Volume 2, No. 8, August 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

TECHINECAL NOTE

Available Online at www.jgrcs.info

CLUSTER BASED SECURITY ARCHITECTURE IN WIRELESS AD-HOC NETWORKS: AN OVERVIEW

Avinash Jethi*[1] and Seema[2]
[1]Asst. Professor,Computer Engg.
Bhai Gurdas Institute of Engg and Technology, Sangrur.
[2]Asst. Professor,Computer Engg.
Yadavindra college of engineering, Guru Kashi Campus,Talwandi Sabo.
avinashjethi@ymail.com

Abstract: Mobile ad hoc networks are growing in popularity due to the explosive growth of modern devices with wireless capability such as laptop, mobile phones, PDA, etc., makes the application more challenging. The mobile nodes are vulnerable to security attacks. Providing security and anonymity to users are critical in wireless ad hoc networks. Ad hoc networks have lots of applications; however, a vital problem concerning their security aspects must be solved in order to realize these applications. The dynamic and cooperative nature of ad hoc networks present challenges in securing these networks. There are recent research efforts in securing ad hoc networks. Amongst security approaches, there are threshold cryptography, certification authority, reputation and authentication. In this paper we introduce and survey these approaches. The approaches taken in this paper could be applied to the analyses of some other security methods for mobile ad hoc networks proposed in the literature.

Keywords: Adhoc networks, authentication, certification, reputation, threshold cryptography, security.

INTRODUCTION

Mobile ad hoc networks are generally characterized by the lack of infrastructure, dynamic network topology, distributed operation, bandwidth constraints, variable capacity links, use of low power devices, limited CPU and memory, limited physical security, and complexity of design of network protocols. However, ad hoc wireless networks are highly appealing for many reasons. The set of applications for mobile ad hoc networks is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The dynamic and cooperative nature of ad hoc networks present challenges in securing these networks. There are recent research efforts in securing ad hoc networks. Amongst security approaches, there are threshold cryptography, certification authority, reputation and authentication. In this paper we survey those approaches and identify the challenges associated with each .

THRESHOLD CRYPTOGRAPHY

In this section we survey different threshold cryptography schemes proposed for ad hoc networks and the solutions suggested in the literature for determining the optimum threshold level. This will be presented in sections 2.1 and 2.2 respectively.

Threshold Cryptography Schemes:

Security schemes for ad hoc networks generally use public-private key mechanism. The overall system has a known public key and its private key is shared by between each server nodes in the system. Each server node stores the public key of other elements and sign request responses using the private key of the overall system. Requests may be update the node's public key or query the public key of the node that is intended for private communication. New public key of the node can be broadcasted since combiner should use the private key of the server system to obtain it. System is secure because adversary does not have enough computational power to break these cryptographic schemes; it is also robust that servers are always able to process update and query requests. Threshold cryptography is the base stone for distribution of trust protocols. The idea of (k, n) threshold scheme was introduced by Shamir in [1]. A (k, n) scheme allows a secret, to be split into shares, such that for a certain threshold k<n, any k components could combine and generate a valid signature; whereas, k-1 or fewer shares are unable to do so. Zhou and Haas in [2], proposed the idea of utilizing threshold cryptography to distribute trust in ad hoc networks. According to [2], the challenges associated with key management services such as issuing, revoking and storing of certificates in ad hoc networks can be resolved by distributing Certification Authority (CA) duties amongst the network nodes.

Optimum Threshold Level

If threshold cryptography is used, it is important to know the value of the threshold *k*. A very high threshold level ensures greater security, but the QoS requirement may not be satisfied. If the threshold level is lowered, it becomes easy for a node to construct its digital certificate within the QoS requirements or specified authentication delay time, but the security aspect is compromised. The threshold level selection process is influenced by various network dynamics such as network density, node speed, node transmission range, threshold requirements etc. In [3], the calculation of the threshold level was modeled as an optimization problem for a certain QOS requirement. However this optimization problem cannot be solved with standard optimization techniques as the function is not known. Therefore, simulations were used to optimize the threshold level function to derive the optimum threshold level. Two ways were investigated to fix the threshold level.

First method: Global Selection, where the threshold level is fixed, i.e. it is the same for all nodes at all times. *Second method:* Local Selection, where the threshold level is selected based on the local environment of a node at that moment. This method is more responsive to the dynamic nature of a mobile network. The results have shown that in global selection protocol, the biggest drawback is that the number of partial certificates required to construct the full certificate is fixed for all the nodes in the network. This results in failure to construct certificates as the QoS requirements cannot be met. According to [3], the network traffic increases steeply as a result of the higher number of certificate construction failures; this could result in network congestion. In local selection protocol, the required number of partial certificates is determined based on the locality of a node. Moreover, it is easier to select the critical threshold value for a given network. However, due to more number of steps involved in the protocol, performance of the protocol drops down for nodes that move at higher speeds. But this can be overcome by setting precedence level to certificate request packets. An intelligent approach to determine the optimum threshold level given a network configuration using neural networks was also proposed in [3]. A trained neural network can be embedded into each node, so that nodes can compute an optimum threshold level for different network conditions and use it in the authentication protocol.

CERTIFICATION AUTHORITIES

In order to have threshold cryptography,certification authorities (CAs) are needed. This section focuses on CAs. The concept and tasks of the CAs is presented in section 3.1, and a comparison between the single and multiple CAs case is given in section 3.2. In section 3.3 the certification schemes in ad hoc networks are given, whereas in section 3.4 the certificate revocation schemes are presented.

Concept of Certification Authorities:

In ad hoc networks, trust is managed locally at the individual nodes. A node is not trusted by a given node until it presents a certificate, and the node in question verifies that the certificate was issued by a trusted CA, and it has not expired nor been revoked. The CAs has the following trust management tasks [4]:
1) Issuing of certificates
2) Storage of certificates
3) Certificate validation
4) Revocation of certificates.

Beyond managing certificates, it is also the CA'sresponsibility to disseminate the public keys of principals to inquiring clients. Every response from the CA is signed with the CA's private key, and so can be validated with the CA's public key. The success of this approach lies in maintaining the secrecy of the private key of the CA. It is also necessary for the CA to remain on-line (i.e. available) to provide these services. There are three major parameters to a distributed key management framework: *fault tolerance,* vulnerability and availability. The first parameter is associated with the number of node failures the system can handle; the second is associated with the number of compromised nodes the system can withstand, whereas the third is associated with the ability of the client to contact the required number of CAs. The optimization of any one of these parameters may adversely affect other parameters and so adversely affect the success of the system. In addition, mobile networks present hostile environments where nodes may easily die or be compromised and no guarantees can be made about the ability to access the necessary nodes for authentication. An ideal key management service for ad hoc networks should provide the best of both worlds: it must be light-weight and simple to mobile nodes, and it must be available in highly dynamic networks.

Certification Authorities Selection:

A single centralized authentication server is unsuitable for ad hoc networks, from the security point of view, as it may be subject to a single point attack. To provide better fault tolerance, it is possible to deploy many copies of the CA in the network. With many such replicas, the system can withstand a number of replicated CAs - 1 failures because the CA service is available as long as there is at least one operational CA. Availability has also been improved since a client node will have a better chance of reaching one of the multiple CAs to get service.Unfortunately, the system has become more vulnerable. An adversary need only compromise one of the many CA nodes to acquire the secret key and so compromise the whole system. The problem of using replicated CAs stems from the fact that each replica has full knowledge of the system secret. The approach is vulnerable against any attacks that compromise a single replica, which should not be considered too difficult considering the inherent physical vulnerability of mobile nodes.

The Threshold Digital Signature scheme was proposed to address this problem [5]. With threshold digital signatures, again the key is divided into *n* pieces and distributed. But now if a client needs a signature onits data, each secret holder will use its piece of the key to generate a partial signature over the data. When client collects *k* of these partial signatures, the client can reconstruct the full signature. Even after achieving an adequately secure CA deployment using threshold digital signature techniques, there still remains one problem.

This set of secure distributed CA nodes should be highly available for the client nodes in the network at all times. In ad hoc networks, there is no guarantee of connectivity between any two nodes at any point in time. In order to increase the availability of the CA(s), it has been proposed to distribute the CA functionality over all nodes participating in an ad hoc network. For example, in [6], every node carries a piece of the CA's secret key. By using threshold cryptography, a node only needs *k* nodes in its neighborhood to achieve authentication using one hop broadcast. This approach has the advantages of high availability at all times, and low communication overhead due to the one hops broadcast-based operation. [7].

An ad hoc network is expected to have a wide variety of nodes with differing computational power as well as differing levels of physical security. Essentially, nodes in a network can be heterogeneous. Based on this heterogeneity assumption, it is interesting to consider distributing the CA functionality only to relatively secure and relatively powerful nodes [7].

Certification Schemes in Ad Hoc Networks:

Different certification schemes have been presented in the literature. We classify a these schemes into cluster-based schemes and non cluster-based schemes and present them in subsections 3.3.1 and 3.3.2 respectively.

3.3.1 Cluster-Based Certification Schemes In A cluster-based architecture for a distributed public key infrastructure that is highly adapted to the characteristics of ad hoc networks was introduced in [8]. In order to adapt to the highly dynamic topology and varying link qualities in ad hoc networks, central instances that would form single points of attack and failure were avoided. Instead, the ad hoc network was divided into clusters, and the cluster heads jointly perform the tasks of a certification authority.

A proactive secret sharing scheme distributes the private network key to the cluster heads in the ad hoc network. Instead of a registration authority, arbitrary nodes with respective warranty certificates may warrant for a new node's identity. Based upon this authentication infrastructure, a multi level security model ensuring authentication, integrity, and confidentiality is provided. Authentication itself is realized in two stages. First, a node gets the status of a guest node. After sufficient authentication, the node will become a full member. An additional important feature is the possibility to delegate the cluster head functionality to another node. [8] Another approach based on trust model and clustering algorithm was proposed in [9] in order to distribute a CA. The clustering algorithm is based on two parameters, security and stability.

The security factor is related to the trust model; only confident nodes can become cluster-head and assure CA role. In each cluster, there are five roles of nodes: The CA Certification Authority of cluster *k* which certificates public key of nodes belonging to the same cluster, the RA Registration Authority which protects CA against attackers. The GW is a gateway node ensuring a connection between two different clusters *i* and *j*, these nodes must be certified by two different CAs. The MN represents a member node *i* which belongs to the cluster *k*. Finally the VNis a visitor node *i* that belongs to cluster *k*, it has low trust certificate. In the clustering algorithm, the stability factor is presented by mobility metric in order to give more stable clusters. The trust model is evolved by monitoring process which allows any node with high trust metric to monitor and evaluate other nodes with low trust metric. To protect CA nodes, a Dynamic Demilitarized Zone (DDMZ) permits to increase security robustness of cluster and endure malicious nodes that try to attack CA or issue false certificates. This approach ensures the security and availability of public key authentication in each cluster and this architecture is adapted to any topology changes.

3.3.2 Non Cluster-Based Certification Schemes In [7], a certification protocol called MP (MOCA Certification Protocol) was proposed. Given the threshold value, *k*, the total number of nodes, *M*, and the number of MOCAs, *n*, the communication pattern between a client and *k* or more MOCA servers is one to (k or more) then back, which means that a client needs to contact at least k MOCAs and receive replies from each of them. To provide an efficient way of achieving this goal, a certification protocol called MP (Moca certification Protocol) was proposed in [7]. In MP, a client that requires certification services sends Certification Request (CREQ) packets. Any MOCA that receives a CREQ responds with a Certification Reply (CREP) packet containing its partial signature. The client waits a fixed period of time for *k* such CREPs. When the client collects *k* valid CREPs, the client can reconstruct the full signature and the certification request succeeds. If too few CREPs are received, the client's CREQ timer expires and the certification request fails. The client is left with the option to initiate another round of certification requests. As a CREQ packet passes through a node, a reverse path to the sender is established. These reverse paths are coupled with timers and maintained long enough for a returning CREP packet to be able to travel back to the sender.

AUTHENTICATION

Due to the ad hoc networks characteristics, the authentication protocols used for routing and data packet delivery in ad hoc networks should be lightweight and scalable. Asymmetric cryptography does not adapt well to ad hoc networks in that the processing required for asymmetric cryptography is very CPU intensive and the technique has been proved to be prohibitively insufficient in wireless ad hoc networks in terms of message overhead and computation complexity. Symmetric cryptography algorithms are fast. Nevertheless, they introduce complexity in key maintenance and exert difficulty in authentication for multicast or broadcast communications. Moreover, radio channels in wireless networks are more erroneous and lossy than the communication links in the Internet. With multiple receivers, there could be a high variance among the bandwidth and radio interference of different receivers, with high packet loss for the receivers with low bandwidth and high radio interference. To verify the correctness of a received packet, the method to put the e-signature on the packet by the public key is basic on an ad hoc network.

However, since a portable terminal used in ad hoc networks has relatively small calculation ability and a lot of calculation time is needed for giving and verification of e-signature. In [11], two methods were proposed to authenticate a consecutive packet efficiently by using a digital signature and a comparatively high-speed hash function. A lightweight authentication protocol that effectively and efficiently provides security properties such as authenticity and integrity for communicating neighbor nodes in MANETs was proposed in [10]. The protocol utilizes one-way hash chains to compute authentication keys, which not only eliminates the high performance overhead imposed by asymmetric cryptography (such as digital signatures), but also avoids the difficulty of key management introduced by secret paired symmetric key.

The protocol also used delayed key disclosure to prevent a malicious entity from forging packets with MACs with an already released key. The authentication protocol is lightweight, scalable and tolerant of packet loss. The performance analysis showed that the protocol incurs low overhead penalty and also achieves a tradeoff between security and performance.An interleaved message authentication scheme was proposed and evaluated in [12].

Interleaved authentication is used to restrain malicious nodes from manipulating messages by implicitly monitoring their actions. A node must share keys with all nodes within a radius of *k*-hops. A receiving node expects *k* authentication codes from different nodes in order to accept a message, if at least one of them does not match the message content, the message is rejected. This means that sets up to *k-1* collaborating malicious nodes are prevented. Figure 9 depicts a communication path with interleaved message authentication with *k*=2.

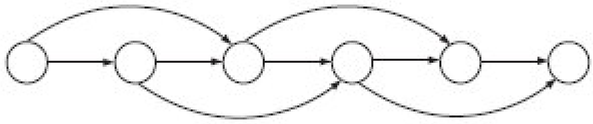

Figure9: A communication path with interleaved message authentication (k=2) [12]

CONCLUSIONS

In this paper we surveyed some of the security approaches used for securing ad hoc networks. These are approaches the threshold cryptography, certification authorities, reputation and trust, and authentication. There are still many challenges and research openings in the area of ad hoc networks security. Also despite the great effort that has been consumed in the study and design of certificate distribution schemes, there are still lots of openings and challenges in this area. For example there are no clear criteria for the CAs selection such as depending on their roles, power, reputation, age in the network, etc.

REFERENCES

[1] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11,pp. 612–613, November 1979.

[2] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13,no. 6, pp. 24–30, November/December 1999.

[3] P. Muppala, J. Thomas, and A. Abraham."QoS-Based Authentication Scheme for Ad Hoc Wireless Networks," itcc, pp. 709-714, International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume I, 2005.

[4] C. R. Davis, "A localized trust management scheme for ad hoc networks", Proceedings of the 3rd International Conference on Networking (ICN'04), pp. 671-675, March 2004.

[5] V. Shoup, "Practical Threshold Signatures", In Theory and Application of Cryptographic Techniques", pp 207–220, 2000.

[6] J. Kong, P. Zerfos, H. Luo, S. Lu, and L.Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks", In Proceedings of ICNP '01.

[7] S. Yi, and R. Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks", ICNP 2002, pp. 202-205.

[8] M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, and L. C. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks", INFOCOM 2004.

[9] A.Rachedi, and A.Benslimane, "Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks," icsnc, p. 72, International Conference on Systems and Networks Communication (ICSNC'06), 2006.

[10] B.Lu, U. Pooch, "A Lightweight Authentication Protocol for Mobile Ad Hoc Networks," itcc, pp. 546-551, International Conference on Information Technology: Coding and Computing (ITCC'05) – Volume II, 2005.

[11] F. Sato, H. Takahira, and T. Mizuno. "Message Authentication Scheme for Mobile Ad hoc Networks," icpads, pp. 50-56, 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.

[12] H.Vogt. "Increasing Attack Resiliency of Wireless Ad Hoc and Sensor Networks," icdcsw, pp. 179-184, Second International Workshop on Security in Distributed Computing Systems (SDCS) (ICDCSW'05), 2005.