

# 移动 Ad hoc 网络安全路由协议研究

李金鹏, 吕光宏, 王立平, 薛 强

(四川大学 计算机学院, 四川 成都 610064)

**摘 要:**移动 Ad hoc 网络是由一组移动终端组成的无线多跳自治系统, 具有无中心、自组织、多跳路由、动态拓扑结构等特点。尽管有带宽受限等缺点, 但无线 Ad hoc 网络具备灵活机动、组网迅速的优势, 在军事通信、民用通信和各种临时通信中具有广阔的应用前景。近来其路由技术、QoS、安全性问题, 尤其是路由协议的安全成为研究的热点。介绍了针对其路由协议的攻击, 重点分析比较了典型的移动 Ad hoc 网络安全路由协议, 最后指出下一步研究的方向。

**关键词:**移动 Ad hoc 网络; 安全路由; 路由攻击

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1673-629X(2008)07-0024-05

## Research of Secure Routing Protocols for Mobile Ad hoc Networks

LI Jin-peng, LÜ Guang-hong, WANG Li-ping, XUE Qiang

(College of Computer Science, Sichuan University, Chengdu 610064, China)

**Abstract:** Mobile Ad hoc network (MANET) is a collection of mobile nodes, these nodes self-organized into a multi-hop wireless network. It has the characteristics of no pre-existing infrastructure, self-organization, multi-hop and dynamic topological. Although it has the disadvantage of limited bandwidth, it plays an important role in military communication, civil communication and temporary communication. Recently, their routing, QoS, safety, especially in the routing protocol security has become a hot spot. Introduced common attacks on the routing protocols. Then focus on the analysis and comparison of typical secure mobile Ad hoc network routing protocol. Finally concluded the next step in the direction.

**Key words:** mobile Ad hoc network; secure routing; routing attack

## 0 引言

移动自组织网 (MANET, Mobile Ad hoc network)<sup>[1]</sup>是由一组兼具收发功能的移动节点组成的多跳临时性自治系统。移动 Ad hoc 网络的主要目标是建立起源节点、目的节点间的高效路由。研究者们提出了许多相关的路由协议如: DSDV<sup>[2]</sup>, AODV<sup>[3]</sup>, DSR<sup>[4]</sup>, ZRP<sup>[5]</sup>, 但大多没有考虑路由协议的安全问题。

文中分析了针对移动 Ad hoc 网络路由协议的攻击, 详细阐述了典型的移动 Ad hoc 网络安全路由协议, 做了比较与总结, 并指出了下一步研究方向。

## 1 移动 Ad hoc 网络的路由攻击

针对移动 Ad hoc 网络路由协议的攻击, 按照方式不同可分为被动攻击和主动攻击。被动攻击是指恶意节点通过侦听节点间的通信, 分析获取有价值的信息,

由于并不破坏网络的正常工作, 被动攻击很难监测。常见的几种针对路由协议的攻击<sup>[6]</sup>如下:

(1) 黑洞攻击 (Black Hole): 恶意节点谎称拥有通往目的节点的最短路径, 从而使数据包不断流向该恶意节点, 形成一个信息“黑洞”。

(2) 路由表毒化攻击 (Routing Table Poisoning): 恶意节点产生并广播伪造的路由信息, 致使节点错误地更新本地路由表。该攻击可导致路由环路、瓶颈和网络分割甚至整个网络瘫痪。

(3) 重放攻击 (Replay): 重放攻击也称为新鲜性攻击, 攻击者通过重放过时的消息或消息片段, 使收到该信息的节点以陈旧的路由信息更新当前路由表, 达到对主体进行欺骗的攻击行为。

(4) Dos 攻击 (Denial of Service) 旨在破坏网络选路功能, 致使整个网络瘫痪的攻击。常见的方式有路由表溢出 (routing table overflow) 攻击和剥夺睡眠 (sleep deprivation torture) 攻击。

(5) 虫洞攻击 (Wormhole)<sup>[7]</sup>: 又称为隧道攻击, 是一种针对无线 Ad hoc 网络路由的严重攻击。它是在两个串谋恶意节点间建立一条私有通道, 攻击者在网

收稿日期: 2007-10-17

作者简介: 李金鹏 (1981-), 男, 山东济宁人, 硕士研究生, 研究方向为无线自组网; 吕光宏, 博士, 教授, 研究方向为无线网络、光网络。

络中的一端记录数据包或信息,通过此私有通道将窃取的信息传递到网络的另外一端,然后再转发出去,造成两恶意节点间有较短通路的假象。

(6)位置信息泄漏(Location Disclosure):恶意节点发送伪造的路由信息,诱使目的节点回应 ICMP 消息,利用分析技术,得出节点位置甚至整个网络的拓扑结构。

## 2 移动 Ad hoc 网络安全路由协议

为保证无线 Ad hoc 网络的可用性、机密性、完整性、安全认证和抗抵赖性,研究者们提出了许多移动 Ad hoc 网络安全路由协议,如 SEAD, SAODV, SRP, SEDYMO 等。

### 2.1 SAODV

SAODV(Secure Ad hoc On-Demand Distance Vector Routing)<sup>[8]</sup>是按需路由协议 AODV 的安全扩展路由协议,采用数字签名和哈希链来实现路由协议的安全。SAODV 扩展了 AODV 的控制信息包,扩展字段如图 1 所示。

Type	Length	Hash Function	Max Hop Count
Top Hash			
Signature			
Hash			

图 1 SAODV 扩展字段

当节点需发送 RREQ 或 RREP 时,SAODV 将 Max Hop Count 字段设为 TTL,产生随机数 Seed 填充 Hash 字段,设置:Top Hash = Hash<sup>Max Hop Count</sup>(Seed),附上本地节点的公钥,并且使用本地私钥对除去 Hop Count 和 Hash 字段的所有字段进行数字签名。然后转发出去,中间节点收到控制消息后,利用消息中的公钥验证签名,通过比较:Top Hash = Hash<sup>Max Hop Count - Hop Count</sup>(Hash)来验证路由跳数。两项验证都通过后,中间节点重新计算 Hash 值:Hash = h(Hash),然后再转发该控制消息。

SAODV 使用数字签名保障控制消息中不可变字段的完整性,实现端到端的验证;使用单向哈希链来保证跳数的正确性。中间节点只需验证签名,计算量小。但该协议假定每个节点都知道所有网络节点的公钥,实现困难。

### 2.2 Ariadne

Ariadne(A Secure On-Demand Routing Protocol for Ad Hoc Networks)<sup>[9]</sup>是一种由 SEAD 的作者提出的基于 DSR 的按需安全路由协议。该协议使用了 TESLA 广播认证方案,它通过消息认证码(MAC)实现对

报文的认证,利用时钟同步和密钥延迟发布来防止伪造消息认证码。

Ariadne 假定源节点和目的节点拥有共享密钥,网络节点拥有其它节点的 TESLA 认证初始值。该协议主要有三方面内容:

①采用允许目的节点验证路由请求的机制;

②提出了三种可以互换的机制来验证路由请求和路由回复中的数据;

③采用了一种有效的哈希算法来验证路径上的每个节点都不能缺少。

Ariadne 采用非对称加密技术和广播认证方案,实现安全路由,开销较小,但是 TESLA 认证方案需要时钟同步的支持,这在移动 Ad hoc 网络中实现很困难,且节点 IP 地址未加保护,易导致位置信息的泄漏。

### 2.3 SRP

SRP(Secure Routing Protocol)<sup>[10]</sup>是一种基于广播方式发现路由的安全协议。该协议使用 MAC 值实现端到端的认证和信息的完整性保护。协议假定源节点、目的节点间建有安全连接(Secure Association, SA),并且拥有共享密钥。SRP 在基础协议上添加了 SRP 扩展包头(Qid, Qseq, SRP MAC),用来实现消息认证。路由发现过程中,首先有源节点产生随机的请求报文标识 Qid 和 32 位的序列号 Qseq,然后将源节点地址、目的节点地址、序列号,利用共享密钥进行完整性计算,将上述值添加到路由请求消息中广播出去。中间节点收到路由请求信息后首先检查 Qid,如路由表中存在,则丢弃,反之,添加本地 IP 地址到节点列表,然后转发。而且中间节点监测邻居节点的路由请求频率,查询频率小的节点有高的报文转发率,以防止恶意节点发送大量报文发起 Dos 攻击。目的节点收到请求消息后,首先检查 Qseq 是否最新,然后通过计算 MAC 值验证消息的完整性,两项都通过后目的节点产生应答消息,沿反向路径传至源节点。

SRP 使用 MAC 值实现身份认证和消息完整性保护,中间节点无需校验,协议实现简单,序列号的使用可防止重放攻击。但中间节点的地址以明文的方式传送不能阻止恶意节点的插入,网络的拓扑信息也容易泄漏。

### 2.4 SAR

SAR(Security-Aware Ad hoc Routing Protocol)<sup>[11]</sup>是一种基于按需路由协议的安全扩展。SAR 借鉴 QoS 机制,提出了 QoP(Quality of Protection)思想,在路由发现和维护过程中以节点的安全等级作为选路标准,来保证获得符合安全需求的路由。

SAR 将节点分成多个安全等级,同一等级的节点

共享一个密钥,节点身份和等级需绑定。路由发现过程中,源节点将本次路由发现的最低安全级别附在 RREQ 中然后广播出去,中间节点首先确认该节点是否符合最低的安全需求,如是则继续转发,否则丢弃。最终建立符合安全级别需求的路由。如果路由发现最终失败,协议规定源节点调整路由发现的安全级别,重新启动路由发现。

SAR 协议引入 QoS 思想,通过实施节点分级制来保障路由协议的安全需求,保证路由协议不受伪造、假冒等攻击。分级制在一定程度上也减少了路由发现过程中的洪泛开销。但是该协议只是一个大体的框架,在身份认证、密钥管理、等级划分等具体问题上还有很多工作。

## 2.5 SRAN

SRAN(Secure Routing Protocol for Wireless Ad hoc Networks)<sup>[12]</sup>是一种按需的多路径安全路由协议。节点需定期广播 HELLO 消息,用来发现邻居节点。发现新节点后,该节点启动分布式认证模型(Distributed Authentication Model, DAM)实现邻居认证,建立本地信任值列表。如节点 A 欲认证邻居节点 B, A 首先查找本地 Trust-table,如找不到,则 A 广播 trust-value-request 消息到本节点的信任节点,如果邻居节点没有 B 的信任值,该邻居节点继续转发该请求消息到其他邻居节点。直到 B 节点或拥有 B 节点信任值的节点反馈相应值到 A。A 收到的信任值可沿多条路径到达, A 利用如下公式计算 B 的信任值:

Trust-value(B) =

$$\frac{\sum_{i=1}^n (\text{trust-value}(i)) \cdot \text{trust-value-rp}(i)}{\sum_{i=1}^n \text{trust-value}(i)}$$

其中: trust-value(i) 指第 i 个反馈节点的信任值, trust-value-rp(i) 指第 i 个反馈节点返回的需认证节点的信任值。A 将计算后的信任值添加到本地信任列表,完成对 B 节点的信任评价。如节点发现邻居节点有非法或自私行为,节点可降低该节点的信任值,当该值小于某阈值时可将该节点列入黑名单,并广播 WARNING 消息通知邻居节点,该机制可隔离非法和自私节点。

协议假定节点拥有共享的组密钥。路由发现阶段,源节点将源节点和目的节点地址、序列号,利用组密钥生成的 MAC 作为 RREQ 广播出去。中间节点检查本地信任值列表,验证上游节点,如信任值低于阈值则丢弃;反之,节点利用组密钥验证 MAC 值。通过验证后再转发该请求消息,该消息沿多条路径转发至目

的节点。目的节点验证 MAC 值,通过后生成 RREP,附上和上游节点共享的私钥生成的 MAC 值,传到上游节点,中间节点验证 RREP 的 MAC 值,通过后利用和上游节点共享的私钥生成新的认证码,替换原有认证码,转发至上游节点,最终建立起安全的多径路由。

SRAN 使用分布式认证模型,建立节点信任关系表,隔离非法和自私节点;采用 MAC 验证路由消息的完整性。这样可抵挡重放、篡改、黑洞等攻击,对自私节点也可及时检测、隔离。

## 2.6 SEDYMO

SEDYMO(Secure Dynamic MANET On-demand Routing Protocol)<sup>[13]</sup>是基于按需路由协议 DYMO<sup>[14]</sup>的安全路由协议。假定有分布式认证中心的支持,主要采用哈希链和数字签名两种安全机制。

SEDYMO 在 DYMO 协议的 RREQ 中增加了三个字段: HashFunc, TopHash, Hash。源节点首先生成一个随机数,作为哈希函数的种子(seed);初始化 Hash 字段为: Hash<sub>0</sub> = seed; TopHash 为: TopHash = H<sup>HopLimit</sup>(Hash<sub>0</sub>),然后将该 RREQ 广播。中间节点收到上游节点 N<sub>i-1</sub> 的 RREQ 后,记录上游节点,替换字段: Hash<sub>i</sub> = H(Hash<sub>i-1</sub>); HopCnt = HopCnt + 1。然后节点验证 H<sup>HopLimit-HopCnt</sup>(Hash) = TopHash,如果通过则更新路由表,转发该信息。收到 RREQ,目标节点验证哈希值后,生成 RREP,将包传送最大跳数(HopLimit)置为: HopLimit = HopCnt<sub>RREQ</sub>,然后沿反向路径转发,直到到达源节点建立路由。

为减少签名开销,提高效率,SEDYMO 采用了基于陷门同态置换的聚合签名方案,但采用公钥密码机制,开销较大,扩展性不强。

## 2.7 SecMR

SecMR(Secure Multipath Routing Protocol for Ad hoc Networks)<sup>[15]</sup>是一种按需的多路径安全路由协议,主要包括邻居鉴别和路由发现两方面。

邻居鉴别:所有节点需定期向一跳邻居节点广播鉴别信息: (t, ID<sub>i</sub>, sig<sub>i</sub>(t, ID<sub>i</sub>), cert<sub>i</sub>),邻居节点利用证书提供的公钥验证签名,实现邻居鉴别。最终每个节点都建立一张一跳邻居列表 N<sub>i</sub>。

路由发现:首先由源节点按需初始化一路由查询消息 Q<sub>S,T</sub>: (ID<sub>S</sub>, ID<sub>T</sub>, seq, hop<sub>cnt</sub>, hop<sub>max</sub>, EPKt(K<sub>S,T</sub>), RouteList, ExcludeList, NextHop, hash<sub>KS,T</sub>(ID<sub>S</sub>, ID<sub>T</sub>, hop<sub>max</sub>)), RouteList, ExcludeList 初始置为空,源节点向邻居节点广播该报文。中间节点验证本节点是否在该报文的 NextHop 列表中;RouteList 表最后一节点是否是鉴别邻居,如两项都满足且 hop<sub>cnt</sub> + 1 < hop<sub>max</sub>,则执行以下操作:

$\text{Hop}_{\text{cnt}} := \text{hop}_{\text{cnt}} + 1; \text{RouteList} := \text{RouteList} + \text{ID}_i;$   
 $\text{ExculdeList} := \text{ExculdeList} + (\text{NextHop} - \text{ID}_i);$   
 $\text{NextHop} := N_i - (N_i \cap \text{RouteList}) - (N_i \cap \text{ExculdeList})$

以上操作保证了路由查询消息向没有收到过该报文的邻居节点转发,减少了洪泛开销,保证了效率。

路由回复:目的节点收到查询消息  $Q_{S,T}$  后解密出  $K_{S,T}$ ,验证哈希值。等待一定间隔,以同样方式验证来自源节点 S 沿不同路径传播的查询报文,且计算得出满足条件:

$$\bigcap_{i=1}^k \text{RouteList}_i = \emptyset$$

的  $k$  条节点分离路径,并针对其中每个查询路由,生成相应的路由回复报文,并广播出去。收到该报文的中间节点,首先验证本节点是否在  $\text{RouteList}_i$  中,如否则丢弃,反之,继续验证  $\text{RouteList}_i$  列表中本节点的前驱和后继节点是否是鉴别邻居,如否则丢弃,反之,广播该报文。最终建立起节点分离的  $k$  条安全路径。

SecMR 使用邻居鉴别实现节点间的认证,隔离非法结点,通过哈希计算实现了端到端的认证,保证了消息的完整性,并且对非法结点的协作攻击有较强的鲁棒性。

### 3 分析与比较

由于移动 Ad hoc 网络本身的特性,传统网络的安全机制不再适用,上述几种典型协议采取不同的安全机制在机密性、完整性、安全认证、不可抵赖性等方面提供了保障。表 1 从安全路由协议的选路方式、选路标准、安全需求、措施等方面进行了比较。

从表 1 可以看出大部分安全路由协议是在按需路由协议上的安全扩展,并且大多需要认证中心(CA)

或安全连接(SA)的支持,安全机制多采用高效的单向哈希链。由于多路径安全协议针对合作攻击有较强鲁棒性,最近研究较多。

### 4 结束语

无线 Ad hoc 网络有着广泛的应用前景。但由于自身的特性,其路由协议容易遭受多种攻击,不可能有一种安全方案能有效地防御各种攻击,而且不同的应用场合安全需求也不尽相同。研究者需结合密钥管理,入侵检测等机制,设计出符合特定安全需求的路由协议。此外,还应注意以下几点:

(1)效率与安全:在安全路由协议中,采用安全措施,必定会导致路由效率的降低。由于无线 Ad hoc 网络的能量和计算能力有限,因此安全协议不能太复杂,应综合考虑路由安全和效率问题。

(2)虫洞攻击:虫洞(Wormhole)攻击是由两个恶意节点合谋进行的一种针对 Ad Hoc 路由协议的严重攻击,目前大部分路由协议都无法处理虫洞攻击。现有的解决方案大多采用 Packet Leashes<sup>[16,17]</sup>机制和 SECTOR<sup>[18]</sup>机制,由于额外开销太大,实际应用性并不强。设计出可避免虫洞攻击的高效路由协议是设计者应考虑的问题。

(3)组播安全:现在安全路由协议多集中在单播路由协议,随着面向组服务的需求增加,组播路由协议的安全也是下一步研究的方向。

#### 参考文献:

- [1] IETF Mobile Ad hoc Networks(MANET) Working Group [EB/OL]. 2001-03. <http://www.ietf.org/html.charters/manet-charter.html>.

表 1 安全路由协议属性比较

Protocol	Routing approach	Routing number	Requirements	Security mechanism
SAODV	On demand	Single path	Public key distribution	Digital Signature, One-way Hash chains
Ariadne	On demand	Single path	Clock Synchronization, Each pair of nodes share key, Publish Authentication TESLA key	One-way hash chains, Message Authentication Code
SRP	On demand	Single path	SA(Secure Association)	Message Authentication Code
SAR	On demand	Single path	key distribution scheme	Quality of Protection
SRAN	On demand	Multipath	All nodes share a group key	Distributed Authentication Model, Message Authentication Code
SEDYMO	On demand	Single path	Distributed Certification authority	Digital Signature, One-way Hash chains
SecMR	On demand	Multipath	Certification authority	Digital Signature, Message Authentication Code

- [2] Perkins C E, Bhagwat P. Highly dynamic destination sequenced distance - vector routing (DSDV) for mobile computers[C]//Proceedings of the SIGCOMM'94. [s. l.]: [s. n.], 1994: 234 - 244.
- [3] Perkins C E, Royer E M. Ad hoc On - Demand Distance Vector Routing[C]//IEEE Workshop on Mobile Computing Systems and Applications. New Orleans, LA, USA: [s. n.], 1999: 90 - 100.
- [4] Johnson D B, Maltz D. Dynamic Source Routing in Ad hoc Wireless Networks[M]. New York: Kluwer Academic Publishers, 1996: 153 - 181.
- [5] Chlamtac I, Conti M. Mobile Ad hoc Networking: Imperatives and Challenges[J]. Ad hoc Networks, 2003, 1(1): 13 - 64.
- [6] Argyroutis P G, Donal M. Secure routing for mobile ad hoc networks[J]. IEEE Communication Survery & Tutorials, 2005, 7(3): 2 - 21.
- [7] Hu Y C, Perrig A, Johnson D B. Wormhole attacks in wireless networks[J]. Selected Areas in Communications, 2006, 24(2): 370 - 380.
- [8] Zapata M G. Secure ad hoc on - demand distance vector (SAODV) routing[EB/OL]. 2005 - 07. <http://www.ietf-report.isoc.org/idref/draft-guerrero-manet-saodv/>.
- [9] Hu Y C, Perrig A. Ariadne: A Secure On - demand Routing Protocol for Ad hoc Networks[C]//Proceedings of the 8th ACM International Conference on Mobile Computing and Networking. Atlanta, GA, USA: [s. n.], 2002: 12 - 23.
- [10] Padimatrators P, Haas Z. Secure Routing for Mobile Ad hoc Networks[C]//SCS Communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio, TX, USA: [s. n.], 2002: 27 - 31.
- [11] Yi S, Naldurg P, Kravets R. Security - aware Ad hoc Routing for Wireless Networks[C]//Proc. of ACM MOB IHOC'01. Long Beach, CA, USA: [s. n.], 2001: 299 - 302.
- [12] Li H Z, Singhal M. A Secure Routing Protocol for Wireless Ad Hoc Networks[C]//Proceedings of the 39th Annual Hawaii International Conference on System Science. Hawaii, USA: [s. n.], 2006.
- [13] Helena R F, Jordi H J. Secure Dynamic MANET On - demand (SEDYMO) Routing Protocol[C]//Proceedings of the Fifth Annual Conference on Communication Networks and Services Research (CNSR'07). Fredericton, Canada: [s. n.], 2007: 372 - 380.
- [14] Chakeres I, Perkins C. Dynamic MANET on - demand Routing [EB/OL]. 2006 - 04. <http://tools.ietf.org/html/draft-ietf-manet-dymo>.
- [15] Macropodi R. Secure Multipath Routing Protocol for Mobile Ad hoc Networks[C]//Proceedings of the Second Annual Conference on Wireless On - demand Network Systems and Services (WONS'05). St Moritz, Switzerland: [s. n.], 2005: 89 - 96.
- [16] Hu Y C, Perrig A, Johnson D B. PacketLeashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks[C]//INFOCOM '2003. San Francisco, California, USA: [s. n.], 2003: 1976 - 1986.
- [17] Hu Y C, Perrig A, Johnson D B. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols[C]//Proceedings of the ACM Workshop on Wireless Security (WiSe'2003). Rome, Italy: [s. n.], 2003: 30 - 40.
- [18] Capkun S, Buttyan L, Hubax J. Sector: Secure tracking of node encounters in multi - hop wireless networks[C]//Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03). Washington, D. C, USA: [s. n.], 2003: 21 - 32.

(上接第 23 页)

累的过程中,就会由量变达到质变,整个组织必定会从中受益无穷,成为一个高效、焕然一新的组织。

缺陷预防是一个渐进的过程,每次只是针对优先级最高的缺陷加以预防,然后就是次高的缺陷,不断地重复下去。每次的缺陷预防都将产生对过程的改进建议,因而过程改进也是逐渐进行的,正如 Watts Humphrey 常说的一句话是:“软件过程改进不是目标,而是一条漫漫长路”<sup>[8]</sup>。

#### 参考文献:

- [1] 梁成才,章代雨,林海静. 软件缺陷的综合研究[J]. 计算机工程, 2006, 32(19): 88 - 90.
- [2] Chang Ching - Pao, Chu Pchih - Ping. Defect Prevention in Software Processes: An Action - Based Approach[J]. Journal of Systems and Software, 2007, 80(4): 559 - 570.
- [3] Song Qinbao, Shepperd M, Cartwright M, et al. Software De-

fect Association Mining and Defect Correction Effort Prediction[J]. IEEE Transactions on Software Engineering, 2006, 32(2): 69 - 82.

- [4] Humphrey W S. 软件过程管理[M]. 高书敬,顾铁成,胡寅译. 北京:清华大学出版社,2003: 342 - 366.
- [5] Biffi S, Halling M. Investigating the Defect Detection Effectiveness and Cost Benefit of Nominal Inspection Teams[J]. IEEE Transactions on Software Engineering, 2003, 29(5): 385 - 397.
- [6] Wagner S, Seifert T. Software quality economics for defect - detection techniques using failure prediction[J]. ACM SIGSOFT Software Engineering Notes, 2005, 30(4): 1 - 6.
- [7] Crosby P B. 质量免费: 确定质量的艺术[M]. 北京: 中国人民大学出版社, 2006: 2 - 15.
- [8] Zahran S. 软件过程改进[M]. 陈新, 罗劲枫, 等译. 北京: 机械工业出版社, 中信出版社, 2002.