

Architectural Framework Design for Authentication Mechanism in Mobile Adhoc Networks (MANETs)

Rajasekhar Yakkali
Gregory Vert
Department of Computer Science and Engineering
University of Nevada, Reno
Reno, Nevada - 89557

Abstract- *Wireless ad-hoc networks do not rely on a pre-existing network structure and are characterized by dynamic changes in the topology. This characteristic makes it difficult to perform the intrusion detection in such networks. The problem gets more complicated with the topological changes in determining whether the node participating in the network transmission is Byzantine or indeed an authenticated node. The thrust of this paper is to develop an efficient design of an architectural framework for authentication of nodes involved in a mobile ad-hoc network.*

Keywords - Mobile Agents, Mobile Adhoc Networks, Authentication, Certificates, Key Management.

1 Introduction

Evolution of the technology has led us from the age of abacus to computers that can communicate and perform major operations on their own. Mobile Adhoc Network (MANET) is one such network, where two or more peers can use appropriate information and communication systems to collaborate spontaneously without requiring centralized coordination. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including the topological discovery and delivering messages must be taken care of by the nodes themselves with routing functionality incorporated into mobile nodes. The network should be able to adaptively alter the routing paths to alleviate any of these ill effects. Moreover, in a military environment, preservation of security, latency, reliability, and fast recovery from the failure are significant concerns. Military networks for example, are designed to maintain a low probability of interception and a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in

any of these requirements may degrade the performance and dependability of the network.

Mobile agents are autonomous software entities that can be dispatched from a node to another to perform an array of tasks. They are designed to constitute the intelligence and functionality to perform the tasks taking into consideration of the fact that the factors involved in proper execution of the task might change. Once deployed on the remote nodes, a mobile agent can function independently of the host machine it has originated from.

2 Approach

A network is a collection of nodes connected together which allows communication and performing tasks accordingly. A Client-Server network as illustrated in Fig.1 is the most general form of network that is used.

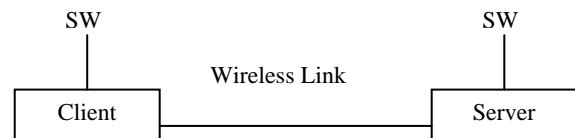


Fig. 1 Client Server Network

Following the same paradigm, software physically residing on each node that could be utilized for the authentication purposes is a constraint in Mobile Adhoc Networks. This would require a large amount of data to be transferred back and forth between two nodes participating in the communication thus increasing the overhead on the network. Mobile adhoc networks include the nodes of asymmetric configuration and require the software to adapt to the localized security policies to perform authentication. Security policies are local to the machine as the mobile adhoc network could include a wide array of nodes with different

configurations and the dynamic topological changes. Security policies tend to change over time period in mobile adhoc networks. Creation of monolithic software that addresses the local security policies of all the machines is a very complex functionality. Furthermore, monolithic software to address authentication in MANETs is prone to increase in contention of the bandwidth and utilization of resources excessively. Authentication mechanism in such a network needs dynamic localized reasoning and mobility. It's a daunting task for the software to provide communication following one-size-fits-all approach. Also localized reasoning reduces the communication overhead formed in the regular client-server architecture. Mobile agents at this juncture can be utilized as a solution to incorporate the intelligence required to adapt to the various configurations of the nodes forming the adhoc network and perform the task. Mobile agents could be transported to the specific nodes to adapt to the localized security policies of the specific node and implement the authentication mechanism accordingly, thus reducing the communication overhead.

This paper proposes an architecture that addresses these specific issues that involves utilization of mobile agents to perform authentication in mobile adhoc networks.

3 Related Work

Public Key Infrastructure (PKI) is generally utilized for trust management between the nodes in the network [1]. Authentication framework proposed in this paper for authentication mechanism in Mobile Adhoc Networks is based on the Diffie - Hellman public key exchange mechanism utilizing hierarchical trust model [2].

In the hierarchical trust model, a root certificate authority (CA) issues certificates to delegated CAs or end users. The CAs in turn issue certificates to end users or to other CAs.

Weimerskirch and Thonet [3] presented a distributed light-weight model for authentication that involves network nodes requesting trust references from neighboring nodes in order to establish the trust relationships needed for trust authentication.

Zhou and Haas [4] analyzed the security threats faced by an adhoc network and proposed the solutions based on redundancies in the network

topology. They propose the use of diversity coding on multiple routes to tolerate both benign and Byzantine failures. Related work includes the key management schemes discussed in [5, 6]

The next section gives an overview of the mobile agents and how they can be used in decreasing the overhead in securing mobile adhoc networks.

4 Background

4.1 Mobile Agents

Mobile Agents (MA) are software programs that have the unique ability to transport themselves from one system to another [7]. This allows processes to migrate from computer to computer. The processes can further split into multiple instances that execute on different machines to accomplish the tasks assigned. Mobile agents have ability to operate asynchronously and independently of the process that created them. The two fundamental concepts in the mobile agent model are the agent and its execution environment. Mobile agents have also been defined as the objects that have behavior, state and location.

Mobile agents, with their ability to relocate to the remote nodes, perform the computation locally reducing the network traffic. They provide an effective means of overcoming network latency by reducing the number of interactions required and the data transmitted through these interactions in the network.

MAs have the ability to sense their execution environment and autonomously react to changes. For example, if the computational load of the host platform is too high and if the host's environment doesn't meet the agent's service expectations, the agent and its data can move to another machine that can better satisfy its computational needs.

4.2 Mobile Adhoc Networks

Mobile Adhoc Network (MANET) is an autonomous system of mobile nodes connected by wireless links with the ability of moving from one location to another. Each node operates not only as an end-system, but also as a routing mechanism to forward packets. The nodes are free to move around and organize themselves into a network. MANET does not require any fixed infrastructure, therefore

it is an attractive networking option for connecting mobile devices quickly and spontaneously.

Mobile Adhoc networks maintain the routing information based on the network routing policies that allow the nodes to self organize accordingly. Consisting of nodes and devices that are autonomously self-organizing in networks, mobile adhoc networks offer a large degree of freedom at a lower cost than other networking solutions.

4.3 Routing Protocols

Routing protocols [8] for Adhoc networks must handle outdated routing information to accommodate dynamic changing topology. Detection of compromised nodes through routing information is difficult due to dynamic topology of Mobile Adhoc Networks. Several routing protocols [9, 10] address the routing mechanisms dealing with dynamic topologies in Mobile Adhoc Networks. Routing protocols in Mobile Adhoc networks is a vast subject on its own and discussion of the topic is beyond the scope of this paper.

4.4 Authentication

Authentication is the process by which a system verifies the identity of a user who wishes to access it [11].

Two basic types of encryption are commonly used are Symmetric encryption and Asymmetric encryption. Symmetric encryption is a type of encryption where the same key is used to encrypt and decrypt the message. This differs from asymmetric (or public-key) encryption, which uses one key to encrypt a message and another to decrypt the message.

The key to successful use of asymmetric encryption is a Key Management system, which implements a Public Key Infrastructure. Without this, it is difficult to establish the reliability of public keys, or even to conveniently find suitable ones.

5 Key Management

A digital certificate is a digital file used to cryptographically bind an entity's public key to specific attributes relating to its identity. It is simply a cryptographic digital attachment to the electronic

message used to establish an entity's identity. Cryptographic schemes such as digital signatures are often employed to protect both routing info as well as data. Public key systems are generally adopted because of their efficiency in key distribution. In public key infrastructure each node has a public/private key pair. Public keys distributed to other nodes, while private keys are kept to nodes themselves and that too confidentially. Third party (trusted) called Certification Authority (CA) is used for key management. CA has a public/private key pair, with its public key known to every node and signs certificates binding public keys to nodes. The trusted CA has to stay online to reflect the current bindings, since the bindings could change overtime. Public key should be revoked if the owner node is no longer trusted or is out of network. A single key management service for an Ad-hoc network is probably not a feasible solution, since it's likely to become bottleneck of the network. If CA is down/unavailable, nodes cannot get the current public keys of other nodes to establish secure connection. Also if a CA is compromised, the attacker can sign any erroneous certificates with the private key. Hence it's more justified to distribute the trust to a set of nodes by letting these nodes share the key management responsibility.

6 Architectural Framework

The authentication model proposed and as illustrated in Fig.2 includes the session level mechanism, password encryption, certificate management and mobile agent mechanism to implement the authentication in MANETs.

Mobile agents employed in this model are broadly classified into three categories based on their functionality. They are Delegation Mobile Agents (MAd), Certification Mobile Agents (MAc) and Authentication Mobile Agents (MAa). MAa, MAd, MAc are the notations we followed in this authentication framework for the authentication, delegation and certification mobile agents respectively. Each and every node in the network hosts MAa and MAd. But only a few authorized nodes namely certification authorities (CA) can provide certification management services. CAs host MAc along with the authentication and delegation mobile agents. Utilization of mobile agents in every aspect of the mobile adhoc network

communication mechanism would rather inundate the network with the mobile agents and is prone to network latencies and bandwidth congestion. To avoid this effect, we have constrained the utilization of mobile agents by allowing only CA's to deploy MA's for authentication purposes.

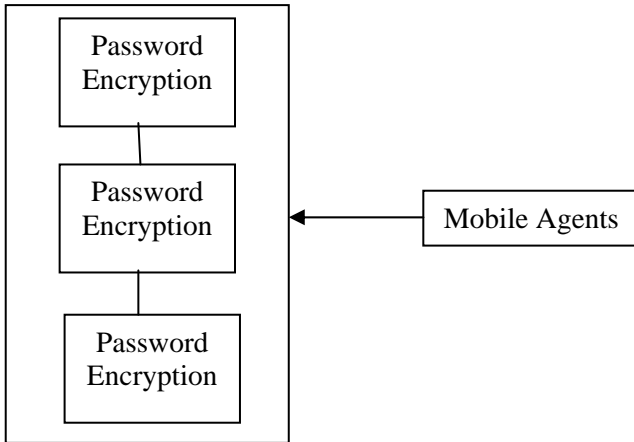


Fig. 2 Authentication Model

Authentication mobile agents (MAa) check the validation of certificates to decide whether the hosts involved in the communication are reliable and authentic. For the new hosts willing to join the network, the MAa agent demonstrates the verification of trust with the new hosts in order to build the level of trust required for the participation in the wireless adhoc network communication.

Delegation mobile agents (MA_d) maintain the delegation list similar to access control list that contains the entries for all the nodes in the network. The delegation list also provides the information of the nodes that possess the authority to issue certificates.

Certification mobile agents (MA_c) are responsible for the certification management services that include issuing, renewal and revoking digital certificates. These agents respond to the requests obtained from the nodes in the network regarding the certificate management services.

A node is not authorized to participate in the network until it presents a valid certificate issued by a certificate authority (CA). Certificate Authorities are the specialized nodes that are only authorized to perform certification management services.

There are several tasks performed during the certificate management:

- Issuing the certificates
- Renewing and revoking the certificates
- Validation of the certificates

6.1 Issuing Certificates

Issuing the certificates is the task that has to be taken care of only by CA's. When a node wishes to join the network, it interacts with one of the CA node's in the network to build trust. The CA interacts with the prospective node and upon its approval for the authentication to be performed; MAa is deployed onto the prospective node wherein the MAa collects all the required information to decide if the node meets the criteria to participate in the network. The authentication mobile agent MAa is deployed on the prospective node and acquires the detailed information about the prospective node such as mac address, ip address, name and environment of the node. Once it is determined that the prospective node can be trusted, the MAa requests the CA's to issue a digital certificate.

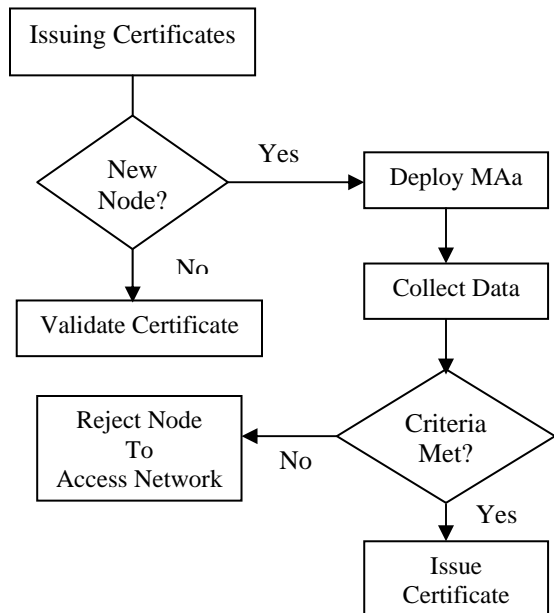


Fig. 3 Flow Diagram for Issuing New Certificates

Fig.3 is a self explanatory flow diagram that describes the process of issuing certificates in our framework. If the MAa determines that the node cannot be trusted, it rejects the request for communication with the network and disconnects the connection, thus reducing the unnecessary communication with the CA, further minimizing the communication costs. Considering the fact that

mobile adhoc networks are not resource intensive, even though the mobile agents are constituted with the ability to relocate from one node to another, mobile agent deployment is constrained in the proposed framework. In this stage of the framework, the authentication mobile agents (MAa) are deployed only by CA and the authentication of the nodes within the network is performed by MAa residing on the regular nodes without the deployment but rather by messaging mechanism as it just requires the validation of the certificate.

ID	Name	Location	Address	Rank	Certificate		
					Exp. Date	Revocation	Status

Fig.4 Profile of the node

Each node in the network maintains a profile. Fig.4 illustrates the profile maintained by each node. Once entered into the network, this profile is being broadcast by delegation mobile agents (MAd) of the particular node. MAd are particularly used for broadcasting and receiving the information in the network to update the profile and delegation list.

Delegation list contains the connect information of the nodes, status of the node and the profile of the nodes. It also includes the information that enables the nodes to distinguish between the CA and end user nodes. This distinction is made possible by providing a ranking to each node in the network. The ranking mechanism involves selection of CA's based on the security infrastructure demonstrated by a node in the network. It also takes into consideration the amount of time the node has been involved in communication within the network and its demonstration of trust in the network. The details of the ranking mechanism and the selection of certificate authorities will be explained in detail in the future work.

Rather than maintaining each and every profile in the network, each node maintains the detailed profile information of its immediate neighboring nodes and the information gets updated through Mad's on each node each time a node changes its location. This reduces the need to maintain the large amount of information and also it reduces the unnecessary communication and data transfer across the network, thus resulting in better utilization of the bandwidth of the network and resources available.

6.2 Renewal and Revocation of Certificates

Renewal and revocation of the certificates owned by the node is taken care by certification mobile agents (MAc). Digital certificates attained by the nodes in the network needs to be renewed before their expiry for the nodes to participate in the communication with the other nodes in the MANET. For a non-certificate authority node, the certificate renewal can be performed by any CA. In the case of CA, it follows the polling method of election for the renewal of certificate by all other active CA's.

Consider the scenario with four CA's $n_k, n_{k+1}, n_{k+2}, n_{k+3}$ in an adhoc network and n_k needs to renew its certificate. It sends out certificate renewal request to all the other CA's in the network. n_k in this case would require two or more than two CA's to sign its certificate for the renewal. Any CA would require $n/2$ or greater than $n/2$ signatures for its certificate renewal.

Similar to issuing certificates to the nodes, only CA can revoke the certificates for the nodes that would eventually restrict those particular nodes to access the network for communication. Fig.5 illustrates the components involved in the renewal and revocation of the certificates.

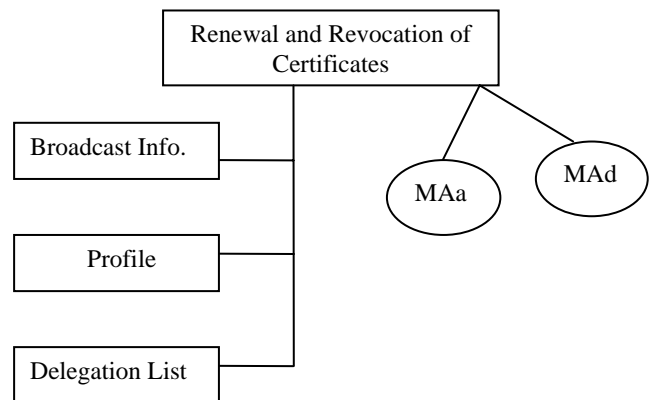


Fig.5 Renewal and Revocation of Certificates

A node on finding the peer node to violate the security policies resulting in compromising the communication or the network sends out the revoke request for the other node to the CA's in the network. MAd's of the CA's update their access control list with the revoke request attained on the specified node it received complaint on. On the revoke requests on the particular node reaching half

the number of nodes in the network, the certificate for the compromising node is revoked and is restricted from accessing the network. A node's certificate can be revoked either if more than half of the CA's agree on the revoking of the certificate of the compromising node. Revoking the certificate of CA would require $2n/3$ CA's to agree on the revoking the certificate of particular CA, where n is the total number of CA's in the adhoc network. MAc of the CA handles all the revoking of the certificates. Once the certificate of a node is decided to be revoked, the information is broadcasted in the network to facilitate the updating of delegation list maintained by each node.

6.3 Validation of Certificates

Validation of the certificates is done by MAa residing on each node at start of the communication with the peer nodes in the network. As each node contains the profiles of the neighboring nodes, MAa's residing on the node utilizes the information contained in the access control list to validate the certificates of the nodes participating in the network.

At any point of time, a profile is not found for a node that is interested in communication, the node incorporates its delegation mobile agent (MAd) with the prospective node's information and transports it to communicate with the CA. MAd gets the profile of the node in question and provides the information back to the authentication agent at the node allowing for the validation to be performed locally.

7 Conclusion and Future Work

This paper discussed about using mobile agents to perform the authentication for the nodes participating in the in MANETs.

In summary, Contributions made through this research are:

- Efficient utilization of network bandwidth with mobile agents in mobile adhoc networks.
- Efficient profile management of the nodes participating in mobile adhoc network.
- Improvement in the security with the proposed authentication model in MANETs.

Scope for the future work:

- Ranking mechanism to elect Certificate Authorities.
- Defining security policies that affect the authentication mechanism in MANETs.
- Trust relationship management in the distributed cluster scenario where a very large network is partitioned into small easily manageable adhoc networks.

8 References

- [1] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet x.509 public key Infrastructure certificate and certificate revocation list (crl) profile," Internet Request for Comments (RFC 3280), April 2002.
- [2] "Diffie-Hellman USM Key Management Information Base and Textual Convention", Network Working Group, RFC 2786.
- [3] A. Weimerskirch and G. Thonet, "A distributed light-weight authentication model for ad-hoc networks," in the 4th International conference on Information Security and Cryptography (ICISC 2001).
- [4] L. Zhou and Z. J. Haas, "Securing Adhoc Networks," IEEE Network Magazine, vol.13, no.6, pp.24-30, November 1999.
- [5] N. Asokan, P. Ginzboorg, "Key Agreement in Ad-hoc Networks", Computer Communications, 23:1627-1637, 2000.
- [6] M. Hietalahti, "Key Establishment in Ad Hoc Networks", Helsinki University of Technology.
- [7] J. M. Bradshaw, "An Introduction to Software Agents," In Jeffrey M. Bradshaw, editor, *Software Agents*, chapter 1. AAAI Press/The MIT Press, 1997.
- [8] J. Broch, D. A. Maltz, D. B. Johnson, Y. Chun Hu, J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols", Proceedings of Mobicom '98.
- [9] C. Perkins, "Ad Hoc on Demand Distance Vector (AODV) Routing", Mobile Adhoc Networking Working Group, Internet Draft, Nov 1997.
- [10] D. B. Johnson, D. A. Maltz, Y. Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IETF MANET Working Group, Internet Draft, April 2003.

[11] S. Leijoki, "Authentication, Authorization and Accounting in Adhoc Networks," Helsinki

University of Technology, May 2000.