An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks

Sharad Kumar Verma[1], **Dr. D.B. Ojha**[2]

[1]Research Scholar, Department of CSE, Mewar University, Chittorgarh, Rajasthan, India
[2]Professor, Department of Mathematics, Mewar University, Chittorgarh, Rajasthan, Indi)

Abstract:
A Mobile Ad-hoc Network (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. Such networks are more vulnerable to security attacks than conventional wireless networks. In this paper, we propose a secure identity-based ad hoc protocol for mobile devices to construct a group key for a setup of a secure communication network in an efficient way and propose a collision-free method for computing such keys. Unlike group key management protocols, we use identity-based keys that do not require certificates which simplify key management. In contrast to other interactive protocols, we only need one broadcast to setup the group key and member removal is also highly efficient.

Keywords: MANET, Network Topology, Identity-based, Key Management.

1. Introduction

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes them selves, i.e., routing functionality will be incorporated into mobile nodes. Such networks are more vulnerable to security attacks than conventional wireless networks. Identity-based encryption (IBE) is a form of public-key cryptography in which a third-party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. Compared with typical public-key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators. An added advantage is that a message recipient doesn't need advance preparation or specialized software to read the communication. In a broadcast encryption scheme a broadcaster encrypts a message for some subset S of users who are listening on a broadcast channel. A user in S can use his private key to decrypt the broadcast. Any user outside the privileged set S should not be able to recover the message. The concept of Broadcast Encryption (BE) was introduced by Fiat and Naor. BE is the problem of sending an encrypted message to a large user base such that the message can only be decrypted by a privileged subset. In an ad hoc network, the privileged subset is changing and dynamic. Hence efficiency in transmission cost has been considered to be a critical problem. In addition, the efficiency of a broadcast encryption scheme is also measured by user storage cost and computational cost at a user's device. We provide a general framework for constructing identity-based and broadcast encryption systems. In particular, we construct a general encryption system called spatial encryption from which many systems with a variety of properties follow. The cipher text size in all these systems is independent of the number of users involved and is just three group elements. Private key size grows with the complexity of the system. One application of these results gives the first broadcast HIBE system with short cipher texts. Broadcast HIBE solves a natural problem having to do with identity-based encrypted email.

2. Preliminaries

The following computational problem and complexity assumption are used in the security analysis of our schemes

2.1 Bilinear Maps

Let G_1, G_2, and G_t be cyclic groups of the same order.

2.1.1 Definition

A bilinear map from $G_1 \times G_2$ to Gt is a function

e : $G_1 \times G_2 \rightarrow G_t$ such that for all u ϵ G_1, v ϵ G_2, a, b ϵ Z,

$$\mathbf{e(u^a, v^b) = e(u, v)^{ab}} \ .$$

Bilinear maps are called pairings because they associate pairs of elements from G_1 and G_2 with elements in G_t. Note that this definition admits degenerate maps which map everything to the identity of G_t.

3. General Diffie-Hellman Exponent Problem

Let p be an integer prime and let s, n be positive integers. Let P,Q ϵ $Fp[X_1, . . . ,X_n]^s$ be two s-tuples of n-variate polynomials over F_p and let f ϵ $F_p[X_1, . . . ,X_n]$. Thus, P and Q are just two ordered sets containing s multi-variate polynomials each. We write P = $(p_1, p_2, . . . , p_s)$ and Q = $(q_1, q_2, . . . , q_s)$. We require that the first components of P,Q satisfy $p_1 = q_1 = 1$; that is, the constant polynomials 1. For a set Ω, a function h : $F_p \rightarrow \Omega$, and a vector $x_1, . . . , x_n$ ϵ F_p, we write

$$\mathbf{h(P(x_1, . . . , x_n)) = (h(p_1(x_1, . . . , x_n)), . . . , h(p_s(x_1, . . . , x_n))) \in \Omega^s.}$$

We use similar notation for the s-tuple Q. Let G_0,G_1 be groups of order p and let e : $G_0 \times G_0 \rightarrow G_1$ be a non-degenerate bilinear map. Let g ϵ G_0 be a generator of G_0 and set g_1 = e(g, g) ϵ G_1. We define the (P, Q, f)-Diffie-Hellman Problem in G as follows: Given the vector

$$\mathbf{H(x_1, . . . , x_n) = (g^{P(x1,...,xn)}, g_1^{Q(x1,...,xn)} \in G_0{}^s \times G_1{}^s, \text{ compute } g_1^{f\,(x1,...,xn)} \in G_1}$$

To obtain the most general result, we study the decisional version of this problem. We say that an algorithm B that outputs b ϵ {0, 1} has advantage ε in solving the Decision (P, Q, f)-Diffie-Hellman problem in G_0 if

$$\mathbf{|\, Pr\, [B(H(x_1, . . . , x_n), g_1^{f(x1,...,xn)}\ ) = 0] - Pr[B(H(x_1, . . . , x_n), T) = 0]\, | > \varepsilon}$$

where the probability is over the random choice of generator g ϵ G_0, the random choice of $x_1, . . . , x_n$ in F_p, the random choice of T ϵ G_1, and the random bits consumed by B.

4. Joux's 3-Party Diffie-Hellman

Let G be a group with prime order q, e : G × G→G^t be a bilinear map, and g be a generator of G. Let ˆg = e(g, g) ε G^t.

R R

- Aman picks a ←Z_q, Anuj picks b ← Z_q,

  and Sharad picks c $\xleftarrow{R}$$Z_q$.
- Aman, Anuj, and Sharad broadcast g^a, g^b, and g^c respectively.
- Aman computes $e(g^b, g^c)a = \hat{}g^{abc}$, Anuj computes $e(g^c, g^a)^b = \hat{}g^{abc}$, and Sharad computes $e(g^a, g^b)c = \hat{}g^{abc}$.

4.1 Boneh and Franklin's IBE Scheme

Let G be a group with prime order q, e : G × G→Gt be a bilinear map, and g be a generator of G. Let ˆg = e(g, g) ε Gt. Let h1 : $\{0, 1\}^* \rightarrow$G and h2 : Gt →$\{0, 1\}^*$ be hash functions. These are all public parameters.

4.1.1 Setup

PKG picks s $\xleftarrow{R}$ Zq. Then g^s is the public key of PKG.

4.1.2 Encryption

If Aman wants to send a message m to Anuj,

he picks r $\xleftarrow{R}$ Zq then computes the following.

Encrypt (g, g^s, "Anuj",m)

$$= (g^r, m \oplus h_2(e(h_1(\text{“Anuj”}), g^s)^r)$$
$$=(g^r, m \oplus h_2(e(h_1(\text{“Anuj”}), g)^{rs})$$

4.1.3 Making a Private Key

PKG may compute the private key of **Anuj** as follows.

$$\text{MakeKey (s, “Anuj”)} = h_1(\text{“Anuj”})^s$$

4.1.4 Decryption

Given an encrypted message (u, v) = $(g^r, m \oplus h_2(e(h_1(\text{“Anuj”}), g)^{rs})$ and a private key w = $h_1(\text{“Anuj”})^s$, Anuj may decrypt as follows.

Decrypt (u, v,w) = v $\oplus$ $h_2(e(w, u))$

$$= m \oplus h_2(e(h_1(\text{“Anuj”}), g)^{rs}) \oplus h_2(e(h_1(\text{“Anuj”})^s, g^r))$$
$$= m \oplus h_2(e(h_1(\text{“Anuj”}), g)^{rs}) \oplus h_2(e(h_1(\text{“Anuj”}), g)^{rs})$$
$$= m$$

How to understand this?

- Let t be the discrete log of h_1("Anuj") base g
- We don't know what it is, but it is well defined
- Now the situation is like 3-party Diffie-Hellman
- Aman has public g^r, private r
- PKG has public g^s, private s
- Anuj has public g^t, unknown (!) t
- $e(h_1(\text{“Anuj”}), g)^{rs} = e(g^t, g)^{rs} = \hat{}g^{rst}$ is like session key for encryption
- Aman and PKG could compute $\hat{}g^{rst}$ just like in Joux's scheme

- But what about Anuj?
- PKG helps him over previously authenticated, secure channel
- PKG computes $(g^t)^s = g^{st}$ and sends it to Anuj
- Anuj can now compute $e(^{gst}, g^r) = \hat{}g^{rst}$
- The point is that Anuj gets g^{st} rather than $\hat{}g^{st}$
- With g^{st}, still one cheat left
- If it was $\hat{}g^{st}$ (which anyone can compute), couldn't apply e anymore

5. Adaptive Security Model

A broadcast encryption scheme is said to be secure if given any S, the subscribers not in S as well as the non-subscribers are not able to extract the message from its cipher-text, meant for the subscribers in S, even through collusion. Formally, the security can be defined using the following game between a challenger A and an attacker B:

i. **Setup:** A runs Setup(λ, n) to generate the public parameters which it passes onto B.
ii. **Query Phase 1 :** B adaptively queries about the secret keys of subscribers $i_1; i_2; : : : ; i_l$ and A responds with the keys $K_{i1} ;K_{i2} ; : : : ;K_{il}$.
iii. **Challenge:** B decides on a set $S^* \subseteq \{1,2,\dots\dots,n\} \setminus \{i_1, i_2,\dots..,i_l \}$ of subscribers it wants to attack. It chooses a pair of distinct messages (M_0,M_1) and gives it to A along with S^*. A chooses a random b ε {0,1} and runs Encrypt (S^*, PP,M_b) to obtain the cipher-text C^* which it gives to B.
iv. **Query Phase 2 :** B continues to adaptively query about the secret keys of other sub- scribers $i_{l+1}, i_{l+2},\dots\dots i_{l+m}$, who are not in S^*, and gets the keys $K_{il+1},Ki_{l+2}\dots\dots,K_{il+m}$.
v. **Guess:** B guesses b' ε {0,1} for b and wins the game if b = b'.

The broadcast encryption scheme against CPA if for all attacks

$$Pr^{(b = b')} = ½ + e(λ)$$

Where e(λ) is a negligible function in λ.

6. Identity Based Security Framework

It is based on the Bohio-Miri scheme and consists of several parts: secure symmetric communication, group broadcast, encryption and signature to support privacy, authentication, integrity, no repudiation, and free key-escrow. Even though the framework is based on the Bohio-Miri scheme, the authors propose a few modifications to reduce its vulnerabilities. It provides two versions of pair wise key agreement: static and dynamic. The static one uses the same static pair-wise key as the Bohio-Miri scheme, providing the most efficient performance.

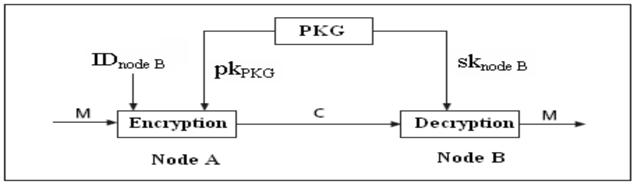

Figure 1: Identity-based encryption scheme.

However, it is fully ID-based, not requiring support structures or online servers. The dynamic pair wise key agreement provides a fresh and distinct key for each session; following the same principles as the static pair-wise key agreement. It also provides a tripartite key agreement to set up secure communication among three entities, and it is used as a primitive for group key management.

7. Conclusion

Security is one of the major issues in MANETs. Their natural characteristics make them vulnerable to passive and active attacks, in which misbehaving nodes can eavesdrop or delete packets, modify packet contents, or impersonate other nodes. We have also presented a description of application fields for ID-based key management. It is important to point out that the major problem with ID-based cryptographic schemes is that they yield only level 2 trust; that is, the private key of users must be known by the key management authority. In conventional networks this is not a major problem, but in MANETs, in which the authority is distributed among online servers or emulated by an arbitrary entity, this may be an issue.

References

[1] D. Boneh and M. Franklin, "Identity- Based Encryption from The Weil Pairing," *SIAM J. Computing*, vol. 32, no. 3, 2003, pp. 586–615.

[2] M. J. Bohio and A. Miri, "Efficient Identity-Based Security Schemes for Ad Hoc Network Routing Protocols," *Ad Hoc Networks*, vol. 2, no. 3, 2004, pp. 309–17.

[3] W. Liu, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," *IEEE Trans. Dependable Secure Computing*, vol. 3, no. 4, 2006, pp. 386–99.

[4] H. Deng, A. Mukherjee, and D. P. Agrawal, "Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks," *Proc. Int'l. Conf. Info. Tech.: Coding and Computing*, vol. 2, 2004, p. 107.

[5] N. Saxena, G. Tsudik, and J. Hyun Yi, "Identity-Based Access Control for Ad Hoc Groups," *Proc.*

Int'l. Conf. Info. Security and Cryptology, 2004.

[6] B. Park and W. Lee, "ISMANET: A Secure Routing Protocol Using Identity-Based Signcryption Scheme for Mobile Ad-Hoc Networks," *IEICE Trans. Commun.*, vol. 88, no. 6, 2005, pp. 2548–56.

[7] J. Pan *et al.*, "Identity-Based Secure Collaboration in Wireless Ad Hoc Networks," *Computer Networks*, vol. 51, no. 3, 2007, pp. 853–65.

[8] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks," *Proc. 2003 Symp. Apps. and the Internet Wksps.*, 2003.

[9] K. Hoeper and G. Gong, "Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation," tech. rep., Centre for Applied Cryptographic Research, Univ. of Waterloo, 2006.

[10] H. Chien and R. Lin, "Improved ID-Based Security Framework for Ad Hoc Network," *Ad Hoc Networks*, vol. 6, no. 1, 2008, pp. 47–60.