新的Ad hoc网络安全路由协议

伏 飞[1]，刘 晶[2]，肖军模[2]

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

【摘要】针对目前Ad hoc网络安全DSR协议的安全性难以保证的现状，提出并证明了能够抵御active-1-y($y\geq 1$)攻击的安全DSR所必须满足的一个充要条件，同时设计了一种新的安全DSR协议—— ESDSR，并证明该协议满足上述充要条件。分析结果表明，与现有各种安全DSR协议相比，ESDSR不仅达到了抵御active-1-y攻击的安全目标，而且具有最低的资源开销，适用于Ad hoc网络环境。

关 键 词 Ad hoc网络; 攻击; 路由协议; 安全

中图分类号 TP393 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.03.017

Secure Routing Protocol for Ad hoc Networks

FU Fei[1], LIU Jing[2], and XIAO Jun-mo[2]

(1. Institute of Command Automation, PLA of University of Science and Technology Nanjing 210007;
2. Institute of Communication Engineering, PLA of University of Science and Technology Nanjing 210007)

Abstract To provide an effective method for verifying security of secure dynamic source routing (DSR) protocols, a sufficient-and-necessary condition against active-1-y($y\geq 1$) adversary for secure DSR protocols is proposed. Then a new secure DSR protocol, named effective secure DSR (ESDSR), which is proved to meet this sufficient-and-necessary condition is presented. Compared with the existing secure DSR protocols, the proposed protocol ESDSR can not only defend against active-1-y adversary, but also consume less resource.

Key words Ad hoc networks; attack; routing protocols; security

随着Ad hoc网络的研究日益深入，这种应用于现代化战场、紧急和灾难等危险场景的新型网络的安全问题正越来越多地受到人们的关注[1]。早期提出的Ad hoc网络路由协议以提高路由性能为设计目标[2-4]，往往忽视路由安全问题。缺乏安全性考虑的路由协议，在敌对环境下，无法抵御敌方的恶意攻击，导致网络无法正常运行。设计具有抵御攻击能力的安全路由协议成为近年来的研究热点[5-6]。

DSR是一种Ad hoc网络按需路由协议，采用源路由方式选路，具有简单、高效的特点。由于DSR协议本身并未考虑安全性问题，在敌对环境下，存在严重的安全隐患。研究人员通过在DSR路由报文中采用密码学手段添加认证信息，先后提出了Ariadne[7]、SRP[8]和endairA[9-10]等安全路由协议。后续分析显示，SRP、Ariadne添加的认证信息存在设计缺陷[10]，并未达到抵御active-1-y($y\geq 1$)攻击[7]的安全目标；endairA虽然达到了抵御active-1-y攻击的安全目标，但是由于在路由应答阶段才能检查并丢弃虚假路由，对网络带宽和能耗造成了严重的浪费。而且，这些安全路由协议普遍缺乏有效的安全验证，难以检验协议的安全性。

为解决上述问题，本文以抵御active-1-y攻击为安全目标，提出了一种新的有效的安全DSR协议ESDSR(effective secure DSR)。与现有各种安全DSR协议的比较显示，ESDSR不仅实现了抵御active-1-y攻击的安全目标，而且具有最低的资源开销。

1 安全DSR协议的充要条件及其证明

安全DSR协议的根本目标是确保存在攻击者时，协议仍然能够得到与网络拓扑相符的正确路由。而对于一条正确路由(如$R_1R_2R_3$)，active-1-y攻击可以构造的虚假路由包括：(1) 添加伪造的节点信息X(如$R_1R_2XR_3$)；(2) 添加与拓扑不符的信息A(如$R_1R_2AR_3$)；(3) 任意删除前面的节点信息(如R_1R_3)；(4) 篡改节点信息(如R_1AR_3)；(5) 改变节点信息顺序(如$R_1R_3R_2$)。针对上述攻击，安全DSR协议通过在

收稿日期：2007 – 10 – 15；修回日期：2008 – 06 – 18
基金项目：部级预研项目
作者简介：伏 飞(1980 –)，男，博士生，主要从事无线网络安全协议方面的研究.

DSR基础上增加数字签名等认证信息来保证报文的完整性(防止信息篡改)和认证性(防止信息伪造)。但由于参与路由协议的节点数目多、位置关系复杂，已有的安全DSR协议添加的认证信息往往存在缺陷，如SRP未能实现中间节点认证(即未能达到认证性)，Ariadne的后续节点可能删除前面节点的信息(即未能达到完整性)。

本文在一定假设前提的基础上，提出安全DSR协议产生正确路由的充要条件。充要条件应保证路由报文满足认证性和完整性，满足充要条件的安全DSR协议产生的路由将与网络拓扑结构一致。

假设前提：(1) 网络中所有链路是双向的；(2) 不考虑加密认证算法本身的安全性问题；(3) 网络具有安全的密钥分发机制；(4) 网络中的节点分为可信节点、外部攻击者和内部攻击者3种；(5) 同SRP、Ariadne和endairA一样，不考虑目的节点T是内部攻击者的情况。

本文在上述假设前提下，提出以下充要条件：(1) 认证信息保证S能够确认$(R_1,R_2,\cdots,R_n)$中任一R_i和目的节点T均为具有合法身份的节点，且保证S能够确认R_i及T确实参与了本轮源节点为S、目的节点为T、序号为Q_{id}的路由发现过程；(2) 认证信息保证S能够确认$(R_1,R_2,\cdots,R_n)$中节点顺序未被篡改；(3) 认证信息保证S能够确认$(R_1,R_2,\cdots,R_n)$中不存在被篡改的节点信息；(4) 认证信息保证S能够确认在传递过程中后续节点无法删除$(R_1,R_2,\cdots,R_n)$中前面节点的节点信息。

定理 1 如果源节点S、目的节点T、序号为Q_{id}的一轮DSR路由发现过程中产生的路由为$(R_1,R_2,\cdots,R_n)$，且认证信息能够满足上述充要条件，则$(R_1,R_2,\cdots,R_n)$是与网络拓扑相符的正确路由。

证明：假设充要条件(1)不成立。S不能确认$(R_1,R_2,\cdots,R_n)$中R_i的合法身份，则恶意节点可添加伪造的节点信息(X)，构造虚假路由$(R_1,R_2,\cdots,R_i,\cdots,R_n)$。而认证信息无法保证$S$确认$R_i$确实参与了本轮源节点为$S$、目的节点为$T$、序号为$Q_{\mathrm{id}}$的路由发现过程，则$R_i$可能未参与本次路由发现过程，$(R_i)$是由恶意节点添加的，因此$(R_1,R_2,\cdots,R_i,\cdots,R_n)$是虚假路由。$T$的证明与$R_i$类似。故假设不成立，充要条件(1)成立。

假设充要条件(2)不成立。认证信息无法保证$(R_1,R_2,\cdots,R_n)$中节点顺序未被篡改，被篡改的$(R_1,R_2,\cdots,R_n)$显然不是正确路由，故假设不成立。充要条件(2)成立。

充要条件(3)和(4)的证明同充要条件(2)。

综上可证得，满足充要条件条件(1)～(4)，则$(R_1,R_2,\cdots,R_n)$未被篡改、删除、添加、伪造，是正确路由。

2 ESDSR协议

本文提出一种新的安全DSR协议ESDSR，并证明该协议满足上述充要条件，即能够抵御active-1-y攻击。而且，ESDSR在目的节点T处验证路由的正确性(根据假设(5)，本文不考虑T是恶意节点的情况)，保证了返回的路由应答报文rrep不包含虚假路由，从而减少了通信资源的浪费。

ESDSR协议路由发现过程如下：

(1) S ->* : (rreq,S,T,Q_{id},h_0),

$h_0=\mathrm{MAC}_{ST}=H_{KST}$[rreq,$S$,$T$,$Q_{\mathrm{id}}$]

(2) R_1->* : (rreq,S,T,Q_{id},R_1,h_1),

$h_1=H[R_1,h_0,\mathrm{MAC}_{R_1T}]$

$\mathrm{MAC}_{R_1T}=H_{KR_1T}$[rreq,$S$,$T$,$Q_{\mathrm{id}}$,$R_1$]

(3) R_2->* : (rreq,S,T,Q_{id},R_1R_2,h_2),

$h_2=H[R_2,h_1,\ \mathrm{MAC}_{R_2T}]$

$\mathrm{MAC}_{R_2T}=H_{KR_2T}$[rreq,$S$,$T$,$Q_{\mathrm{id}}$,$R_1R_2$]

(4) T->R_2: (rrep,S,T,Q_{id},R_1R_2,MAC_{TS}),

$\mathrm{MAC}_{TS}=H_{KTS}$[rreq,$S$,$T$,$Q_{\mathrm{id}}$,$R_1R_2$]

(5) R_2->R_1 : (rrep,S,T,Q_{id},R_1R_2,MAC_{TS}),

(6) R_1->S : (rrep,S,T,Q_{id},R_1R_2,MAC_{TS}),

(7) 用h_1替换h_0。

在上述过程中，源节点S广播携带标识S、T、Q_{id}及h_0的rreq报文，其中，h_0是用于T对S认证的MAC_{TS}。中间节点R_1收到rreq报文后，首先添加自己的节点信息R_1，然后计算:

$\mathrm{MAC}_{R_1T}=H_{K_{R_1T}}$[rreq,$S$,$T$,$Q_{\mathrm{id}}$,$R_1$]

$h_1=H[R_1,h_0,\mathrm{MAC}_{R_1T}]$

式中 $H_{K_{R_1T}}$ 表示带密钥的Hash算法[11]； K_{R_1T} 为R_1和T的共享密钥；H表示不带密钥的hash算法，且全网公开。

R_2的操作与R_1类似。直到rreq报文到达T。T依次计算出h_0、h_1和h_2后，验证rreq报文中携带的h_2的正确性。如果不正确则丢弃；正确则计算MAC_{TS}，并生成包含S、T、Q_{id}标识以及路由信息R_1R_2和MAC_{TS}的rrep报文。rrep报文延路由R_1R_2的反方向传输到源节点S。

定理 2 源节点S、目的节点T、序号为Q_{id}的ESDSR路由发现过程建立的一条路由$(R_1,R_2,\cdots,R_n)$是与网络拓扑相符的正确路由。

证明：(1) S能够验证rrep报文中MAC_{TS}，从而确认T具有合法身份。根据MAC_{TS}覆盖了S、T和Q_{id}，S能够确认T确实参与了本轮源节点S、目的节点T、序号Q_{id}的路由发现过程。又根据假设“T不是恶意节点”，进而S相信MAC_{TS}覆盖的$(R_1,R_2,\cdots,R_n)$是T验证通过的，S相信T确认的信息。

(2) 对于T收到的rreq中$(R_1,R_2,\cdots,R_n)$以及h_n，$h_n=H[R_n,h_{n-1},\mathrm{MAC}_{R_nT}]=H[R_n,[R_{n-1},h_{n-2},\mathrm{MAC}_{R_{n-1}T}],\mathrm{MAC}_{R_nT}]=\cdots=H[R_n,[R_{n-1},[R_{n-2},\cdots,[R_1,h_0,\mathrm{MAC}_{R_1T}],\cdots,\mathrm{MAC}_{R_{n-2}T}]\,\mathrm{MAC}_{R_{n-1}T}]\,\mathrm{MAC}_{R_nT}]$。因为$T$可计算出$\mathrm{MAC}_{R_iT}=H_{K_{R_iT}}[\mathrm{rreq},S,T,Q_{\mathrm{id}},R_i]$$(0<i<n)$，从而能够确认$R_i$具有合法身份，同时$\mathrm{MAC}_{R_iT}$覆盖$S$、$T$和$Q_{\mathrm{id}}$，因此$T$能够确认$R_i$参与了本轮协议。又由证明(1)中$S$对$T$的信任关系，故充要条件(1)得证。

(3) 恶意节点A对$(R_1,R_2,\cdots,R_n)$中节点顺序的篡改只可能发生在路由请求或路由应答阶段。假设在路由请求阶段，A收到包含$(R_1,R_2,\cdots,R_i)$的rreq报文，对应地可得$h_i=H[R_i,[R_{i-1},[\cdots[R_{j+1},[R_j,h_{j-1},\mathrm{MAC}_{R_jT}],\mathrm{MAC}_{R_{j+1}T}]\cdots]\,\mathrm{MAC}_{R_{i-1}T}]\,\mathrm{MAC}_{R_iT}]$。$A$调换其中$R_j$与$R_{j+1}$的顺序为$(R_1,R_2,\cdots,R_{j+1}R_j,\cdots,R_i)$，对应的$h_i'=H[R_i,[R_{i-1},[\cdots[R_j,[R_{j+1},h_{j-1},\mathrm{MAC}'_{R_{j+1}T}],\mathrm{MAC}'_{R_jT}]\cdots]\,\mathrm{MAC}'_{R_{i-1}T}]\,\mathrm{MAC}'_{R_iT}]$。由于只有拥有$K_{R_{j+1}T}$的节点$R_{j+1}$和$T$才能构造$\mathrm{MAC}'_{R_{j+1}T}$，因此$A$无法构造$\mathrm{MAC}'_{R_{j+1}T}$等认证信息，进而无法构造$h_i'$，因此篡改发生在路由请求阶段的假设不成立。同理，易证得篡改发生在路由应答阶段的假设不成立。故得证充要条件(2)成立。

(4) 恶意节点A对$(R_1,R_2,\cdots,R_n)$中节点信息的篡改只可能发生在路由请求或路由应答阶段。假设在路由请求阶段，A收到包含$(R_1,R_2,\cdots,R_i)$的rreq报文，A将其中的R_j改为R'_j，类似(3)中的证明可知，A无法构造$(R_1,R_2,\cdots,R'_j,\cdots,R_i)$对应的$h_i'$，因此篡改发生在路由请求阶段的假设不成立。同理，易得证篡改发生在路由应答阶段的假设不成立。故得证充要条件(3)成立。

(5) 反证法。假设充要条件(4)不成立，存在恶意节点A，A收到包含$(R_1,R_2,\cdots,R_i)$的rreq报文，其中$h_i=H[R_i,h_{i-1},\mathrm{MAC}_{R_iT}]$。$A$删除节点$(R_{j+1},R_{j+2},\cdots,R_i)$构造虚假路由$(R_1,R_2,\cdots,R_j)$$(j<i)$，由类似证明(3)的证明可知，$A$无法获得相应的认证信息$h_j=H[R_j,h_{j-1},\mathrm{MAC}_{R_jT}]$，因此无法删除$(R_{j+1},R_{j+2},\cdots,R_i)$。同理可得证$A$无法删除$(R_1,R_2,\cdots,R_i)$中任何节点信息，故假设不成立。充要条件(4)成立。

综上得证ESDSR满足充要条件(1)～(4)，故ESDSR得到的是正确路由，定理2得证。

3　与现有安全DSR协议的比较

本文从安全性(能否抵御active-1-y攻击)、计算开销(认证密码算法)、通信开销等3个方面分别比较ESDSR、SRP、Ariadne和endairA：

(1) 安全性(能否抵御active-1-y攻击)：SRP和Ariadne无法抵御active-1-y攻击，存在产生虚假路由的可能性。endairA和ESDSR能抵御active-1-y攻击(可以证明endairA满足本文提出的充要条件)。因此，本文仅讨论能够抵御active-1-y攻击的ESDSR和endairA的计算和通信开销。

(2) 计算开销(认证密码算法)：endairA采用数字签名算法计算认证信息，而ESDSR采用MAC及hash算法。文献[12]指出在同等软硬件环境下，对同等长度报文进行计算，数字签名比Hash以及MAC的计算开销大3～4个数量级。ESDSR与endairA的路由报文长度接近，符合文献[12]的前提，因此ESDSR比endairA耗费的计算开销少。

(3) 通信开销：对endairA而言，在路由请求阶段，每个中间节点在收到的rreq报文中仅插入自己的节点标识，T无法验证rreq报文中路由的正确性；在路由应答阶段，中间节点首先根据接收的rrep报文中前面节点添加的认证信息验证路由正确性，然后采用邻居节点检查机制验证rrep报文的路由信息中自己的前后节点是否是正确的邻居节点。如果两方面都成立，则继续转发该rrep；如果有一方面不成立，则丢弃该rrep。对ESDSR而言，在路由请求阶段，每个中间节点都在rreq报文插入认证信息，因此T能够直接验证rreq中路由的正确性。如果正确，T发送应答报文rrep；如果不正确，T不发送rrep。根据前面的分析可知，endairA发现并丢弃虚假路由的时刻要比ESDSR晚，因此在存在恶意攻击的情况下，endairA将比ESDSR耗费更多的通信资源。为方便讨论，本文假设网络中一跳传输的通信开销为e，路由请求阶段产生虚假路由$(R_1,R_2,\cdots,R_i,R_{i+1},\cdots,R_n)$，其中$R_i$是恶意节点插入的不存在的节点信息。endairA中包含该虚假路由的rreq报文从R_i传到T，相应耗费的通信开销为$(n-i+1)e$，然后包含该虚假路由的rrep报文从T传到R_{i+1}，R_{i+1}借助邻居节点检查机制发现其虚假性，相应的开销为$(n-i)e$，故endairA共耗费通信资源$E_{\mathrm{endairA}}=(2n-2i+1)e$；在ESDSR中$T$能够发现该虚假路由，因此耗费的通信开销仅包含rreq报文从R_i传到T的部分，即$E_{\mathrm{ESDSR}}=(n-i+1)e$。显然，

$E_{ESDSR}<E_{endairA}$，而且$n-i$越大，ESDSR节省的能量越多。

根据上述分析可得，与现有各种安全DSR协议相比，本文提出的ESDSR不但保持了最优的安全性能，同时还保持了最低的资源开销，因此更加适合于资源受限的Ad hoc网络。

4 总 结

本文针对现有安全DSR协议存在的主要问题，结合DSR协议按需源路由的特点，在一定假设前提下，以能够抵御active-1-*y*攻击、得到正确路由为安全目标，给出了一个安全DSR协议必须满足的充要条件，并提出了一种新的安全DSR协议ESDSR，证明了ESDSR满足充要条件。将ESDSR与现有安全DSR协议进行了比较，结果显示不论是安全性还是能耗，ESDSR都优于现有安全DSR协议，因此更加适合于通信资源有限的Ad hoc网络。

参 考 文 献

[1] YANG H, LUO H Y, YE F, et al. Security in mobile Ad hoc networks: challenges and solutions[J]. IEEE Wireless Communications, 2004, 11(1): 38-47.

[2] JOHNSON D, HU Y C. The dynamic source routing protocol(DSR)for mobile Ad hoc networks for IPv4. DSR)[J/OL]. [2008-01-24]. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr.

[3] PERKINS C, BELDING R E, DAS S-. Ad-hoc on-demand distance vector(AODV)[J/OL]. [2007-012-24]. http://www. ietf. org/ internet-drafts/ draft-ietf-manet-aodv.

[4] PERKINS C, BHAGWAT P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers[C]//Proceedings of the SIGCOMM ’94 Conference on Communications Architectures, Protocols, and Applications. London, UK: ACM Press, 1994.

[5] HU Y C, PERRIG A. A survey of secure wireless Ad hoc routing[J]. Security & Privacy Magazine, 2004, 2: 28-39.

[6] PATWARDHAN A, PARKER J, JOSHI A, et al. Secure routing and intrusion detection in Ad hoc networks[C]// Proceedings of the 3rd International Conference on Pervasive Computing and Communications. Kauai Island: IEEE Press, 2005.

[7] HU Y C, PERRIG A, JOHNSON D B. Ariadne：a secure on-demand routing protocol for Ad hoc networks[J]. Wireless Networks, 2005, 11(1-2): 21-38.

[8] PAPADIMITRATOS P, HAAS Z. Secure routing for mobile Ad hoc networks[C]//Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio: Sage Science Press, 2002: 27-31.

[9] ACS G, BUTTYAN L, VAJDA I. Provably secure on-demand source routing in mobile Ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2006, 5(11): 1533-1546.

[10] BUTTYAN L, VAJDA I. Towards provable security for ad hoc routing protocols[C]//Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks. Washington DC, USA: ACM Perss, 2005.

[11] KRAWCZYK H, BELLARE M, CANETTIKENT R. HMAC: Keyed-Hashing for message authentication[J/OL]. [2008-01-24]. http://www.ietf.org/internet-drafts/draft-ietf-manet-hmac.

[12] POTLAPALLY N, RAVI S, RAGHUNATHAN A, et al. Analyzing the energy consumption of security protocols[C]//Proceedings of the 2003 International Symposium on Low Power Electronics and Design (ISLPED ’03). Seoul, Korea: ACM Press, 2003.

编 辑 熊思亮