一种新的移动 Ad hoc 网络安全路由协议*)

刘 晶[1] 伏 飞[2] 肖军模[1]

(解放军理工大学通信工程学院 南京 210007)[1] (解放军理工大学指挥自动化学院 南京 210007)[2]

摘 要 Buttyan L. 等指出了移动 Ad hoc 网络典型安全路由协议 Aridane 的缺陷,并提出了一种自称可以抵御 active-1-y(y≥1)型攻击的路由协议 EndairA[9]。文章通过分析发现 EndairA 不能抵御一种 active-0-1 型攻击,即中间人攻击,并据此提出了一种新的安全路由协议 EndairALoc。分析表明 EndairALoc 不仅保持了 EndairA 原有的安全性,而且还能够抵御中间人攻击和虫洞攻击。另外该协议采用对称密钥机制替代了 EndairA 中使用的公钥签名机制,降低了安全路由所需的能耗。

关键词 Ad hoc 网络,安全,路由协议,攻击

Secure Routing for Mobile Ad hoc Networks

LIU Jing[1] FU Fei[2] XIAO Jun-Mo[1]

(Institute of Communications Engineering, PLA Univ. of Sci. & Tech., Nanjing 210007)[1]

(Institute of Command Automation, PLA Univ. of Sci. & Tech., Nanjing 210007)[2]

Abstract Buttyan L. et al. found out a security flaw in Aridane and proposed a secure routing protocol, EndairA, which can resist attacks of active-1-1 according to ref[9]. But unfortunately we discover an as yet unknown active-0-1 attack, "man-in-the-middle attack", which EndairA can't resist. So we propose a new secure routing protocol, EndairALoc. Analysis shows that EndairALoc can not only inherit security of EndairA, but also resist "man-in-the-middle attack" and even wormhole attack. Furthermore EndairALoc uses pairwise secret keys instead of public keys EndairA used, so compared with EndairA, EndairALoc can save more energy in the process of routing establishment.

Keywords Ad hoc networks, Security, Routing protocols, Attack

1 引言

移动 Ad hoc 网络(MANET, mobile Ad hoc network)是一种不依赖于固定基础设施的自组织无线网络,其组网方便、快捷、不受时间和空间限制等优势,使它在军事和民用领域具有广泛的应用前景[1]。但是其无固定基础设施、节点能量有限、网络拓扑变化频繁、使用无线信道等特点,使得现有各种安全机制不能直接被应用到该网络中。因此,Ad hoc 网络安全问题已受到学术界的广泛关注,安全路由是其中的一个研究方向。

设计安全路由协议的目标是通过增加安全机制来抵御各种攻击,使得通信双方获得正确可靠的路由。目前已提出的安全路由协议包括 SRP[2]、Aridane[3]、SAODV[4]、ARAN[5]、SADSR[6]、SEAD[7]等。其中 SRP、Aridane 是 DSR[8]上发展而来的典型的安全路由协议。SRP 要求路由发现过程的源节点与目的节点预共享密钥,并采用二者的消息认证码(MAC)来保护 rreq 和 rrep 报文。Aridane 是由卡内基梅隆大学提出的,与 SRP 不同的是它增加了源节点与中间节点之间的安全关联,除源节点和目的节点通过 MAC 进行身份认证外,中间节点在路由请求阶段可采用数字签名等方式向源节点认证自己的身份,并且其作者声称该协议能够抵御 active-1-1 型攻击(定义见 2.1 节)。

2005 年 Budapest 大学的 Buttyan L. 等指出一种 SRP 和 Ariadne 不能抵御的 active-1-1 型攻击,并提出一种新的安全路由协议 EndairA,宣称该协议可以抵御 active-1-y(y≥1)攻击[9]。但我们经分析发现了一种 EndairA 不能抵御的 active-0-1 攻击(与 active-1-y 关系见 2.1 节),我们称之为中间人攻击。针对该缺陷,在 EndairA 的基础上,我们提出了一种利用节点位置信息的安全路由协议 EndairALoc。分析表明该协议除保持 EndairA 原有的安全性,还具有抵御中间人攻击和虫洞攻击的能力。另外,我们使用对称密钥机制替代 EndairA 采用的公钥签名机制,从而减少了网络的路由能耗,延长了网络寿命。本文第 2 节介绍攻击模型与 EndairA 协议;第 3 节指出 EndairA 协议的缺陷;第 4 节提出一种新的安全路由协议 EndairALoc;第 5 节对 EndairALoc 进行安全分析和性能分析;最后进行了小结。

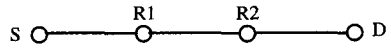
2 攻击模型与 EndairA

2.1 攻击模型

Active-n-m 型攻击[3]:n 代表攻击者捕获的合法节点数目(假设攻击者可以获取被捕获节点的全部密钥信息),m 代表攻击者拥有的恶意节点数目。攻击者可将被捕获节点的密钥信息拷贝给这些恶意节点,使它们均能以合法身份参与网络活动。捕获的合法节点越多,攻击能力越强大。因为一个变节的内部合法节点可以执行一个外部非法节点的所有攻击行为,不能抵御 active-0-1 型攻击,必然不具备抵御 active-1-1 型攻击的能力。

*)基金项目:国家自然科学基金资助项目(69931040),江苏省自然科学基金资助项目(BK2004015)。刘 晶 博士生,主要研究领域为网络信息安全;伏 飞 博士生,主要研究领域为无线自主网;肖军模 教授,博士生导师,主要研究领域为网络信息安全。

2.2 EndairA 协议



1) S -> * : (rreq,S,D,Q_{id}),

2) R_1 ->* : (rreq,S,D, Q_{id},R_1),

3) R_2->* : (rreq,S,D, Q_{id},R_1R_2),

4) D->R_2 : (rrep,S,D, Q_{id},R_1R_2, Sig_D),

5) R_2->R_1: (rrep,S,D, Q_{id},R_1R_2, Sig_DSig_{R2}),

6) R_1->S : (rrep,S,D, Q_{id},R_1R_2, $Sig_DSig_{R2}Sig_{R1}$,)

图 1 EndairA 协议

图 1 显示了 EndairA 协议路由建立过程：源节点 S 首先生成 rreq 报文，Q_{id} 为 rreq 报文序列号，下一跳节点收到后仅将自己的标识加入 route list 中就广播出去，依此类推，直至到达目的节点 D。D 首先检查 route list 中最后一个节点是否是自己的邻居节点，如果不是则丢弃；如果是，D 生成 rrep 报文，其中 Sig_D 是对前面所有字段的数字签名，然后发送给上一跳节点 R_2。R_2 检查自己是否在 route list 中以及 route list 中自己的前后节点是否是邻居节点，如果不是，则丢弃；如果是，则在报文尾部加上对前面所有字段的数字签名。然后发送给上一跳节点，依此类推，直至到达源节点 S。S 首先检查 route list 中第一个节点是不是邻节点，然后验证所有的签名。如果成立，则接受此 route list 为可靠的路由。

从上述可知，EndairA 采用中间节点在 rrep 报文中签名的机制，而 Aridane 则采用中间节点在 rreq 报文中签名的机制[3]。文[9]详细论述了后者容易遭受一种 active-1-1 攻击——恶意节点能够通过删除上一跳节点的签名来构造虚假路由。EndairA 克服了 Aridane 的这个缺陷，Buttyan L. 等也宣称 EndairA 能够抵御 active-1-y(y≥1) 型攻击。但是，我们发现了一种 EndairA 不能抵御的 active-0-1 型攻击——中间人攻击。

3 EndairA 的缺陷

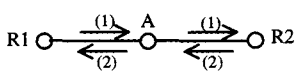
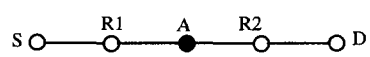


图 2 中间人攻击模型

图 2 显示了中间人攻击过程。攻击者 A 转发 R_1、R_2 间的报文，使得 R_1、R_2 以为互为邻居，而且对中间人的存在毫无所知。这是一种间接的攻击形式，在因特网中这种攻击模型早已得到广泛应用。移动 Ad hoc 网络中该攻击使得不在一跳通信范围内的两个节点以为互为邻节点。



1) S -> * :(rreq,S,D,Q_{id}),

2) R_1-> *: (rreq,S,D, Q_{id},R_1),

3) A -> * : (rreq,S,D, Q_{id},R_1),

4) R_2-> * :(rreq,S,D, Q_{id},R_1R_2),

5) D->R_2 :(rrep,S,D, Q_{id},R_1R_2, Sig_D),

6) R_2->A(R_1) :(rrep,S,D, Q_{id},R_1R_2, Sig_DSig_{R2}),

7) A-> R_1 :(rrep,S,D, Q_{id},R_1R_2, Sig_DSig_{R2}),

8) R_1->S :(rrep,S,D, Q_{id},R_1R_2, $Sig_DSig_{R2}Sig_{R1}$,)

图 3 EndairA 协议攻击实例

图 3 给出 EndairA 协议遭遇中间人攻击的实例。假设恶意节点 A 处于 R_1、R_2 之间。第 6 步，R_2 欲将携带有自己签名的 rrep 报文发送给 R_1，但实际上 A 接收该报文，并在第 7 步中原封不动地转发给 R_1，R_1 收到后检查 route list，发现 R_2 和 S 都是它的邻节点，添加签名后发送给 S。S 发现 R_1 为邻节点且验证签名正确，接受(R_1 R_2)为一条正确的路由。

上述攻击实例表明，中间人攻击是一种 active-0-1 攻击，不需要捕获合法节点就能达到破坏路由的目的。在战场等敌我矛盾突出的网络环境中是非常危险的。

另外 EndairA 采用的公钥签名机制需要消耗大量计算资源和能量资源。尤其对于拓扑变化频繁的 Ad hoc 网络，路由需要不断的建立和更新，这样将直接影响网络的寿命。

4 EndairALoc 协议

针对 EndairA 存在的问题，我们提出一种 Ad hoc 网络安全路由协议 EndairALoc，具有抵御中间人攻击和虫洞攻击的能力，且弥补了数字签名方案资源开销过大的问题。

协议假设：

(1)密码系统是理想的，不考虑密码系统自身的安全问题；

(2)网络内部节点两两预共享对称密钥，用于构造消息认证码，散列范围包括它前面的各个字段；

(3)通信双方节点是合法节点，即仅考虑中间转发节点为恶意节点；

(4)网络中节点能够通过某种定位机制[10]获取自己的位置信息；

(5)节点通信范围固定，只有在通信范围内的两个节点才能直接发送和接收对方数据。

1) S -> * : (rreq,S,D,Q_{id}),

2) R_1->* : (rreq,S,D,Q_{id},R_1),

3) R_2->* : (rreq,S,D,Q_{id},R_1R_2),

4) D->R_2 : (rrep,S,D, Q_{id},R_1R_2,L_D ,MAC_{DS}),

5) R_2->R_1:(rrep,S,D,Q_{id},R_1R_2,L_D L_{R2},$MAC_{DS}MAC_{R2S}$)

6) R_1->S :(rrep,S,D,Q_{id},R_1R_2,$L_DL_{R2}L_{R1}$,

$MAC_{DS}MAC_{R2S}MAC_{R1S}$)

图 4 EndairALoc 协议

图 4 显示了 EndairALoc 协议路由建立过程。第 4 步，目的节点 D 构造 rrep 报文，其中 L_D 为 D 的位置信息，MAC_{DS} 为消息认证码，散列范围包括前面各个字段。同理后续中间节点也依次在 rrep 报文中增加自己的位置信息及 MAC，直至到达源节点 S。S 首先验证各消息认证码，如果正确，再检查位置信息列表 $L_DL_{R2}L_{R1}$ 中各相邻节点是否在相互的通信范围内。如果验证通过，则接受该 route list 为正确的路由。

假设图 3 的攻击者存在于 EndairALoc 协议运行环境中，当 rrep 报文最终到达源节点 S，S 检查位置信息列表 L_DL_{R2} L_{R1}，依据 $L_{R2}L_{R1}$ 之间距离远超出节点通信范围，可以判断出该 route list 不是正确的路由。

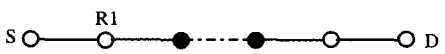


图 5 虫洞攻击模型

(下转第 109 页)

础上，提出了一个改进的 LSB 隐写算法，该算法采用载体图像中最低两位隐藏信息，使用了 F_1、F_{-1}、F_1F_{-1}、$F_{-1}F$ 四种变换。文中还对 RS 分析方法和统计分析法进行了阐述，并利用这两种技术对新算法的安全性进行了分析。理论分析及实验结果表明，改进算法提高了传统 LSB 算法的安全性，可以抵御 RS 分析方法和统计分析法的攻击。

参 考 文 献

1 陈波，谭运猛，吴世忠. 信息隐藏技术综述[J]. 计算机与数字工程，2005，33(2)：21～23
2 Wu D C, Tsai W H. A steganographic method for images by pixel-value differencing[J]. Pattern Recognition Letters, 2003, 24: 1613～1626
3 Zhang X, Wang S. Steganography using multiple-base notational system and human vision sensitivity[J]. IEEE Signal Processing Letters, 2005, 12(1): 67～70
4 Chang C C, Tseng H W. A Steganographic method for digital images using side match[J]. Pattern Recognition Letters, 2004, 25: 1431～1437
5 夏煜，郎荣玲，等. 基于图像的信息隐藏检测算法和实现技术研究综述. 计算机研究与发展，2004，41(14)：728～736
6 Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images[J]. Magazine of IEEE Multimedia (Special Issue on Security), 2001, 8 (4): 22～28
7 Fridrich J, Du R, Long M. Steganalysis of LSB encoding in color Images[R]. ICME'2000, New York, USA, 2000
8 邓倩岚，林家骏. 基于统计的 LSB 隐写分析方法[J]. 计算机安全，2006，1：23～24
9 Westfeld A, Pfitzmann A. Attacks on steganographic systems [J]. Lecture Notes in Computer Science, 1999, 1768: 61～76
10 Ker A D. Steganalysis of LSB matching in grayscale images[J]. IEEE Signal Processing Letters, 2005, 12(6): 441～444

(上接第 89 页)

另外，目前没有任何路由协议声称可以抵御虫洞攻击。如图 5 所示，两个合谋节点 A 之间的虚线表示“虫洞”，合谋节点通过“虫洞”转发来自合法节点的信息，导致 R_1、R_2 误以为互为邻节点。攻击节点运用与中间人攻击同样的手段转发 rrep 报文，同理 EndairA 无法抵御这种攻击，最终 S 会接受 (R_1R_2) 为一条正确路由。但在 EndairALoc 中，源节点 S 检查位置信息列表 $L_D L_{R2} L_{R1}$，L_{R2} 与 L_{R1} 之间距离远远超出节点通信范围，故可知相应 route list 不是正确路由，即 EndairALoc 协议具有抵御虫洞攻击的能力。

5 安全和性能分析

5.1 安全性分析

EndairALoc 除能够抵御中间人攻击以及虫洞攻击，还保持了 EndairA 原有的安全性，分析如下：

(1)恶意结点修改报文中的控制信息及位置信息：控制信息包括身份标识、序列号等，位置信息是节点的位置。这些消息包含在消息认证码的散列范围中，因此任何破坏完整性的操作都将被源节点检查消息认证码时发现。

(2)恶意结点丢弃 rreq 或 rrep 报文：EndairALoc 仍属于改进的 DSR 安全路由协议，一个路由请求将返回多条应答路由，少量的恶意节点将不会影响路由的建立。

(3)重放攻击：恶意结点向网络中传播以前传送过的 rreq 或 rrep 报文，由于报文中携带的序列号保证了消息的新鲜性，这些重放报文将被其它结点作为滞后报文丢弃。

5.2 性能分析

安全路由协议较普通路由协议扩展了安全功能，必然相应地引入一定的网络负载和能耗。源节点消息认证码的验证和位置信息列表的检查增加了源节点的计算开销和路由建立的时延，但因路由请求阶段简单快捷，节点操作步骤少，只有路由应答报文传播过程中节点需计算消息认证码，并且一次路由请求可以获得多条路由信息，因此路由开销整体不大。另外 EndairALoc 采用的是计算量小的对称密钥密码体制的消息认证码，而不是 EndairA 选择的公钥密码体制的数字签名的方式。文[11]对公钥密码算法和对称密码算法的能耗做了量性分析，分析结果如表 1 所示，公钥密码算法比对称密码算法的能耗大几个数量级，因此 EndairALoc 减小了节点计算量，延长了网络寿命。综上可知，EndairALoc 在增强了安全性的同时，并没有带来过多的能耗，更加适合 Ad hoc 网络这种能量受限的网络。

表 1 不同加密算法的能耗

算法	能耗
Public-key(RSA, DSA, ECDSA)	100～500mJ
Secret-key(DES, AES, IDEA)	2～5uJ
Hash(MD5, SHA, HMAC)	0.5～1uJ

小结 本文通过对安全路由协议 EndairA 的分析，指出该协议虽然避免了 Aridane 协议的缺陷，但是并非具有其所声称的能够抵御所有 active-1-y 攻击的能力。我们发现了一种 EndairA 不能抵御的 active-0-1 型攻击——中间人攻击，并据此提出了一种新的安全路由协议 EndairALoc。分析表明该协议不仅保持 EndairA 原有的安全性，而且具有抵御中间人攻击和目前没有任何协议可以抵御的虫洞攻击的能力。另外，由于该协议利用对称密钥机制替代了 EndairA 中采用的公钥签名机制，因此降低了路由建立所需的能耗。未来我们将进一步研究能够抵御更强的敌手模型的新的 Ad hoc 网络安全路由协议。

参 考 文 献

1 Hu Y C, Perrig A. A survey of secure wireless Ad hoc routing. Security & Privacy Magazine, IEEE, 2004, 2: 28～39
2 Papadimitratos P, Haas Z. Secure routing for mobile ad hoe networks. In: Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. San Antonio TX, 2002. 27～ 31
3 Hu Y C, Perrig A, Johnson D B. Ariadne: a secure on-demand routing protocol for Ad hoc networks. In: Proc. of the Eighth ACM Intl Conf. on Mobile Computing and Networking (MOBICOM 2002). Atlanta, GA, 2002. 23～28
4 Zapata M G. Se curing Ad hoc routing protocols. In: Proc. of ACM workshop on wireless Security. Atlanta, Sep. 2002. 1～9
5 Sanzgir K, Dahill B. A secure routing protocol for Ad hoc networks. In: Proc. of the 10 IEEE Intl. Conf. on Network Protocols, 2002. 1～10
6 Ghazizadeh S, Ilghami O, Sirin E. Security—aware adaptive dynamic source routing protocol. In: Proc. of the 27th Annual IEEE Conf. on Local Computer Networks, 2002
7 Hu Y C, Johnson D B, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless Ad hoc networks. Ad hoc Networks, 2003, 1(1): 175～192
8 Johnson D B, Maltz D, Hu Y C. The dynamic source routing protocol for mobile Ad hoc networks. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt, 2005
9 Buttyan L, Vajda I. Towards provable security for Ad hoc routing protocols. In: Proc. of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, 2005
10 AdHoc Positioning System (APS). GLOBECOM 2001 - IEEE Global Telecommunications Conference, 2001(1): 2926～2931
11 Potlapally N, Ravi S, Raghunathan A, Jha N. Analyzing the EnergyConsumption of Security Protocols. ISLPED'03, 2003