移动 Ad hoc 网络路由协议安全研究*)

易 平 蒋巍川 钟亦平 张世永
(复旦大学计算机与信息技术系 上海200433)

摘 要 移动 ad hoc 网络是一种完全由移动主机构成的网络,其主要特点为网络拓扑易变,带宽、能源有限。这些特点使得适应于固定网络的安全策略在移动 ad hoc 网络上不能很好地发挥作用,需要设计一些针对其特点的解决方案。该文介绍了针对移动 ad hoc 网络路由协议安全方面的最新研究进展,首先介绍了移动 ad hoc 网络的安全弱点和攻击类型,其后对一些典型方案进行了说明,分析了各种方案的优点和缺点,并进行了综合比较。文中分析了目前协议存在的一些问题并提出了相应的改进方法,最后指出了下一步研究方向。

关键词 网络安全,移动 ad hoc 网络,路由协议

A Survey of Secure Routing for Mobile Ad Hoc Networks

YI Ping JIANG Yi-Chuan ZHONG Yi-Ping ZHANG Shi-Yong
(Department of Computing and Information Technology Fudan University, Shanghai 200433)

Abstract A mobile ad hoc network is a collection of mobile nodes that are dynamically and arbitrarily. It has several salient characteristics: dynamic topologies, bandwidth-constrained, variably capacity links, energy-constrained operation, limited physical security. Due to these properties, mobile ad hoc networks present great challenges for research in security. The paper surveys the state of the art in secure routing protocol for mobile ad hoc networks. Firstly, we provide security threats applicable and attacks to mobile ad hoc networks. Secondly, we cover some representative solutions. We also provide a comparison and discussion of their respective merits and drawbacks, and propose some improvements for these drawbacks. Finally, we outline future research directions.

Keywords Network security, Mobile ad hoc networks, Routing protocol

1 引言

移动 ad hoc 网络作为一种新型的移动多跳无线网络,与传统的无线网络有很大不同,它不依赖于任何固定的基础设施和管理中心,而是通过传输范围有限的移动节点间的相互协作和自我组织来保持网络连接和实现数据的传递。移动 ad hoc 网络的独特的结构产生了一些突出的特点[1]:(1)动态的拓扑结构:节点可在网络中任意移动,随时加入和退出网络。(2)有限的资源:无线通信带宽有限,移动节点的能源也有限。(3)多跳的通信:无线节点发射功率有限,发送报文到接收区域外的节点时,需要其他节点来中转信息,因此任意一个节点既是主机又是路由器。(4)脆弱的网络安全:由网络的自组织性、节点的移动性和无线通信信道,使得 ad hoc 网络更容易遭受各种攻击,其安全问题更加严峻。

移动 ad hoc 网络最初用于军事领域,如战场上坦克之间和海面上舰艇之间的组网,但是由于其建网方式灵活,配置快捷方便,构造成本较低等优势,它逐渐运用于商业和民用环境之中,如会议数据交换、紧急援救、偏远地区等一些需要临时组网的应用中。

与固定有线网络相比,移动 ad hoc 网络面临更多的安全威胁,在固定网络中,敌方需搭接电缆才能偷听,需要寻找防火墙或网关的漏洞才能访问内部资源。但对于移动 ad hoc 网络,无线信道使得窃听随处可在,节点的移动性使得敌我双方无边界,防火墙无法应用。因此,移动 ad hoc 网络比固定网络更容易遭受各种安全的威胁,如窃听、伪造身份、重放、篡改报文和拒绝服务等等。

本文首先分析了移动 ad hoc 网络的安全弱点和路由攻击类型,然后综述了现行的各种解决方法,并指出了各种方案的优点和缺点。本文第2节介绍安全弱点和攻击类型,主要分析由移动 ad hoc 网络独特的结构所造成在安全方面的弱点及各种针对路由协议的攻击。第3节介绍几种典型的路由安全方案。第4节对论述的各种路由安全协议进行了综合比较,指出了存在问题及改进方法。最后对全文进行了总结,提出了下一步的研究方向。

2 移动 Ad hoc 网络的路由攻击类型

2.1 篡改

路由协议假定网络中节点都是相互合作的,转发报文的节点不会修改与其无关的路由信息,所以不检查路由信息的完整性。这使攻击者能够十分容易更改路由信息中任何字段,例如:AODV 路由中的序号和跳数,DSR 路由包中的路由节点序列等,从而产生错误的路由,如重定向、回路等,导致整个网络性能下降。攻击者能够篡改路由报文的根本原因在于节点无法对路由报文进行完整性检测。

2.2 冒充

因为路由协议并不认证报文的地址,所以攻击者可以声称为某个节点加入网络,甚至能够屏蔽某个合法节点,替它接收报文。其根本原因在于节点不能鉴别报文的来源。

*)国家863计划信息安全技术主题资助项目(2001AA142050);国家信息安全关防项目(2001-研3-011);上海市科学型中小企业技术创新资金(种子资金)资助项目(0151H1312)。易 平 博士生,主要研究领域为网络安全、移动计算。蒋巍川 博士生,主要研究领域为网络安全与人工智能。钟亦平 副教授,主要研究领域为系统结构、网络通信。张世永 教授,博士生导师,主要研究领域为计算机网络的应用和安全、数据通信。

2.3 伪造

攻击者可以伪造并广播假的路由信息。例如：广播某条存在的路由已中断，或编造一条并不存在的路由。它可造成回路、分割网络、孤立节点等。其原因在于无法验证报文的内容。

2.4 拓扑结构与通信量分析

在路由查询和发送报文中都包含有明确的路由信息，如DSR报文头部就含有从源节点到目的节点的路由。攻击者能够通过偷听这些报文分析出节点相邻情况、所处位置等拓扑信息，可进一步通过流量分析，得出节点在网络中的功能和角色。借助这些信息，攻击者可准确地进攻网络控制节点或军事网络中的指挥员。

2.5 资源消耗攻击

攻击者发送大量无用报文，如路由查询报文或数据报文，消耗网络和节点资源，如带宽、内存、CPU、电池等。

2.6 WORMHOLE 攻击[2]

两个串通的攻击者，采用专用通路直接相联，越过正常的拓扑结构，直接转发路由查询报文，造成错误的路由拓扑信息。图1为 WORMHOLE 攻击示意图，从 S 节点到 D 节点的正常路由应该为 $S-A-B-C-D$，但攻击者 $M1$ 和 $M2$ 通过 ABC 建立虚拟专用通道来转发路由查询报文，这样形成了 $S-M1M2-D$ 的路由。因为后者路由跳数少，源节点选择了 $S-M1M2-D$ 作为发送路由。

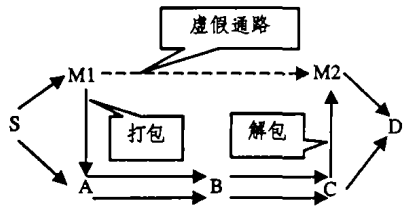

图1 WORMHOLE 攻击示意图

2.7 BLACKHOLE 攻击[3]

在路由查询中攻击者在没有至目标节点的路由情况下，抢先宣布有到目标节点的路由，使源节点建立通过该节点的路径，在随后的报文发送中，抛弃通过该节点的报文，形成抛弃报文的黑洞。

2.8 RUSHING 攻击[4]

在按需路由协议中，攻击者短时间内发送大量路由查询遍布整个网络，使得其它节点正常的路由查询无法提交处理而被抛弃。

3 路由安全

路由协议是移动 ad hoc 网络中的一个重要的部分，因为它直接决定了网络功能的实现和效率。由于移动 ad hoc 网络与固定网络具有不同的特点，如节点移动、多变拓扑，使得常规的路由协议不适用于移动 ad hoc 网络。近年来提出了许多适用于移动 ad hoc 网络的路由协议，如 DSR[5]、AODV[6]、DSDV[7]等，这些路由协议在设计时充分考虑了 ad hoc 的特点，却没有考虑到安全方面的因素。这使得上述路由协议在安全方面存在重大隐患。下面介绍几种典型的路由安全方案。

3.1 SRP[8]—Secure Routing Protocol

SRP 对现有的按需路由协议进行扩充，实现辨别和抛弃假的路由信息，从而防止攻击者对路由信息的篡改、重放和伪造，确保获取正确的拓扑信息。协议前提为源节点与目标节点存在共享密钥，以进行认证和通信。

SRP 在路由报文中扩充一个安全报头，其包含标识、序列号和报文鉴别码(MAC)。当源节点发起路由请求(RREQ)时，它将源地址、目的节点地址和报文标识通过共享密钥计算出报文鉴别码，并随报文一起发送。中间节点转发报文，同时记录节点的路由请求频率，它用频率的倒数作为处理的优先级，这样可防止攻击者发出大量无用的路由请求来阻塞网络，因为这些请求的优先级将迅速降低，以至于不再处理。中间节点一般不能回答路由请求，只有当中间节点与源节点有共享密钥并有至目标的路由时才能回答路由请求。当路由请求报文到达目标节点时，目标节点首先使用共享密钥计算报文鉴别码来检验报文的完整性。如果路由请求是合法的，它会像源节点一样发出一个带有报文鉴别码的路由回答(RREP)。如果校验未通过，路由请求报文就会被扔掉。当路由回答报文返回到源节点时，同样检验完整性，符合时接受其路由。路由出错(RRER)报文不需安全报头，由发现链路中断的节点直接发到源节点。

此方法的优势有三点，其一协议简单，无需修改原路由协议，只需进行扩充就可实现安全保障。其二，密钥管理简单，它只需收发两端拥有密钥进行校验，网络中的节点既不拥有密钥也不参与校验，这既简化了密钥管理又减轻了节点的运算量。其三，适用面广，采用端到端的鉴别，可适用于多种网络协议。它有两处不足，其一，路由协议为提高查找效率，中间节点能根据缓存来回答路由请求，此时因为没有与中间节点的共享密钥而无法认证。其二，无法认证路由维护信息，路由失败时，由中间节点产生的路由错误信息无法进行鉴别，因为源节点与路由中间节点没有共享密钥。

3.2 Ariadne[9]—A Secure On-Demand Routing Protocol for Ad Hoc Networks

Ariadne 是一种基于 DSR[5]、使用 TESLA[10]技术的安全路由协议。TESLA 是一种广播认证技术，它通过报文鉴别码(MAC)来实现对报文的认证，利用时钟同步和密钥延迟发布来防止伪造报文鉴别码。它的基本过程是发送方先发送报文和报文鉴别码，随后再发送用于验证报文鉴别码的密钥，接收方接收后先存储报文再接收密钥进行认证。为了保证先接收报文后接收密钥的顺序，要求收发双方时钟同步。Ariadne 的前提是收发双方建立共享密钥、网络中各节点拥有其它节点的 TESLA 认证初始值，各节点时钟要求基本同步。

S: $h_0 = MAC_{K_{SD}}(REQUEST,S,D,id,ti)$

S->*: $(REQUST,S,D,id,ti,h_0,0,0)$

A: $h_1 = H[A,h_0]$ $M_A = MAC_{K_{AD}}(REQUEST,S,D,id,ti,h_1,(A),0)$

A->*: $(REQUST,S,D,id,ti,\underline{h_1},(\underline{A}),(\underline{M_A}))$

B: $h_2 = H[B,h_1]$

$M_B = MAC_{K_{BD}}(REQUEST,S,D,id,ti,h_2,(A,B),(M_A))$

B->*: $(REQUST,S,D,id,ti,\underline{h_2},(A,\underline{B}),(M_A,\underline{M_B}))$

C: $h_3 = H[C,h_2]$

$M_C = MAC_{K_{CD}}(REQUEST,S,D,id,ti,h_3,(A,B,C),(M_A,M_B))$

C->*: $(REQUST,S,D,id,ti,\underline{h_3},(A,B,\underline{C}),(M_A,M_B,\underline{M_C}))$

D: $M_D = MAC_{K_{SD}}(REPLY,D,S,ti,(A,B,C),(M_A,M_B,M_C))$

D->C: $(REPLY,D,S,ti,(A,B,C),(M_A,M_B,M_C),\underline{M_D},0)$

C->B: $(REPLY,D,S,ti,(A,B,C),(M_A,M_B,M_C),M_D,(\underline{K_{C_1}}))$

B->A: $(REPLY,D,S,ti,(A,B,C),(M_A,M_B,M_C),M_D,(K_{C_1},\underline{K_{B_1}}))$

A->S: $(REPLY,D,S,ti,(A,B,C),(M_A,M_B,M_C),M_D,(K_{C_1},K_{B_1},\underline{K_{A_1}}))$

图2 Ariadne 协议的路由查询过程

路由查询中实现了收方能够认证发方身份，发方能够认证路由回答报文中的每个节点，路由序列不能被篡改。收发双方通过共享密钥来实现相互认证。发方使用与收发共享密钥计算出路由查询报文的报文鉴别码，随报文一起发送。中间节

点收到路由查询报文时，将本节点的标识加入到节点序列中，并重新计算节点序列的 HASH 值，然后用本节点的 TESLA 密钥计算整个报文的报文鉴别码，附在报文中转发给邻居节点。目标节点收到路由查询报文时，首先使用共享密钥认证发方身份，然后使用节点列表重新计算节点序列的 HASH 值，校验节点序列的完整性。校验通过后，目标节点形成报文路由回答沿原路返回到源节点。路由回答报文返回过程中，各节点将自己的 TESLA 认证密钥附上。返回到源节点后，源节点通过这些密钥来校验报文的完整性。如果校验通过，则接受报文。图2显示一次路由查询的过程，S 为源节点，D 为目标节点，A、B、C 为中间节点，id 为报文标识，ti 为时间，H 代表 HASH 运算，K_A 代表节点 A 的 TESLA 认证密钥，MAC_K 代表使用密钥 K 计算报文鉴别码。底划线的部分表示与前次报文不同的部分。

路由维护时，中间节点发出路由出错(RRER)报文，并附加上本节点的 TESLA 认证信息，所有 RRER 途经节点存储该报文，等待密钥公布并认证，如果通过认证则修改路由表，否则抛弃该报文。

本方法的优势在于使用对称加密技术和广播认证技术，与非对称加密技术相比，它大大降低了节点的运算量，节省了节点资源。缺点有三点，其一，要求各节点进行时钟同步，这种要求对于移动 ad hoc 网络是不现实的。其二，网络中的各节点都要发送自己的 TESLA 密钥以供其它节点认证，这需要占用不少带宽。其三，节点收到报文不能立刻认证，需要等待 TESLA 密钥的公布，这造成了一定时间的延迟。

3.3 ARAN[11] — Authenticated Routing for Ad Hoc Networks

ARAN 适用于按需路由协议，利用公钥证书和公认的 CA 来实现认证的路由。ARAN 前提条件要求有信任的证书服务器来发放和管理证书，每个节点加入网络前必须从证书服务器获取一个公开密钥的证书。

路由查询时，源节点发出一个经过签名的路由查询报文。第一跳节点校验源节点签名后，签名并附上自己的证书。随后每个转发节点都先校验前一个节点的签名，然后用自己的签名和证书替代上个节点的签名和证书。路由查询报文到达目标后，目标节点校验签名，然后产生路由应答，沿来路返回，途径的每个节点与来时一样进行校验和签名。源节点收到路由应答，校验目的节点的签名正确后接受其路由。路由中断时，路由维护报文由发送节点签名后直接转发至源节点，中间节点不再进行修改。图3显示 ARAN 路由查询中如何进行签名和证书的更替，S 为源节点，D 为目标节点，A、B 为中间节点，$CERT_S$ 为源节点的证书，N 为一个随机整数，t 为发送时间，N、t 用于防止重放攻击。

S->*: [REQUEST, D, $CERT_S$, N, t] K_S-
A->*: [[REQUEST, D, $CERT_S$, N, t] K_S-] K_A-, $CERT_A$
B->*: [[REQUEST, D, $CERT_S$, N, t] K_S-] K_B-, $CERT_B$

图3 ARAN 路由查询

本协议的优点为两点：其一，ARAN 使用公开密钥算法实现了报文鉴别、完整性和不可抵赖性。在路由查找和路由应答中使用端到端和单跳的认证来阻止伪造，使用数字签名来阻止报文篡改。从安全的角度来看，它提供了较完善的安全功能。其二，路由报文经过的每一个节点都相互签名认证，所以攻击者没有机会加入网络进行攻击。缺点为：其一为中间节点不能回答路由请求，必须由目的节点来回答，降低了路由协议的效率。其二为使用公开密钥算法来进行认证，会导致节点计算负载过重，如果攻击者发出大量路由请求，会导致节点来不及进行认证而无法处理正常的路由信息。其三，如果被攻破的节点从内部发动攻击，该算法不能抵抗，因为攻击者拥有合法的证书。其四，要求有一个公共的 CA 来维护每一个节点的证书，该 CA 失败将导致整个网络的安全失效。

3.4 SEAD[12]-Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks

SEAD 是基于距离向量 DSDV[7]的安全路由协议，基本思想是利用 HASH 链中的元素来认证路由更新报文中的序列号和跳数。所谓单向 HASH 链，即先选择一种 HASH 函数，如 $MD5$[13]，再选择一个0－1之间的随机数 X，令 $H_0=X$，$H_1=MD5(H_0)$，$H_2=MD5(H_1)$，依此计算出一系列数 H_0，H_1，H_2，$\cdots H_n$，这一系列数就叫单向 HASH 链。利用这一系列数可实现认证，如已知 H_8 要鉴别 H_5 是否合法，只要计算出 $MD_5(MD_5(MD_5(H_5)))$ 与 H_8 相对照即可。因此，只要拥有认证元素 H_n，所有 HASH 链中的元素均可鉴别。

SEAD 的前提是有信任的实体来分配和维护各节点的认证元素。每一个节点在路由更新中从自己的 HASH 链中选出一个元素用于认证。节点选择 HASH 值的算法为，假定网络最大跳数为 m，HASH 链为 H_0，H_1，H_2，$\cdots H_n$，将 HASH 链分为 n/m 组，每一组用于认证一个序列号，组内的 HASH 值用于认证跳数。例如：序列号 i，令 $k=n/m-i$，其组内元素为 H_{km}，H_{km+1}，$\cdots$，H_{km+m-1}，如果跳数为 j，则 HASH 值 H_{km+j} 即可用于认证序列号为 i 跳数为 j 的路由更新。由于单向 HASH 链的特性，能够防止攻击者伪造一个比真实序列号大的报文，或比真实跳数小的报文。当节点收到路由更新报文时，它首先利用 HASH 值进行认证，如果认证通过则修改路由表，否则抛弃该报文。此方法的优点为采用单向 HASH 链算法进行认证，大大降低了节点的运算复杂度。缺点为在网络运行整个过程都需要有信任的实体来分配和维护每个节点的认证元素。因为 HASH 链中的元素会被用完，用完后节点要重新计算一条 HASH 链，其认证元素 H_n 要由信任实体重新分配给所有节点。该信任实体容易引起单点失败，它若被攻击者攻破了，则整个网络路由协议无法认证了。

3.5 SAODV[14,15] — Secure Ad Hoc On-Demand Distance Vector

SAODV 是基于 AODV[6]的路由安全协议，它的前提条件是要将网络中所有节点的公钥分发到各节点，以便用于签名认证，它使用两种机制来保证 AODV 的协议安全。一种是数字签名，用来保证报文中不需变化部分的完整性，提供端到端的鉴别。另一种是单向 HASH 链，用来保证路由报文中可变的部分如跳数的认证。

源节点路由查找时，发出带有数字签名和 HASH 值的路由查询报文，中间节点收到路由查询报文时，首先校验数字签名和 HASH 值，能通过时处理该报文，否则抛弃该报文。路由查询报文到达目的节点时，节点形成路由回答报文，同样进行数字签名和计算 HASH 值后沿来路返回。与 ARAN 不同的是中间节点并不需要相互签名认证，只有源目的节点对路由报文进行数字签名，中间节点只需验证数字签名，而不需形成数字签名，计算量比 ARAN 少了一半。

对于 AODV 路由查找中，中间节点如何回答路由查询的问题，采用双签名方法来解决，即源节点在发出路由查询报文中设立一个标志位并带上一个返回路由回答报文的签名，这样，中间节点可根据附带的签名生成报文返回源节点。对于路由出错报文的处理方法为对产生该报文的节点进行数字签名，这样就可防止攻击者编造报文。

该协议的优点在于采用双签名机制解决了中间节点回答路由请求的问题。缺点是采用公开密钥算法，中间转发节点需要检验数字签名，计算负载比较大。

3.6 SLSP[16] — Secure Link State Routing for Mobile Ad hoc Networks

SLSP 是基于链路状态的路由安全协议。它保护使用链路状态算法的路由协议，例如：ZRP[17]。算法前提为每个节点持有公钥和私钥，并将公钥发送给所有节点。SLSP 对链路状态更新报文扩充一个安全报头，通过数字签名来提供认证和完整性，报文序列号来防止重放攻击，单向 HASH 链来限制转发次数。各节点周期性地向网络节点广播经过签名的链路状态更新报文。网络中节点收到链路状态更新报文后，首先检查签名和报文完整性，如果检查通过则接受该报文，若没达到最大转发次数则转发该报文，如果检查没通过则抛弃该报文。SLSP 还包括邻居监视机制，每个节点将其 MAC 地址和 IP 地址经过签名后发给邻居节点，邻居节点记录相应地址。它有两个用途，其一，它可防止伪造 IP 地址。其二，用来记录邻居发送报文的频率，如果发送报文的频率过高，超过一定限额，就可以认定为攻击者，对其发出的报文不再处理而直接抛弃，这样就可将攻击者滥发的报文限制在单跳邻居范围之内，有效地防止了拒绝服务攻击。该协议的优点在于采用邻居监视机制来防止拒绝服务攻击。缺点是采用公开密钥算法，各节点既要生成本节点报文的数字签名又要检验其它节点报文的数字签名，计算负载比较大。

4 路由安全协议的比较与分析

表1对本文介绍的五种比较典型的路由安全协议进行了分析和比较。它们有一些共同的特点，需要事先通过信任的实体或证书服务器将密钥、证书或认证元素发布到各节点，协议都能够抗击前述的各种网络进攻，如冒充、伪造等，但都只局限于攻击者的单个进攻，针对联合进攻，如 wormhole[2]攻击，各个协议都无法对付，文[18]专门提出一种方法 Packet leashes 抵抗 wormhole 攻击，它基于精确的时间或位置信息来发现并阻止它的攻击。

表1 路由安全协议的比较

协议名称	适用的路由协议	协议前提	主要的安全技术	认证部分	优势	缺点
SRP	DSR	源节点与目标节点建立共享密钥	报文鉴别码	源地址、目的地址、报文标识	算法简单、适用面广	缺乏对路由维护信息的保护、中间节点不能回答路由请求
ARIADNE	DSR	发布 TESLA 认证密钥、源目标节点建立共享密钥、各节点时钟同步	单向 HASH 链、报文鉴别码	整个报文、路由序列	采用对称密钥和 TESLA 技术，计算量小、管理简单	要求节点时钟同步、发送认证密钥占用带宽、认证有延迟
ARAN	AODV DSR	建立证书服务器，发布和维护每个节点的公钥证书	数字签名	整个报文	实现了鉴别、完整性和不可否认性	计算量大、需要信任的 CA、中间节点不能回答路由请求
SEAD	DSDV	发布认证初始值	单向 HASH 链	序列号、跳数	计算负载小	需要信任的实体来分配和维护各节点的认证元素
SAODV	AODV	分发节点公钥	数字签名、单向 HASH 链	整个报文	中间节点可以回答路由请求	采用公开密钥算法计算量大
SLSP	ZRP	分发节点公钥	数字签名、单向 HASH 链	整个报文	采用邻居监视机制来防止拒绝服务攻击	采用公开密钥算法计算量大

以上的路由安全协议存在的问题及改进方法：

(1)有些协议在设计上强调了安全性，而忽视了可用性。没有充分考虑到移动 ad hoc 网络节点计算能力弱、电池和通信带宽有限的特点，如 ARAN、SAODV、SLSP 协议，采用公开密钥证书加数字签名的安全机制，在安全方面是完善的，但由于数字签名的生成和检验都是计算量非常大的、非常耗时的，这对于本身计算能力弱，同时还要承担转发报文和运行应用程序的移动节点来说，是一项沉重的负担，如果大量报文同时到来，节点就会因为检验数字签名过慢而来不及处理报文，导致拒绝服务。安全协议的设计上要充分考虑到移动 ad hoc 网络资源有限的特点，尽量采用报文鉴别码和单向 HASH 链等运算量小的安全技术，以减少节点的运算时间和能量消耗。不宜采用数字签名等计算量大的算法。

(2)设计上为了保证安全性，屏蔽了路由协议的某些功能，降低了路由协议的有效性。例如 SRP、ARAN 协议为保证安全、降低算法的复杂性都取消了中间节点回答路由请求的功能，必须由目标节点产生路由回答，降低了路由查询的效率。为了解决该问题，可采用 TESLA 认证或共享密钥来实现对中间节点路由回答认证。

(3)有些协议的前提条件要求在网络运行过程中需要集中的服务器支持。如 ARAN 要求有证书服务器管理各节点公钥证书，SEAD 要求信任的实体来分配认证元素。集中的服务器虽然保证了协议的安全，但却带来了单点失败的威胁，如果该服务器被攻破，则整个网络安全就失效了。因此，在设计上应尽量不用集中的服务器，如果要用也只能在初始阶段，网络运行时或者不用或者用分布式的 CA 来实现。

(4)有些协议提出的要求是网络难以提供的。如 Aridne 协议要求网络所有节点时钟同步，这对于大型网络是难以实现的。

总结与展望 由于移动 ad hoc 网络的独特结构，使得常规的安全方案无法应用，必须针对其特点设计专门的安全解决方案。本文首先介绍了移动 ad hoc 网络的安全弱点和攻击类型，其后分析了六种典型的路由安全协议，对它们进行了综合比较并指出其存在问题及改进方法。

移动 ad hoc 网络路由安全的研究是一个年轻而又迅速发展的领域，总体来说，下一步发展应包括以下几个方面：

(1)进一步提高性能，降低算法对资源的要求。移动 ad hoc 网络中节点本身的计算能力和电池能量都十分有限，还要参与网络交换。网络安全作为网络正常运行的一种保障，不应该也不允许占用节点大量的资源，不能因为增加了安全措施而降低了网络性能，影响了网络的正常运行。应该设计和采用一些对资源要求少的算法，如：使用对称密钥算法取代公开密钥算法等。

(下转第64页)

开发的新业务快速部署在网络中，而在传统的电信网络，业务是通过事先在中间节点进行业务配置来实现的，即静态的业务配置机制。在 TBMBA 中运营商能以较低的成本实现丰富业务种类、保持业务增长目标。因此与传统的网络模式相比，客户和运营商都获得了满意的结果。

结束语 本文介绍了主动网络的体系结构和电信网络的现状，并遵照主动网络的原则和电信行业发展的趋势，提出了基于主动网络的电信业务模型。利用 TBMBA 运营商能有效地完善运营价值链，进行创新业务的开发，保持业务增长。

AN 提出了一种全新的体系结构，但是 *AN* 离实际应用还有距离，必须解决效率、安全等问题，才能真正推广。因此，面对主动网络提出的挑战，我们还必须作出不断的努力。

参 考 文 献

1 Smith J M, et al. Activating Networks: a progress report. Computer, 1999(324)

2 Merugu S, Bhattacharjee S, Zegura E, Calvert K. Bowman: A Node Os for Active Network . Infocom, 2000

3 Tennenhouse D L, Wetherall D. Towards an Active Network Architecture. In Multimedia Computing and Networking 96, 1996

4 CRA. Research Challenge for the Next Generation Internet. http://www. whitehouse. gov/WH/EOP/OSTP/NSTC/html/97ann-rpt. html.

5 Active storage network. http://www. ece. cmu. edu/~asn/research. html

6 任丰源，任勇，山秀明. 主动网络的研究和发展[J]. 软件学报，2001, 12(11): 1614～1622

(上接第40页)

(2)提供对组播的安全保护。组播的应用能够有效地减少网络流量，特别适用于军事指挥网络。现行大多数的安全方案只停留在如何保护路由信息的完整性，如何实现对单个节点的认证，没有考虑如何实现对组播的安全支持。只有少数如文[19,20]论述了安全的组播，对移动 ad hoc 网络环境下的安全组播的研究还很不完善，需要进一步发展。

(3)如何保护节点通信量和位置的信息。通过通信量的分析能够确定网络中节点的角色，再确定节点的位置，就可将攻击指向网络的要害，如：网控中心、集中的 CA 或军事指挥网中指挥员等。

各种针对中路由协议的攻击及对策。如：wormhole、rushing 攻击等，因为移动 ad hoc 网络的复杂性，也许还存在许多新类型的攻击尚未发现。

(4)路由安全算法研究主要集中在 DSR、AODV、DSDV 路由协议上，还应拓展其范围，设计一些其他路由安全算法，如基于位置的路由安全协议、基于能量的路由安全协议、层次路由安全协议等。

(5)链路层和高层的安全协议的研究。

参 考 文 献

1 Corson S, Macker J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, Jan. 1999

2 Hu Y-C, Perrig A, Johnso D B. Wormhole Detection in Wireless Ad Hoc Networks: [Technical Report TR01-384]. Department of Computer Science, Rice University, Dec. 2001

3 Deng Hongmei, Li Wei, Agrawal D P. Routing Security in wireless Ad hoc Networks. IEEE Communications Magazine, Oct. 2002. 70～75

4 Hu Y-C, Perrig A, Johnson D. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In: Proc. of the ACM Workshop on Wireless Security (WiSe 2003), Westin Horton Plaza Hotel, San Diego, California, U S A, 2003

5 Johnson D B, Maltz D A, Hu Y-H. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09. txt, 15 April 2003. http://www. ietf. org/internet-drafts/draft-ietf-manet-dsr-09. txt

6 Perkins C E, Belding-Royer E M, Das S R. Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July 2003. http://www. ietf. org/rfc/rfc3561. txt

7 Perkins C, Nhagwat P. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In: Proc. of the ACM SIGCOMM Conf. on Communication Architectures, Protocols, and Applications, Aug. 1994. 234～244

8 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, Jan. 2002

9 Hu Y C, Perrig A, Johnson D B. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks. In: Proc. of the MobiCom 2002, Sep. Atlanta, Georgia, USA, 2002

10 Perrig A, Canetti R, Song D, Tygar J D. Efficient and secure source authentication for multicast. In: Proc. of Network and Distributed System Security symposium, Feb. 2001. 35～46

11 Sanzgiri K, et al. A Secure Routing Protocol for Ad Hoc Networks. In: Proc. of 2002 IEEE Intl. Conf. on Network Protocols (ICNP), Nov. 2002

12 Hu Y-C, Johnson D B, Perrig A. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: Proc. of the 4th IEEE Workshop on Mobile Computing Systems & Applications, WMCSA, IEEE, Calicoon, NY, June 2002 . 3～13

13 Rivest R L. The MD5 Message-Digest Algorithm, RFC1321, April 1992

14 Zapata M G. Secure Ad hoc On-Demand Distance Vector Routing. ACM Mobile Computing and Communications Review (MC2R), 2002, 6(3): 106～107

15 Zapata M Z, Asokan N. Securing Ad-Hoc Routing Protocols. In: Proc. of the 2002 ACM Workshop on Wireless Security (WiSe 2002), Sep. 2002. 1～10

16 Papadimitratos P, Haas Z J. Secure Link State Routing for Mobile Ad Hoc Networks. In: IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 Intl. Symposium on Applications and the Internet, Orlando, FL, Jan. 2003

17 Haas Z J, Pearlman M R. The Performance of query control schemes for the Zone Rounting Protocol, ACM/IEEE Trans. net, 2001, 9(4): 407～438

18 Hu Y-C, Perrig A, Johnso D B. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In: Proc. of the Twenty-second Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2003), IEEE, San Francisco, CA, April, 2003

19 Kaya T, Lin G, Noubir G, Yilmaz A. Secure Multicast Groups on Ad Hoc Networks. In: Proc. of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), George W. Johnson Center at George Mason University, Fairfax, VA, USA, 2003

20 Lazos L, Poovendran R. Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information. In: IEEE Intl. Conf. on Acoustics Speech and Signal Processing, Hong Kong, China 2003