. Mutka and L. Ni, "Private and Secure Service Discovery via Progressive and Probabilistic Exposure," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 11, pp. 1565-1577, Nov. 2007.
2. M. Nidd, "Service Discovery in DEAPspace," IEEE Personal Communications, August, pp. 39-45, 2001.
3. C. Ellison, UPnP Security Ceremonies V1.0, Intel Co., http://www.upnp.org/download/standardizeddcps/UPnPSecurity Ceremonies_1_0secure.pdf, Oct. 2003.
4. Sun Microsystems, Jini Technology Core Platform Specification, http://wwws.sun.com/software/jini/specs/, June 2003.
5. S. Czerwinski, B.Y. Zhao, T. Hodes, A. Joseph, and R. Katz, Architecture for a Secure Service Discovery Service," in Proceedings of MobiCom, 1999.
6. F. Zhu, M. Mutka, and L. Ni, "A Private, Secure and User-Centric Information Exposure Model for Service Discovery Protocols," IEEE Trans. Mobile Computing, vol. 5, pp. 418-429, 2006.