基于可信度的分布式组播密钥管理研究

许建真，梁克会，董永先
（南京邮电大学 计算机学院，南京 210003）

摘　要：局部分布式组播密钥管理将安全信息限制在若干个服务器节点上，如果这些节点本身可信度不高，将会导致整个网络的安全受到威胁。在局部分布式组播密钥管理中引入了服务器节点的可信度机制，通过可信度的计算来维护一个可信度较高的密钥更新服务器组。仿真结果表明，引入可信度机制，可以提高 Ad hoc 网络中密钥更新的成功率以及减少更新延迟时间，从而达到提高整个网络安全的目的。

关键词：可信度；密钥管理；局部分布式；自组织网络；网络安全
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2010)01-0271-03
doi:10.3969/j.issn.1001-3695.2010.01.080

Study of distributed multicast key management based on creditability

XU Jian-zhen, LIANG Ke-hui, DONG Yong-xian
(*College of Computer, Nanjing University of Posts & Telecommunications, Nanjing* 210003, *China*)

Abstract: The local distributed multicast key management limits the security information in several server nodes. If these nodes have not enough creditability, they will cause the whole network insecurity. This paper introduced the node creditability in the local distributed key management system. By calculation of their creditability, selected nodes with higher creditability as servers. The simulation results show that with the node creditability the key updating success rate in Ad hoc network is improved, and its delay time is reduced, so the entire network security has been enhanced.
Key words: creditability; key management; local distributed; Ad hoc network; network security

作为一组无线移动节点的集合，Ad hoc 网络可以在没有任何网络基础设施和集中化管理的情况下进行通信。网络中不需要任何类似于基站或者移动交换中心这样的集中化控制设施。Ad hoc 网络为用户提供了不受限制的移动性和连通性。正是由于 Ad hoc 网络具有开放媒质、动态拓扑、缺乏中心授权、分布式合作、受限的网络能力等基本特点，使其特别容易受到攻击，Ad hoc 网络的安全问题已经成为制约其快速发展的一个重要因素。

加密技术是一些网络通信安全机制的基础，密钥管理技术是加密系统成功应用的关键部分，它是取得安全组通信的基石[1]。有线网络的安全组通信研究取得了许多进展，提出了多种高效的组密钥协议[2,3]。为了解决 Ad hoc 网络的安全问题，人们也提出了多种密钥管理技术[4,5]。根据拓扑结构的不同，可以把这些密钥管理方案分为集中控制式、分布式和分层分组式[6~8]。

1　局部分布式密钥管理

分布式密钥管理[9,10]又分为完全分布和局部分布。局部分布式密钥管理技术[11]将密钥分发中心变为网络中的一组服务器节点，由这组节点共同承担密钥管理的责任，这就改善了完全分布式密钥管理负载过大和服务时间过长的问题，提高了密钥更新的成功率。在服务器组内利用 (t,n) 门限共享技术[12,13]，每次选择 t 个服务器节点联合完成组密钥的更新和分发，实现一个分布式的密钥分发中心。由于在网络中只有若干个固定的节点参与密钥的生成，这个方案的缺点是：分担密钥分发责任的节点不能随意离开网络，由于其身份的特殊性有可能成为网络的瓶颈，尤其是当某些服务器节点本身安全没有保证的情况下，将会影响整个网络的安全。为了解决这个问题，本文提出了基于可信度的局部分布式组播密钥管理技术。

2　基于可信度的分布式密钥管理

2.1　系统描述

在 Ad hoc 网络的局部分布式密钥管理的研究中，假设所有服务器节点均是一直可信的，在实际应用中并不现实，如有个节点在系统初始化时可信度很高，但是在后来其成为了一个恶意节点，可信度变得很低。在局部分布式密钥管理中，无论这一节点的可信度有多低，都仍然会在服务器组中参与密钥的生成和分发，这无疑会威胁到整个系统的安全。本文中增加了一个服务器可信度的计算，当某服务器节点可信度低于一个设定值时，就将其在服务器组中删除，并重新在其他非服务器节点中选择一个可信度高的节点加入服务器组，这样就维护了一个安全性较高的服务器组。

2.2　系统初始化

在系统初始化前，本文先约定如下符号的含义：

PK/SK：系统的公/私钥；

收稿日期：2009-04-20；**修回日期**：2009-06-03

作者简介：许建真（1966-），男，安徽砀山人，副教授，硕导，博士，主要研究方向为计算机通信与网络互联技术（xujz@njupt.edu.cn）；梁克会（1984-），男，江苏徐州人，硕士研究生，主要研究方向为计算机通信与网络互联技术；董永先（1984-），女，江苏常州人，硕士研究生，主要研究方向为计算机通信与网络互联技术.

S_i:节点 i 的共享秘密份额;

ID_i:节点惟一的身份标志;

$Cert_i$:节点 i 的证书;

PK_i/SK_i:节点 i 的公/私钥;

W_i:节点 i 的可信度;

DEK:组密钥。

初始时,系统需要一个离线的密钥管理中心为服务器节点颁发证书和分配共享秘密份额。假设组播组中共有 N 个成员节点,选择其中可信度最高的 M 个作为服务器节点,服务器节点构成服务器组。在进入组播组之前,每个成员节点自己生成或由密钥管理中心生成并分发一对公/私密钥 $PK_i/SK_i(1\leqslant i\leqslant N)$,并且中心为每个成员颁发一张证书 $Cert_i$。密钥管理中心负责生成组播组的公/私钥 PK/SK,SK 为系统共享秘密,选取秘密共享的门限值为 t,$1\leqslant i\leqslant M$,并按照门限秘密共享技术为 M 个服务器节点生成共享秘密份额 S_i,$1\leqslant i\leqslant M$。

系统的组密钥管理服务由服务器组来提供,所以系统建立之初首先要由服务器节点形成服务器组,初始过程采用类似 Wu 等人[14]的方法。当一个服务器节点加入组播组时,它首先广播一个加入服务器组的请求,请求报文包含的主要条目为:

ID_i	$Cert_i$	SEQ_i	W_i	TTL	isServ	$[h(ID_i,W_i,SEQ_i)]^{SK_i}$	$(TTL)^{SK_i}$

其中:ID_i 代表节点的身份;$Cert_i$ 表示节点的证书;SEQ_i 表示请求报文的序列号;W_i 是服务器节点的可信度;TTL > 0 表示报文的生命期;isServ 表示是否是服务器节点;后面两项为相关项的签名,用来验证请求报文的完整性。收到请求的服务器节点回复响应消息。经过这个过程,组播组的成员被分成服务器节点、转发节点和普通节点,转发节点负责连接这些服务器节点,构成一个连通的服务器组。由于 Ad hoc 网络节点的移动性,服务器组的结构处于动态的变化中,需要服务器节点周期性地更新,保持服务器节点间路由的有效性。更新的周期根据网络的实际情况确定。服务器组在形成和更新过程中,把最小 ID 的服务器节点设定为组控制器。组控制器负责发起组密钥和服务器组密钥的定时更新以及管理服务器组,服务器组密钥用于加密组密钥发送给各个服务器节点。

2.3 组密钥的生成

在服务器组形成的过程中,密钥管理利用(t,n)门限共享技术。为了提高在通信链路相对不好的情况下密钥更新的成功率,选取的服务器节点数目应该大于门限 t,如 $t+h$,有一个冗余量 h。请求服务的服务器节点用最先响应的 $t-1$ 个节点的密钥信息,加上自己的密钥信息,生成组通信密钥。本文采用类似 Wu 等人[14]的 RSA 算法,生成过程如下:

a)执行组密钥更新的服务器节点 X_i,生成组密钥种子 seed,再选取要联合的其他 $t+h-1$ 个服务器,向其他节点发送密钥服务请求,请求报文包含 seed。

b)签名$(seed)^{S_j} \bmod p$,然后通过安全信道发送给请求服务器节点 X_i。

c)服务器节点 X_i 联合最先响应的 $t+h-1$ 个节点密钥信息,加上自己的密钥信息,计算

$$\prod_{j=1}^{t}((seed)^{S_j})^{l_j(0)} \bmod p = (seed)^{\sum_{j=1}^{t}S_j l_j(0)} \bmod p$$

产生一个完整的签名 $(seed)^{SK}$。

d)服务器节点 X_i 对产生的签名 $(seed)^{SK}$ 用散列函数 $h(\cdot)$进行计算得到组密钥:

$$DEK = h(h(seed^{SK}))$$

在组密钥管理算法中,需要门限 t 个服务器节点联合才能生成组密钥,在网络的运行过程中,当某服务器节点的可信度低于某个门限值时,就将该节点强制退出服务器组,并从其他节点中重新选择一个可信度较高的节点加入服务器组。每个节点的信任度列表中都包括记录,假设每个节点在加入组播时可信度都是 1,节点 i 按照下式动态计算并更新其可信度值:

$$W_i(t+1) = \sum_{a\in A} W_{ia}(t)\times P_a + \sum_{b\in B} W_{ib}(t)\times P_b$$

其中:A 为通常的权重项集合,如移动性、电源等;B 为主观性角色权重项集合,如会议组织者;$W_i(t+1)$是节点 i 在下一时刻的可信度值;P_a 和 P_b 为集合 A 和 B 的权值;W_{ia} 和 W_{ib} 为在集合 A 和 B 中各项对应权值。

2.4 组播组成员信息的维护

Ad hoc 网络节点处于不停的移动中,组播组的成员可能随时加入或离开。所以,成员的状态信息管理对及时更新组密钥、保障系统的前向和后向安全非常重要。

采用服务器节点分布存储组播组成员信息方式,而不是采用一个集中的服务器来管理,避免了单点失效问题。组成员的维护管理采用向服务器节点注册的方法,方法类似于局部分布式密钥管理。这里只是介绍服务器节点更新过程:每次一个服务器节点发起更新并向其他节点发出请求信息时,所有收到这些信息的服务器都查看该服务器节点的可信度,当可信度低于某个设定值 α 时,就将该服务器强制离开服务器组,然后检查其他非服务器节点的可信度;如果存在可信度最高且最高比 α 大的节点,就将该节点加入服务器组,并更新密钥,此时服务器组更新成功,否则更新失败。服务器节点的更新如图 1、2 所示。在图 1 中,服务器组检测到节点 1 的可信度低于 α 值,所以将节点 1 强制离开服务器组,并选择了可信度较大的节点 2 作为新的服务器节点加入到服务器组(图 1 和 2)。

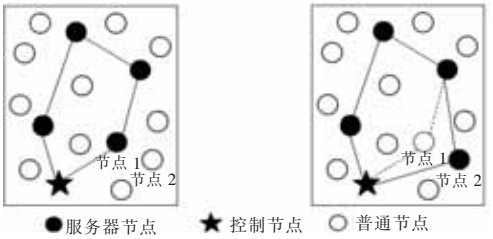

图 1 可信度低节点 1 删除前 图 2 可信度低节点 1 删除后

为了减少通信开销,维护信息都是发生在局部范围,最大移动距离 H 的选择可以根据具体的网络节点数、服务器节点数以及网络的环境参数而定。

2.5 组密钥更新与分发

组播组成员是动态变化的,在新节点加入或原节点离开组播组时,为了保证组播通信的前向和后向安全,必须更新组通信密钥。由于普通节点的加入和退出情况与分布式密钥管理相同,在此不再论述。下面仅讨论服务器节点加入和退出的情况。

a)服务器节点的加入。当一个节点向服务器节点发出的请求报文中 isServ 置 1 时,表示该节点要加入服务器组。密钥更新中,根据组密钥管理算法生成新的组通信密钥 DEK 和服务器组密钥 SKEK,用原来的组通信密钥加密 DEK 后组播给原来的组成员节点,用原来的服务器组密钥加密 SKEK 组播给原来的服务器节点,并用新加入服务器节点的公钥加密 SKEK,

单播给该服务器节点。

b)服务器节点的离开。当一个服务器节点要离开或由于可信度低被强制离开组播组时,首先向服务器组内其他节点发送离开请求,同时向注册到自己的各普通节点发送离开声明,收到离开声明的节点重新注册到其他服务器节点。经过一定时间间隔,服务器节点离开。根据组密钥管理算法,收到请求的服务器节点生成新的组通信密钥 DEK 和新的服务器组密钥 SKEK,由于不能用原来的 SKEK 加密组播新密钥 DEK,使用各服务器节点公钥加密新生成的 SKEK 和 DEK,单播给各服务器节点。各服务器节点解密后,向注册到自己的各个节点用各自的公钥加密新 DEK 后单播。

3　仿真结果及分析

在 Ubuntu 8.04 下搭建一个 NS2 仿真平台,用本方案(CDKM)在组密钥成功率、更新延迟时间和通信量三个方面与已有的局部分布式密钥管理方案(DKM)进行比较。为了使实验结果更能显现方案效果,本文在实验中安排某个服务器节点可信度由高于 α 变为低于 α。仿真过程中忽略计算延迟。

首先利用 NS2 中无线模块的 setsest 和 cbrgen 生成场景文件和数据文件,仿真中移动模型采用 PWP,空间区域为1 200 × 1 200,节点数量为 60 个,节点在空间中随机运动,每个节点的通信半径为 300 m,节点的移动速度为 5 m/s,节点到达指定位置后停留 5 s,模拟时间为 200 s,服务器比例为 0.1,即服务器节点有 6 个,秘密共享门限是 5,仿真过程中有一个节点的可信度一直在下降,在此情况下密钥更新成功率随时间变化如图 3 所示。

仿真结果表明,本文的基于可信度的分布式密钥管理方案和分布式密钥管理方案在刚开始时均有较高的更新成功率,随着仿真的进行,其中某个服务器节点可信度越来越低,DKM 方案中密钥更新成功率一直下降。而 CDKM 在 80 s 左右时密钥更新成功率又有了很大的提高,这是由于在 80 s 左右时可信度低的服务器节点被强制离开了服务器组,而又加入了一个可信度高的节点。

对密钥更新过程中的延迟时间进行仿真,结果如图 4 所示。由图可知,由于服务器组中有个节点可信度不高,导致 DKM 方案中密钥更新延迟时间随时间增加而一直增大,最终延迟时间高达 0.6 s。CDKM 方案中在 80 s 时延迟时间达到 0.7 s,这是由于删除和添加服务器节点导致密钥更新延迟时间增加,80 s 后由于服务器组节点可信度均很高,密钥更新延迟又恢复到 0.3 s 左右。因此 CDKM 要优于 DKM 方案。

图 5 是关于 DKM 和 CDKM 两种密钥管理方案的通信量比较的仿真结果,此处通信量定义为密钥更新过程中发送包的总数量与包大小的乘积。为了使图更加简洁,本文采用了归一化方法。由图可知,由于 CDKM 方案增加了可信度计算并且报文比 DKM 方案大,整体上比 DKM 方案通信量要大,并且当服务器节点删除和加入时,通信量会有所增加。当服务器节点删除和加入完毕,CDKM 方案通信量又恢复到起始阶段大小。

4　结束语

本文提出了一种基于可信度的局部分布式密钥管理方案,该方案通过节点可信度计算来删除服务器组中可信度低的节点,然后选择一个可信度高的节点作为服务器节点,以此提高组密钥更新成功率并减少更新延迟时间。仿真结果表明,选择合适的可信度值,本方案可有效提高密钥更新成功率并减少更新延迟时间。由于只有当服务器节点可信度低于限定值时才发生节点更新,该系统只需增加少量通信量就可以有效地保证 Ad hoc 网络密钥更新的成功率。但是,该方案仍然会在一定程度上增加通信量,并在增减服务器节点时带来密钥更新延迟时间增大,且当服务器组中节点频繁地加入和退出时,将会导致通信量有很大的增加。在考虑了组播安全性能的情况下,该方案在组播效率方面的性能会有所下降。

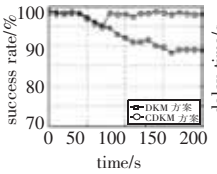

图 3　DKM 和 CDKM 密钥更新成功率比较

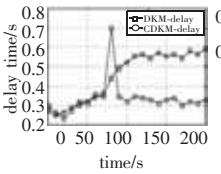

图 4　DKM 和 CDKM 密钥更新延迟时间比较

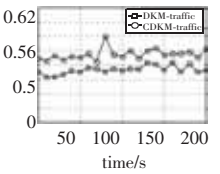

图 5　DKM 和 CDKM 密钥更新过程中通信量比较

参考文献:

[1] XU Ming-wei, DONG Xiao-hu, XU Ke. A survey of research on key management for multicast[J]. Journal of Software, 2004,15(1): 141-150.

[2] MOYER M J, RAO J R, ROHATGI P. A survey of security issues in multicast communications[J]. IEEE Network, 1999,13(6): 12-23.

[3] WALLNER D, HARDER E, AGEE R. RFC 2627, Key management for multicast: issues and architectures[S]. [S. l.]: Internet Engineering Task Force, 1999.

[4] 肖德贵,杨金,罗娟. 基于多项式和分组的无线传感器网络密钥管理方案[J]. 计算机应用研究,2009,26(3):680-685.

[5] 孙海波,张权. 基于密钥矩阵的组播密钥管理方案[J]. 计算机工程,2008,34(21):112-114.

[6] LEE S L, JEUN I K, SONG J S. Mixed key management using Hamming distance for mobile Ad hoc networks[C]//Proc of the 7th International Conference on Computational Science. 2007:665-672.

[7] ZHANG Li-ping, CUI Guo-hua, YU Zhi-gang. An efficient group key agreement protocol for Ad hoc networks[C]//Proc of International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008). 2008:1-5.

[8] HIETALAHTI M. A clustering-based group key agreement protocol for Ad hoc networks[J]. Electronic Notes in Theretical Computer Science, 2008,192(2):43-53.

[9] KUANG Xiao-hui, HU Hua-ping, LU Xi-cheng. A new group key management framework for mobile Ad hoc networks[J]. Journal of Computer Research and Development, 2004,41(4):704-710.

[10] 张玉臣,王亚弟,刘　,等. Ad hoc 网络环境下分布式密钥管理[J]. 武汉大学学报:理学版,2009,55(1):85-88.

[11] ZHOU Li-dong, HASS Z J. Secure Ad hoc networks[J]. IEEE Networks, 1999,13(6):24-30.

[12] 陈礼青,张福泰. 基于门限秘密共享的动态安全组播密钥协商[J]. 计算机工程,2008,34(1):147-149.

[13] ZHANG Jiang, LUO Jian-guang, LI Bin, *et al*. SIKAS: a scalable distributed key management scheme for dynamic collaborative groups[C]//Proc of IEEE International Conference on Multimedia and Expo. 2006:1205-1208.

[14] WU Bing, WU Jie, FERNANDEZ E B. Secure and efficient key management in mobile Ad hoc networks[J]. Journal of Network and Computer Applications, 2007,30(3):937-954.