

基于随机矩阵预分配的卫星网络密钥管理

潘艳辉^{1,2} 王 轲¹ 吴 杨¹ 郑燕茹² 罗盛君²

(军械工程学院计算机工程系 石家庄 050003)¹ (西安卫星测控中心 西安 710033)²

摘 要 基于对称密码体制的密钥管理方案的关键是取得安全与性能的平衡。针对卫星网络节点资源受限的特点,提出了按照随机矩阵分配节点密钥元素的方法。该方法简化了密钥环的构造,而且能够确保任意节点之间可建立互不相同的会话密钥。给出了相应的密钥更新机制。仿真结果表明,该方法能够在保证安全性的同时显著降低密钥存储与计算开销。

关键词 卫星网络,密钥管理,对称密钥,快照序列拓扑,分簇

中图法分类号 TP393.08

文献标识码 A

Satellite Network Key Management Based on Pre-distribution According to Stochastic Matrix

PAN Yan-hui^{1,2} WANG Tao¹ WU Yang¹ ZHENG Yan-ru² LUO Sheng-jun²

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)¹

(Xi'an Satellite Control Center, Xi'an 710043, China)²

Abstract To key management scheme based on symmetrical cryptographic system, it is crucial to get balance of security and performance. According to satellite network nodes resource constraints, a key elements distribution method was introduced based on random matrix for nodes. It simplified the construction of key rings, and can make sure that any node can establish different session keys with different other nodes. Then we gave the corresponding key update mechanism. The simulation results show that this method can guarantee security and reduce storage and computing cost by keys significantly at the same time.

Keywords Satellite network, Key management, Symmetric key, Sequent snapshots topology, Clustering

1 引言

由于卫星网络节点暴露于公共的空间环境中,以及其无线移动通信所固有的脆弱性,使得卫星网络安全问题突出。与传统网络一样,有效的密钥管理方案是解决卫星网络安全问题的基础。结合卫星网络的特点与安全需求,文中设计了一种轻量级高安全性的卫星网络对称密钥管理方案(Symmetric Key Management for Satellite Network),记为 SKM-SN。

2 相关研究分析

按照所依赖的密码体制可将密钥管理方案分为基于对称密码与基于公钥密码体制的密钥管理方案,前者更适用于资源受限型网络环境。基于对称密码体制的密钥管理方案主要有:基于矩阵方法、预分配随机密钥环方法、基于多项式方法等,形成了多种典型的密钥管理方案^[1,2]。

Blom 等人^[3]运用矩阵密钥分配方法提出了一种对称密钥生成方案,它被称为是 λ -安全的,即数量不超过 λ 的受损节点是无法破坏网络中的任何安全链路的。该方案最大的优点是能够保证网络中任何两个节点之间都能建立对密钥。其存在的不足是要求 $\lambda+1$ 维的向量乘法操作,且向量中每个元素

的长度与对密钥相同,因此其计算开销不容忽视。此外,该方案在生成矩阵时需要预先知道网络的部署规模 N ,因此其扩展性也不好。

为突破安全阈值的限制,文献[4]对其做了进一步改进,提出了一种基于随机密钥矩阵的分配方法。网络建立密钥预装载在节点中供节点之间协商建立通信对密钥,每个节点预装载密钥矩阵的一行和一系列密钥元素。然后,任意两个节点间通过交换密钥向量来建立二者的通信对密钥,使得每一对节点之间的通信对密钥均不相同,提高了系统抗俘获的安全能力。

类似地,文献[5]针对密钥预分配中密钥环较大的问题,提出了一种基于向量组合的密钥预分配方案(Key Management Scheme Based on Linear Combination of Vector Group, LVG 方案)。该方案降低了任意两节点生成密钥重复的概率,不存在安全阈值,提高了抵抗俘获攻击的能力。节点的密钥存储量近似等于节点度的大小,降低了存储开销。而且通过一次广播完成节点对密钥的建立,降低了通信开销,但 k 维向量的乘法仍然存在较大计算开销。

Eschenauer 等人^[6]首次提出了随机密钥预分配方案,其通常称为 E-G 方案,在密钥建立阶段,每个节点都被分配到了一组密钥,称为密钥环,通过它邻居节点之间能够以一定的

潘艳辉(1982—),女,博士生,主要研究方向为卫星网络路由与安全性;王 轲(1964—),男,博士生导师,主要研究方向为网络安全;吴 杨(1985—),男,硕士生,主要研究方向为卫星网络安全认证协议;郑燕茹(1975—),女,工程师,主要研究方向为卫星网络仿真;罗盛君(1985—),女,工程师,主要研究方向为卫星网络测试。

概率建立共享密钥。在此基础上,Chan 等人^[7]提出了 Q-Composite 随机密钥预分配方案,该方案要求邻居节点之间至少存在 q 个共享密钥才能建立共享密钥,进一步提高了该类方案的安全性。

3 SKMSN 方案

3.1 初始化阶段

假设存在一个地面密钥分发中心(Key Distribution Center, KDC)负责节点密钥初始化。在网络部署前由 KDC 构造一个密钥池 S , 密钥池的大小 $|S| \gg N$, N 是网络节点数。由 KDC 从 S 中随机抽取不放回地选择密钥元素生成 w 个密钥矩阵, 每个矩阵由 $m \times m$ 个密钥元素构成, 这 w 个密钥矩阵形成密钥矩阵集 $M = \{M_1, M_2, \dots, M_w\}$, 生成 M 所需的密钥数量为 $|M| = m \times m \times w$ 。每个密钥矩阵有唯一的标识号, 对任意一个节点 X , KDC 从 M 中随机选择 $r \geq \lceil (w+1)/2 \rceil$ 个密钥矩阵元素作为密钥备选矩阵集 M' , $|M'| = r$, 再从备选集 M' 中的每个矩阵元素中选取一行和一列密钥作为该节点的密钥环, 并选取用于节点与地面站控制中心进行通信的主密钥 K 。则密钥环 R 的大小为:

$$|R| = (m+m-1) \times |M'| + |K| = (2m-1) \times |M'| + |K| \quad (1)$$

3.2 会话密钥建立

依据鸽笼原理, 网络中任意两个节点 A 和 B 至少从同一个矩阵元素中选择密钥元素。假设这个相同的矩阵元素标识为 t , 由于 A 和 B 是取自同一个矩阵 M_t 中的行和列密钥向量, 因此两个节点所取的行列之间必然存在至少两个交点, 如图 1 所示。

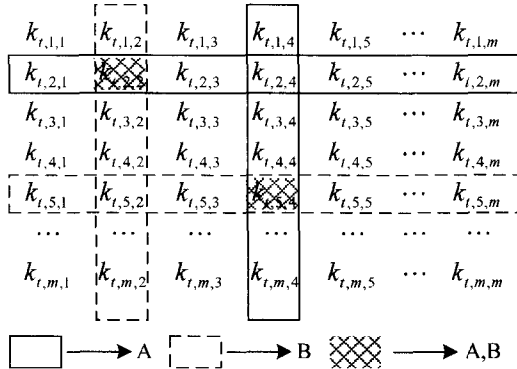


图 1 SKMSN 的密钥协商原理

因此 A 与 B 至少有两个相同的密钥元素。假设 A 选择 M_t 中的第 2 行第 4 列的元素, B 选择 M_t 中的第 5 行第 2 列元素, 则它们有两个共同的密钥 $k_{t,2,2}$ 和 $k_{t,5,4}$, 这是节点之间进行会话密钥协商的依据。会话密钥建立步骤如下:

Step1 相邻节点广播密钥相关标识

网络中每个节点向其邻居节点广播一个握手消息后, 该消息由两部分组成: 节点 ID 和密钥环中密钥的标识信息, 包括矩阵标识、密钥向量在矩阵中的行和列标识。

$X \rightarrow \text{Broadcast: } \{(M_D, L_D, C_D), (M_D, L_D, C_D), \dots, (M_D, L_D, C_D) \parallel H(N_X)\}$

例如假设相邻两个节点 A 和 B :

$A \rightarrow \text{Broadcast: } \{(a, b, c), (t, 2, 4), \dots, (d, e, f) \parallel H(N_A)\}$

$B \rightarrow \text{Broadcast: } \{(a, b, c), (t, 5, 2), \dots, (d, e, f) \parallel H(N_B)\}$

Step2 查找相同密钥元素

节点收到广播消息后, 首先验证消息来源是否真实, 提取发送节点的标识 N_A 并计算其 Hash 值 $H(N_A)$, 看其是否与消息中的 Hash 值一致。如果不一致则丢弃该握手消息。否则首先查找消息中的密钥矩阵标识与本地密钥矩阵相同的标识值, 如果存在多个相同的密钥矩阵, 则以查找到的第一个密钥矩阵作为其公共密钥矩阵, 这样可以节省星上计算资源, 对公共密钥的获取并不存在影响。之后将二者从同一矩阵中取出的密钥向量的行或列标识进行交换, 即可得公共密钥元素的标识。

例如, A 和 B 相同密钥矩阵的标识为 t , 则 A 与 B 相同的密钥元素是 $(t, 5, 4)$ 和 $(t, 2, 2)$ 。

Step3 计算公共密钥

节点分别根据与相邻节点相同的密钥元素以及主密钥和标识来计算与相邻节点的公共密钥, 将其作为二者通信的对密钥。

例如:

$$K_{A \rightarrow B} = K \otimes (t, 5, 4) \otimes (t, 2, 2) \otimes H(N_A) \otimes H(N_B)$$

$$K_{B \rightarrow A} = K \otimes (t, 5, 4) \otimes (t, 2, 2) \otimes H(N_B) \otimes H(N_A)$$

$$K_{AB} = K_{A \rightarrow B} = K_{B \rightarrow A}$$

K_{AB} 即为卫星节点 A 和 B 之间的通信密钥。由于每个节点的标识不同, 因此通过这种方式协商的对密钥是唯一的, 不同节点对之间建立的通信对密钥均不相同, 即使出现两对节点间预装载密钥相同的特殊情况也是如此。

3.3 密钥更新

密钥更新是进行密钥管理、保证密钥安全的一个重要环节。该对称密钥管理方案有两类: 主密钥和会话密钥。根据密钥管理原则, 不同性质的密钥其更新应区别对待。下面分别描述其更新方法。

1) 主密钥更新

对于主密钥, 文献^[8]提出了较好的算法, 文中采用其地基测控网密钥更新方式, 其过程不在此赘述。

2) 会话密钥更新

通常情况下, 卫星网络节点数目相对固定, 在其正常运行周期内, 已有节点退出和新节点加入网络的事件较少发生, 卫星网络节点间安全连接关系的改变是随卫星网络拓扑结构的改变而改变的。因此, 文中主要考虑卫星网络密钥周期性更新事件。利用卫星网络动态拓扑可以按时间间隔转化为静态快照拓扑序列的特点, 选择适当的时机进行密钥更新。其中, 快照序列拓扑的划分方法参考文献^[9-11]。

其更新过程如下:

Step1 生成随机数

在当前周期末触发密钥更新事件, 网络中任一个节点 X 生成随机数 R_X , 并用当前周期的密钥加密。

Step2 相邻节点广播密钥协商消息

在具有星间链路的 LEO 卫星网络中, 卫星节点一般只与邻居节点直接建立星间链路。因此, 卫星网络中节点的直接邻居只会存在于同一轨道上和相邻轨道上, 可将广播消息限制在该范围内。该消息包括节点标识、新密钥声明信息。

Step3 计算新周期密钥

邻居节点接收到密钥更新协商广播消息后, 首先判断消息来源是否与消息尾部一致, 如果不一致则丢弃, 否则用当前密钥对消息前半部分进行解密。之后用双方生成的随机数和相互的标识以及当前周期的密钥进行异或, 生成下一周期的

会话密钥。进入下一周期后即删除前一周期内使用的密钥,启用当前周期内的密钥。在卫星网络生存期内如此往复,不断更新节点对之间的通信密钥,保证密钥的安全性,防止伪造和重放攻击的发生。

例如:

$$K_{A \rightarrow B}^{i+1} = K_{A \rightarrow B}^i \otimes R_A \otimes R_B \otimes H(N_A) \otimes H(N_B)$$

$$K_{B \rightarrow A}^{i+1} = K_{B \rightarrow A}^i \otimes R_A \otimes R_B \otimes H(N_A) \otimes H(N_B)$$

$$K_{A \rightarrow B}^{i+1} = K_{B \rightarrow A}^{i+1} = K_{B \rightarrow A}^{i+1}$$

4 方案分析

4.1 安全性分析

由于卫星网络节点暴露在公共的空间环境中,并且卫星节点与地面测控站之间存在姿态控制信息的交互,因此,通过空中直接“捕获”或通过地面测控站间接“控制”的方式,攻击者可能“俘获”正常运行的卫星节点,然后利用该节点通过重放信息获得其它节点的安全认可,进一步实施黑洞、拒绝服务等攻击。本方案从两个方面抵抗这类攻击,一方面任意一对节点间均可建立会话密钥,能够始终保持网络的全连通性,与此同时避免出现重复密钥,消除不同链路之间的安全关联性,确保网络中任意一对节点间的会话密钥均不相同,提高了密钥信息的私密性。因此,任意节点被俘获后均不会影响到其它节点对之间的密钥安全性,如图2所示,具有较好的抗毁性。

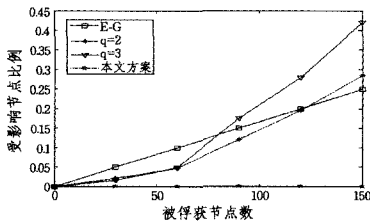


图2 抗毁性分析

由此可知,当捕获节点数较少时 Q-Composite 的抗毁性能相对于 E-G 有所改善,但随着被捕获节点数的增加,其抗毁性能急剧下降,而本文方案的抗毁性能几乎不受捕获节点数的影响,在抗毁性上明显优于其它方案。

4.2 性能分析

1) 密钥存储开销较小

本方案密钥数量与节点规模之间的关系是:

$$N = \binom{w}{r} \times (m \times m)^r = \frac{w!}{r! \times (w-r)!} m^{2r} \quad (2)$$

$$|R| = (2m-1) \times r + 1$$

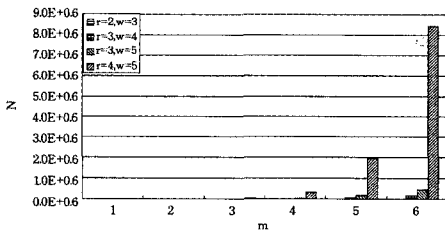


图3 网络规模增长趋势

依据式(2),对于低轨道卫星网络来说,当 $w=5, r=3$ 时,每个节点仅需存储 10 个密钥便可支持 640 个节点规模的卫星节点是一种较好的选择。在 $m \in [1, 6]$ 区间,支持的网络规模增长趋势如图3所示。显然,本文方案的密钥环长度增长趋势缓慢,而能够支持的网络规模显著增大,即随着网络规

模的增大所需的密钥存储空间消耗无明显变化。

2) 计算开销

由于密钥矩阵是影响安全性的主要因素,为分析密钥矩阵的维数对节点间共享密钥建立时间开销的影响,我们分别取不同维数的密钥矩阵在 VC++6.0 环境中进行了仿真,并与同样采取密钥矩阵的文献[2]中的 Cheng 方法进行了对比。为消除网络环境中的随机因素对仿真结果的影响,采用了对每一个密钥矩阵分别进行 100 次仿真后再取平均值的方法,仿真结果如图4所示。由此可知,对于相同维数的密钥矩阵,本文方法采用标识交换的方法有效降低了密钥建立过程所消耗的时间,而且,随着密钥矩阵维数的增多,该方法的优势更加明显。

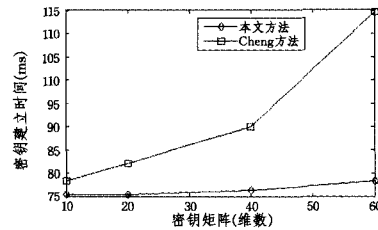


图4 密钥建立时间开销对比

结束语 本文提出了适用于卫星网络的密钥管理方案 SKMSN,它采用预分配主密钥与对密钥结合的方式,利用卫星网络拓扑结构的规则时变性特点对传统方法进行优化,进一步提高了密钥管理方案的性能。仿真分析结果表明该方案具有较好的抗毁能力且开销需求比较低。

参考文献

- [1] 黄杰,黄蓓.无线传感器网络中一种基于公钥的密钥分配方案[J].通信学报,2011,32(10):52-58
- [2] Suganthi N, Priya R S M, Sumathy V. An efficient and dynamic key management scheme for mobile Ad hoc networks[J]. European Journal of Scientific Research, 2011, 55(4): 538-548
- [3] Blom R. An optimal class of symmetric key generation systems [C]// Advance in Cryptology-EUROCRYPT'84. 1984: 335-338
- [4] Cheng Y, Agrawal D P. Efficient pairwise key establishment and management in static wireless sensor networks[C]// Proceeding of the 2nd IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2005
- [5] 张涛.无线传感器网络密钥管理方案的研究[D].赣州:江西理工大学,2009
- [6] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press, 2002: 41-47
- [7] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks[C]// Proceedings of the 2003 IEEE Symposium. On Security and Privacy. Washington: IEEE Computer Society, 2003: 197-213
- [8] 张志强,张永健,王宇,等.低轨卫星网络中基于轨道分簇的密钥更新算法[J].电子与信息学报,2010,32(3):687-692
- [9] 王京林,晏坚,曹志刚. LEO 卫星网络快照序列路由算法优化[J].宇航学报,2009,30(5):2003-2007
- [10] 周云晖,孙富春,张拔.一种基于时隙划分的多层卫星网络 QoS 路由协议[J].计算机学报,2006,29(10):1813-1822
- [11] 赵东杰,杨海涛,赵洪利.基于链路特性的卫星网络拓扑更新周期研究[J].计算机应用研究,2009,26(12):4669-4671