International Journal of Soft Computing 9 (3): 151-155, 2014
ISSN: 1816-9503

Certificateless Routing Method for Mobile Ad Hoc Networks

[1]A. Rex Macedo Arokiaraj and [2]A. Shanmugam
[1]Anna University, Chennai, Tamil Nadu, India
[2]Bannari Amman Institute of Technology, Sathyamanaglam, Tamil Nadu, India

Abstract: Secure communication, an important aspect of any networking environment is an especially significant challenge in mobile ad hoc networks. Masquerading and eavesdropping are major threats to the security of wireless communications and mobile networks. The scheme proposed in this study describes the framework to solve the security threats by designing a certificateless based cryptography scheme. Certificateless Routing Method (CRM) as a combination of ad hoc node address and public key cryptography. CRM is a certificateless public key cryptography solution in that public keys of mobile nodes are directly derivable from their known Ad hoc node address plus some common information. Thus, it eliminates the need for certificate-based authenticated public-key distribution essential in conventional public-key management schemes. CRM is an efficient construction method of address-based public/private keys cryptography which not only ensures high-level authentication to node exchange information but also enables efficient network-wide secure key update via a single broadcast message. It also provides general information about how to choose the secret key sharing parameters used with public key cryptography to meet desirable levels of security and authentication. The advantages of CRM over existing certificate-based solutions are justified through extensive simulations. The proposed scheme CRM gives a new innovation towards more effective and efficient security design for MANETs.

Key words: Mobile ad hoc networks, security, authentication, public key management, certificateless routing

INTRODUCTION

A Mobile Ad Hoc Network (MANETs) is a group of mobile and wireless devices which communicates between them without the assistance of any infrastructure. The network is self-organized and is adaptive to topology changes arising from either mobility or link outages. The participating network nodes are equipped with radios that have limited communication range. In order to communicate with nodes outside their direct wireless transmission range, nodes forward packets for other nodes, resulting in multi-hop routes. The lack of infrastructure, shared wireless medium, node mobility, resource constraints of mobile devices, bandwidth-limited and error-prone channels and so on. In this proposed scheme, it deals with public/private key management, the foundation on which to drive the address based cryptography mechanism for MANETs security.

Literature review: Conventional key management techniques may either require trusted certificate server or not (Papadimitratos and Haas, 2002). The infrastructureless nature of MANETs prevents the use of server based protocols such as Kerberos (Neuman and Ts'o, 1994). Therefore, this study focus on discussing serverless and certificateless approaches. All the nodes are preload with a global symmetric key which is vulnerable to any point of compromise if any single node is compromised, the security of the entire network is collapsed. It lacks scalability because it is difficult to establish symmetric keys between existing nodes and newly joined nodes. Second, securely updating the overall symmetric keys in the network is a nontrivial. Last, it requires each node to store (N-1) keys (assume N nodes) which may represent a significant storage overhead in a large network. Symmetric-key techniques (Hu *et al*., 2003) are also given a commonly drawback for not supporting efficient authentication because each key is known to at least two nodes.

There has been a lot of literature on public-key management in MANETs (Zhou and Haas, 1999; Kong *et al*., 2001; Narasimha *et al*., 2003; Yi and Kravets, 2003; Bechler *et al*., 2004) for example. These schemes all depend on Certificate-Based Cryptography (CBC) which uses public-key certificates to authenticate public keys by binding public keys to the node ID. A main concern with CBC-based approaches is the need for certificate-based public-key distribution. One naive method is to preload each node with all the others public-key certificates prior to network deployment. This approach can neither scale

Corresponding Author: A. Rex Macedo Arokiaraj, Anna University, Chennai, Tamil Nadu, India

well with the increasing network size, nor handle key update in a secure and cost-effective way. Another approach of on-demand certificate retrieval ARAN (Sanzgiri *et al*., 2005) may cause both unfavorable communication latency and often tremendous communication overhead.

An efficient alternative to CBC, Id-Based Cryptography (IBC) (Shamir, 1984; Saxena *et al*., 2004) has been gaining momentum in recent years. It allows public keys to be derived from entities known identity information thus, eliminating the need for public key distribution and certificates. This nice feature has inspired a few IBC-based certificateless public-key management.

In this study, it finds the new solution for existing public key management; it is an address based cryptography key management scheme called CRM for special-purpose MANETs administered by all the nodes which are available in the network.

Construction method of address based public/private keys: In CRM, each node's public and private key is composed of a node address element and a network-wide common element. Common key elements enable very efficient network-wide public/private key updates via a single broadcast message. It also discuss efficient key agreement, public-key encryption, authentication based on such public/private and secret key distribution similarly to Khalili *et al*. (2003).

MATERIALS AND METHODS

CRM: This study illustrates the method of CRM. CRM uses the node address with certificateless cryptography to give the end to end authentication. Route invention in CRM is based on route invention packet from source node and route reply packet from destination node. The route packets are encrypted based on CRM. Only authorized nodes participate at each hop between source and the destination. Assume key generation is known by all authorized nodes.

Route invention: In Fig. 1, a simple ad hoc network when the first authorized node enters in the network is treated as a node N1 and consecutive authorized nodes are namely N2, N3 and N4 and so on based on its entry time in the network. Then, node N1-N4 updates No. of nodes available in the network.

Whenever, a node N1 desires to undertake secure communication with another node N4, the source node N1 generates its encrypted broadcast message (RDP) and send to the network and waits for a reply message from node N4:

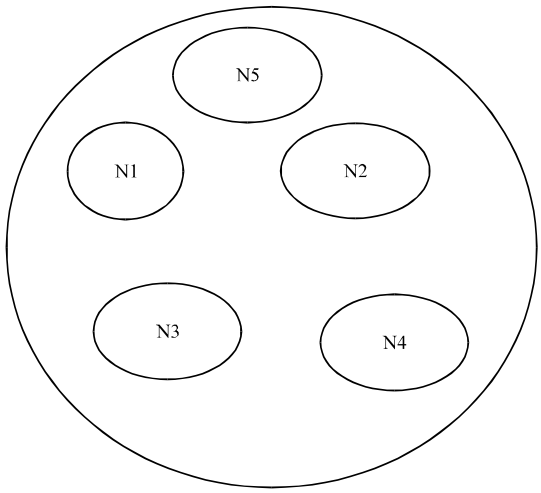

Fig. 1: A simple ad hoc network

Table 1: Notations

AD_{N1}	Address of node N1
E[ ]	Encryption
D[ ]	Decryption
EnT_{N1}	Entry time of node N1 in the network
CuT_{N1}	Current time of node N1
ExT_{N1}	Exit time of node in the network
PuK_{N1}	Public key of node N1
PrK_{N1}	Private key of node N1
RDP_{CN1}	Route discovery packet identifier of node N1
REP_{CN4}	Reply packet identifier from N4
C	Count no. of message generated
NN	No. of node in the network

$$N1 \rightarrow \text{broadcast: } E[RDP, AD_{N4}, [EnT_{N1}, CuT_{N1}, ExT_{N1}]] PrK_{N1} \quad (1)$$

In Table 1 the broadcast message includes a packet type identifier ("RDP"), the node destination address AD_{N4} and the combination of EnT_{N1}, CuT_{N1}, ExT_{N1} with node N1 private key PrK_{N1}. Note that the RDP_{CN1} is encrypted by the source the contents can not be viewed any unauthorized node. The purpose of the RDP_{CN1} is to uniquely identify the RDP coming from a source based on its C value. Each time performs route invention, it increases the RDP counts C. When a node receives an RDP message, it sets up a reverse path back to the source by recording the neighbor from which it received the RDP. This is in anticipation of eventually receiving a reply message that it will need to forward back to the source. The receiving node use sending node public key which it extracts the details to validate the authentication and verify that message has not expired. The receiving node also checks the C tuple to verify that it has not already processed this RDP, nodes do not forward messages with already-seen tuples. The receiving node encrypts the contents of the message, appends its own encryption scheme and forward broadcasts the message to each of its neighbors:

$$N3 \rightarrow \text{broadcast: } E[RDP, AD_{N4}, [EnT_{N1}, CuT_{N1}, ExT_{N1}] PrK_{N1}] PrK_{N3} \quad (2)$$

Let N3 be a neighbor that has received from the RDP broadcast which it subsequently rebroadcasts (Eq. 2) Upon receiving the RDP's neighbor validates the signatures for both the RDP initiator and the neighbor it received the RDP from using the private secret key of N3 in the RDP. Then, removes's signature, records as its predecessor, signs the contents of the message originally broadcast by and appends its own information. Then rebroadcasts the RDP. Each intermediate node along the path repeats the same steps as Eq. 2.

The encryption scheme prevents spoofing attacks that may alter the route or form loops. Let be a neighbor that has received from the RDP broadcast which it subsequently rebroadcasts the receiving the RDPs and the neighbor validates the information for both the RDP initiator and the neighbor it received the RDP from using the encryption in the RDP. Then removes its information, records as its predecessor, encrypt the contents of the message originally broadcast by and appends its own encrypted information. Then, rebroadcasts the RDP.

Route setup: Eventually, the message is received by the destination N4 who replies to the first RDP that it receives for a source and given information. The reverse steps to find the path From N4 to N1. First the REP message has sent to neighbor N3. That is the node address N4 is encrypted by private key of N4 (Eq. 3). Then, the REP message reaches to node N1 to find the actual path:

$$N4 \rightarrow N3: E[REP, AD_{N1}]PrK_{N4} \quad (3)$$

$$N3 \rightarrow N1: E[REP, AD_{N1}]PrK_{N4}PrK_{N3} \quad (4)$$

This RDP need not have traveled along the path with the least number of hops; the least-hop path may have a higher delay either legitimately or maliciously manifested. In this case, however, a non-congested, non least-hop path is likely to be preferred to a congested least-hop path because of the reduction in delay. Because RDPs do not contain a hop count or specific recorded source route and because messages are encrypted at each hop, malicious nodes have no opportunity to redirect traffic with the exploits. After receiving the RDP, the destination unicasts a reply (REP) packet back along the reverse path to the source. In between node verify its encrypted information and pass the REP message to its next node in a reverse direction. Each node checks the encrypted information of the previous count C as the REP is returned to the source.

Key revocation: An RSA based design which is currently the most prevalent public key cryptosystem. The system generates RSA key pair is denoted by as {PuK, PrK} where PrK is the system secret/private key and PuK is the system public key. PrK is used to encrypt for all the entities in the network. A encryption by the PrK_{can} be verified by the well known system public key PuK.

By address based cryptography scheme PrK is shared among nodes in the entire network. Each nodes holds a secret key which is used decrypt the route discovery message send by any one of nodes.

Besides the system key pair each entity N also maintains a personal RSA private and public key pair $\{PuK_N, PrK_N\}$. This pair of personal keys is used in end to end security to realize cipher key exchange, message privacy, message integrity and non-repudiation.

To encrypt the personal keys, each node N also holds in the format (Ni, PuK_{Ni}, EnT_{Ni}, CuT_{Ni}, ExT_{Ni}) which may read it is encrypted that the personal public key of node Ni is PuK_{Ni} from entry time of EnT_{Ni}, CuT_{Ni} and ExT_{Ni}. It is valid if it is encrypted by PrK_{Ni}.

RESULTS AND DISCUSSION

CRM is implemented in ns-2 simulator. The network simulator (ns-2) helps us to evaluate the communication aspects of the method such as route discovery and average route load in ad hoc wireless network.

CRM simulates a MANET with 30 nodes deployed in 700×700 square filed. Nodes initially are uniformly distributed and node mobility are emulated according to the random way point model. The simulation run for constant node speeds of 5, 10 and 15 m sec^{-1} with pause time to 5 sec and use 25 CBR sessions with random source and destination pairs trough the simulations. The average route discovery delay measures the average latency from the time of sending a RDP to receiving the route reply. Figure 2 shows CRM always exhibits shorter route discovery delay than ARAN and IBC.

The average route load measures the average amount of routing packet byte transmitted per delivery of data packet byte. Figure 3 shows ARAN and IBC higher than that of CRM for larger sizes of routing packets.

The data packet latencies for the four protocols are little difference as shown in Fig. 4. Although, ARAN has higher route acquisition latency, the number of route discoveries performed is a small fraction of the number of data packets delivered. Hence, the effect of the route acquisition latency on average end to end delay of data packets is significant in CRM. The processing of data packets is identical when using four protocols and so the average latency is nearly the same.

The average path length graphs are almost identical for four protocols as shown in Fig. 5. This indicates that even though CRM does not explicitly seek shortest paths,

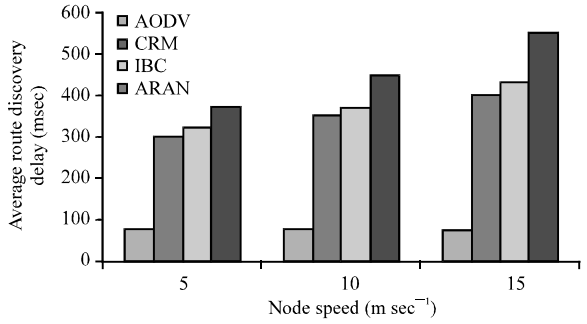

Fig. 2: Average route discovery delay

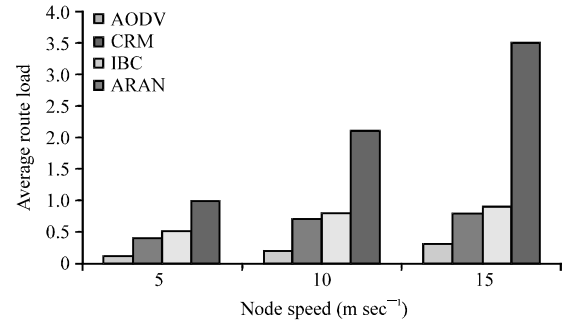

Fig. 3: Average route load

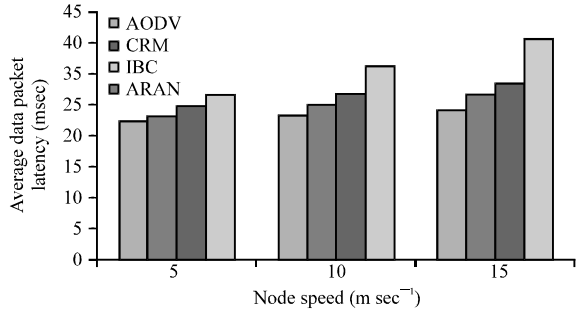

Fig. 4: End to end delay of data packets

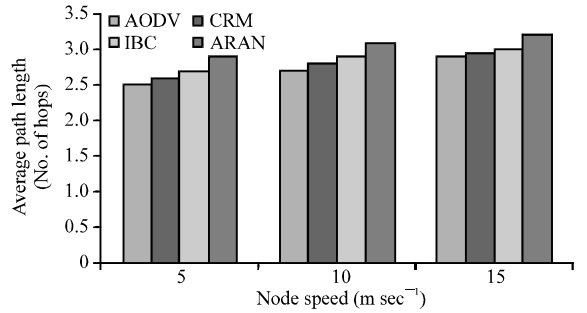

Fig. 5: Average path length

the first route discovery packet to reach the destination usually travels along the shortest path. Hence, CRM is as effective in finding the shortest path as AODV. It should be noted, however that in networks with significantly heavier data traffic loads, congestion could prevent the discovery of the shortest path with CRM. To summarize the CRM has significant advantages over ARAN and IBC in secure routing design.

CONCLUSION

In this study, CRM described a solution to security support in Mobile Ad Hoc Network (MANETs). The model has been motivates by three main factors: any security system is completely unbreakable. It seeks to maximize the service availability in each network environment: this is crucial to supporting ubiquitous service for mobile users. The solution has to fully decentralize to operate in a large network. To this end, researchers have addressed certificate issues including ARAN and IBC. The experiences in implementation and simulations have shown positive results for this approach CRM.

REFERENCES

Bechler, M., H.J. Hof, D. Kraft, F. Pahlke and L. Wolf, 2004. A cluster-based security architecture for ad hoc networks. Proceedings of the 23rd IEEE Computer and Communications Societies Annual Joint Conference, March 7-11, 2004, Hong Kong, China, pp: 2393-2403.

Hu, Y.C., D.B. Johnson and A. Perrig, 2003. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Int. J. Ad Hoc Networks, 1: 175-192.

Khalili, A., J. Katz and W. Arbaugh, 2003. Toward secure key distribution in truly ad hoc networks. Proceedings of the International Conference on Applications over Ad-Hoc Networks, January 27-31, 2003, IEEE Xplore, pp: 342-346.

Kong, J., P. Zerfos, H. Luo, S. Lu and L. Zhang, 2001. Providing robust and ubiquitous security support for mobile ad-hoc networks. Proceedings of the 9th International Conference on Network Protocols, November 14, 2001, Riverside, CA., USA., pp: 251-260.

Narasimha, M., G. Tsudik and J.H. Yi, 2003. On the utility of distributed cryptography in P2P and MANETs: The case of membership control. Proceedings of 11th International Conference on Network Protocols, November 4-7, 2003, IEEE Computer Society Washington, DC, USA., pp: 336-345.

Neuman, C. and T. Ts'o, 1994. Kerberos: An authentication service for computer networks. IEEE Commun. Maga., 32: 33-38.

Papadimitratos, P. and Z.J. Haas, 2002. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed System Modeling and Simulation Conference, January 27-31, 2002, San Antonio, USA., pp: 193-204.

Sanzgiri, K., D. LaFlamme, B. Dahill, B. Levine, C. Shields and E.M. Belding-Royer, 2005. Authenticated routing for ad hoc networks. IEEE J. Sel. Areas Commun., 23: 598-610.

Saxena, N., G. Tsudik and J.H. Yi, 2004. Identity-based access control for ad hoc groups. Proceedings of the International Conference Information Security and Cryptology, December 2-3, 2004, Seoul, Korea, pp: 362-379.

Shamir, A., 1984. Identity based cryptosystems and signature schemes. Proceedings of the Information Conference on Advances in Cryptology, August 19-22, 1984, Santa Barbara, California, pp: 47-53.

Yi, S. and R. Kravets, 2003. Moca: Mobile certificate authority for wireless ad hoc networks. Proceedings of Second Annual PKI Research Workshop, April 28-29, 2003, Gaithersburg MD., USA.

Zhou, L. and Z.J. Haas, 1999. Securing ad hoc networks. IEEE Network, 13: 24-30.