이동 Ad Hoc 네트워크 환경에서 클러스터링 구조에 기반한 인증 메커니즘

이 도*, 신용태*
*숭실대학교 컴퓨터학과
e-mail : {litao,shin}@cherry.ssu.ac.kr

An Authentication Mechanism Based on Clustering Architecture in Mobile Ad Hoc Networks

Tao Lee*, Youngtae Shin*
*Dept. of Computing, SoongSil University

Abstract

In contrast with conventional networks, mobile ad hoc networks usually do not provide online access to trusted authorities or to centralized servers, and they exhibit frequent partitioning due to link and node failures and node mobility. For these reasons, traditional security solutions that require online trusted authorities or certificate repositories, but those are not well-suited for securing ad hoc networks. Moreover, a fundamental issue of securing mobile ad hoc networks is to ensure mobile nodes can authenticate each other. Because of its strength and efficiency, public key and digital signature is an ideal mechanism to construct the authentication service. Although this is already mature in the internet application, providing public key based authentication is still very challenging in mobile ad hoc networks. In this paper I propose a secure public key authentication service based on clustering model and trust model to protect nodes from getting false public keys of the others efficiently when there are malicious nodes in the network.

1. Introduction

With the advancement of Wireless technology, mobile communication becomes popular in recent years. There is an increasing attention on the research of mobile distributed computing. A mobile ad hoc network is a collection of nodes with no infrastructure and these nodes are connected with wireless communication. All networking functions(e.g., routing, mobility management, etc.) are performed by the nodes themselves in a self-organized manner. Also, the topology of the ad hoc network is dynamically changing and nodes of the ad hoc network are often mobile. A major challenging in designing mobile network is to protect the vulnerability from malicious node's attacks. As other distributed networks, security in ad hoc networks is based on key management mechanisms. So a special key management mechanism should be developed to suit ad hoc network environment. In this paper, we propose a new key management system based on clustering architecture with trust model. Our trust model follows the "web of trust" approach proposed in PGP mechanism, and we altered this mechanism and merged some new approachs into this mechanism. The first one of our contributions in this network model is based on clustering models in mobile ad hoc networks. The second one is each node need to send its own

public key to its clusterhead in order to improve the efficiency and reliability of authentication. The third one is establishing a reelection mechanism to ensure the clusterhead is not compromised. The works aim at providing a secure, scalable and distributed authentication in mobile ad hoc networks.

The key features of my design are as follows. The system does not rely on any trusted-third party. Authentication can be performed in a self-organized manner. All the nodes are divided into different clusters ,each cluster has a clusterhead that elected by all nodes in the cluster. Nodes in the cluster monitor the behavior of each other and update the trust tables accordingly. After that, each node sends its public key to the its clusterhead and Clusterheads exchange their own public keys among them. Our public key management mechanism endures the false certificate issued by dishonest users and malicious nodes, and avoids them to be selected as clusterheads or introducing nodes. these features provide a secure and available authentication service in the ad hoc networks.

The paper is organized as follows: Section 2 discusses the related works. The architecture of this approach is described in section 3. Finally, We conclude the paper in section 4.

2. Related Works

Traditional network authentication solutions rely on physically present, trust third-party servers, or called cetificate authorities (CAs). Popular network authentication architecture include X.509 standard and Kerberos. However, ad hoc networks are infrustructureless, and there is no centralized server for key management. Hence, converntional key management mechanisms do not suit the requirement of ad hoc networks.

Pretty Good Privacy is proposed by following a web-of-trust authentication model . PGP uses digital signatures as its form of introduction. When any user signs for another user's public key, he or she becomes an introducer of that user's public key. As this process goes on, a web of trust system is established. Another active research area is security function sharing, including a popular method for threshold secret sharing. The basic idea is distributing the functionality of the centralized CA server to several specific nodes or all the nodes.

For improving the efficiency and security of the communication, the nodes in the network are generally partitioned into individual clusters. Each cluster is managed by a special node called clusterhead. The clusterheads are responsible for the formation of clusters.

Our approach is inspired and influenced by the works above. What distinguished it from them is our special key management mechanism driven view of MANETs, which let clusterhead sends public keys of all its members to requesting node. Moreover, clusterheads exchange their public keys each other to keep relationship among them. To cope with getting false public key we design a improved web of trust approach to guarantee getting an authentic public key of target node. However, in this approach each node acts as a CA, so as to each node manages its trust table and monitors each other in the cluster. Finally, requesting node selects the public key of the target node by computing the majority votes in the target cluster.

3. Public Key Management Architecture

3.1 The Clustering Model

Obtaining a hierarchical organization of a network is well-known and well-definded problem of distributed networks. Clustering has been proved effective in minimizing the amount of storage for communication information, and optimizing the use of network bandwidth. In the beginning, several nodes get together and intend to set up a mobile ad hoc network environment. First, we adopt an on-demand weighted clustering algorithm to divide all the nodes into the appropriate clusters. To decide which one should be a suitable clusterhead, we take into account its priority, transmission power, mobility and battery capability. The following features are considered in our weighted clustering algorithm.

- The clusterhead election procedure is not periodic and invoked as rarely as possible. This reduce the system computation and communication costs.
- Each clusterhead can ideally support M (a pre-defind system threshold) nodes to ensure efficient functioning. A high throughput of the system can be achieved by limiting or optimizing the number of nodes in each cluster.
- The battery power can be efficiently used within certain transmission range. Consumption of the battery is more if a node acts as a clusterhead than an ordinary node.
- Mobility is an important factor in deciding the clusterhead. Reaffiliation occurs when one of the ordinary nodes moves out of a cluster and joins another existing cluster. In this case, the amount of information exchange between the node and the corresponding clusterhead, is local and relatively small.
- A clusterhead is able to communicate better to its neighbors if they are closer to the clusterhead within the transmission rang. This it due to signal attenuation with increasing distance.
- Every node be assigned a fixed priority-rating before it join in an ad hoc networks, that stands for the degree of node.

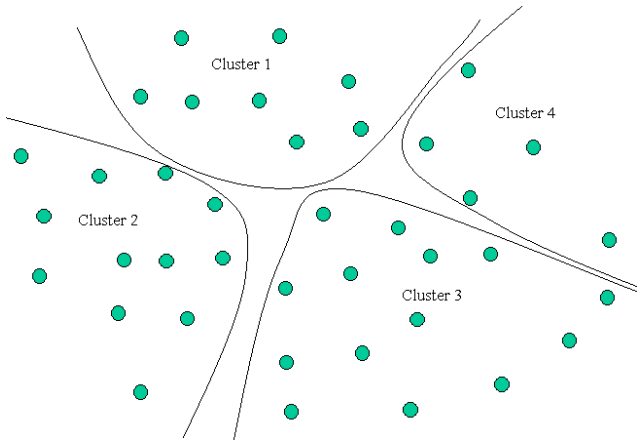

Figure 1. clusters in mobile ad hoc network

Clusterhead election procedure

Step 1 : Find the neighbors of each node N (i.e., nodes within it transmssion range). Each node has a pre-difined priority-rating value Pn.

Step 2 : For each node, calculate the sum of distances, Sn, with all its neighbors.

Step 3 : Compute the running average of the speed for every node. This gives a measure of mobility and is denoted by Mn.

Step 4 : Compute the time, Tn indicates how long can this node act as a clusterhead. Because a clusterhead consumes more battery power than an ordinary node.

Step 5 : Calculate a combined weight En = c1Pn + c2Sn + c3Mn + c4Tn, for each node n. The coefficients c1,c2,c3 and c4 are the weighing factors for the corresponding system parameters.

Step 6 : Choose the node with a minimum En to be the clusterhead. All the neighbors of chosen clusterhead can no longer participate in the election algorithm.

Step 7 : Repeat step 2 to 6 for the remaining nodes not yet assgined to any cluster.

Due to the dynamic nature of the system considered, the nodes as well as the clusterheads tend to move in different directions, thus disorganizing the stability of the configured system. So, the system has to be updated from time to time. After the nodes in the ad hoc networks divided into several clusters, every node exchange information between each other in the cluster. Apart from the view of efficiency, we believe clustering improves the security of a network as well.

3.2 Trust Model

Mobile ad hoc network lacks of centralized server for management and monitoring. Therefore, its security measure relies on individual nodes to monitor each other. Furthermore, each node acts as a certificate authority, so that each node can get all the public keys and IDs from other nodes in the same cluster. For preventing the requesting node from getting false public key from malicious node, we adopt web of trust approach to help node to get reliable public key of target node. For helping nodes to store the trust relationship with other nodes, each node build a trust table that consists of Tid, Gid, Tpk and trust value. Tid indicates unique ID of target node, Gid indicates gateway ID (i.e., if the target node not in its transmission range, this node has to combine the trust values to a singl value, and gateway is the next hop to target node), Tpk indicates the public key of target node, and trust value indicates the authentication metric as a continuous values between 0.0 and 1.0. If the target nodes are not directly within its transmission range , it combine the trust values with other nodes to a single value in the same cluster. Therefor, each node build a trust table to store the public key and trust value for identifying other nodes and securing the communication among them.

This turst model uses digital signatures as its form of introduction. Any node signs another's public key with its own private key a eastablish a web of trust system.

3.3 public key certification

The clusterheads exchange their public keys each other as soon as it is elected. Furthermore, all the members of the cluster are all in the transmission range of clusterhead, so the clusterhead can collect all the public keys of its members in its cluster. When node s want to get the authentic public key of node T1 which belongs to cluster T. First, node S sends request to its own clusterhead, the clusterhead reply the public key of clusterhead T to node S. Then, node S sends encrypted its public key and target node ID with clusterhead T' public key to clusterhead T. Clusterhead T sends the public keys of all its members to node S and multicasts the request to its cluster. Next, all the nodes send encrypted public key of target node to node S. After that, node S select the public key with the majority votes as the authentic public of node T. If the majority encrypted packets can not be decrypted by corresponding public keys that provided by their clusterhead, it indicates their clusterhead is compromised, so that the cluster needs to reelect the clusterhead .

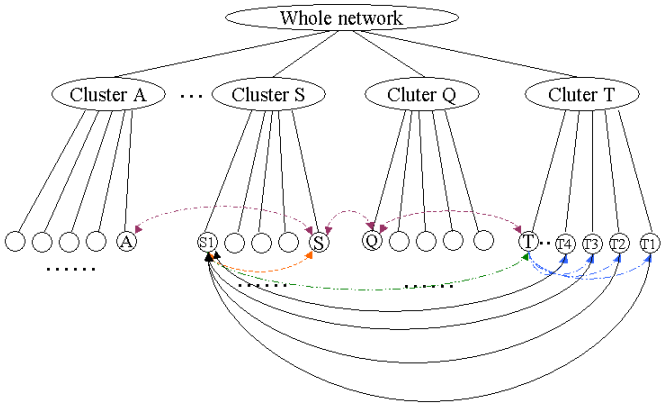

Figure 2. Public key certification

Operation of public key certification

1. Nodes S1 want to communicate with node T1 that in cluster T, so node s1 sends request to its own clusterhead S .

2. Clusterhead S replys the public key of clusterhead T to node S1. Because of clusterheads exchange its own public key among them periodically, so each clusterhead has other clusterheads' publik keys.

3. Node S1 sends encrypted request and its public key with clusterhead T's public key to clusterhead T. Clusterhead T replys it signed public keys of all the nodes in its cluster with its private key to node S . At the same time, Clusterhead t multicasts the request to its cluster.

4. All the nodes in cluster T send it signed public key of node T1 and corresponding trust value with its private key to node S.

5. Collects the reply messages m∈M from nodes in cluster T, where m={ PKT,VTi,T,….}SkTi. PKT denotes the public key of node T, VTi, T denotes the trust value from Ti to T1, and SkTi denotes the secret key of node Ti. The reply message is signed by the secret key of node Ti, SkTi.

7. Compares the received public keys which have high trust values and selects PKT1 with the majority votes. Let igood∈Igood and ibad∈Ibad, where igood are the nodes that thought to be honest (agree on Pkti with the majority) and ibad are the remaining nodes that thought to be dishonest.

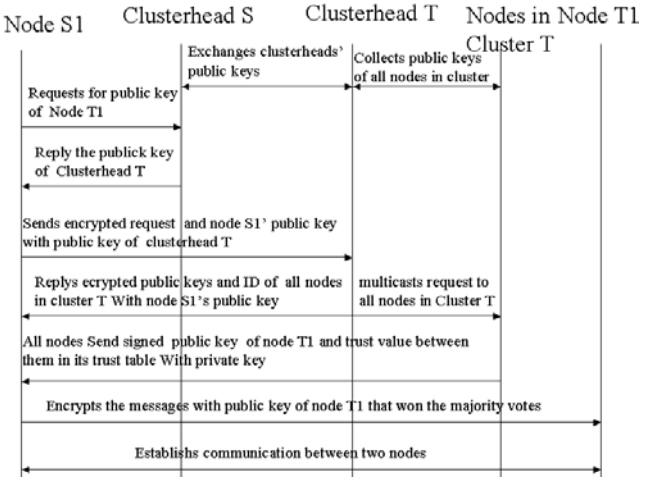

Figure 3. Operation of public key certification

4. Conclusion

This paper describes a clustering based approach in public key authentication for mobile ad hoc wireless networks. To this end, we propose a trust model that allows nodes to monitor and rate each other with quantitative values. We define the network models as clustering-based, such that nodes in the network are divided into different groups with unique IDs. In this work, a new clustering based public key authentication mechanism is developed. The design is targeted for high fault tolerance, improving security and efficiency of communication. Our approach ensures the security and availability of public key authentication in the inherently insecure and unrelible mobile ad hoc networks

5.references

[1] V. Karpijoki, " Security in Ad Hoc Networks," Helsinki University of Technology, Tik-110.501 Seminar on Network Security, Telecommunications Software and Multimedia Laboratory, 2000.

[2] S.Garfinkel, " PGP: Pretty Good Privacy," O'Reil ly & Associates Inc., USA 1995.

[3] A. Abdul-Rahman, " The PGP trust model," EDI-Forum: the Journal of Electronic Commerce, April 1997.

[4] L. Zhou and Z. J. Hass, " Securing Ad Hoc Net works," IEEE Networks Magazine, vol. 13, issue 6, 199 9.

[5] S. Basagni, " Distributed Clustering for Ad Hoc Networks," Proceedings of ISPAN'99 International Sym posium On Parallel Architectures.

[6] Edith C. H. Ngai and Michael R. Lyu ,"Trust- and Clustering Based Authentication Services in Mobile Ad Hoc Networks", Department of Computer Science and Engin eering The Chinese University of Hong Kong Shatin, Ho ng Kong.

[7] Gang Xu and Liviu Iftode, "Locality Driven Key Management Architecture for Mobile Ad-hoc Networks *Department of Computer Science, Rutgers University*

[8] Srdjan ˇ Capkun, Levente Butty´an† , and Jean-Pi erre Hubaux, "Self-Organized Public-Key Management fo r Mobile Ad Hoc Networks", Laboratory for Computer Communications and Applications (LCA) School of Infor mation and Communication Sciences (I&C) Swiss Federa l Institute of Technology Lausanne (EPFL) CH-1015 Lau sanne, Switzerland

[9] Mainak Chatterjee, Sajal K. Das and Damla Turgu t, "An _ On-Demand Weighted Clustering Algorithm (W CA) for Ad hoc Networks", Center for Research in Wir eless Mobility and Networking (CReWMaN) Departmen of Computer Science and Engineering University of Tex as at Arlington Arlington, TX 76019-00