Preserving Identity Privacy in Wireless Mesh Networks

†Md. Shariful Islam, †Md. Abdul Hamid, †Choong Seon Hong and ‡Beom-Hwan Chang

†Department of Computer Engineering, Kyung Hee University

‡Electronics and Telecommunications Research Institute

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

***Abstract*— Wireless mesh network (WMN) has emerged as a key technology for a numerous number of applications because of its ease of deployment, low cost and flexibility of use. WMN infrastructure is a multihop network where mostly the nodes are static in nature. Preserving identity privacy is an important issue in this type of multihop WMN which has been given a little attention in the research community. Compromising privacy may lead an attacker to reveal user's identity, his profiles and gain information about mobility. In this paper, we present an anonymous authentication scheme between mesh client and mesh router for preserving identity privacy and security in data communication in WMN. We have also shown the security and performance analysis of the proposed scheme.**

I. 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. Privacy and authentication are important security issues in this type of multihop wireless mesh network (WMN) which has been given a little attention in the research community. In WMN, all the traffic from a mesh node usually goes through a gateway router. In order to get a service a mesh client needs to authenticate itself first, but, if this authentication procedure reveals the identity of a mesh client, then it actually compromises the privacy of the client participating in the communication. A mesh node's behaviour can be easily traced due to wireless channel, multi-hop nature, and the fact that converge traffic pattern goes through the gateway router. For preserving privacy, it is highly required that the mesh node should be anonymous.

In contrast to traditional networks mobile wireless networks including WMNs extend the concept of privacy from identity-protection, known as sender and receiver-anonymity, to location-privacy and motions-pattern-privacy of communicating entities [13]. In this context, mobility implies additional threats to privacy by uncovering the geographical location of nodes as well as their motion.

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. Fig. 1 gives an abstract view of such 3-tier architecture of a community mesh network. In the lower tier, we have the mesh clients that are usually mobile though some are static. Wireless Mesh routers in tier-2 form the actual wireless backbone of the mesh network, which we refer as infrastructure network. Mesh routers are powerful static wireless devices with single or multiples radios. Routers are infact connected to the internet through some gateways or WHS (Wireless Hot Spots). So, most of the traffic in this type of networks goes through the gateway.

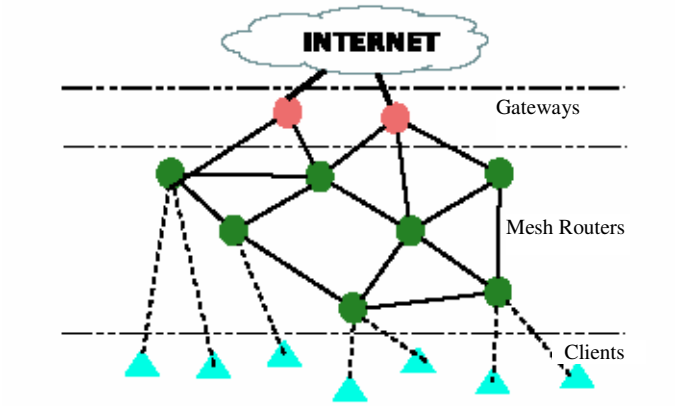

Fig. 1 An abstract view of a 3-tier Mesh Network.

For a mobile client to get secure service (i.e., internet), first it has to perform a mutual authentication and key agreement with its neighbouring 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 make it difficult for an attacker to trace a mobile client's identity and whereabouts. We use Chaums blind signature [2] in our authentication mechanism to achieve anonymity and privacy.

The rest of the paper is organized as follows. Section II discusses the related works. In Section III, we point out the security challenges that need to be addressed in Wireless Mesh Networks. Section IV briefly discusses about the cryptographic primitives that we have used. In Section V, we describe the motivation followed by Section VI that discusses the proposed mechanism. In section VII, we have analyzed the

This work was supported by the IT R&D program of MIC/IITA. [2007-S022-01,The Development of Smart Monitoring and Tracing System against Cyber-attack in All-IP Network]

proposed scheme and finally we conclude in Section VIII with a direction to the future works

II. Related Works

Wireless mesh network (WMN) represents a paradigm shift away from the rigid, long-lead planning and implementation of the wired backbone, and toward a real-time plug-and-play deployment model that is up to the challenges of today's rapidly-changing connectivity environment. Security is an important issue in multi-hop WMN and not much research works are done till now in area of WMN security. In [4], the authors have identified the operations to be secured in WMM as Corrupted TAPs, routing and fairness, and proposed some solutions to secure the operations. However, they ignored the class of attacks on mesh clients and behaviour of a malicious node. Zhang et al. in [5] have come up with an attack resilient security architecture for multihop wireless mesh networks. They have modelled WMN architecture as credit card based e-commerce system and showed that a mesh client need not to be bound to a specific WMN operator, can get ubiquitous network access by a universal pass issued by a third-party broker. They used identity-based cryptosystem for authentication and key agreement between mesh clients and routers. A framework is presented in [8] for achieving location privacy in wireless network.

In [11], the authors have shown an effective way to model a node-capture attack in multihop WMN by formulating it as an integer-linear programming minimization problem. They claim that privacy-preserving key establishment protocols can help to prevent minimum cost node capture attack. In [6], the authors have identified that the mesh network is vulnerable to privacy attacks because of the open medium characteristics of the wireless channel, its limited size and fixed topology. They propose an Onion routing algorithm that protects the routing information from the attackers. The authors have focused on the traffic privacy by proposing a penalty based routing algorithm in [7]. But, they used source routing scheme for their protocol. They have ignored how to deal with identity privacy and not mentioned how authentication and key agreement are performed between mesh nodes. We focus on anonymous authentication between client and router which actually preserves the identity privacy for mesh clients.

Other than WMNs, Privacy issue has been studied in multihop wireless networks like ad hoc network. Kong et al in [15] have proposed an untraceable anonymous on-demand routing protocol for ad hoc networks. In [16], a neighbourhood authentication protocol has been proposed that allows neighbouring nodes to authenticate each other without revealing their identities. As destination ID need to be revealed for route discovery, only conditional anonymity is achieved for destination.

III. Security Requirements

The security requirements for a mesh network can be categorised into the following three broad criteria as [5]:

Infrastructure Security: A mesh infrastructure is the wireless backbone network consists of the mesh routers and the WHS(Wireless Hot Spot) or Gateway. Infrastructure security deals with the security of signaling and data traffic transmitted over the infrastructure. As these intermediates nodes are typically stationary and are within the full control of the WMN operator, it is easy to achieve infrastructure security.

Network Access Security: Deals with communication security between a mesh client and a router. We will mainly focus on network access security in this paper.

Application Security: Mesh clients data applications can be secured with the help of using higher layer mechanisms like IPSec, TLS or VPNs

We have considered the following security requirements that need to be fulfilled for secure communication of data in wireless mesh network.

1) Router-Router AKA: This is the part of infrastructure security which requires that neighboring intermediate routers/WHS should mutually authenticate each other and establish a session key or long term shared key.

2) 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 check whether these routers are legitimate or not.

2) Router-Client Key Agreement: The mesh router and client should establish a shared session key to encrypt 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.

5) Privacy: Privacy is a very important security requirement and the main focus in our paper. A client should not reveal its identity while authenticating itself to a router. No entity other than the mesh client himself and the WMN operator should know the real identity and location of the mesh client. Otherwise they can be a victim of privacy attack

IV. Preliminaries

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

A. Blinding

A blind signature is a special form of digital signature [2]. Just as in any digital signature scheme, only signers can create blind signatures using their private keys, while anyone can verify a blind signature using the public key of the signers. Unlike a normal digital signature scheme, however, the signer does not learn which messages he is actually signing. Moreover, the signer does not know which blind signatures he is actually creating. Creating a blind signature for a message involves two parties, which we call the signer and the receiver. The receiver only needs to know the public key, while the signer knows both the private key and the public key. An important example of a blind signature scheme is David Chaum's Blind Signature Protocol for the RSA cryptosystem.

B. Chaum's Blind Signature Protocol:

This blind signature protocol is based on the RSA digital signature algorithm [2]. Assume that the receiver wants to get a signature on a message m that corresponds to an integer between 0 and n, Chaum's Blind Signature Protocol then consists of the following three steps:

Blinding: The receiver picks a blinding factor r, which is a random integer between 0 and n, and computes the value:

$m' = m \times r^e \bmod n$

The receiver sends m' to the signer. The m' is the message to be signed by the signer and not the original message m.

Signing: The signer uses its private key d to compute the value:

$s' = (m')^d \bmod n$.

The signer returns s' to the receiver.

Un-blinding: The receiver extracts the signature:

$s = s'/r \bmod n$

So, the receiver ends up with a pair (m,s) satisfying the equation $s = m^e \bmod n$. This is exactly the verification relation for standard RSA signatures. It should be noted that the signer does not know which message m has actually been signed. Because of the random blinding factor r, the message m' is statistically independent of the actual message m. Thus, blind signature schemes find a great deal of use in applications where sender privacy is important.

V. Motivation

Communication in a wireless mesh network occurs mainly between mesh clients to wireless gateways and vice versa. Fig. 2 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 MR1, because MC is within the transmission range of the MR1, and relies on that router to get service. Data generated or received by the MC must go through all intermediate routers (MR1, MR2 and MR3) in a hop by hop fashion.

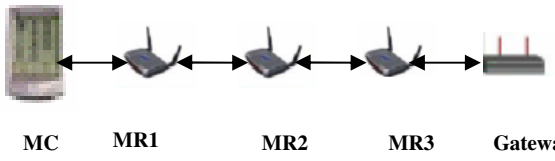

Fig. 2 Communication model of a mesh network

As data are traversed in a multihop fashion and some nodes act as forwarder, a malicious attacker can trace the behaviour of a mesh client, like who is accessing what kind of data? So, in this kind of network architecture it is always preferable for the client to remain anonymous by hiding its identity, otherwise, it can be a victim of privacy attack. So, the main motivation is that no other entity other than the Wireless Mesh Network operator should know the real identity and location of the mesh client.

VI. Proposed Scheme

Our proposal considers the network access security where a MC needs to authenticate itself with a MR within its transmission range. We assume that any broadcast message from the mesh router will receive by the mesh clients 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. Mesh routers in our proposal will act as authentication servers. Mesh clients will produce credentials and make those credentials anonymous through blind signing by the MRs. Afterwards, mesh clients use the authorized credentials to establish a shared secret and mutual authentication with the mesh routers.

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 neighbouring nodes.

We assume that these devices that form the infrastructure are energy rich and can use asymmetric cryptography to perform key agreement and authentication. Suppose two mesh routers A and B have their secret keys x_A and x_B. So, they can establish a common secret key K_{AB} using well-known Diffie-Hellman scheme [12] as follows. Let, p be a large prime and α be a primitive element mod p, both known to A and B.

(M1) A→B : $y_A = \alpha^{xA} \bmod p$
(M2) B→A: $y_B = \alpha^{xB} \bmod p$
(M3) A and B computes: $K_{AB} = \alpha^{xAxB} \bmod p$
(M4) A→B: $\{C\}\ K_{AB}$
(M5) B→A: $\{C+1\}\ K_{AB}$

As shown above, both A and B establishes a common secret. They can now mutually authenticate each other using a challenge encrypted with the common secret key. In M4, A sends a challenge C encrypted with K_{AB} to B. B can now decrypt the challenge C and response with (C+1) encrypted under K_{AB} and sends it to A. Now, both A and B are mutually authenticated and ascertain that they have a secret key K_{AB} shared between them, which can be used for secure communication between A and B. In this way, all the intermediate routers can mutually authenticate each other.

Now, we consider the case of authentication and key agreement between a mesh client and a router. First, the 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:

(A1) MR → * : Pub_{MR}, $Cert_{MR}$, $\{t1\}_{PrivMR}$
(A2) MC→ MR : $C_{ID} = C * \{r\}_{PubMR}$
(A3) 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. 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 (A1). After receiving (A1), the MC first verifies the certificate of the MR by using the public key of the WMN operator. It then generates a nonce n1 and signs its own ID along with the fresh nonce n1 as: $\{n1, ID\}_{privMC}$. It then creates a credential C using a one-way hash [3] as $C = h(n1, ID, \{n1, ID\}_{privMC})$. As the credential includes a signature by the client, it ensures the non-repudiation that no other client could produce the same credential. Now , it chooses a blinding factor r, which is a random integer between 0 and n, where n is the RSA modulus and blinds the credential C using the blinding factor r encrypted under public key of the mesh router as $C_{ID} = C \times \{r\}_{PubMR}$ and sends it to the mesh router MR in message (A2). After receiving (A2), MR signs C_{ID} with its private key $Priv_{MR}$ as $C_S = \{C_{ID}\}_{PrivMR} = r \times \{C\}_{PrivMR}$ and returns the signed anonymous credential back to the mesh client in message (A3). 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 / r results in a valid signature on C as $C' = \{C\}_{PrivMR}$ due to the property of blind signature as described in Section II.

So, now the mesh client holds an authorized credential (C) and its verifiable signature (C') that acts as an authenticator. The mesh client uses this pair (C, C') for authentication and key agreement with the mesh routers they are attached with. Note that, the signature on a credential can be verified by anyone who knows the public key of the MR that signed the credential. We assume that all mesh routers under a WMN operator knows each others public key. So, that whenever a mesh client moves to the vicinity of another router of the same WMN operator, 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 establishes a fresh session key for secure data transmission. This works in the following steps:

(A4): MC→ MR: $\{N_A, C, C'\}_{PubMR}$
(A5): MR→ MC: $N_B, \{N_A\}K_{MR\text{-}MC}$
(A6): MC→ MR: $N_B, N_A, \{m\}K_{MR\text{-}MC}$

In message (A4), the mesh client generates a fresh nonce N_A and encrypts it along with the authorized credential and the signature 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 (A4), the mesh router decrypts N_A and C with its private key $Priv_{MR}$ and verifies the signature using the corresponding public key.

Now that the mobile client is authenticated, both the mesh router and client will produce a session key. A well known hashing algorithm Secure Hash Algorithm (SHA-1)[14] is used for creating the session key. SHA is secure because it is computationally infeasible to find a message that corresponds to a given message digest, or find two different messages that produce the same message digest.

First, the mesh router MR generates a nonce N_B and creates a session key as $K_{MR\text{-}MC} = SHA(C,N_A,N_B)$. In message (A5), it sends the new nonce N_B with nonce N_A encrypted under the new session key $K_{MR\text{-}MC}$. After receiving (A5), the mobile client create the session key as $K_{MR\text{-}MC} = SHA(C,N_A,N_B)$, decrypts and verifies N_A and C. In message (A6), 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.

VII. ANALYSIS OF THE PROPOSED SCHEME

In this section we present security and performance analysis for the proposed scheme.

A. Security Analysis

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 A2 and A3 in Section VI). 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. Moreover, authorized credentials are never transmitted in plain text and always combined with fresh nonce which makes it impossible for an outsider to claim a session to a particular user. So, user transaction profiles are untraceable and replay attack is protected.

Through message A1 (Section VI) 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 VI using message A4, A5 and A6. Also, router-router key agreement and authentication are shown in Section VI through messages M1-M5 using Diffie-Hellman and challenge-response [17] technique respectively.

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 A5 and A6 in Section VI.

The correctness of the protocol means that after execution, both the communicating parties will have a belief that they share a fresh session key. This can be verified using a formal logic [10] widely used to reason about beliefs, encryption and protocols. Suppose two communicating entities A and B have a shared secret S and produced nonce N_a and N_b. From A's viewpoint B creates the session key K_{AB} which is determined by N_b. Now, after getting N_b, A also produces the session key K_{AB} and sends B a message encrypted under the fresh key. If B can decrypt the message, then both are assured that they have a fresh session key.

B. Performance Analysis

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

TABLE I
COMMUNICATION OVERHEAD (# OF MESSAGES REQUIRED)

		Router-router AKA	Router-client AKA
Ours	MR	2	1
	MC	0	2
[5]	MR	-	2
	MC	-	1

Computation overhead is measured in terms of the number of operations required for authentication. 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 (message A4 in Section VI) per session, is required. On the other hand a mesh router also engaged with only two public key operations (one for decryption and another for signature verification) and else are hash and symmetric key operations, which is also not a burden on the routers those are assumed to be computationally rich. So, from the computational overhead point of view this is an efficient protocol.

TABLE III
COMPUTATION OVERHEAD (# OF OPERATIONS REQUIRED)

		Public key	Sig. Verification	Nonce	Hash	Symmetric key
Ours	MR	1	1	1	1	2
	MC	1	0	1	1	2
[5]	MR	2	1	1	2	1
	MC	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. But, [5] does not consider intermediate router-router AKA. 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].

VIII. 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 blind signature technique. We have shown that our mechanism ensures identity privacy of the mesh client in a community mesh network. It also assures mutual authentication among mesh routers and clients. In future, we plan to develop an authentication mechanism for intermediate clients if a router is multihop away from the communicating client. We also intend to focus on the case of a roaming mesh client of a different operator that wants to authenticate anonymously in a visiting mesh network.

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 proc 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.

[10] M.Burrows, M. Abadi and R. Needham, "*A logic of Authentication*," in Proc. Of Royal Soc. London,1989, vol. 426, pp.233-271.

[11] P. Tague, R.Poovendran "*Modeling node capture attacks in multi-hop wireless networks*," Ad Hoc Networks, vol. 5 issue 6, August 2007. pp. 801- 814

[12] W. Diffie and M. E. Hellman, "*New Directions in Cryptography*," IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644-654.

[13] X. Hong, J. Kong, M. Gerla, "*Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks*," Special Issue on Wireless Network Security, Wiley Interscience Press (2006).

[14] "*Secure Hash Standard*," Federal Information Processing Standards Publication 180-1 April 17, 1995.

[15] J.Kong and X. Hong, "*ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ah-Hoc Networks*," in proceedings of ACM international Symposium on Mobile Ad Hoc Networking and Computing, June 2003.

[16] Y. Zhang, W.Liu and W.Luo, "*Anonymous Communication in Mobile Ad Hoc Networks*," in proceedings of INFOCOM, 2005.

[17] A. Menezes, P. van Oorschot, and S. Vanston, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1996