移动 Ad hoc 网络的一种安全路由协议*)

蒋廷耀 李庆华 李 鹏

(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 移动 ad hoc 网络的开放、动态、分布式特性对网络安全问题提出了巨大挑战。本文指出了几种典型安全路由协议的缺陷,并提出了一种新的安全路由协议 AMDSR。它采用对路由请求消息进行逐跳认证、端-端完整性检查和监听的方法来扩展 DSR 协议的安全功能,并确保建立最快速的路径。AMDSR 监听邻居结点广播的路由消息而不似传统协议混杂收听所有消息,具有更好的适用性。

关键词 Ad hoc 网络,路由,安全

Secure Routing for Mobile Ad-hoc Networks

JIANG Ting-Yao LI Qing-Hua LI Peng

(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)

Abstract Mobile ad hoc networks (MANETs) bring great challenges in security due to its high dynamics, link vulnerability, and complete decentralization. With routing being a critical aspect for MANETs, existing routing protocols however are not sufficient for security requirements. This paper presents a secure routing protocol based on end-to-end integrity check and hop-by-hop authentication of discovery request. Monitor technique without working in promiscuous mode is adopted to prevent compromised neighbor nodes' Byzantine behaviors. The proposed protocol guarantees the quickest path.

Keywords Ad hoc networks, Routing, Security

1 引言

移动 ad hoc 网络(MANETs)不需要固定的基础设施和集中式管理,在战场、紧急救灾、电子会议、传感器(sensor)互连等需要临时快速配置网络的场景中有着巨大的应用前景,然而由于其开放、动态、分布式特性,使得其更易遭受网络入侵。MANETs 是由移动结点相互提供路由而组成的一种 P2P 网络,研究适合于其低带宽、低存储容量、低计算能力特性的高效路由技术是一个关键问题。已出现了一些未考虑安全问题的协议,典型的如主动路由协议 DSDV[1]、按需路由协议 AODV[2]、DSR[3],其中按需协议更适合于无线环境。我国学者在 ad hoc 网络协议方面也做了一些重要工作[4~9]。近来又出现了一些考虑了安全因素的路由协议[10~18],但由于针对 MANETs 的入侵行为的多样性和 MANETs 本身的脆弱性,这些协议尚存在各种缺陷。本文提出了一种新的安全路由协议 AMDSR(Authenticating and Monitoring Dynamic Source Routing),它扩展了 DSR 协议的安全功能,堵塞了过去一些协议中的安全漏洞,并确保提供最快速的路径。AMDSR 监听邻居结点广播的路由消息而不似传统协议混杂(promiscuous)收听所有消息,具有更好的适用性。

2 相关工作

对 MANETs 的入侵有来自于网络外部未认证结点的攻击,也有内部已获认证但变节结点的攻击,其中内部攻击更难识别和防范,对 MANETs 路由的攻击较有线网络或传统的基于基站的无线网络更具多样性,恶意结点往往通过修改或伪造路由信息,或模仿其它结点的行为来产生路由环、延迟或丢弃路由信息、产生非最优路径、形成黑洞、发起 DoS 攻击等,破坏或降低路由协议的正常功能。目前,已出现的一些典型安全路由协议,如:SRP[10]、ARAN[11]、SAODV[12]、SAD-SR[13]、Ariadne[14]、Context[15],是对 DSR 或 AODV 的安全扩展,但都存在安全漏洞,下面结合图 1 进行简要讨论。

2.1 ARAN、SADSR 协议

ARAN、SADSR 假定存在一个可靠的证书服务器 CA,结点进入网络前从 CA 获得一个绑定了结点 ID 和公钥的证书,结点间使用证书相互进行身份认证。ARAN 协议思想如下:初始,源结点 S 广播一个路由发现请求 $RREQ$,$RREQ=\langle RDP, D, S.certificate, Ns, t\rangle_{K_S^-}$(用 S 的私钥对()中的内容进行数字签名),RDP 是请求标志,数 Ns 和时戳 t 用来防止路由环。$X1$ 收到 S 的路由请求 $RREQ$,用 $RREQ$ 中 S 的证书所携带的公钥验证 S 的签名。如合法,$X1$ 用自己的私钥签名 $RREQ$ 并加上自己的证书广播给 $X2$,$X2$ 收到 $X1$ 的消息 $(\langle RREQ\rangle_{K_{X1}^-}, X1.certificate)$后,去掉 $X1$ 的签名和证书,加上自己的签名和证书再广播出去,经 $X3$、$X4$ 到达 D(经 $X6$、$X5$ 的请求分组被 $X3$ 抛弃),D 验证 $X4$ 的签名,再验证 $RREQ$ 中 S 的签名后生成一个路由响应分组 $RREP$,将 $RREP$ 沿着 $RREQ$ 的反向路径单播回 S,其间 $RREP$ 仍需逐跳(hop-by-hop)认证和端-端完整性检查。但假定 $X3$ 是恶意结点,它应将 $RREP$ 单播给反向路径中的下一个结点 $X2$,但它却可将 $RREP$ 单播给 $X5$,而 $X5$ 不能觉察到 $X3$ 的恶意行为,因为证书和签名都是合法的。$RREP$ 再经 $X6$、$X2$、$X1$ 到达 S,端-端完整性检查也是合法的,因 $X3$ 并未修改 $RREP$。结果路由被修改并加长,因此,文[11]声称 ARAN 能确保提供最快速的路径的结论是错误的。同样的情况也发生在 SADSR 协议上,这里不再赘述。

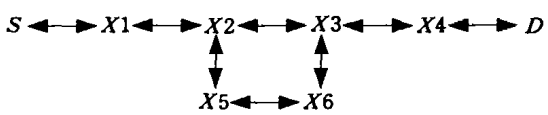

图 1 一个简单的 ad hoc 网络

*)本文得到国家自然科学基金(60273075)资助。蒋廷耀 副教授,博士研究生,当前研究方向:网络安全,移动计算。李庆华 教授,博导,研究兴趣,网格计算,网络安全。李 鹏 硕士研究生。

2.2 Ariadne、Context、SRP 协议

Ariadne、Context、SRP 协议假定源、目的结点共享一个密钥，使用单向哈希函数进行端-端完整性检查。Ariadne 协议思想如下：S 初始一个经过加密的路由请求 $RREQ$，并广播消息($RREQ, h(r))(h'(r)=h(h'^{-1}(r)), h$ 是哈希函数。)，r 是源、目的结点的共享密钥。$X1$ 收到 S 的请求消息后广播消息($RREQ, X1, h^2(r)$)，$X2$ 收到 $X1$ 的消息后广播($RREQ, X1, X2, h^3(r)$)，之后 $X3$ 应广播给 $X4$ 一个消息($RREQ, X1, X2, X3, h^4(r)$)，但它却可展开攻击，而是广播消息($RREQ, X1, X2, X6, X5, X3, h^6(r)$)，最终 D 计算 $h^7(r)$ 并验证 $RREQ$，不会觉察到路由表的修改，也就是说 Ariadne 能确保恶意结点不能从路由表中删除结点但不能排除插入结点的恶意行为。

文[15]介绍了一个安全路由协议，本文简称为 Context 协议，它是对 Ariadne 的改进，但仍存在如下缺陷：恶意结点可以自由地不经认证地将自己加入到路由表中；修改消息中的哈希值而直到目的结点才能发现有修改发生，且消息发送不具有不可抵赖性；在路由维护阶段，指控恶意行为的消息也可被攻击者任意修改。如 X2 指控 X3 有恶意行为，X1 却可将指控对象修改为 X6，根据投票机制，由于没有其它结点指控 X6，信誉系统会误认为 X2 是恶意指控。Ariadne、Context、SRP 协议的一个共有缺陷就是源、目的结点外的其它结点可以任意伪造或修改路由错误消息(ERROR)而不能进行身份认证和完整性检查。

2.3 SAODV 协议

它假定有一 CA，结点可以相互认证，采用 RSA 签名路由控制分组 $RREQ$、$RREP$、$ERROR$，使用单向哈希函数对跳步数认证，中间结点验证签名和哈希值。但恶意结点可以通过假装目的结点是它的邻居结点，或声称一个任意大的目的顺序号，或隐藏真实的路径长度的方法来破坏路由功能。例如图 1 中，$X2$ 到 D 有 2 条路径：$X2, X3, X4, D$ 和 $X2, X6, X5, X3, X4, D$。当 $RREQ$ 到达 $X3, X6$ 时，$X3, X6$ 都会通过 $X2$ 返回一个 $RREP$，但恶意结点 $X6$ 可以采用将其包含在 $RREP$ 中的目的顺序号为任意大的方法来获得路径，而没有使网络获得最优路径且恶意结点包含到了路径中。

3 AMDSR 协议

本文采用和 SAODV、ARAN 和 SADSR 相同的网络假定，即有一可靠 CA，结点进入网络前从 CA 获得一个证书，可以相互认证公钥。协议基本思想是对路由请求消息进行逐跳认证和源、目的间端-端的完整性检查，采用看门狗(watchdog)监视邻居结点的行为。看门狗技术在文[16]、CONFIDANT [17]、CORE [18]、Context 协议中都有应用，但它们都假定结点处于混杂收听模式，即能收听到邻居结点单播或广播的任何消息，这是一个不现实的前提，并且会在采用有向天线的网络里失效。AMDSR 协议里，结点处于正常工作模式，仅监听广播消息，这样可适用于有向通信。

AMDSR 协议分为路由发现和路由维护 2 个阶段，路由发现由下列 5 步组成：

Ⅰ. 请求初始化。源点生成一个路由请求分组 $RREQ$，它包含一个 5 元组〈请求标志，源结点，目的结点，请求顺序号，源结点的证书〉和用源点的私钥对该元组的数字签名 2 部分，一个空的路由表(req_list)保存到高速缓冲区中，路由表由一个 3 元组〈源结点，目的结点，请求顺序号〉标识，网络中每个结点保存着最近到达它并广播出去的路由表。随后源结点对 $RREQ$ 和路由表签名，并将 $RREQ$、路由表、签名、源结点的证书组合成请求消息广播出去。

Ⅱ. 请求传播。请求消息以洪泛方式传播，收到请求消息的中间结点用消息所携带的证书中的公钥验证消息发送者的签名，这可以防止网络外结点的攻击。如签名合法并且该请求是第一次到达，则该结点移出消息中的签名和证书，将自己添加到路由表的末尾，随后用该结点自己的私钥对 $RREQ$ 和路由表签名，并将 $RREQ$、路由表、签名、该结点的证书广播出去。如接收到的请求消息不是第一次到达，这意味着要么是多路径中(如 $X2$、$X6$ 广播的路由请求消息都能到达 $X3$)滞后的请求到达，要么是再次接收到了自己曾经传播过的路由请求。前一种情况不做任何处理，用于请求分组尽快传送；后一种情况，结点转而监视邻居结点传送路由请求的情况，若发现邻居结点没有正确执行路由功能则报警，用于排除在路由表中插入或删除结点的恶意行为。

Ⅲ. 请求接收/响应初始化。目的结点验证请求分组 $RREQ$ 中源结点的签名，若合法则生成一个路由响应分组 $RREP$，它由一个 3 元组(响应标志，路由表，目的结点的证书)和用目的结点的私钥对该元组的签名 2 部分构成，随后将 $RREP$ 以单播方式沿着路由表中源到目的结点的反向路径传播。

Ⅳ. 响应传播。中间结点将接收到的响应分组简单的转发给反向路径中的下一个结点。

Ⅴ. 响应接收。源结点验证响应分组中目的结点的签名，如合法则将路由表存放到缓冲区(可能有多个响应，按到达先后顺序存放)，数据分组随后将按路由表中的路径发送，如签名不合法则抛弃。

路由维护阶段，由路径中的各结点跟踪路由是否有效。当一结点发现路径断开时，生成一个路由错误分组 $ERROR$，签名后单播给源结点，源结点验证 $ERROR$ 生成者的签名后根据该结点的信任值决定是否选取缓冲区中的下一条路径或重新发起一次路由发现进程。网络中各结点维护着关于其它结点的是否正确执行了路由功能的一个信任值，由接收的报警消息用投票机制进行信任评估。

Procedure list

Concatenate($item1, item2, \cdots$)：连结 $item1, item2$ 等项

cache ($item1, item2, \cdots$)：将 $item1, item2$ 等项存放到高速缓冲区

unicast($item1, item2, \cdots$)：单播消息

broadcast($item1, item2, \cdots$)：广播消息

sign(x)：对 x 签名，即对 x 作哈希操作并用结点的私钥加密，将结果添加到 x 的末尾

verify (x)：用 x 所包含的证书中的公钥验证签名，如签名正确返回真值，否则返回假值

remove(x)：移出 x 中的签名和证书

find($item1, item2, item3$)：在存放路由表的高速缓冲区中查找源结点为 $item1$，目的结点为 $item2$，请求顺序号为 $item3$ 的匹配项，如有返回相应的路由表，否则返回 NULL 值。

Action at source node *S* when a new route to destination D is needed

```
RREQ=sign(concatenate(REQ,S,D,S.certificate,req_sequence));
/* REQ 是请求分组标志,req_sequence 是请求顺序号 */
req_list=; /*req_list 是路由表 */
cache( S,D,req_sequence,req_list);
brd_msg=sign(concatenate(RREQ,req_list));
broadcast(brd_msg,S.certificate); /* 广播路由请求消息 */
```

Action at node *x* when received a request message req_msg

```
if verify(req_msg) then
    remove(req_msg);
    if x<>D then /* x 不是目的结点 */
        find_req_list= find(S,D,req_sequence)
        if find_req_list =NULL then /* 请求消息是首次接收 */
            req_list=concatenate(req_list,x);
            cache(S,D,req_sequence,req_list)
```

```
            brd_msg = sign (concatenate (RREQ, req_
              list));
            broadcast(brd_msg,x.certificate);
        else
            if req_list ( ) concatenate (find_req_list, req_
                msg's sender) and x included in req_list
                then flooding an alarm message;
    else /* x 是目的结点 */
        if verify(RREQ) then
            req_list=concatenate(S,D,req_sequence,req_
              list)
            RREP = sign (concatenate (REP, req_list,
              x.certificate)); /* REP 是响应分组标志 */
            unicast(RREP) ; /* 沿着 req_list 中的反向路
              径单播 RREP */
        else
            flooding an alarm message
Action at node x when received a response message RREP
if x=S then /* x 是源结点 */
    if verify(RREP) then
        store req_list into cache and later send data packet
        along the path in req_list
else
    unicast(RREP);
```

图2 AMDSR 算法

4 安全和性能分析

AMDSR 可以防范网络外未认证结点的入侵和内部结点的无合谋攻击。恶意结点的典型攻击行为有以下4种：

Ⅰ. *恶意结点修改或伪造假的路由控制分组 RREQ、RREP、ERROR* 对这3种分组的修改都可由逐跳认证或端-端完整性检查识别出来，AMDSR 确保只有源结点才可生成 RREQ，只有目的结点才可响应 RREP。虽然恶意结点可以伪造 ERROR，但具有不可抵赖性，而 Ariadne，Context 和 SRP 协议不具有这种特性。

Ⅱ. *恶意结点修改路由表* 在 RREQ 传送阶段，结点不仅认证其上游邻居结点广播的路由表而且监听其下游邻居结点广播的路由表。任何恶意修改路由表的行为都将被发现。在 RREP 传送阶段，修改行为由端-端完成性检查发现。AMDSR 协议克服了 ARAN、SADSR、Ariadne 协议中恶意结点向路由表中插入结点而加长路由的缺陷，并且结点仍处于正常接收模式而非过去协议中的混杂接收模式。

Ⅲ. *恶意结点丢弃 RREQ/RREP* 这将不会影响路由的建立，因为通过洪泛方式，经过其它结点的路由会建立，这将反而不利于恶意结点包含到路由中。

Ⅳ. *重放攻击* 即恶意结点向网络中传播以前传送过的路由控制分组，这类分组将作为滞后分组被其它结点丢弃。

本协议为 MANETs 路由协议扩展了安全功能，相应地也带来了一定的网络负载。签名、认证和端-端完整性检查增加了路由控制分组的延迟，但因控制分组的数量远少于数据分组的数量，所以其增加的延迟影响小，而且只有 *RREQ* 的传播需经逐跳认证，而 *RREP* 和 *ERROR* 的传播不需要逐跳认证，尽量减少了认证所带来的延迟。AMDSR 不能确保路径最短(跳步数最少)，但能保证提供最快速的路径，源结点总是优先选择早到达的 *RREP* 中所携带的路由表作为数据分组传递的路径。AMDSR 提高了 DSR 在存在入侵的网络环境中的路由发现能力，减少了恶意结点加入路由并丢弃分组的机会，因而必然会提高数据分组传递率。

结论和未来工作 本文分析了过去一些典型协议在安全性问题上的缺陷，提出了一个新的安全路由协议 AMDSR，它采用了工作于正常收听模式而非传统杂收模式的监听机制，确保了在源、目的结点间建立最快速的路径，并指出了文[11]中的相应错误结论。本文还分析了协议的安全特性和网络性能，未来我们将在网络仿真器 ns2[19] 上评价所提出的协议的性能，研究存在 DoS 攻击和合谋攻击的网络环境中的新的安全路由协议。

参 考 文 献

1 Perkins C E, Bhagwat P. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers. Computer Communications Review, Oct. 1994. 234～244

2 Perkins C E, Royer E. Ad-hoc on-demand distance vector routing. In: Proc. of Second IEEE Workshop on Mobile Computing Systems and Applications, 1999. 90～100

3 Johnson D B, Maltz D A. Dynamic source routing in adhoc wireless networks. In: T. Imielinski, H. Korth eds. Mobile Computing, Kluwer Academic Publishers, Dordrecht, 1996. 153～181

4 熊焰，苗付友，王行甫. SCR：一种 Mobile Ad Hoc 网络链路状态分组路由算法. 电子学报，2003，31(5)：645～648

5 姚尹雄，王豪行. AQF：一种新的移动 Ad Hoc 网络自适应 QoS 结构框架. 电子学报，2003，30(5)：727～730

6 张文柱，李建东，翁继伟，刘凯. 分布式无线网络中依据用户妥善安排的多址接入协议. 计算机学报，2003，26(5)：530～538

7 Zhou Bosheng, Wu Jieyi, Fei Xiang, Zhao Jian. Pcba: A priority-based competitive broadcasting algorithm in mobile ad hoc networks. J. Comput. Sci. &Technol., 2003, 18(9): 598～606

8 Tian Hui, Li Yingyang. AN MAC protocol suppority multiple traffic over mobile ad hoc networks. *Journal of Electronics*, 2003, 20(2): 116～120

9 Sun Xuebin, Zhong Zheng. Link perdurability based routing for mobile ad hoc networks. Journal of Electronics, 2003, 20(4): 299～304

10 Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks. In: Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. San Antonio, TX, 2002. 27～31

11 Sanzgir K, Dahill B. A secure routing protocol for ad hoc networks. In: Proc. of the 10th IEEE Intl. Conf. on Network Protocols, 2002. 1～10

12 Zapata M G. Securing ad hoc routing protocols. In: Proc. of ACM workshop on wireless Security, Atlanta, Sep. 2002. 1～9

13 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

14 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

15 Paul K, Westhoff D. Context aware detection of selfish nodes in DSR based ad hoc networks. In: Proc. of IEEE GLOBECOM02, 2002. 2424～2428

16 Marti S, Giuli T. Mitigating routing misbehavior in mobile ad hoc networks. In: Proc. of the 6th Annual ACM/IEEE Intl. Conf. on Mobile Computing and Networking, 2000. 255～265

17 Buchegger S, Boudec J Y L. Performance analysis of the CONFIDANT protocol. In: Proc. of the 3rd ACM Intl. Symposium on Mobile Ad Hoc Networking and Computing, 2002. 226～236

18 Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proc. of the Communication and Multimedia Security 2002 Conf. Sep. 2002. 186～192

19 http://www.isi.edu/nsam/ns