一种实用的 Ad hoc 网络鉴别路由协议 AARP*)

铁满霞[1,2] 李建东[1,2] 王育民[1]
(西安电子科技大学 ISN 国家重点实验室 西安 710071)[1]
(西安电子科技大学信息科学研究所 西安 710071)[2]

摘 要 针对 Ad hoc 网络的鉴别路由协议 ARAN 存在路由查找过程复杂、计算复杂度高、缺乏会话密钥协商等缺点,本文提出了一种简单实用的鉴别路由协议 AARP。该协议避免采用公钥加密算法,简化了路由查找过程,降低了计算复杂度,利用节点对路由消息的签名,有效抵制了各种恶意攻击,同时利用 DH 交换,完成会话密钥协商。本文还通过 CK 模型分析了 AARP 协议的安全性,结果表明:若 DDH 假设成立、数字签名算法可抵抗选择消息攻击,则 AARP 协议在 UM 下是 SK-secure 的,且具有完善的前向保密性 PFS、已知密钥安全 KKS 等属性。相比 ARAN 协议,AARP 对于通常节点资源受限的 Ad hoc 网络而言,更为实用。

关键词 Ad hoc,路由安全,公钥体制,ARAN,AARP

AARP: An Applicable Authenticated Routing Protocol

TIE Man-xia[1,2] LI Jian-dong[1,2] WANG Yu-min[1]
(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)[1]
(Information Science Institute, Xidian University, Xi'an 710071, China)[2]

Abstract ARAN has some disadvantages of poor routing performance and high computing complexity, and also lacks session key negotiation. To resolve these problems, this paper presents an Applicable Authenticated Routing Protocol, abbreviated as AARP. Avoiding public key encryption, AARP simplifies the procedure of routing searching and reduces the computing complexity. Exploiting signature scheme, AARP successfully defeats many different types of identified attacks. Adopting Diffie-Hellman algorithm, it implements the session key negotiation. Then, with Canetti-Krawczyk model, this paper analyzes its security at detail. The results show that AARP is SK-secure in UM if DDH hypothesis is made and signature algorithm is secure against chosen message attack. The AARP protocol also possesses the security attributes of PFS and KKS etc. Compared to ARAN, AARP is simpler and more applicable, especially suitable for Ad hoc networks with nodes of limited CPU processing capability.

Keywords Ad hoc, Route security, Public key infrastructure, Authenticated routing for Ad-Hoc networks (ARAN), Applicable authenticated routing protocol (AARP)

1 引言

无线媒体的开放性、分布式对等等因素使得多径传播的多跳 Ad hoc 的路由安全比传统网络的路由安全更具挑战性。Ad hoc 网络路由协议通常面临以下几种攻击[1]:

(1)利用更改进行攻击。恶意节点通过改变控制消息字段或者利用虚假信息转发路由消息,引起网络业务重定向和拒绝服务攻击(Denial-of-Service, DoS),如更改路由序号的重定向,更改跳数的重定向,更改源路由的拒绝服务攻击及建立隧道等攻击方法。

(2)利用模拟进行攻击。当节点误描述它的网络身份,譬如改变发出分组的 MAC 或 IP 地址,此时就会产生欺骗,这种攻击很容易与更改攻击联合使用。

(3)利用伪造进行攻击。虚假路由消息的产生可归为伪造攻击类型,此类攻击很难辨识是否为无效的构造,如虚假路由错误和污染路由缓存等。

因此一种良好、健壮的安全路由算法不仅要能防止上述攻击,而且要确保每个节点均能成功进行路由查找和路由维护。目前主要有两种类型的安全路由协议:一种是在现有基本路由协议的基础上添加一些措施,以提供安全性,如 Seung Yi 等提出的安全 Ad hoc 路由(Secure Aware ad hoc Routing, SAR),Papadimitratos 等提出的移动 Ad hoc 网络的安全路由协议(Secure Routing Protocol for mobile ad hoc networks, SRP);另一种则为考虑安全因素新设计的路由协议,如 Kimaya Sanzgiri 等提出的 Ad hoc 网络的鉴别路由(Authenticated Routing for Ad-Hoc Networks, ARAN)[2];Stephen Carter 等提出的安全状态辅助的 Ad hoc 路由(Secure Position Aided Ad hoc Routing, SPAAR)。后一类协议相比前一类通常提供的安全性要高,但这些协议设计均不够完美,有的过于复杂,有的则难以实现。其中 ARAN 不像某些协议,如 SPAAR 还需要添加全球定位系统(Global Positioning System, GPS)硬件设备,它只需一些额外的存储与处理开销,就可以抵抗大部分的攻击。因此 ARAN 在诸协议中表现突出,引起人们的关注。

ARAN 协议相比无安全的基本路由协议而言,具有了安全性,但却存在如下缺点[3]:

*)基金项目:国家杰出青年科学基金(60725105);国家自然科学基金重大项目(60496316);863 计划课题(2007AA01Z217);国家自然科学基金项目(60572146)。**铁满霞** 副教授,博士研究生,主要研究方向为宽带无线 IP 技术、移动通信、信息安全等;**李建东** 教授,博士生导师,博士,主要研究方向为宽带无线 IP 技术、移动通信、软件无线电、ad hoc 自组织网络等;**王育民** 教授,博士生导师,研究方向为信息论、编码、密码等。

(1)路由查找过程复杂。ARAN 路由协议包含路由查找和路由维护两部分,其中路由查找由端到端的鉴别和最短路径证实两个阶段完成,相比无安全的基本路由协议而言,增加了协议的复杂性,影响效率。

(2)计算复杂度高。ARAN 协议中每个节点不仅签名,而且还要做公钥加密计算,资源受限的节点将不堪重负。

(3)节点存储量大。由于路由查找消息中不包含源路由,则每个节点在路由查找过程中必须存储前趋节点的地址,当网络规模较大时,节点存储问题不容忽视。

上述缺陷使得 ARAN 不仅在通常节点资源受限的 Ad hoc 网络中难以得到应用,而且由于缺乏路由建立过程中同步完成会话密钥的管理与分发功能,使得路由建立后会话数据的交互还需依赖其他协议进行密钥分发。

笔者在尽可能降低计算、路由查找及存储等复杂度前提下,设计一种简单实用的鉴别路由协议(an Applicable Authenticated Routing Protocol, AARP),并利用 DH(Diffie-Hellman)交换完成会话密钥的协商,为通信节点提供密钥分发服务。最后,在 Canetti-Krawczyk 模型下给出该 AARP 协议的安全性证明,并比较 AARP 与 ARAN 的算法性能。

2 AARP 路由协议

AARP 采用公钥密码技术为路由协议提供安全保障与会话密钥的协商,它包括证书申请、路由查找、路由维护及证书吊销等过程。

2.1 公钥证书

AARP 需要一个可信任的证书服务器 T,其公钥被所有合法节点知晓。在进入 Ad hoc 网络前每个节点必须向 T 申请一个证书。节点 A 从 T 申请到的证书定义如下[4]:

$$Cert_A=[IP_A, K_{AP}, notBefore, notAfter]K_{TS} \quad (1)$$

节点 A 的证书 $Cert_A$ 包含节点 A 的 IP 地址 IP_A、节点 A 的公钥 K_{AP}、证书起始时间 $notBefore$、证书截止时间 $notAfter$ 以及利用证书服务器 T 的私钥 K_{TS} 进行的签名。网络中所有节点必须具有 T 颁发的有效证书,以便在交换路由消息时向其它节点证实自己的身份。

2.2 路由查找

2.2.1 路由请求

当源节点 A 需要一条至目的节点 X 的路由时,发起路由查找广播,即路由请求分组,定义如下:

$$A\rightarrow broadcast:[REQ, IP_X, ID_A, a.G, Cert_A]K_{AS} \quad (2)$$

路由请求包括分组类型标识 REQ、目的节点 X 的 IP 地址、路由查找标识 ID_A、源节点 A 的临时公钥 $a.G$ 与证书 $Cert_A$ 以及利用源节点 A 的私钥 K_{AS} 进行的签名。

假设系统采用的公钥算法为椭圆曲线 ECC 算法,G 为椭圆曲线的基点,则 a 为源节点 A 的临时私钥,$a.G$ 为源节点 A 对应的临时公钥。

路由查找标识 ID_A 表示路由查找的新鲜性,每次源节点 A 执行路由查找时,均单调增加该值,而其它节点需为 A 节点存储最新的路由查找标识。路由查找标识编码空间应足够大,以保证在一定时间内不会发生溢出现象。

当其邻接节点收到路由请求分组后,判断路由查找标识 ID_A 是否新鲜,验证源节点 A 的证书 $Cert_A$ 是否有效及签名是否正确。若验证分组无效,则直接丢弃;否则,在路由分组请求分组后添加自己的证书与签名广播转发给其每个近邻。

假设 B 为收到 A 的路由请求广播的近邻节点,则 B 转发的广播如下:

$$B\rightarrow broadcast:[[[REQ, IP_X, ID_A, a.G, Cert_A]K_{AS}], Cert_B]K_{BS} \quad (3)$$

B 的近邻 C 收到路由请求广播后,判断路由查找标识 ID_A 的新鲜性,验证证书 $Cert_A$ 和 $Cert_B$ 的有效性及节点 A 和 B 签名的正确性。若验证分组未通过,则丢弃;否则在消息后附加自己的证书与签名再广播转发。C 重广播的路由请求如下:

$$C\rightarrow broadcast:[[[[[REQ, IP_X, ID_A, a.G, Cert_A]K_{AS}], Cert_B]K_{BS}], Cert_C]K_{CS} \quad (4)$$

路径上的每个节点重复此步骤,直至到达目的节点 X。

2.2.2 路由应答

目的 X 收到路由请求后,验证路由查找标识 ID_A 的新鲜性,验证所有证书与签名是否正确。若验证未通过,则直接丢弃;否则更新本地存储的节点 A 的相关信息,做出应答。假设反向路由的第一个节点为 D,则目的节点 X 发出的路由应答如下:

$$X\rightarrow D:[REP, ID_A, IP_A, IP_B, IP_C, IP_D, Cert_X, x.G]K_{XS} \quad (5)$$

路由应答包括分组类型标识 REP、源节点 A 发出的路由查找标识 ID_A、源路由、目的节点 X 的临时公钥 $x.G$ 与证书 $Cert_X$ 以及利用目的节点 X 的私钥 K_{XS} 进行的签名。

节点 D 验证目的节点 X 的签名与路由查找标识,若不正确,则直接丢弃;否则存储该路由信息并转发至前趋节点 C。每个前趋节点对路由应答进行同样处理,最后源节点 A 收到此路由应答分组后,验证签名与路由查找标识正确后,便得到一条新路由。

源节点 A 和目的节点 X 分别在本地进行 DH 计算,便得到会话密钥 $a.x.G=x.a.G$,用于保护通信数据的安全。

2.2.3 中间节点直接返回路由应答

特别定义的是,在 AARP 的路由查找中,若某个中间节点假设为节点 I 已知至目的节点 X 的路由,且该节点位于节点 C 和 D 之间,则中间节点 I 可直接返回路由应答,定义如下:

$$I\rightarrow C:[MREP, ID_A, Cert_I, IP_A, IP_B, IP_C, IP_I, IP_D]K_{IS} \quad (6)$$

该分组包含中间节点的路由应答标识 $MREP$、源节点 A 发出的路由查找标识 ID_A、中间节点 I 的证书 $Cert_I$、源至目的节点的路由及利用中间节点 I 的私钥 K_{IS} 进行的签名。

允许中间节点直接返回路由应答,节省了路由查找时间,提高了网络效率。

2.3 路由维护

AARP 为一种按需协议,用于验证节点跟踪路由是否有效。当一条路由在其生命期内没有出现业务,则该路由在路由表中被标为无效。无效路由上的某个节点收到数据,将引起该节点产生错误消息,沿着反向路径发往源节点,还利用错误消息报告有效路由上的链路。由于节点移动而损坏,所有的错误消息被签名。对于源 A 和目的 X 之间的一条路由,节点 B 产生其近邻节点 C 的路由错误消息如下:

$$[ERR, IP_A, IP_X, Cert_B, ID_B]K_{BS} \quad (7)$$

该消息沿着至源的路径无修改转发,该分组包括节点 B 的路由消息标识 ID_B(可与节点 B 的路由查找标识为同一值)确保错误消息的新鲜性。由于消息带签名,恶意节点不能产生其它节点的错误报告消息,同时签名也使错误报告消息的发送者不可抵赖。

异常行为通常来自恶意节点,但有时也会来自出了故障的正常节点,AARP 对此不加区分,均做出相同响应。异常行为包括无效证书的使用、不正确的签名消息以及路由错误消

息的滥用。

2.4 证书吊销

在某些对安全要求苛刻的环境中，所需的证书吊销机制必须非常可靠，因而花费也就相应比较昂贵。但由于无线网络的低投入和开放式管理环境的低安全标准，二者权衡可采用有时限的证书来提供最佳的吊销服务。

当需要吊销一个证书时，受信证书服务器 T 向 Ad hoc 网络发送广播消息通知此吊销信息。假设被吊销的证书为 $Cert_r$，则吊销广播消息为

$$T \rightarrow broadcast:[REVOKE, Cert_r]K_{TS} \quad (8)$$

收到此消息的任何节点向它的近邻广播此消息，并将此吊销通知存储下来直到被吊销的证书正常过期为止。

3 AARP 协议的 CK 模型分析

Canetti 和 Krawczyk 提出了一种模块化分析密钥交换 KE(Key Exchange)协议的思想，称之为 Canetti-Krawczyk 模型[5-7]，简称 CK 模型。它不仅提供一种简单有效的方法分析 KE 协议，而且利用该模型还可进行安全 KE 协议的设计。

3.1 CK 模型简介

CK 模型主要包含认证链路模型(Authenticated-links Model，AM)、非认证链路模型 (Unauthenticated-links adversarial Model，UM)以及认证器(Authenticator)三个重要的组成部分。

(1)AM 模型

AM 模型可被视为理想环境。在 AM 环境下，攻击者只能通过传递由参与者产生的真实消息激活主体。攻击者可以选择不传递消息，但一旦传递，就只能传送一次，并且忠实地传送到消息的预定目的地，且不能篡改消息。

(2)UM 模型

UM 模型可被视为真实环境。UM 下的攻击者除了具备 AM 模型中的能力外，还可主动激活主体与另外一个主体的会话，并可任意篡改和重放消息。

为了区分各种攻击和确保信息在被暴露的情况下尽可能地安全，CK 模型将攻击分为三类，即攻陷参与者(Party Corruption)、会话密钥查询(Session Key Query)以及会话状态暴露(Session State Reveal)。

(3)认证器

定义 1[5] 令 π 和 π' 为两个消息驱动的 n 方协议，称 π' 在 UM 下仿真 π，仅当对任意 UM 下的攻击者 U，必然存在 AM 下的攻击者 A，使得协议输出 $UAUTH_{\pi',U}$ 和 $AUTH_{\pi,A}$ 计算上是不可区分的。

定义 2[5] 编译器 C(Compiler)是一种算法，其输入一个协议，输出另一个协议。对任意 AM 下的协议 π，如果协议 $C(\pi)$ 在 UM 下具有和协议 π 相同的属性，则将这样的编译器 C 称为认证器。

所谓认证器就是一个协议编译器，使得 AM 下安全协议可以转换为 UM 下安全程度相同的协议。

定义 3[5] 消息传输 MT(Message Transmission)协议，其唯一功能就是将一条消息由一个参与者发送给另一个参与者。

定理 1[5] 如果 λ 是一个 MT-认证器，那么，C_λ 也是一个 MT-认证器。

(4)会话密钥安全 SK-secure

攻击者 U 除了通常的攻击手段外，还能够进行测试会话查询(Test-Session Query)，即可在其运行的任何时刻，从那些已完成的、没过期的、没被暴露的会话中选择一个作为测试会话(Test-Session)。设 k 是该会话的会话密钥，当 U 对测试会话查询时，掷币 $b, b \xleftarrow{R} \{0,1\}$，若 $b=0$，将 k 给 U；否则，从协议产生密钥的概率分布空间随机选择一个值 r 给 U。U 不允许对该会话和其匹配的会话发动会话状态暴露、会话密钥查询及攻陷参与者攻击。最后，U 输出一个比特 b'，作为 b 的猜测。

定义 4[5] 一个 KE 协议 π 是 SK-secure 的，当且仅当满足以下两条性质：

性质 1 协议 π 能够保证任意两个诚实的实体在完成协议后能够得到相同的密钥。

性质 2 在 UM 下的攻击者 U 正确猜出比特 b 的概率不超过 $0.5+\varepsilon$，其中 ε 为一个在安全参数下可忽略的概率(其中 ε 称之为“优势”)。

定理 2[5] 令 π 是一个 AM 下 SK-secure 的 KE 协议，λ 是一个 MT-认证器，那么，$C_\lambda(\pi)$ 是一个 UM 下 SK-secure 的 KE 协议。

3.2 利用 CK 模型分析 AARP 协议

认证器 1[5,6]：基于数字签名的 MT-认证器 λ_{Sig}

设：安全参数为 k；m 为实体 P_i 传送给实体 P_j 的消息。

1. P_i 将消息 m 发送给 P_j；

2. 收到 m 后，P_j 选取一个随机数 $r, r \xleftarrow{R} \{0,1\}^k$，并将 $\{m,r\}$ 发送给 P_i；

3. 收到 $\{m,r\}$ 后，P_i 构造 $\{m, Sig(P_i,(m,r,.P_j))\}$，并发送给 P_j；

4. 实体 P_j 后，验证签名的正确性，则接受消息 m。

定理 3[5,6] 假设签字体制能够抗击选择消息攻击，那么协议 λ_{Sig} 在 UM 下模拟了协议 MT。

AARP 使用了认证器 λ_{Sig}，可将其中的认证器去掉而得到 AM 模型下的协议，记作 π，只需证明 π 在 AM 模型下是 SK-secure 的。

根据 AM 的定义，当两个未被攻陷的实体完成协议时，均得到了未被篡改的 $x.G$ 和 $a.G$，故建立了相同的会话密钥，且路由查找标识 ID_A 将 $x.G$ 和 $a.G$ 与特定的匹配会话绑定，π 协议满足定义 4 的性质 1。下面证明 π 协议满足定义 4 的性质 2。

DDH 假设 设 Z 为椭圆曲线上的群点，a,b,c 分别从 Z 中均匀选择，则 $A_0=\{[m.G,n.G,p.G]:m,n,p \xleftarrow{R} Z\}$ 和 $A_1=\{[m.G,n.G,m.n.G]:m,n \xleftarrow{R} Z\}$ 的概率分布在计算上不可区分。

假设在 AM 下攻击者 A 在 π 协议的执行过程中，能以不可忽视的优势 ε' 区分会话密钥和随机数，即可构造一个算法 Y 能以不可忽略的优势区分 A_0 和 A_1。设 Y 的输入为 $(m.G, n.G, p.G)$，且该三元组是 A_0 或 A_1 的概率均为 0.5，算法 Y 使用攻击者 A 作为子过程，且假设 M 为 A 在交互过程中所激发的会话次数的上限。算法 Y 描述如下：

a)激活 A 和在 AM 下运行 π 协议的 n 个鉴别实体 $P_1, P_2, \cdots, P_n$(其中鉴别实体为源节点或目的节点)进行仿真交互；

b)当 A 激活一个实体建立新的会话，Y 代表另一对应角色实体按照 π 协议执行。当会话过期时，参与者将相应的会话密钥从内存中擦除；当一个参与者被攻陷或某个会话被暴露时，Y 将这个参与者或会话的相关信息发送给 A；

c)选择 $r \xleftarrow{R} \{1 \cdots M\}$，当第 r 个会话被激活时，Y 令作为源节点的参与者 P_i 将消息 $P_i \rightarrow P_j:[REQ, IP_{P_j}, ID_{P_i}, m.$

$G, Cert_{P_i}]K_{P_iS}$发给作为目的节点的另一参与者P_j；

d)P_j受到消息后，Y令其将消息$P_j \rightarrow P_i$:$[REP, ID_{P_i}, IP_{P_i}, IP_{P_{i+1}}, IP_{P_{i+2}}, \cdots, Cert_{P_j}, n.G]K_{P_jS}$发送给$P_i$。若第$r$个会话被$A$选中进行测试会话查询，则$Y$将$p.G$作为查询的响应给$A$；

e)若第r个会话被暴露了或者A选择别的会话作为测试会话，或者A没有选择测试会话就停止，则Y输出$b' \xleftarrow{R} \{0, 1\}$并停止；

f)若A停止且输出b'，则Y停止，输出和A相同的b'。

可见，Y所激发的A的运行直到A停止或Y终止A的执行，与A对抗π协议的正常运行是一致的。当A选中第r个会话作为测试会话时，A得到的响应是$p.G$，若Y的输入来自A_0，则响应是真实的会话密钥；若Y的输入来自A_1，则响应为一个随机数；而前面指出，Y的输入是A_0或A_1的概率均为0.5，则A猜中响应是真实的会话密钥还是随机数的概率是$0.5+\varepsilon'$，由于ε'不可忽略，这意味着攻击者A能以不可忽略的优势猜中密钥；通过输出和A相同的b'，Y猜中其输入是来自A_0或A_1的概率也为$0.5+\varepsilon'$。当A没有选中第r个会话作为测试会话，则A得到的响应为一个随机数，Y猜中其输入是A_0或A_1的概率为0.5。

由于A选中第r个会话作为测试会话的概率为$\frac{1}{M}$，则没有选中的概率为$1-\frac{1}{M}$，因此D猜中其输入来自A_0或A_1的概率为$(0.5+\varepsilon')\frac{1}{M}+0.5\times\left(1-\frac{1}{M}\right)=0.5+\frac{\varepsilon'}{M}$，其中$\frac{\varepsilon'}{M}$不可忽略，则$Y$就以不可区分的概率猜中了其输入来自$A_0$还是$A_1$，这与DDH假设相悖。所以，$\pi$协议满足定义4的性质2。

定理5 DDH假设成立的条件下，π协议在AM下是SK-secure的。

由定理2、定理4和定理5容易得到：若DDH假设成立及签名算法可抵抗选择消息攻击，则AARP协议在UM下是SK-secure的。

4 性能分析

双向密钥控制[8]：根据AARP协议，源节点和目的节点之间的会话密钥是由双方给出的有关安全参数决定的，该协议中$a.G$和$x.G$虽以明文形式传输，但$a.x.G=x.a.G$只能在源和目的之间共享，第三者无法获知，安全参数$a.G$和$x.G$每次均是由源和目的随机选取的，因此双方均无法单独控制密钥的生成。

消息完整性保护：在路由查找过程中，使用了数字签名的方法实现了消息完整性保护功能。

KKS[9]：安全参数$a.G$和$x.G$每次均是由源和目的节点随机选取的，因此每个会话密钥具有独立性，AARP协议具有KKS性质。

PFS[10]：公钥证书仅用于签名验证，临时公钥用于DH密钥交换，因而即使源和目的节点的长期私钥被泄漏，攻击者面对DH难题也无法求解以前的会话密钥，从而保证了会话密钥的安全性，协议具有PFS属性。

Non-KCI, Non-UKS：协议在CK模型下可证明是安全的，因此具有Non-KCI, Non-UKS属性[11]。

AARP相比ARAN不仅完成了会话密钥的协商，而且简化了路由查找过程，避免使用公钥加密算法，有效降低了协议计算复杂度，改进分组定义，降低了路由上的节点存储复杂度。表1给出源到目的节点的路由长度为5跳的情况下协议ARAN与AARP的路由查找过程的性能对比，这里不考虑AARP中间节点返回路由应答的情况，其中路由查找时间是仿真实验的结果，仿真实验在主频为P4 3.0G、内存为256M、操作系统为Windows XP的计算机上进行，其中签名采用椭圆曲线数字签名算法ECDSA(Elliptic Curve Digital Signature Algorithm)，加密采用椭圆曲线加密算法ECES(Elliptic Curve Encryption Scheme)，密钥长度为192位，杂凑算法为SHA-256，且运行在文献[12]指定参数的椭圆曲线上。

表1 协议性能比较

协议	交互轮数	签名(MN)	验证签名(MN)	公钥加密(MN)	公钥解密(MN)	路由查找时间(ms)
ARAN	20	16	38	6	6	336.66
AARP	10	6	20	0	0	145.21

可见，AARP协议的性能明显优越于ARAN的性能，更适合应用在Ad hoc网络中。

结束语 本文提出了一种新颖的鉴别路由协议AARP，不仅性能良好、安全性高等，而且实现了会话密钥的动态协商，为节点间的通信数据提供密钥分发服务。AARP协议如ARAN一样能有效地抗击大部分的恶意攻击。但与ARAN相比，协议交互次数少、计算复杂度低，可以说AARP协议不失为一种更有效、更实用的按需路由安全协议，能更好地满足Ad hoc网络对路由及数据的安全需求。

参 考 文 献

[1] Papadimitratos P, Haas Z J. Secure Routing for Mobile Ad hoc Networks// Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference CNDS 2002

[2] Sanzgiri K, Dahill B. A Secure Routing Protocol for Ad Hoc Networks// Proceedings of the 10th IEEE International Conference on Network Protocols (ICAP'02)

[3] 铁满霞，李建东，王育民. WAPI协议的可用性分析与改进. 计算机科学，2007(10)

[4] RFC3280, Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[5] Canetti R, Krawczyk H. Analysis of key-exchange protocol and their use for building secure channels// Proceeding of Eurocrypt 2001, LNCS 2045. Berlin, Springer-Verlag, 2001: 453-474

[6] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key-exchange protocols. 30th STOC, 1998: 419-428

[7] Bellare M, Rogaway P. Entity authentication and key distribution// D. Stinson ed. Advances in Cryptology, -CRYPTO' 93, Lecture Notes in Computer Science Vol. 773, Springer-Verlag, 1994: 232-249

[8] Mitchell C J, Ward M, Wilson P. Key control in key agreement protocols. Electronics Letters, 1998, 34: 980-981

[9] Blake-Wilson S, Johnson D, Menezes A. Key exchange protocols and their security analysis// Proceedings of the sixth IMA International Conference on Cryptography and Coding. 1997

[10] Guher C G. An identity-based key-exchange protocol// Proceedings of the Eurocrypt 89. Belgium, 1990: 29-37

[11] Canetti R, Krawczyk H. Universally composable notions of key exchange and secure channels// Proceeding of Eurocrypt 2002, LNCS 2332. Berlin, Springer-Verlag, 2002: 337-351

[12] 无线局域网产品采用的ECDSA和ECDH密码算法：椭圆曲线和参数. http://www.oscca.gov.cn/UpFile/20060118b.pdf