A Privacy Preserving Authentication Mechanism for Wireless Mesh Networks

Md. Shariful Islam, Md. Abdul Hamid and Choong Seon Hong
Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Yongin, Gyeonggi 449701, Korea

{sharif, hamid}@networking.khu.ac.kr and cshong@khu.ac.kr

Abstract

Due to its ease of deployment, low cost, self-configuring and self-healing capabilities, Wireless Mesh Networks (WMNs) have emerged as a key technology to be used in a wide scale applications in personal, local, campus, and metropolitan areas. Security and more specifically privacy is an important issue in this type of multi-hop WMN which has given a little attention in the research community. We focus on privacy compromise of a mesh client in a community mesh network that may lead an attacker to reveal mesh clients identity, his other profiles and gain information about mobility. In this paper, we have presented an authentication mechanism with the aid of blind signature that ensures a mesh client to anonymously authenticate itself with a nearby mesh router and thereby preserve identity privacy. We have also presented the security and performance analysis of the proposed scheme.

1. INTRODUCTION

Mesh networks are getting popular since lower cost, ease of use and fast in deployment making it a good choice for a wide variety of applications in personal, local, campus and metropolitan areas. Security and more specifically privacy is an important issue in this type of multihop WMN which has given a little attention in the research community.

In our proposal we consider a community Mesh Network [1] which is an open mesh structure where any client node can participate. Usually these types of networks are deployed by operators in a residential or commercial area for providing internet access via gateways.

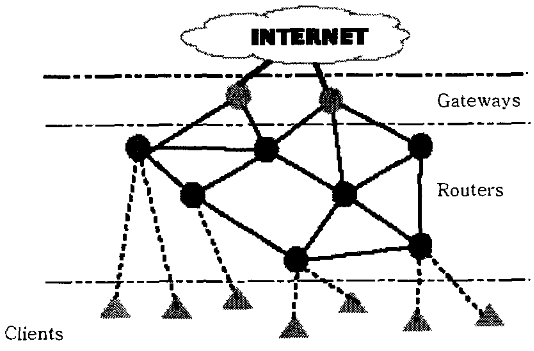

Figure 1: Abstract view of a 3-tier mesh network

Figure 1 gives an abstract view of such 3-tier architecture of a community mesh network. For a mobile client to get secure service (i.e. internet), first it has to perform a mutual authentication and key agreement with its neighboring Mesh Router it is attached with and the mesh routers along the path has to have an authentication and key agreement among them. Privacy is an important issue for multihop WMNs. A client's data may have to traverse through multiple intermediate routers to the gateway. So, it is always preferable for the mobile clients to remain anonymous to its neighboring mobile devices which makes it difficult for and an attacker to trace a mobile client's identity and whereabouts. We use two cryptographic primitive such as blind signature [2] and one-way hash functions [3] in our authentication mechanism to achieve anonymity and privacy.

The rest of the paper is organized as follows. In Section 2, we pointed out the security challenges that need to be addressed in Wireless Mesh Networks. Section 3 briefly discusses about the cryptographic primitives that we have used. In section 4, we describe the motivation which follows by section 5 that discusses the proposed mechanism. In section 6 we have analyzed the proposed protocol and finally we conclude in the section 7 with a direction to the future works.

This research was supported by the MIC, Korea, under the ITRC support program supervised by the IITA (IITA-2007-(C1090-0701-0016))

2. SECURITY CHALLENGES IN WMN

1. **Router-Client authentication:** A mesh router should authenticate a requesting client to prevent unauthorized network access. The client should also authenticate the mesh router to shun bogus mesh routers if attackers.
2. **Router-Client Key Agreement:** The mesh router and client should establish a shared key to encrypt and authenticate messages transmitted between them.
3. **Mutual authentication of Routers:** Mesh routers should authenticate each other by using the private key/ public key pair they have received from the WMN operator and can establishing a session key or long term shared keys.
4. **Integrity Verification:** This is done either end-to-end, or each intermediate mesh router, or both. [4]
5. **Privacy:** No entity other than the mesh client himself and the WMN operator should know the real identity and location of the mesh client.[5]

3. PRELIMINARIES

This section briefly describes the cryptographic primitives used in our scheme.

3.1 Blind Signature

The blind signature scheme [2] is a variation of the digital signature scheme in which the content of a message is disguised from its signer. Blind signature schemes can be implemented based on a number of well-known digital signature schemes, such as the Rivest-Shamir-Adleman (RSA) scheme. To produce a signature on a message, a user first "blinds" the message with a "blinding function" *f*, typically by combining it with a random "blinding factor" *k*, and then forwards the blinded message to the signer. The signer signs the blinded message using a standard signing algorithm, say $SA(m)$, which denotes the signature of A on m, and sends the result back to the user, who then "unblinds" it with an "unblinding function" g to obtain the signer's signature on the original message. The algorithm is designed such that $g(SA(f(m))) = SA(m)$. Blind signature schemes find a great deal of use in applications where sender privacy is important.

3.2 One-way Hash

One-way hash function h is a powerful yet computationally efficient cryptographic tool, which takes a message of arbitrary size as its input and outputs a fixed string of digits. "One way" means that it is computationally infeasible to derive original input from the output.

4. MOTIVATION

Communication in a wireless mesh network occurs mainly between mesh clients to wireless gateways and vice versa. Figure2 shows a general communication scenario that we will consider when describing our protocol. So, when a mesh client (MC) wants to send or receive some data it must have to authenticate itself with the nearest Mesh Router (MR), in this case MR_1, because MC is within the transmission range of the MR_1, and relies on that router to get service and data generated or received by the MC must go through all intermediate routers (MR_1, MR_2, MR_3) in a hop by hop fashion.

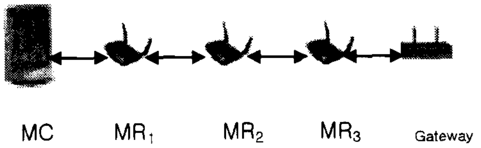

Figure 2: Communication model of mesh network

First consider the case of mutual authentication among the network nodes (i.e. mesh routers and gateways) that form the infrastructure. All the mesh routers are assigned certified private key/ public key pairs from the WMN operator when the network is established. So, these nodes can mutually authenticate each other using the private/public key pair and establish pair-wise secret keys to be used to secure transmission of data between neighboring nodes [4].

Some works have done addressing the location privacy and traffic privacy issues in WMN [6][7][8]. But, our goal is to achieve the anonymity and privacy of the mesh client (MC) so that no other entity in the network able to know about the identity, user profile, mobility and other whereabouts of the user. So, the mesh client (MC) needs to authenticate itself to the mesh router (MR) in a way such that it will not reveal any information regarding its identity.

5. PROPOSED MECHANISM

Our proposal considers the network access security where a Mesh Client (MC) needs to authenticate itself with a Mesh Router (MR) within the transmission range. We assume that any broadcast messages from the mesh router will receive by the mesh client in a single hop and a mesh client can reach a mesh router in a single hop. We also assume that the WMN operator acts as an offline trusted third party and issues key pairs (public/private keys) and public key certificates to MRs and MCs before deployment.

The protocol works in two phases. First, the mesh client (MC) generates some credentials and then makes these credentials anonymous [9] by signed it blindly by the signer (i.e. MR). The credentials and the signature on it act as a verifiable authenticator. This works in the following steps:

(M1) MR → * : Pub_{MR}, $Cert_{MR}$, $\{t1\}Priv_{MR}$
(M2) MC→ MR : $C_{ID} = \{n1\}_{PubMR}$ x C
(M3) MR→MC : $C_S = \{C_{ID}\}_{PrivMR}$

A mesh router periodically broadcasts beacon messages that contain its public key Pub_{MR} along with its certificate signed by the private key of the WMN operator. It also generates a fresh timestamp t1 and signed it with its private key $Priv_{MR}$ to defend against message replay attack [5]. The mesh clients MCs within the transmission range of the MR will receive this beacon message (M1). After receiving (M1), the mesh client (MC) first verifies the certificate of the MR by using the public key of the WMN operator. It then generate two nonce n1 and n2 and signs its own ID along with the fresh nonce n2 as : {n2,ID}privMC. It then create a credential C using a one-way hash [3] as C = h(n2, ID, $\{n2, ID\}_{privMC}$) and blinds the credential C using the nonce n1 encrypted under public key of the mesh router as $C_{ID} = \{n1\}_{PubMR}$ x C and sends it to the mesh router MR in message (M2). After receiving (M2), MR signs C_{ID} with its private key PrivMR as $C_S = \{C_{ID}\}_{PrivMR}$ = n1 x $\{C_{ID}\}_{PrivMR}$ and returns the signed credential back to the mesh client in message (M3). Note that the signer here has no knowledge of what it is signing. Once the signed credential is returned to the mesh client, the computation of C_S/ n1 results in a valid signature on C_{ID} due to the property of blind signature [2]. So, now the mesh client holds a verifiable credential and its signature that acts as an authenticator.

After execution of this phase, both the mesh router and client share a credential C_{ID}, which the router can distribute among other mesh router under the control of same WMN operator. So, that whenever a user moves to the vicinity of another router, it can authenticate itself with that router using the same credential it produces in the initial phase.

At the second phase, whenever it wants to get service, it uses the credentials to authenticate itself with the MR and establish a fresh session key for secure data transmission. This works in the following steps:
(M4): MC→ MR: $\{N_A, C_{ID}\}_{PubMR}$
(M5): MR→ MC: N_B,$\{N_A\}K_{MR-MC}$
(M6): MC→ MR: N_B, N_A, $\{m\}K_{MR-MC}$

In message (M4), the mesh client generates a fresh nonce N_A and encrypts it along with the authorized credential it produced in the first phase with the public key Pub_{MR} of the mesh router for authentication and sends it to the mesh router MR. After receiving (M4), the mesh router decrypts N_A and C_{ID} with its private key $Priv_{MR}$ and verifies the credential C_{ID}. Now that the mobile client is authenticated, both the mesh router and client will produce a session key. First, the mesh router MR generates a nonce N_B and creates a session key as $K_{MR-KC} = h(C_{ID},N_A,N_B)$.

In message (M5), it sends the new nonce N_B with nonce N_A encrypted under the new session key K_{MR-KC}. After receiving (M5), the mobile client create the session key as $K_{MR-KC} = h(C_{ID},N_A,N_B)$, decrypts and verifies N_A and C_{ID}. In message (M6), it sends both the nonce values and encrypts a message using the session key just created. The mesh router can now decrypt the message with the session key. So, both the communicating parties ascertain that they are using a fresh session key.

6. ANALYSIS OF THE PROPOSED SCHEME

The use of blind signature ensures the mesh client to authenticate anonymously without disclosing any other information. The user creates a credential and makes it signed from the mesh router (message M2 and M3 in Section 5). Since the blind signature technique is used, the signing party can not know anything about what it signs. As the credential and its signature are used for authentication, user *privacy* is preserved.

Through message M1 (Section 5) a mesh router authenticates itself through its public key certificate and by showing knowledge of corresponding private key. *Mutual authentication* for mesh router and mesh client is described in Section 5 using message M4, M5 and M6.

Confidentiality and *integrity* can be achieved using symmetric key encryption and Message Authentication Code (MAC). Both communicating entities can use the fresh session key to accomplish this using message M5 and M6 in Section 5.

We measure the *communication overhead* by the number of message transmissions required between router-router and router-client authentication and key agreement (AKA). As show in Table I, in router-clients AKA, a router needs 1 message transmission while a client needs 2 messages. The proposed scheme is highly efficient as 2 messages are the minimum number for any authenticated key establishment protocol.

TABLE I

COMMUNICATION OVERHEAD(# of msg required)

		Router-Client AKA
Ours	MR	1
	MC	2
[5]	MR	2
	MC	1

Table II shows that most of the operations performed by a mesh client are hash and symmetric cryptographic functions, which are computationally feasible for a mesh client and only 1 public key operation per session is required. On the other hand routers also engaged with only two public key operations (one for decryption and another for signature verification) and else are hash and symmetric key operations. So, from the *computational overhead* point of view this is an efficient protocol.

TABLE I

COMMUNICATION OVERHEAD(# of operations required)

	Public Key	Sig. Verification	Nonce	Hash	Symm. Key
Ours	1	1	1	1	2
	1	0	1	1	2
[5]	2	1	1	2	1
	1	1	1	2	1

Both communication and computation overhead of our scheme are compared with that of [5] as shown in Table I and Table II. The number of message required for client- router AKA is same in [5] as ours. Table II shows that our scheme has less computation overhead than [5] as it requires lesser public key and hash operations. Moreover, we have shown privacy preserving authentication which was not the case with [5].

7. CONCLUSION AND FUTURE WORKS

In this paper we have introduced the requirement of anonymity and privacy in WMN and proposed a privacy preserving authentication technique with the aid of using blind signature. We have shown that our mechanism ensure anonymity and privacy of the mesh client. It also assures mutual authentication among mesh routers and client. In future, we will focus on the case of a roaming mesh client of a different operator that wants to authenticate anonymously in a visiting mesh network.

8. REFERENCES

[1] I. F. Akyildiz, X. Wang and W. Wang, "*Wireless Mesh Network: A Survey*", in Computer Networks and ISDN Systems, Volume 47, Issue 4, March 2005.

[2] David Chaum, "*Blind signatures for untraceable payments*", in Advances in Cryptology-CRYPTO'82, pages 199-203, 1983.

[3] R. Rivest, "*The MD5 message digest algorithms*", IETF RFC 1321,1992.

[4] B. Salem and J-P Hubaux, "*Securing Wireless Mesh Networks*", in IEEE Wireless Communication, Volume 13, Issue 2, April 2006 pp. 50 - 55.

[5]Y. Zhang and Y. Fang, "*ARSA: An attack resilient security architecture for multihop wireless mesh networks*", IEEE Journal on Selected Areas in Communication, Vol.24 No.10, October,2006.

[6] X.Wu , N. Li, "*Achieving privacy in Mesh Networks*", in proceedings if SASN'06, pp- 13-22, October 30,2006.

[7] W. Taojun, X. Yuan and Y.Cui, "*Preserving traffic privacy in Wireless Mesh Networks*", in prod of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06).

[8] H. Chun-Yih and H.J.Wang, "*A framework for location privacy in Wireless Networks*", in proc of ACM SIGCOMM Asia Workshop, 2005.

[9]J. Camenisch and A. Lysyanskaya. "*An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation*", In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2001), volume 2045 of Lecture Notes in Computer Science, pages 93-118. Springer, 2001.