异步及不可靠链路环境下的先应式秘密共享

郭渊博[1,2], 马建峰[1]
(1. 西安电子科技大学教育部计算机网络与信息安全重点实验室, 陕西西安 710071;
2. 解放军信息工程大学电子技术学院, 河南郑州 450004)

摘 要: 现有先应式秘密共享假设系统具有同步时钟且主机间存在可靠通道, 这在现实的分布式环境中很难保证. 本文给出了异步且不具可靠通信通道环境中一种先应式秘密共享方案. 通过引入由协议事件和系统中主机本地时钟双重驱动的时间片概念, 定义了异步模型下先应式秘密共享的运行状态及其转换过程, 从而给出了异步环境中先应式秘密共享的有效方案; 同时设计了一个消息可靠传输协议, 可在主动链路攻击情况下保证主机间消息的正确传输. 分析表明, 我们的方案是有效的, 且不会对系统的通信和计算性能带来太大影响.

关键词: 先应式秘密共享; 不可靠链路; 异步模型; 系统恢复; 份额更新
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2004) 03-0399-05

Proactive Secret Sharing in Asynchronous Networks with Unreliable Links

GUO Yuan-bo[1,2], MA Jian-feng[1]
(1. The Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi. an, Shaanxi 710071, China;
2. School of Electronic Technology, Information Engineering University of PLA, Zhengzhou, Henan 450004, China)

Abstract: Existing proactive secret sharings (PSSs) are all based on the synchronous time model and reliable links assumptions, which are impractical in distributed environments, such as Internet. This paper proposes a practical PSS for asynchronous networks with unreliable links. The asynchronous PSS is obtained by introducing a concept of time phase, which is defined not only in terms of protocol events, but also in timings of all participants. Based on this concept, the states and their transitions of asynchronous PSS can be characterized. And, the reliable communications between participants are yielded by the development of a reliable message transmit protocol. Analyses show that our method is efficient, and has a low overhead in terms of communication and computation.

Key words: PSS; unreliable links; asynchronous model; system recovery; shares refresh

1 引言

先应式(Proactive)秘密共享(PSS)[1~6]的基本思想是"分布+更新": 首先按照秘密共享的方法将秘密信息分解成一些秘密份额, 然后定期对份额更新. 因此, 只要保证给定时间段内被攻破的主机个数不超过预定门限数, 就可在更新阶段恢复被攻破的主机, 重建系统安全环境. 由于更新后的新旧份额间不存在任何相关性, 即更新完成之前所收集到的信息对未来攻击无效, 因此攻击者无法根据旧份额推导出现有份额的任何信息. 尽管 PSS 有这样的好处, 已知文献中的方案大都基于同步的时钟模型和主机间存在可靠通信通道的假设. 这在现实的分布式环境中很难保证. 通过引入可由协议事件和系统中各主机的本地时钟双重驱动的时间片概念, 本文定义了异步模型下先应式秘密共享的状态及其转换过程, 从而给出了异步环境中一种实用有效的先应式秘密共享方案; 同时设计了一个消息可靠传输协议, 可在存在主动链路攻击情况下保证参与方之间消息的正确传输.

2 系统模型及要求

对系统模型所做的任何额外假设都会为所实现的系统引入一些脆弱点. 为避免引入过多脆弱点, 以使方案具有广泛适用性, 本文未对系统提出过多要求, 而是假设异步的分布式环境, 如 Internet 等.

定义 1(异步) 异步包括两方面的含义: 一是不要求系统中各主机间的本地时钟保持一致; 二是不对消息传递的延迟时间、主机运行速率等施加任何限制.

定义 2(分布式) 分布式环境中, 攻击者不仅可以实施窃听等被动攻击, 且能够实施消息插入、修改、删除、重放等主动攻击; 其攻击目标不仅包括系统中的主机, 还包括主机间的通信链路.

收稿日期: 2002-10-22; 修回日期: 2003-10-22
基金项目: 国家自然科学基金重大研究计划项目(No. 90204012); 国家高技术研究发展计划(863 计划)课题(No. 2002AA143021); 教育部优秀青年教师资助计划; 教育部科学技术重点研究项目; 总装备部武器装备基金项目

在不违背上述模型的基础上,对系统行为进行以下限制.

系统要求:

(1) 系统中每台主机开始恢复时要求以干净的代码重新启动并加载干净的协议;

(2) 各主机中存储着维护系统运行的必须信息,如其它主机的IP、所用的密码参数等. 这些信息可能会在系统运行中动态变化,因此不能以只读方式存储,而应采用密码方法保护;

(3) 尽管不要求各主机的本地时钟具有统一的绝对时间,但要求其相对时间(运行速率)精确程度差别不大;

(4) 采用了公平链路[7]的假设:即尽管链路不保证传递所有消息,但当某一主机向某一目标发送了无数多消息时,总会有一些消息被成功传递. 在具多路由等特点的 Internet 环境中该假设是合理的.

3 方案设计

311 时间片的定义

首先给出份额更新和主机恢复的概念:

定义 3(份额更新) PSS 运行过程中使得各主机由旧份额生成新份额的过程称作一次份额更新.

定义 4(主机恢复) 每次更新之前,各主机按照一定的方法,帮助被入侵了的主机重新找回丢失了的或被破坏了的份额的过程,称作该主机的一次恢复.

为区分新旧份额以及 PSS 的不同运行次数,按如下方式对份额和协议运行分配序号:

(1) 在系统初始化阶段,系统为每台主机分配序号为 0 的份额;

(2) 如果恢复协议运行的结果是帮助被入侵的主机找回被破坏了的序号为 u 的份额,则此后更新协议所得到的新份额序号为 u+ 1,协议的该次运行是第 u+ 1 次运行.

异步环境中的时间片不能以绝对时间定义,而应以与异步环境中 PSS 数据更新的周期相关的事件定义.

由于入侵可能破坏主机中的份额,因此驱动主机恢复的一个明显条件就是系统感知到入侵. 然而并非所有入侵都可为系统所感知,为了使系统在未感知到入侵的情况下仍可恢复被破坏了的主机,需要用到本地时钟的概念.

基于主机的本地时钟可规定时间片的最大长度. 即使系统未感知到入侵,只要某主机当前时间片达到了最大值,就可向系统中的所有主机广播恢复请求,且自身开始运行主机恢复协议(其细节见第 3 节).

以序号为 u+ 1 的时间片为例,可得关于时间片开始和结束的定义:

定义 5(时间片开始) 时间片 u+ 1 开始,当且仅当时间片 u 内系统感知到攻击者对系统中某台主机的入侵,或某主机的当前时间片 u 已达到系统规定的最大值.

定义 6(时间片结束) 时间片 u 结束,当且仅当更新协议成功地将份额集 u 更新为 u+ 1,且系统中所有主机都已成功地将序号为 u 的份额从本机中删除.

显然,时间片表示了秘密份额集的最大生命周期,且与所用门限方案的门限值及攻击者的攻击能力有关. 其示意图如图 1 所示.

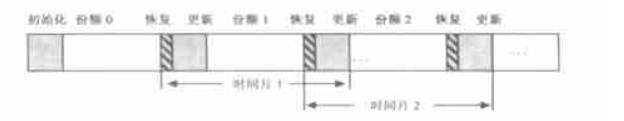

图 1 时间片示意图

312 系统状态及描述

下面是异步 PSS 的 6 种运行状态,其转换方式如图 2 所示:

(1) 初始化状态:按照初始化协议要求对系统中各主机进行初始化配置. 成功后系统进入正常状态;

(2) 正常状态:系统运行良好,未发现入侵,也没有主机提出更新请求. 可进行正常操作,如联合签名、加密等;

(3) 入侵状态:某正确主机发现其它某个主机提供的数据不正确,或 IDS 发现入侵时进入该状态. 向系统管理员报警后转入恢复状态;

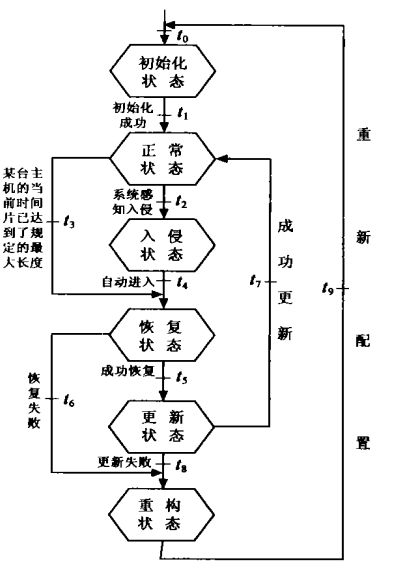

图 2 系统状态转换过程

(4) 恢复状态:标志着一个新的时间片开始. 除了可由入侵状态进入以外,系统中某台主机的当前时间片达到了最大值后也进入该状态;

(5) 更新状态:系统成功恢复后进入该状态. 用于对包括秘密份额在内的秘密信息进行先应式更新. 更新完成后系统重新进入正常状态;

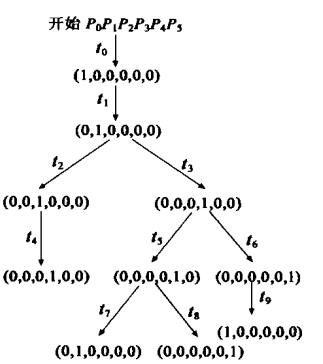

图 3 状态转换图的可达树

(6) 重构状态:系统中某台主机恢复或更新失败时进入重构状态. 这时,需对系统重新配置.

支持状态转换的三个协议(系统初始化协议、主机恢复协议和份额更新协议)的细节将在第 5 节讨论.

用 P_0~ P_5 分别表示上述 6 个状态,可得图 3 所示的系统状态转换可达树. 从图中可以看出,该转换具有可达性、完整性和可恢复性,且不会出现死锁和二义性.

结论 1 PSS 可在异步环境中按照以上定义的方式正确运行.

4　可靠消息传输协议

可靠消息传输协议用于保证主动链路攻击下消息的可靠传输. 每当系统中的两个主机需要通信时, 就调用该协议, 以保证通信消息的正确传输.

协议假设　攻击者在一个时间片内攻破链路数目的上界为õ(n- 1) / 28.

协议配置　系统具有密钥为(Scert, Vcert) 的用于全局签名的先应式签名方案(PDS)[3~6, 8]. 每个主机 i 分别拥有如 RSA 等传统签名密钥对(S_i, V_i) 以及 Scert 对 i 及 V_i 的签名 Scert (i, V_i). 每一时间片内都要更新这些密钥, 以消除攻击者的破坏. 因此可将时间片 u 内主机 i 的签名密钥对表示为(S_i^u, V_i^u).

协议步骤　以主机 i 向主机 j 传输消息 M 为例.

(1) 主机 i 向系统中所有主机广播(M, i, j, v, V_i^u, S_i^u(M, i, j, v, V_i^u) , Scert(i, V_i^u)) . 其中 i、j 是收发双方标识符; v 是当前版本号, 由当前时间片和该时间片内协议运行次数组成;

(2) 系统中每一个正确主机收到消息后, 根据消息中指示的接收方 j 原封不动地将消息转发过去;

(3) 主机 j 收到消息后, 先用自身保存的全局签名公钥 Vcert 验证(i, V_i^u) 的有效性, 然后用 V_i^u 验证(M, i, j, v, V_i^u) 的有效性. 如均有效, 则以同样的方式向主机 i 返回一个 Ack;

(4) 如在给定时间内主机 i 没有收到j 返回的 Ack, 则向管理员报告出错, 系统进入入侵状态.

协议分析　主动的链路攻击对消息的破坏包括: 消息删除、插入、修改、替换和重放. 其中, 消息删除可破坏消息传输服务的可用性, 消息插入、修改、替换、重放可破坏所传输消息的完整性.

(1) 服务可用性:

由每时间片内攻击者至多破坏系统中 s[õ(n- 1) / 28 条链路的假设可知, 每两台主机间至少存在 n- s\ õ(n+ 1) / 28 条未被破坏的链路. 故存在一台既可与主机 i 也可与主机 j 通信的主机 m. 若 m 未被破坏, 则可在接收到 i 广播来的消息后将其转发给j. 根据公平链路假设, 若 m 与j 均未被破坏, 该消息总会在一定时间内被主机 j 正确接收; 同理, 主机 j 发送的Ack 也总会被主机i 所接收. 若主机 i 在一定的时间内没有收到Ack, 说明主机 m 或j 已遭到入侵, 这时系统进入入侵状态. 正确恢复之后, j 总可以正确地接收到M.

(2) 消息完整性:

消息插入: 任何想以 i 的名义发送消息的攻击者为了使j 相信该消息的确是i 所发, 必须伪造签名 Scert(i, V_i^u).

消息的修改和替换: 攻击者必须修改或替换签名 S_i^u(M, i, j, v, V_i^u) . 攻击者不知道 S_i^u, 故只能使用其密钥 Sc, 这将由对 Scert(i, V_i^u) 的验证所发现.

消息的重放: 版本号 v 保证了重放将被识别.

结论 2　可靠传输协议可在主动链路攻击存在的情况下保证所传递的消息成功正确地到达目的地.

5　几个基本协议及安全性分析

下面给出 3.2 中所涉及协议的细节并讨论其安全性.

511　初始化协议

协议配置　要求各主机间具有加密和认证的通道.

协议步骤　(假设系统中有 n 个主机) :

(1) 为各主机 i 生成一对初始的传统集中式签名密钥对(S_i^0, V_i^0) .

(2) 生成全局签名密钥对(Scert, Vcert) , 其中 Scert 由和系统各用户相对应的份额集($Scert_1^0$, $Scert_2^0$, , , $Scert_n^0$) 组成. (Scert, Vcert) 在下次初始化前保持不变, 但份额集($Scert_1^0$, $Scert_2^0$, , , $Scert_n^0$) 在每个时间片内都要更新.

(3) 使用 Scert 对每个主机 i 的标识符及该主机的签名公钥 V_i^0 签名, 得到 Scert(i, V_i^0) 并将[Vcert, $Scert_i^0$, Scert(i, V_i^0)] 分配给各个主机 i.

(4) 将系统所需要维护的秘密信息 X 按照传统的 PSS 方式[1~6] 分解为 n 个份额(X_1^0, X_2^0, , , $_n^0$) , 并将份额 X_i^0 分配给主机 i.

(5) 对于所分配到的份额 $Scert_i^0$ 和 X_i^0, 各主机用自己的签名密钥 S_i^0 签名, 得到 S_i^0($Scert_i^0$) 和 S_i^0(X_i^0) .

注: 主机 i 所分配的信息中, 临时信息 S_i^0、V_i^0、$Scert_i^0$、X_i^0、Scert(i, V_i^0) 、S_i^0($Scert_i^0$) 以及 S_i^0(X_i^0) 需要在每个时间片更新, 只能本地存储; 但 Vcert 作为验证密钥, 其机密性虽无关紧要, 但完整性很重要, 且在系统重新配置之前保持不变, 因此可以只读方式本地保存.

协议分析　加密且认证了的通道保证了系统中所有消息传递的安全性、正确性与可靠性; 数据生成的正确性可由所系统所采用的 PSS 及 PDS 本身的机制所保证.

结论 3　初始化协议保证了系统需要维护的秘密信息 X 及用于系统全局签名的私钥Scert 按照正确的方式进行了分布, 其份额被安全正确地发送给了系统中的各个主机.

512　主机恢复协议

该协议用于消除入侵对主机的破坏, 以重新恢复被破坏了的 X 和Scert 的份额. 其触发条件是系统感知到对某主机的入侵或系统中某主机的当前时间片达到最大值. 感知到入侵时, 系统中的主机有两类: 感知到入侵的和未感知到入侵的. 对于前者, 协议的任务是恢复已被破坏的信息. 由于初始化阶段分配的 Vcert 及维护系统正常运行必须的信息(具体见 113) 以只读方式保存, 因此仍可用. 可调用第 4 节的可靠传输协议, 向系统中所有其它主机发出信息恢复请求, 然后等待从其它主机到来的信息; 若一直等待不到, 则向系统管理员发出失败警告.

对于未感知到入侵的主机 i, 收到 j 送来的恢复请求后, 按以下步骤运行(以恢复序号为 u 的份额集为例) :

(1) 从 ROM 中读取 Vcert 并验证所存储的[Scert(i, V_i^u) , (i, V_i^u)] 的有效性;

(2) 如有效, 则利用 V_i^u 验证[(S_i^u($Scert_i^u$) , $Scert_i^u$] 和[S_i^u(X_i^u) , X_i^u] 的有效性;

(3) 如有效, 说明自身的临时信息未被破坏, 调用可靠传输协议并按照 PSS 和 PDS 所规定的恢复步骤与其它正确的主机一道参与主机 j 所维护的两个秘密份额 $Scert_i^u$ 和 X_i^u 的恢

复;

(4) 若 V_i^u、$Scert_i^u$ 或 X_j^u 无效, 说明主机 i 自身也被破坏. 此时调用可靠传输协议, 向系统中的所有其它主机发出恢复请求, 并等待从其它主机到来的信息; 如果一直等待不到, 则向系统管理员发出恢复失败的警告.

系统未感知到入侵时, 若某主机当前时间片已达到最大值, 则调用可靠链路传输协议向系统中的所有主机广播恢复请求, 此时系统中各主机操作步骤与上述协议类似.

协议分析 由与第 4 节类似的分析可知, 协议中[Scert(i, V_i^u), (i, V_i^u)] 、[S_i^u($Scert_i^u$), $Scert_i^u$] 和[S_i^u(X_i^u), X_i^u] 的验证是有效且正确的. 由于可靠链路传输协议保证了消息的可靠传输, 将系统门限值定义为所用的 PSS 及 PDS 中门限值较小的一个, 则主机份额恢复过程的安全性与正确性可由 PSS 及 PDS 的自身机制所保证.

结论 4 主机恢复协议保证了系统中每个被破坏了的主机都能安全正确地恢复自身所维护着的秘密份额.

513 份额更新协议

以序号为 u 的份额集更新为序号为 u+ 1 的份额集为例.

该协议运行之前恢复协议已成功恢复了被破坏的主机, 每个主机 i 都拥有属于自己的正确的序号为 u 的份额 $Scert_i^u$ 和 X_i^u.

协议步骤 以主机 i 为例

(1) 生成新的签名密钥对(S_i^{u+1}, V_i^{u+1}), 并调用可靠传输协议向系统中所有其它主机广播(i, V_i^{u+1});

(2) 调用可靠传输协议并按所采用的 PSS 和 PDS 所规定的步骤与系统中其它主机一道参与每个主机 j 的两个份额($Scert_i^u$, X_j^u) 到($Scert_j^{u+1}$, X_j^{u+1}) 的更新;

(3) 按照 PDS 的规定步骤与系统中其它主机一起对每个主机 j 的(j, V_j^{u+1}) 签名, 生成 Scert(j, V_j^{u+1});

(4) 接收第 2 步生成的属于自己的两个新份额($Scert^{u+1}$, X_i^{u+1}) 和第 3 步生成的 Scert(i, V_i^{u+1}), 并验证其有效性;

(5) 如有效, 则用 S_i^{u+1} 对 $Scert^{u+1}$ 和 X_i^{u+1} 签名, 得到 S_i^{u+1}($Scert^{u+1}$) 和 S_i^{u+1}(X_i^{u+1}), 否则向系统报告出错.

协议分析 可靠传输保证了协议中的消息能正确到达接收方, 秘密份额($Scert_i^u$, X_i^u) 更新为($Scert_i^{u+1}$, X_i^{u+1}) 的安全性与正确性可由 PSS 及 PDS 本身的机制所保证. 由与第 4 节类似的分析可知, 各主机对收到的新的临时值($Scert^{u+1}$, X_i^{u+1}) 和 Scert(i, V_i^{u+1}) 的验证有效且正确的.

结论 5 份额更新协议保证了系统中每个主机都能够安全正确地更新所需更新的所有临时信息.

由结论 1~ 5 可知:

结论 6 按照本文所给方法, 可在异步的分布式环境中安全正确地实施先应式秘密共享.

6 相关工作

IBM 苏黎世实验室的 Christian Cachin 等人[9] 和 Microsoft 的 Lidong Zhou 等人[10] 近期也对异步环境下的 PSS 问题进行了研究. 然而文献[9]中的方案主要考虑的是双门限(t, k, n) 在异步模型下的可验证问题以及异步模型下的先应式密码系统问题. 由于该方案假定时间片仅与超时机制相关, 而与先应式协议无关, 因此可用于先应式密码系统(Proactive Cryptosystems), 而不仅仅是先应式秘密共享(Proactive Secret Sharing). 该方案中使用了秘密信息的二维分享技术并使用了一个用于系统中各主机通过网络向自身发送时序消息的定时器协议, 其模型也可用于一个时间片内更新协议不会终止的场合. 文献[10]中的方案则就事论事地讨论了具有特殊的组合结构的秘密共享(Combinatorial(n, t+ 1) Secret Sharing) 的异步先应式方案. 其中的时间片是关于先应式组合结构的秘密共享专门定义的, 因此通用性最差. 此外, 这两种方案都仅从时钟的角度定义了时间片的概念, 而没有考虑相关的协议事件, 如系统感知到入侵等. 从效率的角度来看, 我们的方案通信复杂性仅为 $O(n^2)$; 文献[9] 中的是 $O(n^3)$, 而文献[10] 则为 $O\left(\binom{n}{t}\right)$.

7 结论及展望

通过引入由协议事件和系统中各主机本地时钟双重驱动的时间片概念, 本文定义了异步模型下先应式秘密共享的运行状态及其转换过程, 给出了异步环境中一种有效的先应式秘密共享方法. 此外, 为满足不可靠链路条件下消息的可靠传输, 以保证先应式方法的正确实施, 还利用系统全局签名和各通信主机单独签名的方法对系统中传输的消息进行认证, 从而设计了一个可靠传输协议. 从现实系统的角度来看, 本文中时间片的定义应当以日或周为单位, 而异步的先应式协议运行所需的开销则以秒为单位, 因此, 所设计的协议不会对系统正常运行带来太大影响.

然而应当注意的一个问题是, 攻击者可能会在短时间内连续攻击多台主机, 从而触发份额恢复与更新协议不断运行, 以致造成系统崩溃. 这种攻击实际上是一种拒绝服务(DoS) 攻击. 对于这种攻击可以利用现有防 DoS 攻击方面的一些方法, 如窃断攻击连接、追踪攻击源等加以防范. 也可以利用协议设计方面的一些技巧, 如设计具有防 DoS 功能的异步先应式协议等. 这些将是我们下一步工作的重点.

参考文献:

[1] A Herzberg, S Jarecki, H Krawczyk, M Yung. Proactive secret sharing or: How to cope with perpetual leakage[A]. Advances in Cryptology2 Crypto'95, the 15th Annual International Cryptology Conference[C]. Heidelberg: Springer2Verlag, 1995. 457- 469.

[2] R Canetti, R Gennaro, A Herzberg, D Naor. Proactive security: Long2term protection against break2ins[J]. CryptoBytes, 1997, 3(1): 1- 8.

[3] S Jarecki. Proactive secret sharing and public key cryptosystems[D]. Cambridge: Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1995.

[4] Y Frankel, P Gemmell, P Mackenzie, M Yung. Optimal resilience proactive public2key cryptosystems[A]. Proceedings of the 38th Annual Symp. On Foundations of Computer Science[C]. New York: IEEE Press, 1997. 384- 393.

[5] T Draelos, V Hamilton, G Istrail. Proactive DSA application and imple2

mentation[R]. Albuquerque: Sandia National Laboratories, 1998.

[6] A Herzberg, M Jakobsson, S Jarecki, H Krawczyk, M Yung. Proactive public2key and signature schemes[A]. Proceedings of the 4th Annual Conference on Computer Communications Security[C]. New York: ACM Press, 1997. 100- 110.

[7] M Aguilera, S Toueg, B Deianov. Revisiting the weakest failure detector for uniform reliable broadcast[A]. Proceedings of the 13th International Symposium on Distributed Computing[C]. Heidelberg: Springer2Ver2lag, 1999. 19- 33.

[8] R Gennaro, S Jarecki, H Krawczyk, T Rabin. Robust threshold DSS sig2natures[A]. Advances in Cryptology2Eurocrypt. 96, International Con2ference on the Theory and Application of Cryptographic Techniques[C]. Heidelberg: Springer2Verlag, 1996. 354- 37.

[9] C Cachin, K Kursawe, Anna Lysyanskaya, Reto Strobl. Asynchronous verifiable secret sharing and proactive cryptosystems[A]. ACM Confer2ence on Computer and Communications Security[C]. New York: ACM Press, 2002. 88- 97.

[10] L Zhou, F. B Schneider, R Renesse. Proactive secret sharing for asyn2chronous systems[EB/OL]. Submitted to ACM Transactions on Infor2mation and System Security. http://research.microsoft.com/users/li2dongz/apssTISS.ps.

作者简介:

郭渊博　男, 1975 年生于陕西周至, 讲师, 现为西安电子科技大学博士生, 主要研究领域为秘密共享、容忍入侵、密码协议设计等. Email: yuan2bo.g@hotmail.com

马建峰　男, 1963 年生于陕西临潼, 西安电子科技大学计算机学院副院长, 教授, 博士生导师, 计算机网络与信息安全教育部/信息产业部重点实验室主任, 教育部学科建设与专业设置专家委员会委员, 陕西省优秀留学回国人员, 电子学会高级会员和 IEEE 会员, 长期从事信道编码、信息安全及信息可生存性等方面的研究.

新书简介

一部导航领域的最新力作面世

由中国电子学会会士, 著名博士生导师刘基余教授编著的最新力作《GPS 卫星导航原理与方法》一书, 是作者和他所指导的研究生 10 多年来从事教学与科研所倾注心血的结晶. 内容丰富新颖, 理论实际兼顾, 既有广度, 又颇有深度, 创新性, 科学性, 系统完整性都很强, 是一部导航界难得的好书, 已由科学出版社正式出版发行.

全书分 9 章 52 节, 计 53 万字. 前 4 章介绍了系统概论, GPS 卫星及其轨道, 信号与信号接收机; 接着三章阐述 GPS 定位, 包括伪距测量, 载波相位测量与动态载波相位测量和数据处理; 最后两章为误差分析及测量的有关实际应用问题. 从书名与编排看, 似乎平常, 然而具体内容却极不寻常, 难能可贵.

该书紧密地依据各类高等院校导航、测绘等相关专业实际, 就原理方法作了系统全面而又深入浅出的阐述, 图文并茂, 引人入胜; 第二是融入了国际国内有关最新科研成果, 并突出了相关学科与交叉学科的相互渗透及技术融合; 第三是兼顾通用性与特殊性, 还注重开拓性, 前瞻性及学科发展动向, 不但给人以系统的专业科学知识, 而且还是给人以启迪, 思考与深究; 第四是工程应用着眼实际, 包括航天、航空、海洋、交通、测绘等诸多领域的工程应用范例与设计规程, 且提供不少颇有参考价值的实测数据及图表, 实在难得.

这部书不仅仅是一部十分优秀的透于各类高等院校导航及相关专业的教科书, 而且亦是一部从事导航及相关专业的科研、生产、教学、应用与管理的科技工作者极好的参考书、工具书.

(谢世富)