文章编号:1001 - 9081(2011)04 - 0981 - 03
doi:10.3724/SP.J.1087.2011.00981

普适环境中基于身份的组密钥管理方案

霍士伟[1],蔡中民[2],罗长远[1]
(1. 信息工程大学 电子技术学院,郑州 450004; 2. 河南商业高等专科学校 计算机应用系,郑州 450044)
(xiangya_85211@sina.com)

摘 要:分析了普适环境中组密钥管理方案的需求,结合基于身份的公钥密码技术和 STR 组密协商协议,设计了一种新的基于身份的可认证组密钥管理方案。针对普适环境中节点随时加入和退出群组的特点,设计了组密钥更新协议,保证了组密钥的前向和后向安全性。方案在满足安全性要求的前提下,具有较小的计算和通信开销。

关键词:普适环境;组播;组密钥管理;基于身份的密钥体制;STR 协议
中图分类号: TP393.08;TP309 **文献标志码**:A

Identity-based group key management scheme in pervasive computing environment

HUO Shi-wei[1], CAI Zhong-min[2], LUO Chang-yuan[1]
(1. *Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan* 450004, *China*;
2. *Department of Computer Applications, Henan Business College, Zhengzhou Henan* 450044, *China*)

Abstract: The requirements of group key management scheme in pervasive environment were analyzed. A new identity-based group key management scheme was proposed by combing the identity-based cryptography and STR protocol. Concerning nodes' free joining and leaving the group, group key renewing protocol was proposed, which could guarantee the forward security and backward security of the group key. The scheme can achieve security requirements and has less computation and communications load.

Key words: pervasive environment; multicast; group key management; identity-based cryptography; STR protocol

0 引言

普适环境是一种主要由移动节点构成、以无线连接为主的网络环境,具有资源受限和网络结构动态变化的特点。在普适环境中,组播是一种基本的通信形式[1]。为了确保组播通信的安全,需要设计适合普适环境的组密钥管理方案[2]。

普适环境中理想的组密钥管理方案应该满足以下要求。

1)分布式:如果采用集中式密钥管理,需要设置一个集中的密钥生成中心。但是,普适环境中节点之间主要以无线形式连接,链路带宽有限,另外节点移动造成网络结构动态变化,因此移动节点和密钥生成中心无法总是保持有效连接,容易出现单点失效问题。因此,理想的组密钥管理应该采用分布式。

2)高安全性:方案要能够提供密钥认证性、前向保密性、后向保密性等安全要求。

3)可扩展性:由于普适环境中的节点具有高度动态性,通信组的成员数目通常是变化的,因此方案要能适应通信群组的变化。

4)低计算量:由于普适环境中的节点计算能力有限,所以方案应该具有较小的计算开销。

5)低通信量:为了适应普适环境中无线链路带宽有限、网络结构动态变化的特点,方案应该具有较小的通信量,以保证较高的成功率,特别是在成员关系发生变化时的通信量,要尽可能的小。

针对普适环境中组密钥管理的要求,设计适合普适环境的分布式组密钥管理方案是正确的选择。现有分布式组密钥管理方案有适合于对等群的 Cliques 协议[3](包括 GDH.1、GDH.2 和 GDH.3 三个协议),基于非平衡二叉树的 STR[4] 协议,基于二叉树的组密钥协商(Tree-based Group Diffie-Hellman, TGDH)协议[5]以及基于不同理论对以上协议的改进方案。其中 STR 方案采用非平衡树结构组织节点,在已有的组密钥协商协议中,通信开销最小。通常情况下,低通信量与低计算量无法同时满足。相关研究表明,在嵌入式平台上,传输信息比执行计算更消耗电能。因此,本文选择具有最小通信量的 STR 协议。但是,STR 协议没有提供密钥认证,无法抵抗中间人攻击等主动攻击。文献[6]利用基于身份密码技术对 STR 协议进行了改进,提供了密钥认证性。但是,文献[6]方案是基于双线性对实现的,在密钥协商过程中,节点需要进行多次双线性对运算,计算开销过大。本文设计了一种新的基于身份的 STR 组密钥管理方案,节点不需要进行复杂的双线性对运算,方案在提供密钥认证和保持通信量较小的前提下,减小了协议计算开销。

1 基于身份的组密钥管理方案设计

本文利用基于身份密码技术来为 STR 组密钥协商协议提供密钥认证。假设系统存在一个离线的私钥生成中心(Private Key Generate,PKG),PKG 在系统建立阶段为节点生成基于身份的私钥。假设每个网络节点拥有唯一的身份标

收稿日期:2010 - 10 - 18;**修回日期**:2010 - 12 - 09。

作者简介:霍士伟(1985 -),男,河北邯郸人,硕士研究生,主要研究方向:无线网络安全、普适计算安全; 蔡中民(1976 -),男,河南商丘人,讲师,主要研究方向:计算机网络、数据库安全; 罗长远(1973 -),男,河南信阳人,副教授,博士,主要研究方向:装备工程、无线通信系统安全。

识。方案包括:系统建立、初始组密钥建立、组成员加入和组成员离开四个部分。

1.1 系统建立

PKG 生成安全参数:选择椭圆曲线 $E(F_p)$ 上的 q 阶循环加法群 G_1,G_1 的生成元为 P;随机选择 $s \in Z_q^*$ 作为系统主密钥,系统公钥为 $P_{pub} = sP \in G_1$;定义以下安全哈希函数:$H_1: \{0,1\}^* \rightarrow Z_q^*$,$H_2: G_1 \rightarrow Z_q^*$;公开参数 $\{P, P_{pub}, G_1, q, H_1, H_2\}$。

假设组播组中有 n 个成员,其身份标识为 $M_i (1 \leqslant i \leqslant n)$,PKG 按如下过程为 M_i 生成基于身份的私钥。

PKG 随机选择 $t_i \in Z_q^*$,计算 $T_i = t_i P, s_i = t_i + sH_1(M_i)$,将 (T_i, s_i) 发送给 M_i,其中 s_i 为用户的私钥,需要妥善保存,T_i 为辅助参数,可以公开。

将所有组成员组织成一棵非平衡二叉树,每个叶子节点代表一个组成员节点,而非叶子节点代表一个虚拟的密钥节点。以四个组成员的组播组为例,形成如图 1 所示的密钥树。

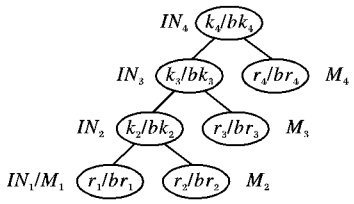

图 1 密钥树

在密钥树中 M_i 表示组成员节点的身份标识;IN_i 表示第 i 层的内部节点,假设最底层的左叶子节点为内部节点 IN_1;r_i 表示组成员节点 M_i 选择的临时密钥;br_i 表示 M_i 的盲密钥,$br_i = r_i P$;k_i 表示内部节点 IN_i 对应的临时密钥,由其中一个子节点的临时密钥和另一个子节点的盲密钥生成;bk_i 表示内部节点 IN_i 对应的盲密钥,$bk_i = k_i P$。由图 1 可以看出,$k_1 = r_1, bk_1 = br_1$。

1.2 初始组密钥建立

在组播初始化时,设群组中共有 n 个组成员节点 $M_1, M_2, M_3, \cdots, M_n$,在初始组密钥建立过程中,$M_1$ 作为赞助节点负责计算和广播内部节点的盲密钥。初始组密钥协商过程如下。

1)每个节点 M_i 随机选择临时密钥 $r_i \in Z_q^*$,计算盲密钥 $br_i = r_i P$,计算签名 $z_i = r_i + s_i H_1(M_i, T_i, br_i)$,广播消息 $\langle M_i, T_i, br_i, z_i \rangle$。

2)收到广播消息后,每个成员 M_j 验证签名:

$$z_i P = br_i + H_1(M_i, T_i, br_i)(T_i + H_1(M_i) P_{pub}); \quad 1 \leqslant i \leqslant n, i \neq j$$

对其他所有组成员的密钥信息进行验证。

3)M_1 计算密钥树所有内部节点的临时密钥 $k_i = H_2(k_{i-1} br_i) (2 \leqslant i \leqslant n)$,计算盲密钥 bk_i 和对 bk_i 的签名 v_i:$bk_i = k_i P, v_i = k_i + s_1 H_1(M_1, T_1, bk_i) (2 \leqslant i \leqslant n-1)$,广播消息 $\langle M_1, T_1, bk_i, v_i \rangle (2 \leqslant i \leqslant n-1)$。

4)收到广播消息后,成员 $M_j (2 \leqslant j \leqslant n)$ 计算:

$$v_i P = bk_i + H_1(M_1, T_1, bk_i)(T_1 + H_1(M_1) P_{pub}); \quad 2 \leqslant i \leqslant n-1$$

对所有内部节点的盲密钥进行验证。

5)每个组成员 $M_i (2 \leqslant i \leqslant n)$ 计算:

$k_i = H_2(r_i bk_{i-1})$

$k_j = H_2(k_{j-1} br_j)$; $i+1 \leqslant j \leqslant n$

通过上述公式递归计算,可以得到密钥树根节点的临时密钥 k_n 即为组密钥。

1.3 组成员加入

假设当前组播组中有 n 个成员 $M_1, M_2, M_3, \cdots, M_n$。新加入节点为 M_{n+1},此时赞助节点 M_s 为原根节点的右子节点 M_n。成员加入过程如下。

1)新成员 M_{n+1} 选择临时密钥 $r_{n+1} \in Z_q^*$,计算盲密钥 $br_{n+1} = r_{n+1} P$,计算签名 $z_{n+1} = r_{n+1} + s_{n+1} H_1(M_{n+1}, T_{n+1}, br_{n+1})$,广播消息 $\langle M_{n+1}, T_{n+1}, br_{n+1}, z_{n+1} \rangle$。

2)更新密钥树,创建一个新的根节点,原来的根节点作为新根节点的左子节点,新成员 M_{n+1} 作为新根节点的右子节点。

3)M_n 生成新的临时密钥 r_n',计算新盲密钥及签名:$br_n' = r_n' P, z_n' = r_n' + s_n H_1(M_n, T_n, br_n')$。计算 $k_n' = H_2(r_n' bk_{n-1}), bk_n' = k_n' P, v_n' = k_n' + s_n H_1(M_n, T_n, bk_n')$。广播 $\langle M_n, T_n, br_n', z_n', bk_n', v_n' \rangle$。

4)所有节点重新计算组密钥,分三种情况:

①M_{n+1} 对 bk_n', v_n' 进行验证并计算 $k_{n+1} = H_2(r_{n+1} bk_n')$;

②M_n 对 br_{n+1}, z_{n+1} 进行验证并计算 $k_{n+1} = H_2(k_n' br_{n+1})$;

③其他节点对 br_{n+1}, z_{n+1} 和 br_n', z_n' 进行验证并计算 $k_n' = H_2(k_{n-1} br_n')$,$k_{n+1} = H_2(k_n' br_{n+1})$。

经过上述计算,所有节点都得到了新的组密钥 k_{n+1}。

1.4 组成员离开

假设群组中当前有 n 个成员,成员 M_d 要离开群组,如果 $d > 1$,则赞助节点 M_s 是 M_{d-1};如果 $d = 1$,则赞助节点是 M_2。

当节点 M_1 离开组播组时,其执行过程与组密钥初始生成类似,即 M_2 作为赞助节点进行组密钥协商。

在其他情况下,当成员离开事件发生后,执行如下算法。

1)更新密钥树,删除 M_d 对应的节点及其父节点,用 M_d 原来的兄弟节点代替 M_d 的父节点。

2)赞助节点 M_{d-1} 选择新的临时密钥 r_{d-1}',计算新的盲密钥 br_{d-1}' 及签名 z_{d-1}',计算所有高层内部节点的新临时密钥 $k_i' (i = d-1, d+1, \cdots, n)$,计算对应的盲密钥和签名:$bk_i', v_i' (i = d-1, d+1, \cdots, n-1)$。广播 $\langle M_{d-1}, T_{d-1}, br_{d-1}', z_{d-1}' \rangle$ 和 $\langle M_{d-1}, T_{d-1}, bk_i', v_i' \rangle (i = d-1, d+1, \cdots, n-1)$。

3)收到广播消息后,其他组成员按下述方法计算新的组密钥。

①$i = d+1$:M_{d+1} 验证 M_{d-1} 发送的消息,计算:

$k_{d+1}' = H_2(r_{d+1} bk_{d-1}'), k_j' = H_2(k_{j-1}' br_j)$; $d+2 \leqslant j \leqslant n$

②$i > d+1$:M_i 验证 M_{d-1} 发送的消息,计算:

$k_i' = H_2(r_i bk_{i-1}'), k_j' = H_2(k_{j-1}' br_j)$; $i+1 \leqslant j \leqslant n$

③$i < d-1$:M_i 验证 M_{d-1} 发送的消息,计算:

$k_{d-1}' = H_2(k_{d-2} br_{d-1}')$, $k_{d+1}' = H_2(k_{d-1}' br_{d+1})$

$k_j' = H_2(k_{j-1}' br_j)$; $d+2 \leqslant j \leqslant n$

通过上述过程所有节点可以计算得到新的组密钥 k_n'。

2 安全性分析

2.1 组密钥保密性

不失一般性,考虑仅有 2 个成员节点 M_1、M_2 协商密钥的情形,公开信息包括 $br_1 = r_1 P$ 和 $br_2 = r_2 P$。M_1 可以计算出 $k_1 = H_2(r_1 br_2)$,M_2 可以计算出 $k_2 = H_2(r_2 br_1)$。可以看出:

$k_1 = H_2(r_1r_2P) = k_2$。

攻击者在已知 $br_1 = r_1P, br_2 = r_2P$ 的情况下,计算出 $k = H_2(r_1r_2P)$ 面临解决椭圆曲线上 Diffie-Hellman 问题(ECDH)。

因此,在两方进行密钥协商的情况下,能够实现组密钥的保密性。当多个用户进行组密钥协商时,其组密钥的保密性能够递归推导证明。

2.2　前后向安全性

前向安全性是指离开群组的节点不能利用旧的组密钥解密新密钥所加密的信息。在本文方案中,节点 M_d 离开后,赞助节点 M_{d-1} 选择了新的临时密钥并重新计算了密钥树高层内部节点的临时密钥和盲密钥。新的组密钥与 M_k 所掌握的密钥没有任何关系,因此 M_d 不能获得新密钥所加密的信息。

后向安全性是指新加入的节点不能利用当前组密钥获得旧组密钥所加密的信息。在本文方案中,节点 M_{n+1} 加入群组后,赞助节点 M_n 选择了新的临时密钥,重新计算了密钥树高层内部节点的临时密钥和盲密钥。M_{n+1} 计算得到的组密钥与旧组密钥没有任何关系,因此,M_{n+1} 不能解密由旧组密钥加密的信息。

2.3　认证性

在初始组密钥协商时,各节点可以对其他节点广播的密钥信息进行验证,确定其合法性。节点 M_i 的广播信息中包含盲密钥 br_i 和签名 z_i。其他节点通过验证等式 $z_iP = br_i + H_1(M_i,T_i,br_i)(T_i + H_1(M_i)P_{pub})$ 来确定其是否合法。这是因为:

$$\begin{aligned} z_iP &= (r_i + s_iH_1(M_i,T_i,br_i))P = \\ &r_iP + H_1(M_i,T_i,br_i)s_iP = \\ &br_i + H_1(M_i,T_i,br_i)(t_i + sH_1(M_i))P = \\ &br_i + H_1(M_i,T_i,br_i)(t_iP + H_1(M_i)sP) = \\ &br_i + H_1(M_i,T_i,br_i)(T_i + H_1(M_i)P_{pub}) \end{aligned}$$

攻击者虽然可以选择 $r_i' \in Z_q^*$,计算 $br_i' = r_i'P$,但是因得不到 s_i 而不能伪造签名 z_i',无法通过其他节点的验证。

另外,赞助节点 M_1 的广播消息中包括内部节点的盲密钥及其签名,其他节点同样可以通过验证签名来确定盲密钥的合法性。

在组成员加入和离开过程中,方案同样提供了认证机制,原理同上述相同。

3　效率分析

本节将对本文方案的计算和通信开销进行分析,并与文献[6]方案进行比较,。在比较计算开销时,主要考虑点乘运算开销(M)和配对运算开销(P)。由于位于密钥树中不同位置的成员的计算开销相差较大,因此计算时取成员的平均计算开销。方案的通信开销包括通信轮数、通信次数和传输消息的总量。本文与文献[6]方案的计算和通信开销如表 1 所示。

表 1　计算和通信开销比较

协议	子协议		计算开销	通信开销		
				轮数	广播数	消息数
本文方案	初始密钥协调		$\frac{13n-14}{2}M$	2	$n+1$	$2n-2$
	成员加入		$8M$	2	2	2
	成员退出	$d=1,2$	$\frac{7n-27}{2}M$	1	1	$n-2$
		$d\geqslant 3$	$\frac{7n-6d-9}{2}M$	1	1	$n-d+1$
文献[6]方案	初始密钥协调		$\frac{9n-9}{2}P+(4n-5)M$	2	$n+1$	$2n-2$
	成员加入		$6P+4M$	2	2	3
	成员退出	$d=1,2$	$\frac{3n-12}{2}P+(2n-1)M$	1	1	$n-2$
		$d\geqslant 3$	$\frac{5n-2d-9}{2}P+\frac{4n-4d-2}{2}M$	1	1	$n-d$

由表 1 中数据可以看出,本文方案同文献[6]中方案的执行轮数都为常数,通信开销都较小。由文献[7]知配对运算时间相当于 9.6 倍的点乘运算时间。因此,同文献[6]方案相比,本文方案具有更小的计算开销,更加适合在资源受限的普适环境中应用。

4　结语

本文结合基于身份的公钥密码技术和具有最小通信量的 STR 组密协商协议,设计了一种新的基于身份的可认证组密钥管理方案,方案在满足安全性要求的前提下,具有较小的计算和通信开销,很好地适应了普适环境的特点和需要。

参考文献:

[1] YANG F, CAI H B, CAO Q Y. BAPUC: A broadcast authentication protocol for ubiquitous computing[C]// 2008 IEEE Conference on Industrial Electronics and Applications. New York: IEEE, 2008: 2560 - 2564.

[2] KIM S, AHN T, HEEKUCK O. An efficient hierarchical group key management protocol for a ubiquitous computing environment[C]// ICCSA 2006, LNCS 3983. Berlin: Springer, 2006: 388 - 395.

[3] STEINER M, TSUDIK G, WAIDNER M. Key agreement in dynamic peer groups[J]. IEEE Transactions on Parallel and Distributed System, 2000, 11(8): 760 - 780.

[4] KIM Y, PERRG A, TSUDIK G. Group key agreement efficient in communication[J]. IEEE Transactions on Computers, 2004, 53(7): 905 - 921.

[5] KIM Y, PERRG A, TSUDIK G. Tree-based group key agreement [J]. ACM Transactions on Information and System Security, 2004, 7(1): 60 - 96.

[6] 宋震, 周贤伟, 窦文华. 一种基于身份标识的 MANET 组密钥协商协议[J]. 电子学报, 2008, 36(10): 1862 - 1868.

[7] 周福才, 徐剑, 徐海芳等. Ad-hoc 网络中基于双线性配对的 STR 组密钥管理协议研究[J]. 通信学报, 2008, 29(10): 117 - 125.