

安全组播来源认证性能分析

何志勇, 赵春生

(四川理工学院计算机学院, 四川 自贡 643000)

摘要: 组播技术可以为群组成员提供安全高效的群组通讯, 出于安全需要对来源进行认证, 来源认证的性能直接影响组播方案的性能。文章讨论了组播系统的安全性, 对密钥管理方案进行了讨论, 分析了 Cametti 等人提出的利用 MAC 概念的组播来源的认证方法, 并对该方法的性能进行了定量分析。分析结果对于评价安全组播来源认证方法的性能具有一定的参考意义。

关键词: 安全组播; 来源认证; 密钥管理; 性能分析

中图分类号: TP393

文献标识码: A

引言

组播通信的安全性较比单播传播更为复杂。组播的安全问题也受到质疑, 相较于点对点传输方式, 组播安全的问题更加复杂。在组播通信中, 发送端与接收端通常是共享一把加密钥匙来加密资料, 所以我们无法辨别资料的来源。如果使用公开密钥签名的方式, 在每次传送消息的同时都要计算签名值, 这会使得系统的负载过大, 降低组播的效率, 如何高效地认证资料来源, 是本文重点分析、讨论的问题。

1 组播安全问题

安全组播通信是指在参与保密通信的所有组成员中构建一个公共密钥(即为组播密钥), 该密钥是根据组播密钥管理协议(GKAP)建立起来的。组播方案的安全性主要从以下的几个指标进行评价^[1]。

保密性: 只有同一组播群组的成员能够解密传送来的资料, 已经离开的成员不能再访问往后的组播资料, 而新加入的成员有可能也会限制不能访问加入之前的组播资料。

认证: 认证的问题包括对群组认证的问题, 必须能够确认某一消息是否是同一个群组的成员所发送出来

以及来源认证的问题, 必须能够辨识出某一消息是由群组中哪一个成员所送出的。

完整性: GKAP 协议确保消息不被组外攻击者修改或伪造。即使组外用户无攻击企图时, 也不能对构建组播密钥产生任何影响。

可扩展性: 可扩展性影响群组密钥管理的性能。在同一个群组中, 每一个成员所需要的计算处理量, 应与群组的大小无关, 群组的成员变动, 应只影响群组的某一小部份而已^[2]。

健壮性: 如果有一小部份的成员受到危害, 例如机密资料被破解等情况, 不应该危及所有的群组成员, 可以将接收群组分割成多个较小群组, 这样就可以避免这种情形发生^[3-5]。

共谋防范: 不允许部分成员经由彼此交换某些秘密, 而得到额外的访问权力。

2 密钥管理

组播环境中, 同一组中的成员共享一把通讯用的共享私有密钥, 在成员变动时更新后的公开密钥如何重新送到其它成员, 一些学者针对这一问题提出了一些解决方法^[2-6,9], 对这些解决方案的评价通常从安全性及性能进行评价, 尤其是性能的评价, 如果设计的密钥更新方

案可扩展性不理想,在组成员数量增加时,往往影响此组播方案的性能。

假设同组的 n 个成员已经共享一把通讯用的共享私有密钥 (K),在删除某一成员时,为了使被删除的成员无法访问接下来的通讯资料,我们必须产生一个新的公开密钥 (K'),再将此公开密钥更新到其它成员。有以下几种方式来完成:

方案一

同一组的每一个成员,与本组的控制中心共享一把个人的私有密钥 (SK_i),当有成员被删除时,控制中心便再选择另一把通讯用的公开密钥 (K'),分别使用其余每一个成员的私有密钥,将公开密钥加密后分送出去。这个方法在每次需要更新公开密钥的时候,必须作 $(n-1)$ 次的加密计算,当成员人数 n 增大时,显然不能满足可扩展性的要求。

方案二

Steiner 等人于 1996 提出一种使用 Diffie-Hellman 公开密钥技术,来建立密钥更新方案^[10],但是这种方案效率并不高,一个有 n 个成员的组就需要 n 的指数次方的运算,在许多的组播环境之下,成员数量 n 增加到一定的程度时,这样的运算量的增加是很难接受的。

方案三

Wallner 等人^[9]的方法有较小的开销,在 n 个成员的组中,每一个成员需要储存 $\log n + 1$ 把密钥,当有成员被删除时,系统重新产生一把新的通讯用的公开密钥,经过 $2\log n - 1$ 次加密处理后,便可以将此公开密钥安全地传送给其余的所有成员,所以此方案的开销为 $2\log n$,下面分析及讨论该方法的优缺点及其改进之处。

3 组播来源认证

组播消息的来源认证问题,分为两类,一类为单一来源,即组播的来源是固定一个端点,例如按次付费的应用;另一类为可变来源,只要是群组的成员都可能成为发送组播消息的人,例如在线视频会议。由于无法用是否拥有唯一的共享通讯密钥来认证消息来源,如果要使用公开密钥签名的方式来认证,那么在实际应用中存在效率低及无法容忍分组丢失问题^[7, 11-12],目前的研究大多集中在消息验证码 MAC 的应用。

MAC 算法是一个不可逆的函数,假设通讯双方 A 与 B 共享一把私有密钥 K ,当 A 要传送消息 M 给 B 时,它会将消息与私有密钥当作参数带入函数中产生消息验证码 $MAC(K, M)$,将消息 M 与消息验证码 $MAC(K,$

$M)$ 一起送给接收端。接收端比对所接收到的 MAC 与其算出来的 MAC,如果相同的话,则接收端可以验证此消息来自合法的发送端,而且接收到的消息没有被更改。

在组播应用下,因为组成员共享同一私有密钥,要直接应用 MAC 的技巧来验证消息来源是无法做到的。Cannett 等人提出了一种利用 MAC 概念的组播来源的认证方法^[7],此方法可以认证单一固定的来源,也可以扩展为任意成员均可成为消息的发送端,在导入机率的概念下,此方案可以动态的调整所需的密钥数量,以符合系统的安全需要。

Cannetti 等人提出的方法假设能猜出某消息的 MAC 的机率最大为 q ,组播群组中的成员最多有 w 个互相勾结:

消息的发送端 S 拥有一组密钥的集合 $R = \{K_1, K_2, \dots, K_l\}$, 其中 $l = e^{(w+1) \ln(1/q)}$ 。

消息接收端 U 拥有 R 的子集合 R_u , 每一个密钥 K_i 在 R_u 的机率为 $1/(w+1)$, 所以每一接收端要拥有 $e^{h(1/q)}$ 把密钥。

S 将消息 M 以及一组 MAC 值 $\{MAC(K_1, M), MAC(K_2, M), \dots, MAC(K_l, M)\}$ 一起传送出。

每一个收端 U 用自己 R_u 之中的密钥来对 M 产生相对的 MAC, 如果有任一个 MAC 不在发送端传来的那一组 MAC 值当中, 则拒绝接受此消息, 因为此项消息可能不是发送端传来的。

在上述的密钥数量的设定当中,可以保证 R_u 被 w 个互相勾结的成员的密钥完全涵盖的机率会小于 q 证明如下: 假设某一把密钥在某一接收者的子集合内, 而且不在任何一个互相勾结的成员的子集合内的机率为 g

$$\left(1 + \frac{1}{w}\right)^w < e \quad (1)$$

$$g = \frac{1}{w+1} \left[1 - \frac{1}{w+1}\right]^w = \frac{1}{(w+1) \left(1 + \frac{1}{w}\right)^w} > \frac{1}{e^{(w+1)}} \quad (2)$$

R_u 被 w 个互相勾结的成员的密钥完全涵盖的机率为:

$$(1-g)^l < \left[1 - \frac{1}{e^{(w+1) \ln(1/q)}}\right]^{e^{(w+1) \ln(1/q)}} < e^{-h(1/q)} = q \quad (3)$$

4 性能分析

消息发送端 S 需要保存 $l = e^{(w+1) \ln(1/q)}$ 把

MAC 密钥。

接收端 R 需要持有 $e h(1/q)$ 把 MAC 密钥。

每一个传送消息的通信开销为 $e(w+1) \ln(1/q)$ 。

发送端 S 的操作时间开销为 $e(w+1) \ln(1/q)$ 次 MAC 运算, 接收端 R 为 $e \ln(1/q)$ 次 MAC 运算。

上述的认证方法有一个好处是复杂度并不是随着成员的总数来变动, 而是随着可能互相勾结的人数 w 以及机率 q 来决定, 该特性可以满足可扩展性的要求, 即每一个别的成员所需要的计算处理的数量, 应该与此群组的大小是独立的。

本方法可以让任何成员来传送组播消息, Cannetti 等人利用伪随机函数的观念来扩展上述的做法:

系统使用 k 把主密钥 $\{K_1, K_2, \dots, K_k\}$, 每一把 K_i 定义一个伪随机函数 f_i 。

要接收消息的成员 V 拥有主密钥 $\{K_1, K_2, \dots, K_k\}$ 的子集合 R_v , 每一个密钥 K_i 在 R_v 的机率为 $1/(w+1)$ 。

要传送消息的成员 U 会得到第二组组的密钥 $S_u = \{f_1(u), f_2(u), \dots, f_k(u)\}$ 。

U 将消息 M 以及一组 MAC 值 $\{MAC(f_1(u), M), MAC(f_2(u), M), \dots, MAC(f_k(u), M)\}$ 一起传送出去。

每一个接收端 R 用自己 R_v 之中的密钥来产生第二组密钥对 M 产生相对的 MAC, 如果有任一个 MAC 不在发送端传来的那一组 MAC 值当中, 则拒绝接受此消息, 因为此项消息可能不是发送端传来的。

上述方法发送端的操作与之前的单一消息的来源作法一样, 而对于接收端来说唯一要增加的工作就是将第二组密钥推导出来, 因此本方法有以下特性:

(1) 可以动态地改变发送端, 只要给定相关的第二组密钥 S_u , 任何一个成员皆可传送消息。

(2) 可以指定某个成员只能在某个时间区段传送消息, 如果这个成员被指定在时间 T 传送消息, 系统可以给定第二组密钥 $f_i(T)$, 并且要求发送端在指定的时间区段传送消息。

5 讨论

组播系统的协议以及架构的设计, 除了需要满足保密性、来源认证的要求外, 可扩展性及封锁性问题更是组播系统需要重视之处。同一个群组中, 每一个成员所需要的计算处理量, 应该尽量与群组的大小无关。群组的成员如果有更改, 应该只会影响组中的某一小部份, 系统的性能不会因为成员的频繁变动而大幅下降。

从 Walther 等人的方法中可以发现, 所有的成员共享一把用来加密消息的通讯密钥, 一旦通讯密钥被入侵者得知, 此入侵者便可以在网络任何一处接收组播消息, 所以本方法没有封锁性。虽然本方法重发密钥时的通信开销可以降至 $O(\log n)$, 每当有成员离开本群组时, 所有的成员共享的通讯密钥就要加以更新。因为一个成员的变动使得所有成员受到影响, 这对于系统的性能有不利的影响。

Mitra 提出 DIUS 的组播架构^[4], 将接收成员分隔为数个子组连结于组安全代理本地服务器中, 这些组安全代理构成一个树状结构, 发送端将消息先往树根传送, 再依序传到下方的节点组安全代理服务器直到接收端为止。每一个组安全代理各自使用不同的对称式加密密钥, 每当组安全代理收到组播消息, 将它解密之后再使用自己的加密密钥将此消息加密, 继续往下方的组安全代理传送。这个方法的好处是如果有某个接收者的对称密钥遭入侵者得知, 只会影响同一个子群组的成员, 所以并不需要将所有成员的通讯密钥加以更动, 它的缺点是经过的中间节点可以解开组播消息的明文, 消息的保密性较差, 虽然 IOLUS 虽然有上述的缺失, 但是它的组播架构拥有不错的封锁性质, 有进行改进的价值。

6 结束语

安全组播源认证问题一直是安全组播通信中的研究热点之一, 本文讨论了组播系统中密钥管理的问题, 提出了组播安全密钥管理及性能方面应改进之处, 定量分析了组播消息的来源认证方法的性能。良好的组播技术可以让群体的成员能够安全又高效地进行群体通讯, 值得我们加以深入的研究与创新。

参考文献:

- [1] 徐明伟, 董晓虎, 徐恪. 组播密钥管理的研究进展 [J]. 软件学报, 2004, 15(1): 141-150
- [2] Noubir G, Zhu F, Chan A H. Key management for simultaneous join/leave in secure multicast [C]. Proc of IEEE International Symposium on Information Theory 2002 325-325
- [3] Chan K in-Ching, Chan S H G. Distributed servers approach for large-scale secure multicast [J]. IEEE Journal on Selected Areas in Communications 2002, 20 1500-1510.

- [4] Mittal S, Iohis A. A framework for scalable secure multicasting [C]. Proc of ACM Conference on Communications Architecture and Protocols, 1997: 277-288
- [5] Refik M, Olva, Alain Pannetrat. Scalable multicast security with dynamic recipient groups [J]. ACM Transactions on Information and System Security, 2000, 3(8): 136-160
- [6] Briscoe B. MARKS: Zero side-effect multicast key management using arbitrarily revealed key sequences [C]. Proc of 1st International Workshop on Networked Group Communication, 1999: 301-320
- [7] Canetti R, Garay J, Itkis G, et al. Multicast security: a taxonomy and some efficient constructions [C]. Proc of IEEE INFOCOM '99, 1999: 708-716
- [8] Limingyan, Poovendran R, Berenstein C. Design of secure multicast key management schemes with communication budget constraint [J]. IEEE Communications Letters, 2002, 6: 108-110.
- [9] Wallner M, Harder E J, Agee R C. Key management for multicast: Issues and architectures [S]. RFC2627, 1999-6
- [10] Steiner M, Tsudik G, Waidner M. Diffie-Hellman key distribution extended to group communication [C]. Proc of 3rd ACM conference on computer and communications security, 1996: 31-37.
- [11] Park JM, Chong E K, Siegel H J. Efficient multicast packet authentication using signature amortization [C]. Proc of the IEEE Symposium on Research in Security and Privacy, 2002: 227-240
- [12] Perrig A, Canetti R, Tygar J D, et al. Efficient authentication and signing of multicast streams over lossy channels [C]. Proc of IEEE Symposium on Security and Privacy, 2000: 56-73

Analysis of Secure Multicast Source Authentication Performance

HE Zhi-yong, ZHAO Chun-sheng

(School of Computer Science, Sichuan University of Science & Engineering, Zigong 643000, China)

Abstract Multicast technology can provide a safe and an efficient group communications for its members out of the security need. The performance of source certification impacts directly the multicast scheme. In this paper, the security of multicast system and the management scheme of key have been discussed, a multicast source authentication method based on MAC concept proposed by Canetti etc. has been analysed and its performance has been quantitatively analysed at the same time. The analysis result has certain reference significance for the performance evaluation of the security multicast source authentication method.

Key words secure multicast authentication, key management, performance analysis