FTP 客户端程序的技术设计思路,基于 Visual FoxPro 语言的 WinINET 函数库,采用面向对象、消息驱动及多线程等技术实现了 FTP 传输工具软件的各种功能,并采用可视化界面设计,用户操作简单方便. 经过测试,FTP 客户端程序具有高度的交互性,可以快速、稳定地实现文件的上传和下载等传输功能,实现了 Internet 上数据信息的快捷共享. 为了在 VFP 各种应用软件中集成该 FTP 客户端程序,对其进行封装,设计成 FTP 类,可直接使用.

参考文献

[1] Douglas E Comer. Computer Networks and Internets[M]. 5th ed. Prentice Hall,2009.

[2] 刘志宇,杨柳. 网络安全中的端口扫描技术[J]. 牡丹江师范学院学报:自然科学版,2009(4):7-9.

[3] 李芙蓉. 基于 Winsock 流套接字的进程通信的实现[J]. 西安文理学院学报:自然科学版, 2010,13(2):81-84.

[4] 高永强,张天刚. 基于 WinSock 的网络编程技术[J]. 山西大同大学学报:自然科学版,2010,26(5):20-22.

[5] WinInet 编程中如何使用异步[EB/OL]. (2012-01-11)[2012-06-24]http://www.doc88.com/p-666164878572.html.

[6] 方冰,张一中. 高性能 FTP 搜索引擎的设计[J]. 南京邮电大学学报,2007,27(3):67-70.

编辑:文心

大规模组播通信密钥管理方案研究

范书平,柴宝杰,佟 林,牛 锐*

(牡丹江师范学院 工学院,黑龙江 牡丹江 157011)

摘 要:在现有组播密钥管理方案的基础上进行扩展,提出一种适用于大规模组播通信的密钥管理方案,并讨论方案中密钥树维数的最佳取值,将改进方案的性能与逻辑密钥层次方案(LKH)进行对比,分析结果表明,本文方案在密钥存储量、更新量等方面优于 LKH.

关键词:组播;密钥管理;密钥树; 更新量

[中图分类号]TP309 [文献标志码]A [文章编号]1003-6180(2012)04-0015-03

相对于点到点的安全通信机制,组播密钥管理方案更加复杂,要保证组成员加入和删除后网络的安全. 此外,安全组播通信还有许多问题要解决,如可扩展性,网络通信量与存储量,组成员失效后密钥更新量等.[1-2] 为了保证组播的通信安全,组播密钥管理方案变得尤为重要. 目前存在的组播密钥管理方案主要有三种,分别是集中式、分布式和分层分组式密钥管理方案. 集中式组播密钥管理方案中存在一个根或组控制器 S,它存储组内所有通信密钥并且整个组内密钥的生成、分发以及更新过程都由其控制,这类方案的缺点:会产生由 S 导致整个组容易暴露的单点失效问题;分布式组播密钥管理方案的容错性好,但是由于缺少集中控制,使得组播通信很难管理;采用分层分组式组播密钥管理方案控制节点与组播成员间形成了一种层次关系,但方案中存在前两种方案之一的缺点[3-4].

1 组播密钥管理方案 LKH 及其改进方案

典型的组播密钥管理方案是 Wallner 和 Wong 提出的逻辑密钥层次(Logical Key Hierarchy,LKH)方案 ,这种方案作为一种集中控制式的密钥管理方案被提出,是一种基于逻辑密钥树的密钥管理方案,树中除叶子节点是组播成员外,其余节点都是逻辑上的节点,用于加密和解密信息并向上层传递下层节点的密钥. 树中所有节点均对应一个密钥,S 存储树中所有密钥,树中最低层的叶子节点与组成员相对应,每个组成员存储从该组成员对应的叶子节点到根节点路径上所有

收稿日期:2012-09-07
基金项目:黑龙江省教育厅科学技术研究项目(12513094)
* 计算机科学与技术专业 2009 级学生

祖先节点对应的密钥. 图 1 为具有 4 个叶子节点的二叉密钥树,与 4 个组成员是一一对应的. S 将存储树中的所有密钥,其中 k_{00} 是所有组成员共享的组密钥. 因此,在逻辑密钥树中,根节点存储 $\{k_{00},k_{10},k_{11},k_{20}\cdots k_{23}\}$,$u_1$ 存储 $\{k_{20},k_{10},k_{00}\}$,u_2 存储 $\{k_{21},k_{10},k_{00}\}$,其他节点以此类推.

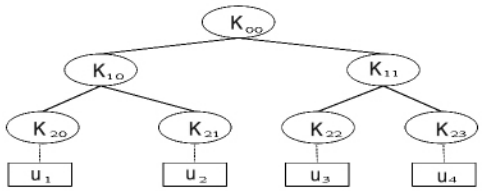

图 1　逻辑密钥树

文献[6]提出了一种改进 LKH 的组播密钥管理方案,并根据节点的剩余能量构造了树结构,树中节点按照从上到下、从左到右能量依次降序排列,即节点的层次越高,能量也越高,且同层节点中,最左侧节点的能量最高,方案中所有节点均为实际的组成员,这与 LKH 有所不同. 但该方案进行了理想化,仅将对 LKH 的改进方案适用于完全二叉树的情形,这在实际部署中几率是很小的. 针对该方案的不足进行改进,将该方案扩展到完全 k 叉树($k>=2$,$k\in Z$),使得改进密钥管理方案适用于大规模组播通信情况,并讨论了维数 k 的最佳取值,并将节点含有的平均密钥个数作为节点失效后的平均密钥更新量.

根据文献[6],当密钥树为二叉树时,设其高度为 $h(h>0,h\in Z)$,则其组成员最多可以有 2^h-1 个,所有成员的总密钥存储量为 $2^h*(h-1)+2$,组控制器端的密钥存储量为 2^h-1. 本文方案中,设密钥树的根节点存储一个密钥,则通过递归运算,当密钥树为 $k(k>1)$ 叉树时,不难得出密钥树中组成员最多可以有 $(k^h-1)(k-1)$ 个,所有成员的总密钥存储量为 $h*k^h/(k-1)-(k^{h-1}-1)*k/(k-1)^2-k/(k-1)+1$,一个节点失效后的平均密钥更新量为 $h*k-(k^{h-1}-1)/((k-1)*k^{h-2})-1/k^{h-1}$;LKH 中,当密钥树为 k 叉树时,不难得出密钥树中组成员最多可以有 k^{h-1} 个,所有成员的总密钥存储量为 $k^{h-1}*h$,一个节点失效后的平均密钥更新量为 $h-1$[7].

2　密钥树维 k 的最佳取值

考虑到逻辑密钥层次方案中,节点的存储量大,且节点删除时密钥通信开销大,这在能量受限的无线传感器网络中是不允许的,文献[6]所提出的改进方案仅考虑二叉密钥树的情况,本文将其扩展为 $k(k>=2)$ 叉树,并对 k 的最佳取值进行讨论,以便确定每个节点的最佳孩子节点个数,最大限度地减少网络开销. 在 Matlab 仿真环境下,利用 M 语言编程,可得到本文方案中 k 的不同取值所对应 S 的密钥存储量、节点失效后网络的密钥更新量情况. 当 $k=1$ 时,每个节点存储自己和祖先节点的密钥,节点的总存储量为 $h(h+1)/2$,一个节点失效后平均密钥更新量为 $h-1$,密钥存储量、更新量显然大于 $k>=2$ 的情况. 从图 2、图 3 中不难看出,在节点数目相同的情况下,随着 k 值的增大,节点的密钥存储量、平均密钥更新量增加的趋势越明显. 因此,可以得出当 k 取 2 时,网络中组控制器的密钥存储量最小,且节点删除后更新代价最小.

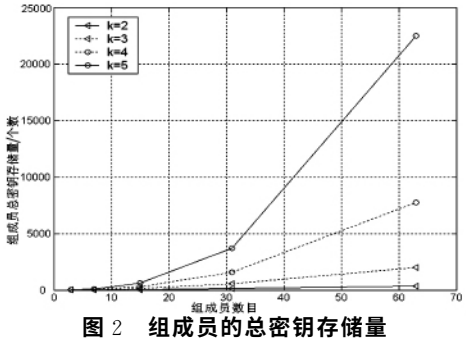

图 2　组成员的总密钥存储量

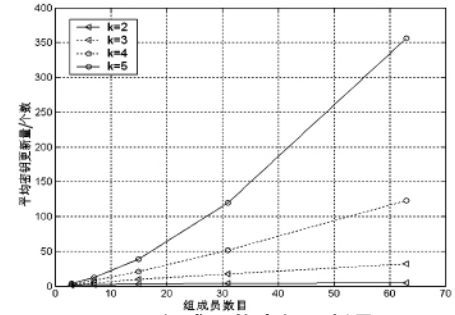

图 3　组成员的密钥更新量

3　性能分析

将本文方案从节点存储量、网络更新量、网络扩展性三方面与 LKH 方案进行对比,并给出两种方案的性能对比情况,设密钥树的高度为 h,树的维数为 k.

3.1　存储量

本文方案与 LKH 方案存储量的对比情况见图 4,从图中可以看出,当两种方案节点数目相同且树的高度相等的情况下,随着树维数的变化,本文方案组控制器的密钥存储量及节点的总密钥存储量都少于 LKH 方案. 这是由于本文方案中密钥树中节点均对应实际的组成员,因此,在节点数目相同时,采用本文方案节点总存储量、组控制器的存储量都少于 LKH.

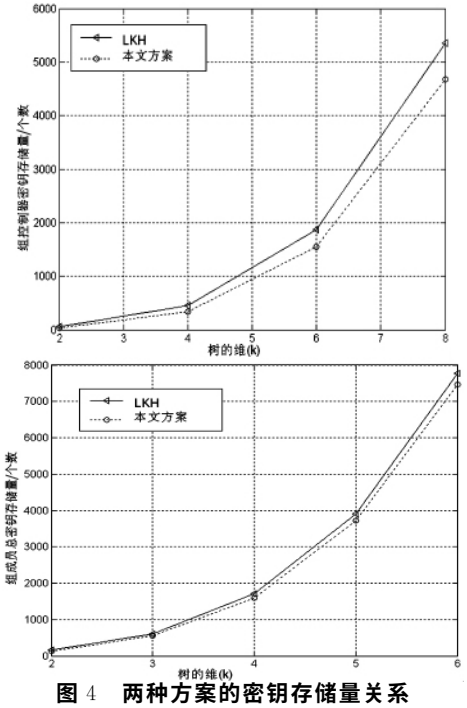

图 4　两种方案的密钥存储量关系

3.2　平均密钥更新量

根据文献[8],当一个组播成员离开时要更新组播组的密钥,防止离开的成员解密其离开后组内的通信内容,称为前向加密,从而保证剩余网络中节点间通信的安全性. 根据前面的分析进行实验,图 5 为两种方案中一个节点失效时密钥更新量的对比情况,从图中可以看出,本文方案在组成员数目相同的情况下,节点失效后平均密钥更新量更小.

3.3　扩展性

当树高为固定值时,采用 LKH 方案树中所能表示的组成员数目为 k^{h-1} 个,本文方案中计算出该数值为$(k^h-1)/(k-1)$,从图 6 中可以看出,当密钥树维数相同的情况下,本文方案表示的成员数目更多,实际应用中,根据组播通信规模的需要可以调整树的高度 h、维数 k,本文方案适用于大规模的组播通信.

4　结论

本文所提出的密钥管理方案适用于大规模的组播通信,方案中的密钥树适用于多叉树,并对树维数的最佳取值进行了讨论,从而使得网络的密钥存储量更小,网络通信量低. 与原有方案相比,特别是当密钥树的维数为讨论的数值时,本文方案扩展性能更好.

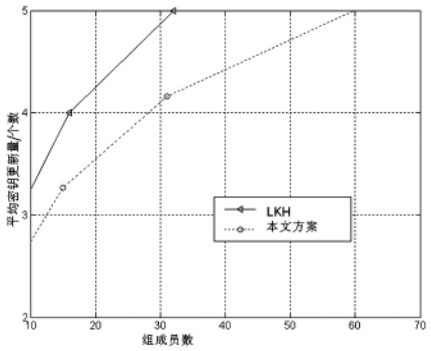

图 5　平均密钥更新量

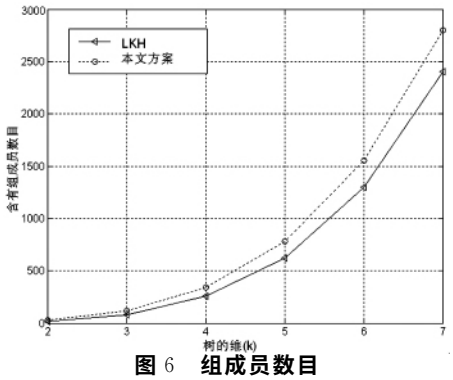

图 6　组成员数目

参考文献

[1] 范书平. 一种无线传感器网络组播密钥管理方案[J]. 牡丹江师范学院学报:自然科学版,2010(1):5-6.

[2] 宣文霞,窦万峰. 基于 LKH 的组播密钥分发改进方案 R-LKH[J]. 微电子学与计算机,2006:23(10),213-214.

[3] 晏轲,谢冬青. 基于逻辑密钥树的密钥管理方案及实现[J]. 计算机工程与应,2006,1 (3):145-147.

[4] 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.

[5] CK Wong, M Gouda, S S. Lam. Secure Group Communications Using Key Graphs[J]. IEEE ACM Trans Networking,2000,8(1):16-30.

[6] 范书平,马宝英,姚念民. 一种针对节点剩余能量的组播密钥管理方案[J]. 计算机工程与应用,2011,47(14),106-108.

[7] 李汉菊,蔡莎莎,张岩. 基于 LKH 的多播密钥管理改进方案[J]. 计算机工程,2005,22(31):152-153.

[8] Snoeyink J, Subhash S, George V. A lower bound for multicast key distribution[J]. Computer Networks,2005,47(3):429-441.

编辑:文心