Secure Cluster Based Routing Protocol Incorporating the Distributed PKI Mechanisms

GeneBeck Hahn*, DaeHun Nyang**, JooSeok Song*, Jae-il Lee*** and BaeHyo Park***
* Department of Computer Science, Yonsei University, Seoul, Korea
** Graduate School of Information Technology and Telecommunications, Inha University, Inchon, Korea
***Korea Information Security Agency
{gbhahn, jssong}@emerald.yonsei.ac.kr, nyang@inha.ac.kr, {jilee, parkbh}@kisa.or.kr

Abstract—**In this paper, we state a method of incorporating the distributed PKI(Public Key Infrastructure) mechanisms to the MANET(Mobile Ad Hoc Networks) routing protocol. For doing this, we assume that MANET regards the CBRP (Cluster Based Routing Protocol) as base routing protocol. By using the basic operations of CBRP and the distributed PKI mechanisms, our scheme efficiently finds a certificate chain and performs the secure routing. This means that by incorporating the distributed PKI mechanisms to the CBRP, our scheme can provide the procedure of certificate chain discovery for packet routing. Also, by signing the HELLO message, our scheme can provide the reliable exchange of authentic routing/topology information.**

I. INTRODUCTION

MANET paradigm relies on the collaborative and self-organizing operations of mobile nodes. Thus, the research issues in MANET have been focused on routing and a few of routing protocols have been proposed, particularly by IETF[1,3,4,5,7]. MANET does not assume a infrastructure such as routers and switching backbones, meaning that MANET does not depend on centralized security solutions and thus allows several security attacks to actively disrupt the routing protocol and disable communications. Thereby, a node must be prepared for the unexpected attacks from various malicious nodes. Recently, a few of protocols are proposed for the secure routing in MANET. The protocols are mentioned in the following articles[2,8,9]. Besides, we find a number of works introducing the concept of PKI to MANET [6,10]. However, according to our survey, there have been few researches mentioning the necessity for the setup of certificate chain in MANET where the distributed PKI is assumed. In our respect, the discovery of certificate chain is essential to provide the PKI certification services to the MANET nodes since a node must find a certificate chain for the trust relationship with communicating nodes that are multi hops away. Thus, we think that in MANET, it is meaningful to exploit the method of discovering the certificate chain.

The organization of this paper is as follows. In section II, we first describe the basics of CBRP. Then, in section III, we explain our scheme in detail and show a number of merits or security implications of our scheme. Finally, we conclude this paper and present future works in section IV.

II. CLUSTER BASED ROUTING PROTOCOL

The CBRP divides the nodes of MANET into a number of overlapping/disjoint 2 hop diameter clusters. For each cluster, a unique cluster head is elected to keep the cluster membership information representatively. Relying on the cluster architecture, the inter cluster routes can be found dynamically. The critical advantage of CBRP is that it can reduce the flooding traffics for route discovery phase and speeds up the process. Fundamentally, the CBRP keeps 3 data structures, i.e., the neighbor table, cluster adjacency table and 2 hop topology database. The neighbor table is used for the link or connectivity sensing and for the cluster formation. The CAT(Cluster Adjacency Table) stores the information about adjacent clusters and is updated through adjacent cluster discovery. The 2 hop topology database keeps a complete information about the network topology that is at most 2 hops away from itself[1].

Depending on the data structures, the CBRP can setup the cluster such that an organized ad hoc network can be formed. Besides, the CBRP allows a cluster to find all its bi-directionally linked clusters and performs the routing based on source routing. Since the CBRP uses the cluster hierarchy, the flooding traffics during the route discovery can be reduced. This means that only the cluster heads are flooded with the RREQ(Route Request) packet to find the source route. For future use, all routes obtained during the route discovery are stored in the route cache[1].

III. SECURE CLUSTER BASED ROUTING PROTOCOL

In this section, we show the secure cluster based routing protocol incorporating the distributed PKI mechanisms to the CBRP. Originally, our scheme resembles to the CBRP, indicating that our scheme inherits the operations for link status or connectivity sensing, cluster formation and route discovery from the CBRP. However, by using the concept of distributed PKI mechanisms, our scheme is tailored to find a reliable certificate chain for secure packet routing. More specifically, our scheme adopts the RSA threshold cryptography to provide the key management services to the nodes in a distributed fashion since assuming a trusted CA(Certificate Authority) is problematic in MANET. This is due to the fact that a CA, responsible for the security of entire network, is a vulnerable point of the network. In this sense, our scheme intends the benefits of distributed CA. Besides, our scheme guarantees the broadcast of reliable HELLO message by signing the HELLO message with the personal RSA private key of a node. The objective of this operation is to reliably exchange the authentic routing and topology information in the HELLO messages. Since the MANET routing can be affected by a few of misbehaving nodes, our scheme tries to ensure the secure distribution of HELLO message and allows a reliable neighbor discovery. In MANET, several malicious adversaries can disrupt the

0-7803-8271-4/04/$20.00 ©2004 IEEE

operations of CBRP by doing the attacks to actively replay, forge or corrupt the topology information. Also, they try to deface the routing information of benign nodes, or to exploit the protocol to mount the DOS attack. Thus, the secure exchange of authentic HELLO message can protect the topology or routing information from modifications while the message is broadcasted between nodes. In case that the genuine nodes receive the maliciously modified HELLO message, our scheme let the nodes discard the message and protect the CBRP from various failures, i.e., the packet dropping, alteration, modification, etc. Finally, our scheme can provide the procedure of certificate chain discovery after the PKI is successfully setup. This must be done to form the trust relationship among communicating nodes that are multi hops away and requires modifications to the route discovery of CBRP.

Now, we explain the detailed operations of our scheme. In our scheme, each node in a cluster stores his personal RSA public and private key pair. This means that a node knows the RSA public keys for all other nodes in the same cluster. This can be done by adding its public key to the HELLO message and broadcasts the resultant message. In addition, each node knows of the RSA public and partial private key pair of corresponding cluster. Specifically, the RSA private key of a cluster is divided into a number of shares and distributed to the nodes in the same cluster. By doing this, all nodes in each cluster can equally share the responsibility to generate the public key certificate for the requesting node. The RSA public key of a cluster is also appended to the HELLO message and broadcasted to the neighboring nodes. When the key setup is completed, the certificate generation is performed jointly by a number of nodes in each cluster. In more detail, for a node to obtain its certificate, a few of nodes in the same cluster generate partial certificates by using their own shares and send out the results to a requesting node. The requesting node then gathers the results and combines them to make a complete certificate. In this way, our scheme can setup an efficient public key infrastructure. Furthermore, by using the route discovery of CBRP, our scheme performs the certificate chain discovery for packet routing/forwarding. Compared with the security solutions for network authentication that primarily relies on the physically present, trusted CA, our scheme adopts the self-securing approach where a number of nodes in a cluster collaboratively serve as the virtual CA. Therefore, our scheme can effectively distribute the certification services to each cluster.

A. Data Structures

In addition to the data structures of CBRP, our scheme requires two data structures, i.e., the certificate cache and the CRL(Certificate Revocation List) table. The certificate cache maintains the certificate of a node sending RREQ to itself, meaning that the certificate of preceding hop node comprising the source route is maintained in the certificate cache of next hop node. Also, the certificate cache keeps the certificate of its communicating nodes. This indicates that the certificate of source is kept in the certificate cache of destination and the certificate of destination is stored in the certificate cache of source. The entries of a certificate cache contain the following:

- The ID of the node corresponding to the received certificate(s)
- The role of the node corresponding to the revoked certificate(s)
- The certificate(s) of the corresponding node

The certificate of a node is cleared from the certificate cache when the corresponding certificate is expired. Also, the CRL table maintains the information about the nodes with revoked certificate. The entries of CRL table contain the following:

- The ID of the node corresponding to the revoked certificate
- The role of the node corresponding to the revoked certificate
- The serial number of the revoked certificate

The certificates involved in the CRL table are those that are invalid but not expired. This means that a node needs not keep the certificates that are both invalid and expired and only stores the certificates which are invalid but not expired in its CRL table.

B. RSA Threshold Cryptography

The RSA threshold cryptography used on our scheme is based on Shamir's threshold secret sharing and the secret shares are distributed to the nodes in each cluster[11]. This can be done with the secret polynomial $f(x)$. If the degree of secret polynomial $f(x)$ is k-1, the k nodes of a cluster can recover the complete secret via Lagrange Interpolation. However, if the number of nodes in the cluster is less than k, the information for complete secret can not be obtained. In our scheme, the threshold k is the number of nodes in each cluster and will not be a large number.

C. Public Key Exchange

In our scheme, the HELLO message is augmented with its own public key and the public key of current cluster. Thus, a node can notify its own personal RSA public key to the adjacent nodes in the same cluster. Besides, a node can let the neighboring clusters know the public key of its own cluster. This means that since the HELLO packets are sent from a number of nodes which belong to the adjacent clusters via a few of gateway nodes, a cluster can know of the respective public keys of adjacent clusters. Basically, this refers to the feature of CBRP where a node can know of the topology which is at most 2 hops away by receiving the HELLO message. Based on the information, a cluster can successfully validate the certificates that are generated by adjacent clusters. This relationship is one of the most important features of our scheme.

D. Certificate Generation

After a cluster hierarchy is formed, a node in the cluster can request to obtain its public key certificate. As stated above, the certificate is generated by the coalition of a few of nodes in the same cluster and this can be done by using the RSA threshold cryptography. Since the other nodes in the each cluster maintain their own shares, they can jointly function as the virtual CA and provide the PKI services to the requesting node. The shares are obtained by dividing the RSA private key of corresponding cluster. In detail, for a node to obtain its own certificate, a number of nodes in a cluster generate the partial certificates by using their respective shares and send the results to a requesting node. The requesting node collects those results and combines them to derive a complete public key certificate. In this way, the PKI can be successfully set up on a cluster basis and the certification services can be provided to any nodes

in a cluster. The certificate is generated in the following cases.

- Whenever a node requests a certificate as a result of cluster formation
- Whenever a node requests a certificate as a result of movement into the new cluster
- Whenever a certificate is updated and reissued as a result of revocation

If a certificate is expired, it must be reissued to the node that owns the corresponding certificate and this is similar to the certificate generation. The only difference is that in this case, the node must present the valid certificate to get a new certificate, indicating that the expired certificate is sent to the nodes in the same cluster and verified by using the cluster public key. Based on the results of validation, a node can either obtain a new certificate or not. In detail, a requesting node can obtain a new certificate if the result of verification is legal. Otherwise, the node cannot obtain a new certificate.

Fig. 1 depicts the certificate generation of our scheme. As presented in Fig. 1, the member 1 requests a certificate service to the nodes in the same cluster. This can be sent directly to the adjacent nodes or pass through the cluster head to reach the nodes that are 2 hops away. When a few of nodes in the same cluster receive the request, they make partial certificates by signing the public key of requesting node with their own shares derived from the RSA private key of corresponding cluster. The results are sent back to the requesting node. After the requesting node receives the partial certificates from a few of nodes in the same cluster, it combines them to make a complete certificate.

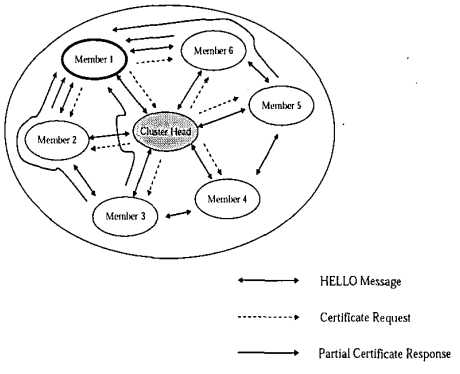

Fig. 1. Certificate Generation

E. *Certificate Chain Discovery*

Depending on the distributed architecture of CBRP, our scheme can reduce the flooding traffics to find the reliable certificate chain, meaning that our scheme can ensure the efficient/fast authentication, integrity and non repudiation. Now, we show the certificate chain discovery procedure in detail. The idea is to use the route discovery of CBRP to setup the certificate chain and thus our scheme inherits the benefits of CBRP. This indicates that the number of nodes that are disturbed are much less because only the cluster heads broadcast the RREQ to find a certificate chain. To establish the certificate chain to the destination, a source broadcasts a RREQ and its certificate. In the same way as the CBRP route discovery, the source sets the destination address to the IP address of destination. Also, the source fills the adjacent cluster head entries with the information about the neighboring cluster heads and the corresponding gateway nodes. All the information can be obtained from the CAT. Following figure shows the procedure of RREQ broadcast:

While sending the RREQ packet, the certificate cache of a node stores the certificate of the node broadcasting the RREQ to itself. This means that certificate of previous hop node comprising the source route is maintained in the certificate cache of next hop node. As described in the Fig. 2, while traversing the intermediate nodes, the certificate of a source remains unchanged till the RREQ reaches the destination. This indicates that the respective nodes verify the certificate of previous hop node and if validated, they substitute the certificate of previous node with their own certificates. Thereafter, the nodes send the resultant RREQ to the neighboring clusters. By doing this, the intermediate clusters can verify the RREQ from the neighboring cluster by using the public key of corresponding cluster. This is the first step of certificate chain discovery.

```
1.  Whenever a member node M receives RREQ and (source and previous node)' certificates, validate the
    certificate of previous node by using the corresponding public key
    If validated, record the certificate of previous node in its cache and continue;
        If the destination D is its neighbor, RREQ and (source and M)'s certificates are just uni-cast to D
        Else
            If M is specified as the Gateway Node [x],
            Uni-cast (relay) the RREQ and (source and M)'s certificates to Cluster Head [x]
        Else
            Discard the RREQ
    Else
        Discard the RREQ

2.  Whenever a cluster head C receives RREQ and (source and previous node)' certificates, validate the
    certificate of previous node by using the corresponding public key
    If validated, record the certificate of previous node in its cache and continue;
        2.1. If it has seen this RREQ before
                Discard it; Otherwise, continue
        2.2. Records its own address in Cluster Address list
        2.3. If the destination D is its neighbor or is 2-hop away
                Uni-cast RREQ and (source and C)'s certificates to D
            Else    for each bi-directionally linked cluster head CH in C's CAT
                        if CH is already in previous RREQ's Neighboring Cluster Head list,
                            skip
                        Else if CH is in Cluster Address list,
                            skip
                        Else
                            record CH entry in Neighboring Clusterhead/Gateway Node pair
                        Broadcast RREQ and (source and C)'s certificates
    Else
        Discard the RREQ
```

Fig. 2. Procedures of RREQ Broadcast

```
1.  Suppose cluster head C receives a RREP and (source, destination and previous node)'s certificates,
    validate the certificate of previous node by using the corresponding public key
    If validated, check if it can also validate the certificate of source.
        If cluster head C can, it digitally signs the {verification_ok} message and send it to the destination
        Else,
            1.1 It decrements Num1 by 1
                Cluster Address [Num1] is the neighboring cluster head that C should forward RREP to in
                order to reach S
            1.2 C tries to find out a gateway node X to Cluster Address [Num1] such that the Calculated
                Route [Num2] could reach X directly
                If it succeeds,
                    If C has an unexpired certificate of X,
                        send RREP and (source, destination and C)'s certificates to X
                    Else  discard the RREP
                Else  C increments Num2 by 1 and C records itself in Calculated Route [Num2]
    Else    discard the RREP
2.  Suppose member node M receives a RREP and (source, destination and previous node)'s certificates,
    validate the certificate of previous node by using the corresponding public key
    If validated, check if it can also validate the certificate of source
        If member node M can, it digitally signs the {verification_ok} message and send it to the destination
        Else,
            2.1. It increments Num2 by 1 and records itself in Calculated Route [Num2]
            2.2. If Cluster Address [Num1] is its Neighbor
                If M has an unexpired certificate of Cluster Address [Num1],
                        send RREP and (source, destination and M)'s certificates to it directly
                    Else    discard the RREP
                Else if Cluster Address [Num1] could be reached by X
                    If M has an unexpired certificate of X,
                        send RREP and (source, destination and M)'s certificates to X
                    Else    discard the RREP
    Else    discard the RREP
```

Fig. 3. Procedures of RREP Broadcast

When the destination receives a RREQ, it will have a complete path information from source to destination and

this can be obtained from the recorded route in the Cluster Address list of RREQ packet. Besides, the destination will have the certificate of source node since the certificate of source is sent out with the corresponding RREQ. By using the path information, the destination can forward a RREP and its own certificate to the source as the reply. Also, the destination sends out a query and the certificate of source to find a certificate chain to the source. While sending the RREP and the certificates of destination and source, the intermediate nodes calculate an optimized certificate chain by using the information in the Cluster Addresses list and put it into the Calculate Route field. Also, the intermediate nodes validate the certificate of previous hop node and if validated, the nodes substitute it with their certificates and send the resultant RREP to the adjacent cluster. By doing this, the intermediate nodes can verify the RREP from the adjacent cluster by using the public key of corresponding cluster and establish the certificate chain. While doing this procedure, the certificate of destination keeps unchanged. The detailed operations are described in the Fig. 3. This is the second step of certificate chain discovery. As a final step, when the source receives the RREP, it will have the certificate of destination and must validate the certificate. Thus, the source must perform the procedure of certificate chain discovery by sending out the query and certificate of destination to the destination.

F. *Certificate Revocation*

Certificate revocation can be performed in one of the following cases.

- Implicit Revocation : Whenever a certificate is expired
- Explicit Revocation : Whenever a node requires to reissue the certificate as a result of invalid user key binding

Similar to the procedure of certificate generation, the certificate revocation is done by the coalition of nodes in each cluster. This means that a number of nodes jointly perform the certificate revocation for a specific node. In detail, a node broadcasts a certificate revocation request to the nodes in the same cluster. The nodes receiving this update the entries to the CRL table and a number of nodes collaboratively revoke the certificate of requesting node. This is for the explicit revocation. After the certificate of a node is revoked, the result is sent out to its neighboring clusters and the destination that previously communicated with the source. For doing this, we use the information maintained in the route cache and introduce an additional control packet called certificate revocation message. By using the packet, our scheme allows the nodes in adjacent clusters and the destination node to successfully clear the corresponding certificate from their certificate cache. For the case of implicit revocation, the expired certificate is automatically erased from the certificate cache of a node. This is due to the fact that a node storing the certificates of other nodes knows the expiration period of corresponding certificates.

Some nice features of our scheme are summarized as follows. First, our scheme incorporates the distributed PKI mechanisms to the MANET CBRP. Thus, the certification services can be provided on cluster basis and the network overloads, i.e., the flooding traffics for a certificate chain discovery, can be critically reduced. Also, our scheme can operate in the frequently changing network topology and membership status. Also, by signing the HELLO message, our scheme enables the distribution of authentic topology information. By doing this, our scheme ensures the secure routing and thus our scheme is robust against a number of malicious attacks, i.e., DOS attack, IP Spoofing, message redirection, etc.

IV. CONCLUSION

In this article, we propose the security mechanisms for MANET based on the CBRP. In our protocol, we adopt the concept of distributed PKI and successfully distribute the role of CA to each cluster by threshold cryptography. This means that each node in a cluster holds its own secret share and several nodes in the same cluster collaboratively provide the certification services, i.e., certificate issuing, renewal and revocation. While providing the certification services, our scheme can scale to the large network and will adapt to the dynamic node mobility and membership change. In the centralized PKI mechanisms, a CA solely provides the certification services for the entire network and this inevitably results in the scalability problem as the size of network increases. Besides, the single CA may be a single point of failure from security aspects. Our scheme protocol successfully solves this problem by incorporating the distributed PKI mechanisms to CBRP and provides the fully distributed security solutions for MANET. Thereby, our scheme can provide the basic security functions like confidentiality, data integrity, authentication and non-repudiation and guarantees that the system security will not be compromised as long as a number of collaborative adversaries that successfully intrude to the system are less than the predefined threshold.

REFERENCES

[1] Mingliang Jiang, Jinyang Li, Y. C., "CBRP:Cluster Based Routing Protocol," *Internet Draft, MANET Working Group, draft-ietf-manet-ietf-spec-01.txt*, pp. 11–15, Tay, 14, August, 1999.

[2] Panagiotis Papadimitratos, Zygmunt J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," *Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks, Jan. 2003*

[3] E.. M. Royer, C. –K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications*, Apr. 1999, pp. 46-55.

[4] D. B. Johnson et al., "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," *IETF Internet Draft MANET Working Group, draft-ietf-manet-dsr-07.txt*, Feb. 2002.

[5] C. E. Perkins, E. M. Royer, S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," *Internet Draft MANET Working Group, draft-ietf-manet-aodv-10.txt*, Jan. 2002.

[6] Srdjan Capkun, Levente Buttyan, Jean Pierre Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," *IEEE Transactions of Mobile Computing*, Vol.2, No.1, Jan-March, 2003.

[7] L. Zhou, Z. Haas, "Securing Ad Hoc Networks", *IEEE Network*, Vol.13, No.6, pp.24-30, Nov. /Dec. 1999.

[8] C. E. Perkins, "Ad Hoc Networking,", *Addison Wesley Professional*, Dec. 2000.

[9] Aram Khalili, Jonathan Katz, William A. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks," *IEEE Proceedings of 2003 Symposium on Applications and Internet Workshops*

[10] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwe Lu, Lixia Zhang, "Providing Robust and ubiquitous Security Supports for Mobile Ad Hoc Networks", *IEEE Proc. ICNP*, pp.251-260, Nov. 2001.

[11] A. Shamir, "How to Share a Secret", Communications of the ACM, 22(11):612-613, 1979