

文章编号:1001-9081(2008)06-1388-04

无线传感器网络随机密钥预分配改进方案

田 丰, 王交峰, 王传云, 潘琢金, 孙小平

(沈阳航空工业学院 计算机学院, 沈阳 110034)

(wangif1021@163.com)

摘要:由于无线传感器网络节点能量、存储能力和计算能力的有限性,使传统的网络安全方案受到挑战。针对无线传感器网络的特点,在预共享密钥和随机密钥分发方案的基础上,提出了一种密钥分配方案。该方案采用只保存密钥池中密钥 ID 号的方法,节省了节点的存储空间。同时,考虑到传感器节点自身资源有限的特点,在满足加密需要的前提下,通过减少会话步骤、简化计算方法来降低传感器节点的工作负荷,从而使得传感器节点存储空间和通信开销都非常小,大大提高了传感器网络的工作效率。

关键词:无线传感器网络;网络安全;密钥分配

中图分类号: TP393.08; TP309 **文献标志码:**A

Improved scheme based on random key predisposition for wireless sensor network

TIAN Feng, WANG Jiao-feng, WANG Chuan-yun, PAN Zuo-jin, SUN Xiao-ping

(College of Computer Science, Shenyang Institute of Aeronautical Engineering, Shenyang Liaoning 110034, China)

Abstract: Due to the limitation of the nodes energy and the limitation of memory resources and computation ability in the Wireless Sensor Network (WSN), the traditional network security is challenged. Fully considering the characteristics of WSN, a key distribution scheme was proposed based on pre-shared key and random key distribution scheme, in which only ID-number of key in key pool was saved so as to save memory resources of sensor nodes. Furthermore, in view of the characteristics of resource limitation of sensor nodes, the working load of nodes was reduced through decreasing conversation steps and simplifying computation approach under the premise of satisfying the encryption needed. Thus in the scheme, the memory resource of the nodes and the correspondence cost are extremely small, and the working efficiency of the sensor network is improved greatly.

Key words: Wireless Sensor Network (WSN); network security; key distribution

0 引言

随着微电子技术、计算技术和无线通信等技术的进步,推动了低功耗多功能传感器的快速发展,使其在微小体积内能够集成信息采集、数据处理和无线通信等多种功能。无线传感器网络(Wireless Sensor Network, WSN)就是由部署在监测区域内大量的廉价微型传感器节点组成,通过无线通信方式形成的一个多跳的自组织的网络系统,其目的是协作地感知、采集和处理网络覆盖区域中感知对象的信息,并发送给观察者^[1]。因而可以被广泛应用于军事斗争、国家安全、环境监测、交通管理、医疗卫生、制造业和反恐抗灾等领域^[2]。

由于无线传感器网络的应用非常广泛,其安全性问题也受到越来越多的关注。传感器节点大部分是分布在野外人所不能够到达的区域,所以一些在传统网络中的安全方案不适用于无线传感器网络。在安全方案中,最为重要的是在节点之间、节点与基站之间进行通信时,对信息进行加密和身份认证^[3-4]。由于节点的能量、存储能力和计算能力受到了很大的限制,传统加密方案如公钥密码技术不适用于 WSN。在安全密码系统中,其核心问题是密钥的分发问题,因此如何根据

无线传感器网络的特点,设计合理、安全、高效的密钥分发方案是提高 WSN 安全的关键问题。

1 传感器网络安全需求和设计原则

由于传感器网络具有资源有限的特点,使得它在安全设计方面存在了很大的挑战。一种比较完善的无线传感器网络安全解决方案应当具备如下基本特征^[5-7]:

1) 扩展性:传感器网络的可扩展性表现在传感器数量、网络覆盖区域、生命周期、时间延迟、感知精度等方面可扩展极限。因此,给定传感器网络的可扩展性级别,安全解决方案必须提供支持该可扩展性级别的安全机制和算法,来使传感器网络保持良好的工作状态。

2) 可用性:传感器网络的安全解决方案所提供的各种服务能够被授权用户使用,并能够有效防止非法攻击者企图中断传感器网络服务的恶意攻击。同时,安全性设计方案不应限制网络的可用性。

3) 应用相关性:传感器网络的应用领域非常广泛,不同的应用对安全的需求也不相同。

为了减少信道阻塞以及信号冲突,节约能量消耗,延长网

收稿日期:2007-12-11;修回日期:2008-02-20。

作者简介:田丰(1958-),男,辽宁沈阳人,教授,博士,主要研究方向:计算机测控、无线传感器网络;王交峰(1980-),男,辽宁沈阳人,硕士研究生,主要研究方向:无线传感器网络;王传云(1984-),男,山东潍坊人,硕士研究生,主要研究方向:无线传感器网络;潘琢金(1962-),男,吉林集安人,教授,博士,主要研究方向:嵌入式计算机系统、计算机检测与控制;孙小平(1963-),男,黑龙江阿城人,教授,博士,主要研究方向:计算机检测与控制。

络寿命,提高网络的容错能力,对于 WSN 中的安全协议,还应遵循以下原则:1)尽量避免使用交互式的安全协议;2)避免信息的分段传输;3)支持传感信息的网内处理;4)较高的容错性能。

2 安全解决方案

针对分布式无线传感器网络结构,现已经提出预共享密钥和随机密钥分发等管理方案。

2.1 预共享密钥分发方案

预共享密钥分发方案是最简单的一种密钥建立过程,所有的传感器节点预配置一个相同的密钥,所有的节点均利用该密钥进行加密、解密、认证以及密钥的协商和更新。这种方案的优点是计算复杂度低,由于网络中只有一个密钥,所以很容易增加新的节点^[8]。但是它的不足之处也非常明显,如果一个节点被攻破,那么网络中所有的节点都将被攻破,整个网络就无安全性可言。

2.2 随机密钥预分配方案^[9]

该方案的基本思想是在节点部署前,部署服务器首先生成一个密钥总数为 P 的密钥池及密钥标识,每个节点从密钥池里随机选取 k 个不同的密钥。节点部署后,两个相邻节点若存在共享密钥,就随机选取其中的一个作为双方的会话密钥。否则,节点通过与其他存在共享密钥的邻居节点经过若干跳后建立双方的一条密钥路径。

根据经典的随机图理论^[10],节点的度 d 与网络节点总数 n 存在以下关系:

$$d = \frac{n-1}{n}(\ln n - \ln(-\ln P_m))$$

其中, P_m 为全网连通概率。若节点的期望邻居节点数为 n' ($n' \ll n$), 则两个相邻节点之间共享密钥的概率:

$$f = 1 - \frac{((P-k)!)^2}{(P-2k)!P!}$$

根据这个公式可以看出,要想达到很高的概率,每个节点要存储大量的密钥和密钥标识。这对资源有限的节点来说是不现实的,而且存储大量的密钥,将会导致整个系统变得脆弱。

2.3 Blom 的密钥预分布方案^[11]

Blom 利用对称矩阵的特性构造了一类会话密钥分发方案,使得节点能够与邻居中的任何节点独立计算会话密钥。Blom 方案具有 λ -secure, 即网络中只有多于 λ 个节点被攻破后, 整个网络才被攻破。每个节点存储负载为 $\lambda+1$ 个密钥长度, 当 $\lambda=n$ 时, 网络是完美安全的。因此该方案要获得高安全性, 则需要高的存储, 而且该方案的计算开销较大。

2.4 基于多项式的密钥对分布方案

Blundo 方案^[12] 使用对称二元多项式的性质 $f(x,y) = \sum_{i,j=0}^t a_{ij}x^i y^j$ 且 $f(x,y) = f(y,x)$ 为网络中的任意两个节点建立配对密钥。应用于传感器网络时,由于节点的能耗要求严格,而该方案计算多项式的计算量比较大,且它的扩展性比较差,当网络规模增大时,可用性不强。

3 方案的设计思想

根据以上算法的一些缺点,本文提出了一种基于无线传感器网络随机密钥预分配的改进方案。本方案在预共享密钥

模型和基本的随机密钥预分布模型的基础上,提出了一种新的密钥分配方案。在基本随机密钥的模型中,节点需要保存基站密钥池中的部分密钥和密钥对应的标识号(ID),这样对资源有限的节点来说非常困难,而且对网络的安全也存在一定的隐患。如果节点保存的密钥太多,那么部分节点被捕获,整个网络就容易受到攻击;如果节点中保存的密钥少,节点在寻找邻居节点时,会很难找到。

因此,本方案采用了只保存密钥池中部分密钥的 ID,通过 ID 来找寻邻居节点。最后,基站广播密钥池中的密钥,节点把用作通话的 ID 对应的密钥保存起来,并进行一些计算来作为节点之间通话的密钥。

3.1 方案的具体实现

协议中所用到符号的说明: | 表示字符串连接操作符, $\{M\}(K_i)$ 表示使用密钥 K_i 对消息 M 进行加密, $MAC(K_i, M)$ 表示使用密钥 K_i 生成 M 的消息认证码。

3.1.1 密钥的协商

1) 在传感器节点布置之前,首先在各节点中存储一个节点共享密钥 K_{master} 和节点与基站通话的主密钥 K_{enc} , 密钥 K_{master} 用作网络建立和节点加入的密钥,其加密公式为:

$$E = \{D\}(K_{master}, C)$$

其中, E 表示加密后的密文; D 表示加密前的明文; C 表示计数器,用作块加密的初始向量。它的认证公式为:

$$M = MAC(K_{master}, C | E)$$

其中, $C | E$ 为计数器值 C 和密文 E 的连接。

2) 建立一个密钥池 P , 并为密钥池 P 中的每个密钥分配一个 ID。在布置节点前,把密钥和密钥对应的 ID 存储在基站节点中,而普通节点仅存储部分密钥的 ID。

$$P = K \cup ID$$

$$K = \{k_1, k_2, \dots, k_n\}$$

$$ID = \{id_1, id_2, \dots, id_n\}$$

其中, k_i 为基站中的密钥, id_i 为密钥 k_i 对应的标识符。

3) 传感器网络配置时,节点被随机散布在指定的感知区域内。在簇形成过程结束后,节点就开始进行密钥发现过程,一个节点 A 向周围邻居节点广播自己的密钥环中所有密钥的 ID、自身的标志信息和位置信息,寻找那些与自己有共享密钥 ID 的邻居节点。

$$A \rightarrow * : \{ID_i, A, L_A\}(K_{master}, C_A), MAC(K_{master}, N_A | \{ID_i, A, L_A\}(K_{master}, C_A))$$

其中 * 表示节点 A 周围的任意节点, N_A 为一个 Nonce 随机数, L_A 是 A 节点的位置信息。

4) 如果节点 B 接受到节点 A 广播来的消息后,检测到 A 和自己有共享的密钥 ID_i ,那么 B 就选择出 ID_1 和 ID_2 , 并把这两个 ID 发送给 A 。

$$B \rightarrow A : \{ID_1, ID_2, B, A, L_B\}(K_{master}, C_B), MAC(K_{master}, N_B | \{ID_1, ID_2, B, A, L_B\}(K_{master}, C_B))$$

A 节点把这两个 ID 和 B 节点的位置信息 L_B 保存在自身节点中,用来以后计算两个节点之间的通话密钥。假如,节点 B 发现和节点 A 没有公共的 ID,那么节点 B 就从 A 发过来的数据包中选择两个 ID,然后把这两个 ID 通知给节点 A 。

5) 经过一段时间后,基站 S 检测簇内节点是否还有发送消息的节点,如果所有节点的通话都已经结束,那么基站 S 先

广播一条消息使节点间的共享密钥 K_{master} 失效, 然后基站 S 开始广播密钥池中的密钥。

$$S \rightarrow * : \{k_1, k_2, \dots, k_n, S, L_S\} (K_{\text{enc}}, C_S), \text{MAC}(K_{\text{enc}}, N_S | \{k_1, k_2, \dots, k_n, S, L_S\} (K_{\text{enc}}, C_S))$$

节点 A 接受到基站广播来的信息后, 从这些密钥中选择出 ID_1 和 ID_2 对应的密钥 k_1 和 k_2 。通过这两个密钥, 节点 A 和节点 B 计算出通话的密钥 K_{AB} :

$$K_{AB} = k_1 \oplus k_2 \oplus L_A \oplus L_B$$

在基站广播密钥结束后, 簇内任意两个节点间都共享一个会话密钥。

3.1.2 新节点的加入与节点的撤消

密钥建立好以后, 普通节点仍保留存储在节点中的 ID 和共享密钥, 由于基站广播密钥前, 使节点间的共享密钥 K_{master} 失效, 因此, 节点间不能再用共享密钥进行会话, 而只能使用建立后的密钥, 这样就可以保证节点的安全性, 即使节点被捕获, 或者共享密钥被泄露, 敌方也不能够用共享密钥对其他节点进行重放攻击。

而保留 ID 和共享密钥的目的是为了新节点的加入。假如有一个新节点 C 加入了已有的网络, 那么它的加入过程如下:

1) 节点 E 首先发送自身的标志信息, 位置信息和密钥的 ID 给基站。

$$E \rightarrow S : \{E, L_A, k_1, k_2, \dots, k_m\} (K_{ES}, C_E), \text{MAC}(K_{ES}, N_E | \{E, L_A, k_1, k_2, \dots, k_m\} (K_{ES}, C_E))$$

其中, K_{ES} 为通过密钥 K_{enc} 推算出来的基站和节点 E 之间的通话密钥。

2) 基站检测到新加入的节点确实是合法节点, 那么基站就广播一条消息, 使簇内节点的共享密钥 K_{master} 有效, 然后节点 E 就广播自己的 ID , 寻找自己的邻居节点。找到邻居节点后, 基站就广播密钥, 广播密钥时, 基站只广播节点 E 中 ID 对应的密钥:

$$S \rightarrow * : \{S, k_1, k_2, \dots, k_m\} (K_{\text{enc}}, C_S), \text{MAC}(K_{\text{enc}}, N_S | \{S, k_1, k_2, \dots, k_m\} (K_{\text{enc}}, C_S))$$

这样新加入的节点就加入了这个网络中了。

如果基站通过节点的一些信息发现一个节点被捕获, 例如, 可以通过一个节点的位置信息被改变, 来判断出该节点已被捕获, 那么就要求该节点从这个网络中删除。删除的任务由基站完成。假如基站 S 发现节点 A 被捕获, 那么基站首先生成一个撤消指令 M_{del} , 该指令包含基站的身份信息 S , 撤消指令 M_{del} 和节点 A 的一些信息。节点撤消指令如下:

$$M_{\text{del}} = \{S, A, del\} (K_{AS}, C_S), \text{MAC}(K_{AS}, N_M | \{S, A, del\} (K_{AS}, C_S))$$

3.1.3 密钥的更新

在许多分布式传感器网络中, 通常每两个节点共享密钥的生命周期会超过两个节点的生命周期。但在一些情况下(如恶意攻击、密钥被破解等), 密钥将失效或过期, 因而共享密钥需要随着时间进行更新。密钥的更新过程为:

1) 基站向簇内所有节点发送一条密钥更新指令 M_{update} :

$$S \rightarrow * : \{s, M_{\text{update}}, L_S\} (K_{\text{enc}}, C_S), \text{MAC}(K_{\text{enc}}, N_S | \{s, M_{\text{update}}, L_S\} (K_{\text{enc}}, C_S))$$

2) 节点接收到以后, 销毁现在使用的密钥, 然后基站再发送一个使共享密钥 K_{master} 有效的指令, 接下来节点起用密

钥建立过程。但此次节点之间使用的 ID 不能用到之前用过的 ID。

3.2 性能分析

3.2.1 安全性分析

本方案中虽然使用了节点之间的共享通话密钥, 但该密钥只是在网络建立时, 或者节点加入时才有效。这样即使共享密钥被泄露了, 那么敌方也不能够通过该共享密钥来进行攻击。因此该方案要比传统的预共享密钥分发方案更加安全。

如果某些节点被捕获, 并且获得了节点中的密钥, 敌方也不能通过这个密钥来攻击网络中的其他节点。即使基站发送密钥包的时候, 敌人监听到了这些密钥, 那么也不能够用这些密钥来攻击网络中的节点, 这样就大大确保了网络的安全性。

由于通信双方共享唯一的会话密钥, 该会话密钥具有身份认证功能, 接收者可以通过数据源认证确信消息是从正确的节点处发送过来的, 从而确保了消息的真实性。

消息认证码将共享密钥和待检验的消息连接在一起进行运算, 从而能够有效地防止攻击者对截获的信息进行篡改, 保证了消息的完整性。

该方案将计数器信息包含在待加密消息中, 共享密钥加密确保了攻击者无法获知和篡改计数器的信息, 计数器的内容又能使接收者确信收到的数据是在最近时间内生成的最新数据, 即消息是新鲜的。

由于引入了加密密钥和随机数, 本方案具备了身份验证、消息保密和内容保鲜等诸多功能并能够有效防止各种攻击如重放攻击, 而使得其可用性大大提高。

3.2.2 效率分析

本方案和随机密钥分发方案相比, 节点只保存了 ID 号, 因此可以推算出本方案中两个相邻节点之间共享密钥的概率。假设 ID 号的大小为密钥大小的 $1/8$, 随机密钥分发方案中密钥环的大小为 k , 那么本方案中 ID 环的大小为 $8k$ 。根据 2.2 节两个相邻节点之间共享密钥的概率公式, 我们可以得出本方案的相邻节点的概率 f' 为:

$$f' = 1 - \frac{((P - 9k)!)^2}{(P - 18k)!P!}$$

可以看出, 本方案的连通概率比随机密钥分配方案有了很大的提高, 例如, 有 50000 个节点, 如果采用随机密钥方案, 在节点中存储 125 个密钥, 那么两个相邻节点的连通概率为 0.27。如果采用本方案, 根据概率公式可以得出节点的连通概率为 0.99。

表 1 三种方案的比较

解决方案	扩展性	内存需求	通信开销	连通概率
预共享密钥	比较好	1	1	1
随机密钥	一般	$2k$	$k + dk$	$1 - \frac{((P - k)!)^2}{(P - 2k)!P!}$
新方案	比较好	$2k$	$k + dk$	$1 - \frac{((P - 9k)!)^2}{(P - 18k)!P!}$
Blom 方案	较好	$2(\lambda + 1)$	$\frac{(\lambda + 1) \times}{(d + 1)}$	1
多项式	差	$T + 1$	T	1

表 1^[13] 对几种常见的密钥分配方案和基于随机密钥预分配的改进方案(以下统称“新方案”)进行了一个基本的比较。其中 P 为密钥池的大小, d 为节点的度, k 为节点密钥环

大小,假设ID的大小为密钥大小的 $1/8$, T 为搜寻共享密钥开销。

4 结语

本文所提出的密钥分配方案在传感器节点中只保存密钥池中密钥的ID,这样大大节省了节点的存储空间,使节点存储的ID数量大大增加,从而在节点寻找邻居节点时很容易找到与自己有共享的ID节点。同时,考虑到传感器节点自身资源有限的特点,通过减少会话步骤、简化计算方法来降低节点的工作负荷,从而使得该方案的传感器节点计算、存储和通信开销都非常小,大大提高了传感器节点的工作效率,使无线传感器网络的整体性能得到提高。

参考文献:

- [1] 孙利民,李建中,阵渝,等.无线传感器网络[M].北京:清华大学出版社,2005.
- [2] 郎为民,程文青,杨宗凯,等.一种基于无线传感器网络的密钥管理方案[J].计算机科学,2005,32(4):147-1541.
- [3] 周贤伟,覃伯平,徐福华.无线传感器网络与安全[M].北京:国防工业出版社,2007.
- [4] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, et al. A survey on sensor networks [J]. IEEE Communications, 2002, 40(8):102-114.
- [5] CHAN HAO-WEN, PERRIG A. Security and privacy in sensor networks [J]. IEEE Computer, 2003, 36(10):103-105.
- [6] PERRIG A, STANKOVIC J, WAGNER D. Security in wireless sensor networks [J]. Communications of the ACM, 2004, 47(6):53-57.
- [7] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks [C]// Proceedings of IEEE 2003 Symposium on Research in Security and Privacy. Washington: IEEE Computer Society, 2003: 197-213.
- [8] 周贤伟,孙晓辉,覃伯平.无线传感器网络密钥管理方案的研究[J].计算机应用研究,2007,24(1):144-147.
- [9] ESCHENAUER L, GLIGOR V. A key-management scheme for distributed sensor networks [C]// Proceedings of the 9th ACM Conference on Computer and Communication Security. New York: ACM Press, 2002: 41-47.
- [10] BOLLOBAS B, FULTON W, KATOK A, et al. Rand Graphs [M]. 2nd ed. Cambridge: Cambridge University Press, 2001: 160-200.
- [11] BLOM R. An optimal class of symmetric key generation systems [C]// Advances in Cryptology: Proceedings of EUROCRYPT 84, LNCS 209. Berlin: Springer-Verlag, 1984: 335-338.
- [12] BLUNDO C, SANTIS D A, HERZBERG A, et al. Perfectly-secure key distribution for dynamic conferences[C]// Advances in Cryptology: CRYPTO'92. Berlin: Springer-Verlag, 1993: 471-486.
- [13] 黄鑫阳,杨明.无线传感器网络密钥管理研究综述[J].计算机应用研究,2007,24(1):10-15.

(上接第1387页)

设置参数 $m = 45, n = 30, p = 1, q = 1$,在RPGW移动模型及RW移动模型下得到方案的服务延迟时间随门限值的变化情况如图5所示。

从图5可以看出,节点采用基于门限担保证书的私钥元分配方案得到私钥元的延迟时间随着门限值的增加而平稳增加,增加趋势近似成线性;另外RPGW移动模型下的服务延迟时间小于RW移动模型下的服务延迟时间,这是因为RPGW移动模型有利于节点之间的协作。

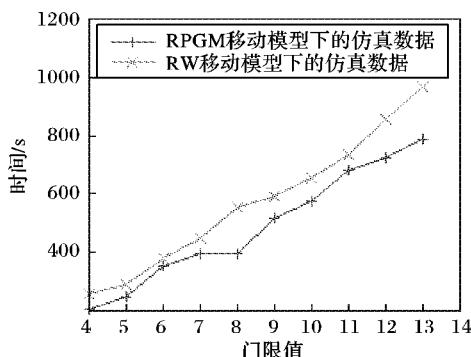


图5 服务延迟时间随门限值的变化情况

6 结语

本文针对私钥元的安全问题,提出了一种基于门限担保证书的私钥元分配方案,通过门限个拥有合法证书的节点的联合担保,确保服务节点的可信、可用,该方案能够抵抗门限个恶意节点联合申请私钥元以重构系统私钥的攻击。最后,对方案的可用性及安全性进行了理论分析,并对方案的实际运行效率进行了仿真,为方案的实际应用提供了理论和实践依据。

参考文献:

- [1] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(1):612-613.
- [2] ZHOU L, HAAS Z. Securing Ad Hoc networks[J]. IEEE Network, 2000, 13(6):24-30.
- [3] KONG JIE-JUN, ZERFOS P, LUO HAI-YUN, et al. Providing robust and ubiquitous security support for mobile Ad Hoc networks [C]// 9th International Conference on Network Protocols (ICNP). Washington: IEEE Computer Society, 2001: 251-261.
- [4] OSTROVSKY R, YUNG M. How to withstand mobile virus attacks [C]// Proceedings of the 10th ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1991: 51-59.
- [5] HERZBERG A, JARECHI S, KRAWCZYK H, et al. Proactive secret sharing or: how to cope with perpetual leakage [C]// Advances in Cryptology-Crypto '95, LNCS 963. Berlin: Springer-Verlag, 1998: 963-976.
- [6] DONG Y, SUN AI-FEN, YIU S M, et al. Providing distributed certificate authority service in cluster-based mobile Ad Hoc networks [J]. Computer Communications, 2007, 30(11/12): 2442-2452.
- [7] 艾东知,Ad Hoc网分布式认证的研究[D].上海:复旦大学,2004.
- [8] BETTSTETTER C, WAGNER C. The spatial node distribution of the random waypoint mobility model [C]// Proceedings of the 1st German Workshop on Mobile Ad Hoc Networks (WMAN). Ulm, Germany: GI, 2002: 41-58.
- [9] CAMP T, BOLENG J, DAVIES V. A Survey of Mobility Models for Ad Hoc Network Research [J]. Wireless Communication & Mobile Computing: Special issue on Mobile Ad Hoc Networking: research, Trends and Application, 2002, 2(5):483-502.
- [10] BECHLER M, HOF H-J, KRAFT D, et al. A cluster-based security architecture for Ad Hoc networks [C]// 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2004). Washington: IEEE Press, 2004, 4: 2393-2403.