An Authenticated Broadcasting Scheme for Wireless Ad hoc Network

Muhammad Bohio , Ali Miri
School of Information Technology and Engineering
University of Ottawa, Ottawa, ON, K1N 6N5, Canada.
{mbohio, samiri}@site.uottawa.ca

Abstract

In this paper, we propose a pairing-based signcryption scheme for authenticated broadcasting, which requires less computation than a previously proposed scheme suggesting identity-based cryptosystem for ad hoc networks. Due to the dynamic nature of ad hoc networks, we allow nodes to generate their own broadcast keys for different groups in the network and change those when associated groups are changed. However, we ensure through our signcryption scheme that broadcast keys would be implicitly controlled by the Trusted Authority (TA), and can be used for as long the private keys are issued. Our keys are based on identities and do not use certificates. We also propose a non-probabilistic method for computing unique broadcast keys for different groups. We use identity-based pairwise symmetric keys as the building block for our broadcast scheme. Such keys are computed non-interactively by the nodes, which reduces communication overhead and simplifies key management in pairwise communication.

1. Introduction

Wireless ad hoc networks are self-configurable and autonomous networks with dynamic topologies. In such networks, participating nodes share the responsibilities of routing, access points, base stations, and other such administrative elements. There are several problems, such as routing, scalability, quality of service and security that need to be solved before implementing these networks in practice. Part of these problems are due to the fact that not all the techniques for conventional wired or wireless networks are appropriate for these environments. Security, in particular poses a challenge as ad hoc networks often contain resource constrained nodes. There are several schemes which may provide strong security solutions but cause computational and memory overhead, for example, the schemes with public key cryptosystem [11,14]. Some authentication schemes require less computations [12, 13] but either provide limited security features or are difficult to implement in practice. Most secure routing protocols focus on authentication. In order to ensure reliable network communication and to identify malicious nodes, authentication and non-repudiation are among the essential requirements. However, confidentiality and data integrity are also crucial requirements [6], but in most of the secure protocols for ad hoc networks these requirements have been ignored, partially considered, or require further setup to achieve all these required features. Our focus is to cover all such mandatory features with minimum computational, memory and bandwidth overhead.

Next sections are organized as follows: in section 2 we discuss related work done in this area and brief overview of our contribution. In section 3 we describe preliminary information required to explain our scheme. In section 4 we explain our approach for authenticated broadcasting and describe pairwise keys, broadcast keys, and signcryption scheme. We discuss performance and security analysis in section 5 and the conclusion is given in section 6.

2. Related Work

Two efficient solutions based on symmetric cryptosystem are proposed in [12] and [13]. In SEAD[12], the security scheme suggested is based on hash chain. Authentication is achieved by, given h_n, h_i can be verified by $h_n = H^{n-i}[h_i]$ for $i < n$. Use of hash chains makes this protocol much faster than public key cryptosystem based protocols. Since, each hash element would be used only once, in case of increased network traffic significantly large number of hash elements are required. In Ariadne[13], same technique of hash chain is

Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR'04)
0-7695-2096-0/04 $20.00 © 2004 IEEE

used but it also provides authenticated broadcasting using TESLA broadcast protocol. There is no message integrity in SEAD where as Ariadne implements Message Authentication Code (MAC) for integrity and uses delayed key disclosure for its verification. Ariadne requires clock synchronization between nodes and end-to-end delay should be known to avoid any forging attack on messages. Such requirements are considered unrealistic for ad hoc network [23], and such solutions are difficult to implement in practice.

In ARAN[14], security is based on public key certificates and it is assumed that keys are *a priori* generated and exchanged between a certificate server and nodes. Any entering node will request a certificate from the server and then would be allowed to participate in the network. Use of certificate based public key cryptography like [14], causes additional overhead for resource constrained nodes due to its computational and memory requirements.

In [15], an accelerated scheme for the key establishment protocol is proposed which uses the technique of Server-Aided Secret Computation (SASC). The SASC technique (also used in [16, 17, 18]) exchanges information with the base station to get expensive computation done by the server. In such protocols a prior arrangement of base station is required which restricts the independence of nodes in return for assistance by the base station.

In [11], the distributed CA scheme proposed by Zhou and Haas [22] has been improved by suggesting the use of Identity Based Encryption (IBE) and a relevant signature scheme. The use of IBE in that scheme simplifies the key management. Authors propose the establishment of distributed Private Key Generation (PKG) service within the network instead of CA. The entering nodes get their private keys from the distributed PKG based on t-out-of-n scheme. However, technical details on computing private keys (generated by t-out-of-n authorities) for the corresponding master public key are not given. It is also mentioned that network initialization stage is vulnerable to Byzantine failures. The use of the suggested IBE and signature scheme is computationally expensive as compared to signcryption scheme proposed in this paper.

2.1. Our Contribution

We use the identity-based pairwise symmetric keys proposed in [1] for authenticated pairwise communication in ad hoc network. We propose pairing-based signcryption scheme for authenticated broadcasting. We allow nodes to generate their own broadcast keys dynamically but ensure implicit control of the TA on such keys and bound those with the private keys issued by the TA. We also present a mechanism to generate unique broadcast keys through a non-probabilistic method under an affordable condition of collusion.

To explain our scheme we briefly describe here the relevant terminologies such as identity based encryption, pairing of points, and the related problems on which the security of our system is based.

3. Preliminary Information

3.1. Identity Based Encryption (IBE)

The idea of Identity Based Cryptosystem was first proposed by Shamir[8] to simplify the conventional Public Key Cryptosystem (PKCS), and make the key management easier. Since then, different schemes were suggested [9, 10], but the first practical IBE was proposed in [2]. In this scheme the identity of the user is used as the public key which makes the key management easier and does not require certificates for implementing key revocation. This minimizes overhead of the conventional PKCS and becomes attractive scheme for mobile and resource constrained devices.

Next, we describe the MapToPoint algorithm [2] that we will use to compute identity based keys.

The Mapping Function: MapToPoint

As described in [2], the MapToPoint function encodes the identity of the user to a point on an elliptic curve as following.

Let E be an elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$, where $p = 2 \ mod \ 3$, and $p = lq - 1$ for some prime $q > 3$. Also q^2 should not divide $p + 1$. Let $\mathbb{G}_1$ be an additive subgroup of points on $E(\mathbb{F}_p)$ of order q. We define the hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{F}_p$, which gives the hash of input ID of any length and the resulting value is an element in the field $\mathbb{F}_p$. Let $y_0 = H_1(ID_X)$, where ID_X is the identity of any user X. The MapToPoint algorithm works as follows on the input $y_0 \in \mathbb{F}_p$:

(1) Compute $x_0 = (y_0^2 - 1)^{1/3} = (y_0^2 - 1)^{(2p-1)/3} \in \mathbb{F}_p$.
(2) Let $Q = (x_0, \ y_0) \in E(\mathbb{F}_p)$, and set $Q_{id\_X} = lQ \in \mathbb{G}_1$.

(3) Output **MapToPoint**$(y_0) = Q_{id\_X}$.

The resulting point Q_{id_X} is the identity based public key of some user X.

Pairing of points

Pairing of any two points P, $Q \in \mathbb{G}_1$ is a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_1$ is an additive group and $\mathbb{G}_2$ is the multiplicative group of points on the elliptic curve. There are two methods for computing the pairing: Weil pairing and the Tate pairing. Technical details on pairing are out of the scope of this paper. For details on these pairings the interested reader is referred to [7,20,21] and elsewhere.

An important property of pairing of points is the bilinearity property, which implies that for any point P on an elliptic curve the bilinear map e has following feature:

$$\begin{aligned} e(2P, P) &= e(P, P)^2 = e(P + P, P) \\ &= e(P, P).e(P, P) = e(P, 2P) \end{aligned}$$

similarly

$$e(aP, bP) = e(P, P)^{ab} = e(abP, P) = e(P, abP)$$

where a and b are any scalar multipliers of point P.

3.2. Bilinear Diffie-Hellman Problem (BDHP)

Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two groups of prime order q and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be an admissible bilinear map and let P be the generator of $\mathbb{G}_1$, then BDHP is defined as given $< P, aP, bP, cP >$ for some $a, b, c \in \mathbb{Z}_q^*$, it is hard to compute $W = \hat{e}\,(P\,,\ P)^{abc} \in \mathbb{G}_2$.

3.3. Elliptic Curve Discrete Log Problem(ECDLP)

The Elliptic Curve Discrete Log Problem is defined as, given a point P of order n on an elliptic curve over field $\mathbb{F}_q$ and point aP for some $a \in \mathbb{Z}_n$, it is hard to compute a.

Next, we explain our scheme describing computation of symmetric keys and the signcryption scheme.

4. Our Approach

We use similar parameters as in [2] for pairing-based cryptography. Let E be an elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$, where $p = 2\ mod\ 3$, and $p = lq - 1$ for some prime $q > 3$. Also, q^2 should not divide $p + 1$. Let $\mathbb{G}_1$ be an additive subgroup of points on $E(\mathbb{F}_p)$ and $\mathbb{G}_2$ be the multiplicative subgroup on $E(\mathbb{F}_{p^2})$ of order q. Let P be a point an arbitrary generator of $\mathbb{G}_1$. We assume a semantically secure symmetric cryptosystem, such as AES, is to be used for pairwise communication once the secret keys are computed. We now describe pairwise and broadcast communication protocols as following.

4.1. Authenticated Pairwise Communication

For authenticated pairwise communication in ad hoc networks, we use identity based pairwise keys proposed by Sakai *et al.* in [1]. We assume that every node receives its private key based on its identity from the Trusted Authority (TA). For some *node A*, its private key D_A will be computed, similarly as in [2] as following:

$$D_A = sQ_{id\_A}$$

where s is the master key of the TA, and Q_{id_A} is computed as: $Q_{id\_A} = MapToPoint(H_1(ID_A))$ as described in section 3.1. All the nodes should be issued private keys similarly using the same master key. *Node A* can then compute its shared key with *node B* as proposed in [1] as:

$$D_{AB} = e\,(sQ_{id\_A},\, Q_{id\_B})$$

Similarly, B can compute:

$$D_{AB} = e(Q_{id\_A}, sQ_{id\_B})$$

and based on the bilinearity property both results can be commonly represented as:

$$D_{AB} = e(Q_{id\_A}, Q_{id\_B})^s$$

For computing the symmetric key that will be used with the suggested symmetric cryptosystem, we define the hash function $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^m$ which gives the hash output of m bits for some input element of group $\mathbb{G}_2$, where m is the size of key as per security requirement. The resulting key is:

$$K_{AB} = H_2(D_{AB})$$

An important observation is that this key agreement is non-interactive and does not require the involvement of TA after the private keys are issued and identities are provided as public parameter.

Above mentioned pairwise communication is efficient since it provides both authentication and privacy using symmetric cryptosystem. However, in case of broadcast messages it consumes additional bandwidth by requiring to send the same message to multiple nodes individually. Thus, in order to minimize such overhead

we provide an authenticated broadcast communication scheme in the following.

4.2. Authenticated Broadcast Communication

The broadcast protocol consists of Initialization, Signcrypt and Unsigncrypt algorithms. Next, we describe the computation and distribution of the broadcast keys in the initialization step.

4.2.1. Initialization Let Q_{id_1} be the public key assigned to *node 1* by the TA, and K_{1N} be the broadcast secret of *node 1* for a group of N nodes. *Node 1* will compute the broadcast parameter P_{1_brdcst} as:

$$P_{1\_brdcst} = K_{1N} \cdot Q_{id\_1}$$

For computing the broadcast secret K_{1N}, we describe two different methods:

(i) K_{1N} can be any random value generated by *node 1* and used as its broadcast secret.

(ii) In case of large network and smaller fields being used, the probability of having any two nodes at any time end up with same random value is negligible but not definite zero. If some definite method is required to ensure that every node has its unique key, the following method ensures that K_{1N} is the unique key that only *node 1* can compute, unless otherwise all other $n-1$ nodes collude. We compute K_{1N} as:

$$\begin{aligned} D_{1N} &= e\,(sQ_{id\_1}\,,\; Q_{id\_2} + Q_{id\_3} + \cdots + Q_{id\_n}) \\ &= e\,(sQ_{id\_1}\,,\; Q_{id\_2}) \cdot e\,(sQ_{id\_1}\,,\; Q_{id\_3}) \cdots \\ &\quad\; e\,(sQ_{id\_1}\,,\; Q_{id\_n}) \\ &= D_{12} \cdot D_{13} \cdots D_{1n} \end{aligned}$$

and $\quad K_{1N} = H_2(D_{1N})$.

The secret K_{1N} should be long enough for the discrete log problem to be hard. *Node 1* will deliver the broadcast parameter P_{1_brdcst} to other users in the group by encrypting in each group-member's pairwise shared key with *node 1*.

Next we describe our proposed signcryption scheme for authenticated broadcasting in ad hoc networks.

4.2.2. Signcryption scheme The signcryption scheme consists of two algorithms: Signcrypt and Unsigncrypt, described as follows.

Signcrypt

In order to signcrypt the message M, *node 1* will compute $h = H_3(M)$, where $H_3 : \{0,1\}^* \rightarrow \{0,1\}^*$. A random value r is generated where $r \in Z_q^*$. A parameter d_1 is precomputed as following and stored for encryption of broadcast messages:

$$d_1 = e\,(Q_{id\_1}\,,\; P)$$

Message M is encrypted with key

$$K_{1\_brdcst} = H_2(\, d_1^{(r+h)}\,)$$

as:

$$C = E_{K_{1\_brdcst}}(M) = M \oplus K_{1\_brdcst}$$

Two parameters U and V are computed as:

$$U = rP\,, \quad \text{and} \quad V = K_{1N}^{-1}\,(r+h)P$$

The broadcast message β consists of three elements as following:

$$\begin{aligned} \beta &= \{C\,,\; U\,,\; V\} \\ &= \{E_{K_{1\_brdcst}}(M)\,,\; rP\,,\; K_{1N}^{-1}\,(r+h)P\} \end{aligned}$$

Unsigncrypt

For decryption of the message, the authorized receivers (i.e. members of the group provided with broadcast parameter $K_{1N}Q_{id\_1}$) will compute the key K_{1_brdcst} as hash of d_2, where d_2 is computed as:

$$\begin{aligned} d_2 &= e\,(K_{1N}Q_{id\_1}\,,\; V) \\ &= e\,(K_{1N}Q_{id\_1}\,,\; K_{1N}^{-1}(r+h)P) \\ &= e\,(Q_{id\_1}\,,\; (r+h)P) \end{aligned}$$

and thus $\quad K_{1\_brdcst} = H_2(d_2)$

Message M is decrypted from the cipher text C as:

$$M = D_{K_{1\_brdcst}}(C) = C \oplus K_{1\_brdcst}$$

After decrypting message M, its hash can be computed as: $h = H_3(M)$, and authentication is verified by computing $Q_{id\_1} = MapToPoint(H_1(ID_1))$, and d_3 as follows:

$$d_3 = e\,(Q_{id\_1}\,,\; U + hP)$$

$$= e\,(Q_{id\_1}\,,\; rP + hP)$$

$$= e\,(Q_{id\_1}\,,\; (r+h)P)$$

Message is verified to be from *node 1* if d_3 is equal to d_2.

Through our signcryption scheme, the broadcast keys are implicitly controlled by the TA. It should be noted that for computing parameter d_3 in unsigncrypt algorithm, receivers of the broadcast message will compute public key Q_{id_1} for *node 1* using the identity for which the sender was issued private key by the TA. If the broadcast key by *node 1* is computed as $K_{1N}Q'_{id\_1}$ e.g. by changing validation date in ID, the verification by other nodes would fail and such broadcast messages will not be authenticated.

5. Performance and Security Analysis

In authenticated pairwise communication, we use symmetric key cryptosystem which is faster and requires less computation as compared to the public key cryptosystem. Our scheme starts with only private keys to be issued to each node and does not require large number of pairwise keys to be generated by the third party. In conventional pairwise key schemes, as suggested in [13], a third party is required to generate $N(N-1)/2$ keys for N nodes and providing every node with $(N-1)$ keys requires $N(N-1)$ keys to be distributed through some secure channel. However, our scheme needs only N private keys to be generated and distributed to N nodes by the TA. Every node can then compute pairwise shared secret for any node at any time without exchanging any information, provided the identities of users (such as email addresses, student or employee IDs etc.) are either published by the TA or sent with the message by the sender. Our scheme requires less storage even in case of large networks, since a node can delete keys which are not in frequent use and can generate such keys any time later without contacting TA or the corresponding nodes.

Our signcryption scheme is modified form of [4] with additional features and different parameters being used. We have one more point multiplication in signcrypt step in parameter $V = K_{1N}^{-1}(r+h)Q_{id\_1}$, that can be alleviated by taking multiplication of $K_{1N}^{-1}.Q_{id\_1}$ for once and use it for all other broadcast messages, since it is independent of message being signcrypted. Hence, we can claim that our scheme is as efficient as [4] with additional features of encryption and nodes being given control of generating broadcast keys as per requirement under the implicit control of TA. Our signcryption scheme requires less computation as compared to using encryption and signatures separately, e.g. as suggested in [11] for ad hoc networks, which requires two more pairings than the scheme described above.

The security of our system is based on discrete log and bilinear Diffie-Hellman problems. In order to discrete log problem be hard enough, the broadcast secret K_{1N} is suggested to be at least 160 bits long, and elements of $\mathbb{G}_1$ at least 512 bits long. In our scheme if a node is compromised or an authorized node is malicious, all the pairwise keys associated to that node and its broadcast key could be misused. It should be noted that in such a case the broadcast parameters of other nodes can not be misused due to signcryption scheme. Methods for detecting the malicious behavior of such nodes is out of the scope of this paper. However, due to our authentication and non-repudiation features, the source is always identified. The pairwise communication in our scheme can also implement any efficient Message Authentication Code (MAC) scheme to ensure data integrity.

6. Conclusion

We have presented an authenticated pairwise and broadcast communication scheme which uses pairing-based cryptography. The pairwise scheme used requires only N private keys to be generated by the Trusted Authority (TA). Users can generate their pairwise symmetric keys non-interactively, provided the identities of users are either published by the TA or sent with the message by the sender.

In order to reduce bandwidth overhead caused by pairwise communication in case of broadcast messages, we have proposed pairing-based signcryption scheme for an authenticated broadcasting. The use of signcryption in broadcast messages requires less computation as compared to using encryption and signatures separately as proposed in [11]. We have also proposed a non-probabilistic method for computing unique broadcast secrets for different groups. Due to the dynamic nature of ad hoc networks, we have allowed nodes to generate their own broadcast keys and update those when associated groups are changed. However, our scheme ensures such keys are implicitly controlled by the TA through our signcryption scheme. Since, our unsigncrypt process is computationally more expensive than signcrypt process, it is possible that it can be mis-used by malicious nodes to generate unwanted, additional computational over-

head for other nodes by sending unnecessary broadcast messages. However, the non-repudiation and authentication in our scheme always identify the source of such attempts and help to deal with such attacks.

Acknowledgements

This work was partially supported by the grants from Natural Sciences and Engineering Research Council of Canada (NSERC), and Bell University Laboratories (BUL).

References

[1] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing", in *The Proceedings of The 2000 Symposium on Cryptography and Information Security*, Okinawa, Japan, pp. 26-28, January 2000.

[2] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing", extended abstract in *The Proceedings of The Advances in Cyptology - Crypto 2001*, Lecture Notes in Computer Science, vol. 2139, Springer-Verlog, pp. 231-229, 2001.

[3] S. S. Al-Riyami and K. G. Patterson, "Certificateless Public Key Cryptography", in the *Cryptology ePrint Archive, Report 2003/126*, July 2, 2003.

[4] J. C. Cha and J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups", in *The Proceedings of The 6th International Workshop on Theory and Practice in Public Key Cryptography*, pp. 18-30, January 2003.

[5] P. S. L. M. Barreto, B. Lynn, and M. Scott, "On the Selection of Pairing- Friendly Groups", in *The Proceedings of The Selected Areas in Cryptography - SAC'03*, Lecture Notes in Computer Science, Springer-Verlag, to appear, Ottawa, Canada, August 2003.

[6] M. Ilyas, *The handbook of Ad hoc Wireless Networks*, CRC Press, 2003.

[7] A. J. Menezes, "Elliptic Curve Public Key Cryptosystem", Kluwer Academy Publishers, 1993.

[8] A. Shamir, "Identity based cryptosystems and signature schemes", in *The proceedings of The Advances in Cryptology- Crypto '84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlog, pp. 47-53, 1984.

[9] S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem", in the *IEEE Journal on Selected Areas in Communication*, vol. 7, no. 4, pp. 467-473, 1989.

[10] H. Tanaka, "A realization scheme for identity-based cryptosystem", in *The proceedings of The Advances in Cryptology - Crypto '87*, Lecture Notes in Computer Science, Vol. 293, Springer-Verlog, pp. 341-349, 1987.

[11] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward Secure Key Distribution in Trully Ad-Hoc Networks", in *The Proceedings of The IEEE Workshop on Security and Assurance in Ad hoc Networks* in conjunction with the *2003 International Symposium on Applications and the Internet*,pp 342-346, Orlando, FL, January 28, 2003.

[12] Y. Hu, A. Perrig, and D. B. Johnson,"SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", in *The Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*,pp 3-13, June 2002.

[13] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", in *The Proceedings of The 8th Annual International Conference on Mobile Comoputing and Networking*, ACM Press, to appear, September 2002.

[14] B. Dahill, B. Levine, E. Royer, and C. Shields, "A Secure Routing Protocol for Ad hoc Networks", in the *Technical Report UM-CS-2001-037*, University of Massachusetts, August 2001.

[15] S. Lee, S-M. Hong, H. Yoon, and Y. Cho, "Accelerating Key Establishment Protocols for Mobile Communication", in *The Proceedings of The 4th Australian Conference on Information Security and Privacy - ACISP' 99*, LNCS 1587, pp 51-63, April 1999.

[16] U. Carleson, "Optimal privacy and authentication on a portable communications system", in the *ACM Operating Systems Review*, vol. 28, no. 3, pp. 16-23, 1994.

[17] C. Boyd and A. Mathuria, "Key establishment protocols for secure mobile communications: A selective survey", in *The Proceedings of The Australian Conference on Information Security and Privacy - ACISP'98*, Lecture Notes in Computer Science, vol. 1438, pp. 344-355, 1998.

[18] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks", in the *IEEE Personal Communications*, vol. 1, pp. 25-31, 1994.

[19] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", in *The Proceedings of Mobile Computing and Networking*, Rome, Italy, pp 189-199, 2001.

[20] L. S. Charlap, D. P. Robbins. "CRD Expository Report 31: An Elementary Introduction to Elliptic Curves", December 1988.

[21] M. Scott, "The Tate Pairing", at www.computing.dcu.ie/ mike/tate.html

[22] L. Zhou and Z. Hass, "Securing Ad Hoc Networks", in the *IEEE Network Magazine*, vol. 13, no. 6, pp. 24-30, November/December 1999.

[23] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing", in *The Proceedings of the ACM Workshop on Wireless Security*, pp. 1-10,September 28, 2002.