LEO 卫星网络中一种安全的按需路由协议

彭长艳 张 权 唐朝京
（国防科技大学电子科学与工程学院，湖南长沙 410073）

摘 要：低地球轨道（LEO）卫星网络的路由是当前卫星通信领域的研究热点，其安全问题也日益受到研究人员的重视。本文通过分析 LEO 卫星网络按需路由协议面临的安全威胁，使用基于身份的签密方案，提出了一种适合卫星网络拓扑特性的安全的按需路由协议。针对协议的密码算法处理时间开销较大的特点，设计了自适应的概率性延迟验证机制，能够降低协议的平均路由建立时间。安全性分析和仿真实验结果表明，该协议能够抵抗多种外部攻击行为，以有限的路由建立时间和路由开销为代价，保证了稳定的包传输率。

关键词：LEO 卫星网络；按需路由协议；安全路由；基于身份签密
中图分类号：TP393 **文献标识码**：A **文章编号**：1003 - 0530(2010)03 - 0337 - 10

A Secure On-Demand Routing Protocol for LEO Satellite Networks

PENG Chang-yan ZHANG Quan TANG Chao-jing
(School of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan, 410073, China)

Abstract: Research on routing in Low Earth Orbit Satellite Networks is a hotspot in areas of satellite communications, and how to secure routing algorithms has been attached increasing importance. After a terse analysis of security threats faced by on-demand routing protocols for satellite networks, a secure on-demand routing protocol is presented, which is on the basis of identity-based signcryption schemes and fit for the features of satellite network topology. According to the protocol's characteristic of heavy time overhead in processing crypto algorithms, a mechanism called delayed verification with adaptive probability is designed for decreasing route discovery time. Security analysis and simulation experiments show that the proposed protocol can resist typical outside attacks and guarantee steady packet delivery ratio at the cost of finite increase in route discovery time and route overhead.

Key words: LEO satellite networks; on-demand routing protocol; secure routing; identity-based signcryption

1 引言

低地球轨道(Low Earth Obit, LEO)卫星与中、高轨卫星相比，具有星地链路传输时延相对较小、频率可高效复用、链路带宽高、用户终端实现简单且功耗低等突出的优势，将成为未来空天地一体化网络的基本组成部分。

由于 LEO 卫星网络中星间链路(Inter-Satellite Link, ISL)的不稳定性、拓扑的动态变化性、星上处理能力的有限性，设计高效、可靠、灵活的路由机制是卫星网络研究面临的重要挑战[1]。根据路由的产生方式，卫星网络路由机制可分为静态路由和动态路由两种。静态路由机制利用卫星网络运行的周期性和可预知性，根据事先计算的路由信息进行数据包的发送，具有算法简单，路由开销小的优点[2]。但是，静态路由机制不能适应星间链路、网络负载的变化，难以找到最优的路径从而可能导致网络性能的显著下降。动态路由机制根据网络流量和链路延迟的变化，自适应地调整路径，从而保证了数据包转发的高效性。

按需路由是一种在自组织网络中广泛使用的反应式动态路由机制。研究人员对原有按需路由协议进行了修改扩充，设计了适合 LEO 卫星网络拓扑特点的按需路由协议，能够降低端到端延迟和延迟抖动，获得较高的包传输率，并保持较小的信令开销[3-5]。

收稿日期：2009 年 4 月 1 日；修回日期：无
基金项目：国家 863 计划项目（2008AA7010305）

卫星网络开放性的特点使其路由协议较传统地面网络更容易受到路由控制信息的窃取、篡改、伪造、重放、拒绝服务等攻击的威胁。在静态的路由机制中,由于路径均已事先通过离线的方式计算,不需要或很少需要卫星之间进行路由信息的交互,因而较少涉及到路由安全方面的问题。但是在动态的路由机制如按需路由中,必须对路由发现过程中交互的控制包进行有效的保护,才能避免各种攻击造成的路由失效或网络性能的下降。然而,现有的大多数 LEO 卫星网络路由协议较少考虑安全问题,一旦路由协议受到攻击,将阻碍协议的正常运行,不能完成路由的发现和维护,或者建立错误的路由,从而导致网络性能的严重下降甚至完全瘫痪。因此,设计满足认证性、机密性、完整性、不可否认性和可用性等安全需求的卫星网络路由协议非常重要。

李□等人将基于信誉度的安全机制加入到卫星网络路由协议中,能够在检测到恶意的内部或外部攻击后,迅速做出反应并将恶意节点排除在路径之外[6]。该协议主要从可用性的角度增强了路由协议的安全性,但是只能在攻击发生后采取一定的补救措施,而不能在路由建立的过程中抵抗各种针对路由控制信息的攻击。

针对按需路由的建立和维护过程中的认证性、机密性、完整性、不可否认性等安全需求,可以使用各种对称密码、非对称(公钥)密码或者两者的组合等机制来满足,目前的研究成果主要集中在自组织网络领域[7]。由于具有更好的扩展性,基于公钥密码的方案得到了较多的关注,其一般采用数字签名实现对路由控制包的认证和不可否认性,并结合对称密码体制满足其它安全需求,利用可信第三方颁发证书以将节点身份与公钥绑定,但是这类方案同时也引入了较多的通信和计算开销,并且需要较为复杂的密钥管理系统对公钥证书和证书撤销列表进行管理。

作为一种新型的公钥密码体制,基于身份密码学[8](Identity-Based Cryptosystem, IBC)不再需要公钥证书,大大简化了传统公钥密码体制中密钥管理方面的开销,能够提高按需路由协议的安全性和性能。Deng 等人将基于身份的签密(Identity-Based Signcryption, IBSC)方案引入到动态源路由协议中,对路由请求和路由应答消息中的不变部分进行签密,而对路由请求消息的可变部分仍然使用"单向哈希链"的方式进行认证[9],不可避免的继承了该方式认证延迟高和易受拒绝服务攻击的缺点,并且该协议没有提供路由消息的机密性保护。Park 等人利用基于身份的签名方案对路由协议进行了扩展,保证了路由信息的逐跳认证[10],但是同样没有采取安全机制来保护路由请求过程中的广播消息。Zhang 等人使用多重签密方案对按需路由协议进行保护,在源节点发出路由请求消息后,中间节点不断地对消息进行签密并广播,直至到达目的节点,目的节点通过单播将消息传回源节点并由源节点统一地验证整个路由消息[11]。但是,由于中间节点不对消息进行验证,可能使攻击者产生的虚假的或错误的路由消息不断地被转发,将造成网络带宽和节点计算资源的消耗,并且难以保证路由协议的可用性和性能。

由于卫星网络在拓扑和星际链路等方面的特性异于传统的地面有线和无线网络,因此原有的路由安全机制并不能直接应用于卫星网络,必须设计符合卫星网络特点的安全路由协议。本文根据 LEO 卫星网络按需路由协议的特点和安全需求,使用基于身份的签密方案,提出了一种新的安全按需路由(Secure On-demand Routing, SOR)协议。第二节简要介绍本文的密码学基础——基于身份的密码体制和签密方案;第三节详细介绍了提出的 SOR 协议的路由发现和维护过程中采用的安全机制,接着设计了基于自适应概率性延迟验证的性能优化策略;第四节和第五节分别对 SOR 协议的安全性和性能进行了分析,最后第六节总结了全文。

2 基于身份的密码体制和签密方案

自从 2001 年第一个应用双线性对的基于身份加密方案[8]提出以后,基于身份密码学得到了飞速的发展,在加密、签名、密钥协商和签密等领域取得了大量的研究成果[12]。IBC 的主要思想是任何实体的公钥都可以由一个任意的字符串(如 IP 地址或 MAC 地址)来定义,而不需要通过网络或其它方法额外地传输公钥,相应的私钥可以事先通过离线的可信机构 PKG(Private Key Generator)生成。由于 IBC 不再需要公钥证书,密钥管理机制相对简单,在信息安全领域特别是无线网络安全领域具有广阔的应用前景[13]。

双线性对是实现众多 IBC 方案的重要基础,其中使用较多的为 Weil 对和 Tate 对。设 q 为安全的大素数,G_1 和 G_2 分别是阶为 q 的加法和乘法循环群,双线性对 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 具有以下性质:

双线性:对所有 $P, Q \in G_1, a, b \in Z$,都有 $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$;

非退化性: 存在 $P,Q\in G_1$,使得 $\hat{e}(P,Q)\neq 1_{G_2}$;

可计算性: 存在一个算法,对任何 $P,Q\in G_1$ 都可以高效地计算出 $\hat{e}(P,Q)$。

签密方案可以在一个逻辑步骤中完成签名和加密,能够同时提供认证性和机密性,与传统的"先签名再加密"的方法相比具有更高的效率。基于身份的签密方案将基于身份密码学和签密两种机制的优势结合起来,有效地降低了计算和通信开销[14]。基于身份的广播签密[15](Identity-Based Broadcast Signcryption, IBBSC)方案是 IBSC 在多接收者条件下的推广,能够同时针对多个接收者完成信息的签密,而不需要分别对每个接收者进行重复的操作,从而节省了计算资源和网络带宽的消耗。广播签密方案包括 Setup, KeyGen, SignCrypt 和 UnSignCrypt 等四个阶段,前两个阶段在所有 IBC 方案中基本相同。PKG 选择系统私钥 $s\in Z_q^*$,选择 $R\in G_1^*$,计算系统公钥 $P_{pub}=s\cdot P$,计算 $\theta=\hat{e}(R,P_{pub})$,选择分别满足一定条件的哈希函数 H_0,H_1,H_2,然后公开所有系统参数。PKG 随后为每个节点生成公私钥对(Q_i,D_i)。下面介绍本文使用的 IBBSC 方案[16]的后两个阶段。

SignCrypt:假定具有公私钥对(Q_A,D_A)的 A 发送消息 M 给 n 个不同的接收者 $ID_1,ID_2,\cdots,ID_n$。A 根据系统参数,明文消息 M,自身私钥 D_A,以及接收者集合的公钥 $Q_1,Q_2,\cdots,Q_n$,得到密文输出 σ,详细过程如下:

A 选择 $r\in Z_q^*$,计算 $X=rQ_A$,$h_1=H_1(X,m)$,以及$Z=(r+h_1)D_A$。

A 计算 $U=rP$,$\omega=\hat{e}(Z,P)$,$c=m\oplus H_2(\omega)$,以及 $W=\theta^r\omega$。对于每一个 $i=1,\cdots,n$,A 计算 $T_i=rH_1(ID_i)+rR$。这样,密文为 $\sigma=(c,U,X,W,T_1,\cdots,T_n,L)$,其中 L 代表接收者与 T_i 的关联。由于对所有接收者来说,密文是相同的,因此密文的长度大于单接收者的签密方案。

UnSignCrypt:任意一个接收者 ID_i 接收到 A 发送的密文 σ 后,利用系统参数,自身私钥 D_i,以及 A 的公钥 Q_A,恢复出明文消息 M,并对消息进行验证。

接收者 ID_i 计算 $\omega'=W\hat{e}(U,D_i)\hat{e}(P_{pub},T_i)^{-1}$,以及 $m'=c\oplus H_2(\omega')$。

ID_i 计算 A 的公钥 $Q_A=H_0(ID_A)$,$h_1'=H_1(X,m')$,比较 $\omega'=\hat{e}(P_{pub},X+h_1'Q_A)$是否成立。如果上式成立,则输出 m',否则返回 $\perp$ 表明验证失败。

根据双线性对的性质,如果 σ 是合法的密文,则

$$\begin{aligned}\omega'&=W\hat{e}(U,D_i)\hat{e}(P_{pub},T_i)^{-1}\\&=\theta^r\omega\hat{e}(rP,sH_1(ID_i))\hat{e}(sP,rH_1(ID_i)+rR)^{-1}\\&=\hat{e}(R,P_{pub})^r\omega\hat{e}(rP,sH_1(ID_i))\hat{e}(sP,rH_1(ID_i))^{-1}\\&\quad\hat{e}(P_{pub},rR)^{-1}\\&=\hat{e}(R,P_{pub})^r\omega\hat{e}(P_{pub},rR)^{-1}=\omega\end{aligned}$$

因此,$m'=c\oplus H_2(\omega')=c\oplus H_2(\omega)=m$,消息得到恢复,并且 $h_1'=H_1(X,m')=H_1(X,m)=h_1$。另外,$\hat{e}(P_{pub},X+h_1Q_A)=\hat{e}(sP,rQ_A+h_1Q_A)=\hat{e}(P,(r+h_1)sQ_A)=\hat{e}(Z,P)=\omega$,即签密方案中的验证应该成功。

3　安全的按需路由协议

下文中主要的符号定义如表 1 所示。

表 1　符号定义表

符号	含义
G_1,G_2	阶为 q(安全的大素数)的加法、乘法循环群
$\hat{e},P$	双线性对 $\hat{e}:G_1\times G_1\to G_2$,$G_1$ 的生成元
P_{pub},s	系统的公钥,私钥,其中 $P_{pub}=s\cdot P,s\in Z_q^*$
ID_A	A 的身份信息
Q_A,D_A	A 的公钥、私钥
H_0	满足 $\{0,1\}^*\to G_1$ 的单向哈希函数
H_1	满足 $G_1\times\{0,1\}^*\to Z_q^*$ 的单向哈希函数
H_2	满足 $G_2\to\{0,1\}^*$的单向哈希函数
N	卫星星座的轨道平面数
M	每个轨道平面的卫星节点数量
RREQ	路由请求(Route Request)消息
RREP	路由应答(Route Reply)消息
RERR	路由错误(Route Error)消息
Src, *Des*	源节点,目的节点

使用 $SignCrypt_{A,B}(m)$表示用 A 的私钥,B 的公钥对消息 m 进行签密运算,而 $SignCrypt_{A,B,C,\cdots}(m)$表示用 A 的私钥,B、C 等的公钥对消息 m 进行签密运算。IBSC 可看成是 IBBSC 的一种特例,下文中将统称为基于身份的签密。此外,除了本文使用的签密方案,其它的签密方案也能应用于 SOR 协议中。

基于身份的密码体制的优点使其非常适合于存储、计算和带宽资源相对有限的卫星网络节点。本节使用基于身份的签密方案,设计了适合 LEO 卫星网络特点的安全按需路由协议,解决了由于外部攻击而产生的各种路由安全问题。

3.1　系统模型

LEO 卫星网络系统通常包括多个轨道平面,在每个轨道平面上运行多个卫星。按照轨道是否通过极地,可以将 LEO 卫星系统分为极地轨道星座和非极地

轨道星座。本文的研究主要针对类似铱星 Iridium 系统的典型极地轨道 LEO 卫星网络。卫星之间通过轨道内或轨道间高带宽的高频或激光星间链路进行通信。同一轨道内的 ISL 在卫星运行过程中保持不变,而不同轨道间的 ISL 在卫星运行过程中是动态可变的,这是因为在不同的纬度,卫星轨道间距离不同。ISL 并不总是处于连通的状态,当卫星节点位于极地区域时,轨道间链路和部分轨道内链路将关闭。使用与文献[3]中相似的方式,将 LEO 卫星网络拓扑抽象为一个如图 1 所示的网格。

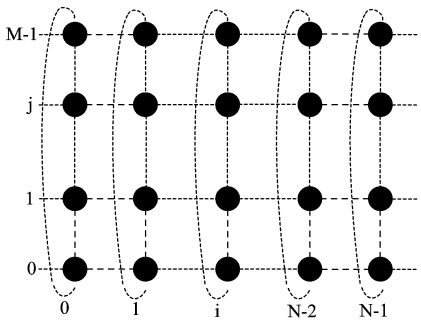

图 1 卫星网络抽象拓扑图

将卫星节点的虚拟坐标唯一地定义为($\bar{x}$, $\bar{y}$), $\bar{x}$ 和 $\bar{y}$ 分别代表轨道平面和卫星在轨道平面的位置,其中 $\bar{x} \in [0,N)$, $\bar{x} \in [0,M)$。在考虑反向缝链路的情况下,对于任意两个通过 ISL 进行连接的卫星节点($\bar{x}_a$, $\bar{y}_b$)和($\bar{x}_c$, $\bar{y}_d$),如果在同一轨道平面内,则 $\bar{x}_a = \bar{x}_c$,且

$$\bar{y}_d = \begin{cases} \bar{y}_b \pm 1, & \bar{y}_b \pm 1 \in [0,M) \\ \bar{y}_b \pm 1 \mp M, & \bar{y}_b \pm 1 \notin [0,M) \end{cases} \qquad (1)$$

如果两个节点的轨道平面相邻,则 $\bar{y}_b = \bar{y}_d$,且

$$\bar{x}_c = \begin{cases} \bar{x}_a \pm 1, & \bar{x}_a \pm 1 \in [0,N) \\ \bar{x}_a \pm 1 \mp N, & \bar{x}_a \pm 1 \notin [0,N) \end{cases} \qquad (2)$$

可信 PKG 为包括卫星节点在内的整个网络系统进行安全机制的初始化工作。对于给定的安全参数 k,PKG 选取两个阶为 q 的循环群 G_1 和 G_2,G_1 的生成元 $P \in G_1$,双线性映射 $\hat{e}: G_1 \times G_1 \to G_2$。PKG 选择系统私钥 $s \in Z_q^*$,选择 $R \in G_1^*$,然后计算系统公钥 $P_{pub} = s \cdot P$,并计算 $\theta = \hat{e}(R, P_{pub})$。PKG 选择满足 $\{0,1\}^* \to G_1$ 的哈希函数 H_0,满足 $G_1 \times \{0,1\}^* \to Z_q^*$ 的哈希函数 H_1,满足 $G_2 \to \{0,1\}^*$ 的哈希函数 H_2。然后 PKG 公开系统参数 $\{G_1, G_2, q, P, P_{pub}, \hat{e}, R, \theta, H_0, H_1, H_2\}$。

PKG 自身初始化完成之后,为网络节点产生其公钥对应的私钥。对于虚拟坐标为($\bar{x}_a$, $\bar{y}_b$)的卫星节点 Sat_i,将其标识与虚拟坐标绑定,作为其身份信息 $ID_i = [Sat_i \| (\bar{x}_a, \bar{y}_b)]$。节点的身份和公钥的计算方法是公开的,任何节点可以方便的得到其它节点的公钥,即 $Q_i = H_0(ID_i)$。节点的私钥由 PKG 计算,$D_i = s \cdot Q_i$,通过安全的信道传输给节点。最终,每个卫星节点均得到了基于身份的公私钥对为(Q_i, D_i)。PKG 的初始化工作完成之后,即可处于离线状态。

3.2 SOR 协议描述

按需路由协议包括路由发现和路由维护两个部分。在路由发现过程中,源节点发出路由请求包,通过“泛洪路由”的方法由中间节点逐跳转发,最终到达目的节点,然后目的节点沿反向路径发送路由应答包至源节点;路由维护机制则旨在检测并管理失效的路径,报告相关的节点以选择其它路径或者启动新的路由发现过程。下面详细介绍 SOR 协议的路由发现和路由维护过程,其中,路由发现又分为路由请求和路由应答两个阶段。

3.2.1 路由请求

在路由请求阶段,源节点广播 *RREQ* 包,中间节点接收到 *RREQ* 后,按照协议规范,修改数据包中的中间节点列表,继续广播 *RREQ*,直至到达目的节点。为了减少泛洪路由的作用范围从而降低路由开销,SOR 利用星间链路具有确定性的特点,采用如下两个方法对 *RREQ* 的转发范围进行约束。

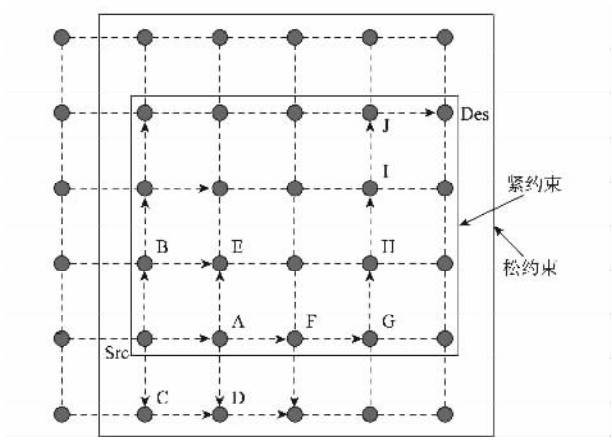

图 2 路由发现

首先,限制每一个 *RREQ* 进行转发的最大跳数。由于卫星数目有限,任意两个节点之间可以通过有限的步骤达到,最大跳数为[$M/2$]+[$N/2$]。但由于在网络发生拥塞时,最小跳数路径不一定是最优路径,因

此实际的最大跳数值略微增加。源节点在数据包中设置 *TTL* 为最大跳数,中间节点转发时将该值减一,如果 *TTL* 值为 0,则停止转发该 *RREQ* 包。其次,使用如图 2 所示的约束矩形限制数据包广播的范围。当源节点和目的节点确定后,即可根据卫星网络拓扑的特点定义一个矩形区域,*RREQ* 只在该区域内进行转发,能够有效地降低路由开销。根据实际情况,可以使用"紧约束"和"松约束"两种限制方法,其中,"紧约束"的限制区域小,路由开销较小,而"松约束"的限制区域较大,因而路由开销较大,但是可以发现更多的有效路由。

源节点根据约束机制,确定路由中可能的下一跳节点的集合,若为紧约束,则下一跳节点集合为[*A*,*B*],否则为[*A*,*B*,*C*]。*Src* 产生如式(3)的 *RREQ* 包并发送至下一跳节点集合(本文以"松约束"为例)。

$$Src\rightarrow[\,A,B,C\,]:$$

$$SignCrypt_{Src,A,B,C}(\,RREQ,Src,Des,Seq,TTL,\{\,\})\,\|$$

$$SignCrypt_{Src,Des}(\,RREQ,Src,Des,Seq\,) \qquad (3)$$

路由控制包中的 *RREQ* 表示包的类型,*Seq* 表示路由请求的序列号,用于区分同一源节点发出的不同的 *RREQ* 消息,*TTL* 为设置的最大跳数,{ }表示转发路径上的中间节点列表。整个包由前后两个部分组成,包的前半部分逐跳变化,只发送至下一跳节点并由其进行反签密操作,而包的后半部分则在整个路由请求的过程中保持不变,并最终到达目的节点。

以节点 *A* 为例描述接下来的路由请求过程。*A* 接收到 *Src* 发出的路由请求包后,将包分为前后两个部分。对于包的前半部分,*A* 利用自身私钥 D_A 和 *Src* 的公钥 Q_{Src} 反签密,从而得到路由消息的内容和验证结果。如果消息内容未能通过合法性验证,*A* 结束对该 *RREQ* 包的处理并丢弃,否则继续进行路由发现机制。*A* 将 *TTL* 的值减一,将转发节点列表修改为 {*A* },根据路由发现的约束机制确定下一跳节点的集合。由于 *RREQ* 来源于 *Src*,在松约束条件下可能的下一跳节点集合为[*D*,*E*,*F*]。*A* 按照式(4)使用自身私钥 D_A 和[*D*,*E*,*F*]的公钥[Q_D,Q_E,Q_F]对路由请求信息进行签密,并组合从 *Src* 接收到的路由请求包的后半部分,发送至下一跳节点的集合。

$$A\rightarrow[\,D,E,F\,]:$$

$$SignCrypt_{A,D,E,F}(\,RREQ,Src,Des,Seq,TTL,\{A\})\,\|$$

$$SignCrypt_{Src,Des}(\,RREQ,Src,Des,Seq\,) \qquad (4)$$

接下来的中间节点继续按照与 *A* 类似的方式,对路由请求包进行处理,然后按照约束机制发送 *RREQ* 包至下一跳节点。对于具有相同源节点和序列号的 *RREQ* 包,以先接收到的包为准,即如果发现已经处理过该 *RREQ* 包,则将其丢弃。

以图 2 为例,假定最终 *RREQ* 包按照路径 {*A*,*F*,*G*,*H*,*I*,*J* }由源节点 *Src* 到达目的节点 *Des*。*Des* 通过反签密得到路由控制消息的内容和验证结果,然后准备路由应答 *RREP* 包。

3.2.2　路由应答

目的节点 *Des* 接收到 *RREQ* 包后,分别对包的前后两个部分进行处理:对于前半部分,利用自身私钥 D_{Des} 和发送方的公钥 Q_J 进行反签密操作,得到 *RREQ* 消息的内容,并验证消息的合法性;而对于后半部分,则使用自身私钥和源节点的公钥 Q_{Src} 进行反签密操作,同样得到源节点的 *RREQ* 消息的内容。然后 *Des* 比较前后两个消息中的相同域,如果内容不相同,则表明路由发现过程中消息遭到恶意修改或者发生错误,于是 *Des* 丢弃该 *RREQ* 包。

如果上述的消息内容均验证通过,*Des* 开始准备路由应答包。与路由请求包的广播发送方式不同,路由应答包根据最先到达的 *RREQ* 包的路径的反向路径按照单播的方式发送至路由请求 *RREQ* 包的发起节点。在图 2 中,假定按照路径 {*A*,*F*,*G*,*H*,*I*,*J* }的 *RREQ* 最先到达目的节点 *Des*,*Des* 将路由应答包单播发回 *Src* 节点。*Des* 发送式(5)内容至节点 *J*。

$$Des\rightarrow J:$$

$$SignCrypt_{Des,J}(\,RREP,Des,Src,Seq,\{J,I,H,G,F,A\})\,\|$$

$$SignCrypt_{Des,Src}(\,RREP,Des,Src,Seq,\{J,I,H,G,F,A\}) \qquad (5)$$

RREP 包同样有两个部分组成,前半部分由节点 *J* 进行处理,而后半部分则由中间节点不断转发直至到达 *Src* 节点。节点 *J* 接收到 *RREP* 包后,使用自身私钥 D_J 和 *Des* 的公钥 Q_{Des} 反签密包的前半部分,得到 *RREP* 消息的内容,并根据节点列表更新自身的路由表。节点 *J* 然后按照式(6),使用 D_J 和下一跳节点 *I* 的公钥 Q_I 签密路由应答消息,并附加上接收到的 *RREP* 包的后半部分,发送至节点 *I*。

$$J\rightarrow I:$$

$$SignCrypt_{J,I}(\,RREP,Des,Src,Seq,\{J,I,H,G,F,A\})\,\|$$

$$SignCrypt_{Des,Src}(\,RREP,Des,Src,Seq,\{J,I,H,G,F,A\}) \qquad (6)$$

节点 *I* 按照类似的方式对 *RREP* 包进行处理,并按照单播的方式转发至下一跳节点。最后,路由发现的发起节点 *Src* 接收到 *A* 发出的如式(7)的路由应答包。

$$A\rightarrow Src:$$

$$SignCrypt_{A,Src}(RREP,Des,Src,Seq,\{J,I,H,G,F,A\}) \| SignCrypt_{Des,Src}(RREP,Des,Src,Seq,\{J,I,H,G,F,A\}) \quad (7)$$

Src 使用私钥 D_{Src} 和 *A* 的公钥 Q_A 反签密包的前半部分，得到 *RREP* 消息的内容和验证结果；接着，*Src* 利用私钥 D_{Src} 和 *Des* 的公钥 Q_{Des} 反签密包的后半部分，同样得到 *RREP* 消息的内容和验证结果；然后 *Src* 比较这两个消息中相同域的内容。如果以上任意一个验证未通过，则 *Src* 丢弃该 *RREP* 包，等待合法的 *RREP* 包或者开始新的路由发现过程。如果协议正常完成，则 *Src* 利用 *RREP* 消息的内容更新路由表，完成路由发现过程，接下来就可以利用该路由信息进行数据包的转发。

以上描述了包含路由发现和路由应答的一个完整的路由建立过程。实际上，中间节点可能存在到目的节点的有效路由，如果直接产生路由应答 *RREP* 包，将能够充分减少整个路由发现的持续时间。

在图2中，假定节点 *F* 在接收到 *Src* 发出经由 *A* 转发的路由请求包后，查找路由表，发现存在一个合法且有效的到达目的节点的路径为 $\{G,H,I,J\}$，于是按照式(8)准备路由应答包并发送至节点 *A*。

$F \rightarrow A$:

$$SignCrypt_{F,A}(RREP,Des,Src,Seq,\{J,I,H,G,F,A\},F) \| SignCrypt_{F,Src}(RREP,Des,Src,Seq,\{J,I,H,G,F,A\},F) \quad (8)$$

在以上消息中，节点列表后增加了一个字段以表明本路由应答包由中间节点 F 产生，其它部分与原有消息相同。*A* 接收到 *RREP* 包后，按照式(9)发送至源节点 *Src*。

$A \rightarrow Src$:

$$SignCrypt_{A,Src}(RREP,Des,Src,Seq,\{J,I,H,G,F,A\},F) \| SignCrypt_{F,Src}(RREP,Des,Src,Seq,\{J,I,H,G,F,A\},F) \quad (9)$$

Src 通过对包的前半部分的处理获得了路由应答消息的内容，并得知 *RREP* 消息来源于 *F*；*Src* 使用私钥 D_{Src} 和 *F* 的公钥 Q_F 经过反签密操作，同样得到 *F* 提供的路由信息。与前文类似，*Src* 比较两部分的内容，然后完成路由发现过程。

3.2.3 路由维护

在按需路由协议中，当由于节点移动或者网络拥塞导致链路不能正常工作时，根据实际的失效原因，节点或者删除包含该链路的路由表信息，或者仅仅将其标记为“非活动”。同时，节点还将向路由中包含该链路的其它节点发送路由错误 *RERR* 包。与路由请求中的方法类似，使用基于身份的签密方案为 *RERR* 包提供安全性保障。

假定在图2中，节点 *A* 到 *F* 之间的链路由于某一原因不可用，如果 *Src*、*D* 和 *E* 节点均存在经过这一链路的路由，则 *A* 向这些节点发送式(10)的 *RERR* 包报告链路失效情况。

$A \rightarrow [Src,D,E]$:

$$SignCrypt_{A,Src,D,E}(RERR,A,F,Seq,Event) \quad (10)$$

Src 节点接收到路由错误包后，利用自身私钥 D_{Src} 和 *A* 的公钥 Q_A 反签密得到消息的内容和验证结果。如果验证通过，则更新节点的路由表，选择别的路径转发消息或者重新开始路由发现过程，否则丢弃该路由错误包。路由错误包沿着相反的路径方向转发，直到所有经过失效链路的路由表内容都得到了更新为止。转发的 *RERR* 路由错误包使用相同的签密机制进行保护。

3.3 自适应概率性延迟验证的性能优化策略

在按需路由协议中，*RREQ* 使用广播方式，而 *RREP* 和 *RERR* 则使用单播，因此网络中的路由控制包主要为 *RREQ*。在大部分使用公钥密码学的安全路由协议中，发送者对 *RREQ* 包进行数字签名，而接收者通过对签名进行验证以保证消息的真实性。然而，由于目的节点只选择一条路径，绝大多数被转发的 *RREQ* 包并未对最终路由做出贡献，反而由于签名的验证增加了路由发现的时间开销。针对这一问题，Zapata 提出了延迟验证的方法，*RREQ* 未经验证而直接转发，只有最终选择的路径上的节点在接收到 *RREP* 并转发后再对 *RREQ* 进行验证，其它的 *RREQ* 则在经过一定的时间后丢弃[17]。当不存在外部攻击且路由协议正常运行条件下，*RREQ* 应该能够通过验证，因此未经验证的 *RREQ* 包的广播不会增加网络开销。

与未使用安全机制的按需路由协议相比，SOR 协议涉及到的签密和反签密操作需要复杂的“对计算”，将会显著增加平均路由发现时间，势必降低协议的性能。因此，SOR 中存在使用延迟验证机制的条件。然而，当网络遭到针对节点或链路的外部攻击时，大量伪造的路由控制包可能进入网络。若使用即时验证的方法，能够在一跳的间隔内停止转发并过滤错误的路由控制包；但是，如果使用延迟验证，将导致控制包在网络中不断被转发，不但浪费了宝贵的网络带宽资源，而且消耗了节点的计算和存储资源。这样一来，延迟验证不完全适合网络的要求，存在一定的局限性。

为了尽量减少安全机制的引入带来的协议性能

损失,在性能和安全性之间达到一定程度上的平衡,本文提出了一种自适应概率性延迟验证(Delayed Verification with Adaptive Probability,DVAP)的性能优化策略,并将其应用于 SOR 的所有路由控制包。其基本思想是:节点以概率 p 对接收到的控制包进行延迟验证;为了适应网络中可能存在的攻击或异常行为,p 根据节点最近接收到的控制包的验证结果动态变化。如果未通过验证的控制包的数量增加,则减小延迟验证的概率 p,否则,增大概率 p 以提高协议的性能。p 的初始值 p_0 的取值范围为[0,1],作为全局系统参数可事先确定。

卫星网络中每个节点都维护一个概率值列表,包括链路标识 *LinkID* 和概率 P,表示对每一个相邻节点之间星间链路接收的路由控制包的延迟验证概率。以 $p_{i,j}$表示节点 i 对从星间链路 j 接收的路由控制包的验证概率,分别考虑验证结果为合法和不合法两种情况下概率 $p_{i,j}$的自适应机制。

如果节点 i 对从链路 j 接收的路由控制包的验证(即时验证或延迟验证)成功后,表明网络中的路由攻击趋于减少,则将 $p_{i,j}$线性增加一个变化值 CV_1。

$$p_{i,j}^{n}=\begin{cases}\min(\ p_{i,j}^{n-1}+CV_1,1\ ) & p_{i,j}^{n-1}<1\\ 1 & p_{i,j}^{n-1}=1\end{cases}\qquad(11)$$

反之,如果路由控制包的验证结果为不合法,则表明网络中存在攻击行为,应迅速减少(指数下降)延迟验证的概率,从而使后续的控制包尽可能多地得到即时验证,避免了路由攻击包的扩散。

$$p_{i,j}^{n}=\begin{cases}\max(\ p_{i,j}^{n-1}-CV_2\times 2^{\alpha},0\ ) & p_{i,j}^{n-1}>0\\ 0 & p_{i,j}^{n-1}=0\end{cases}\qquad(12)$$

式中 $\alpha\geq 0$,并且一般来说 $CV_2\geq CV_1$,因此 $p_{i,j}$减少得较快而增加得较慢。

下面在 SOR 协议的基础上简要介绍 DVAP 机制的使用。

在路由请求包的转发阶段,中间节点 i 根据链路标识 j 在概率值列表中查找 $p_{i,j}$,以概率($1-p_{i,j}$)对 *RREQ* 包进行即时验证。如果对 *RREQ* 进行了验证,若验证未通过,则丢弃该包,否则继续转发,然后节点根据验证的情况更新 $p_{i,j}$。如果没有对 *RREQ* 进行验证,则节点将其保存在缓存中然后按照协议继续转发,并对路由表中的相应记录标记为“未验证”(Unverified);然后节点等待 *RREP* 包,若超过了时间门限值 T_w,表明节点未被包含到最终的路径中,则删除缓存和路由表中的相关记录。

路由请求包 *RREQ* 到达目的节点之后,*Des* 按照原 SOR 协议进行处理,选择一条路径并按反向路径发送 *RREP* 包。

在路由应答阶段,中间节点对 *RREP* 包使用 DVAP 机制:如果对 *RREP* 包进行了验证,若结果为合法,则节点使用与原协议相同的方法处理并转发 *RREP* 包,反之若结果为不合法,则将其丢弃并删除缓存中 *RREQ* 包(如果包存在);节点根据验证的结果情况更新 $p_{i,j}$;如果没有验证 *RREP* 包,则将其保存在缓存中并按照正常的协议流程继续转发 *RREP* 包至 *Src*,然后对路由表中的相应记录标记为“未验证”。

处理完 *RREP* 包后,如果缓存中包含“未验证”的 *RREQ* 或 *RREP* 包,节点按照如下步骤开始延迟验证过程:

1:如果存在“未验证”的 *RREQ* 包,使用反签密算法验证 *RREQ* 包,若验证结果合法,转到 2,否则转到 5;

2:如果相应 *RREP* 包已进行验证,转到 4,否则转到 3;

3:如果存在“未验证”的 *RREP* 包,则开始验证,若验证结果合法,转到 4,否则转到 5;

4:删除缓存中相关的路由控制包和路由表中的相应标记,确认路径的有效性,节点根据验证的情况更新 $p_{i,j}$,退出验证过程;

5:删除缓存中相关的路由控制包和路由表中的相应路径,分别向 *Src* 和 *Des* 节点发送包含相应信息的 *RERR* 包,使其选择别的路径或者重新开始路由发现过程,节点根据验证的情况更新 $p_{i,j}$,然后退出验证过程。

在基于身份的签密方案的反签密操作中,大约有三分之一的时间用于对内容进行验证。因此,与 SOR 协议相比,DVAP 机制以一定概率的安全性损失、较低的存储开销和协议复杂性为代价,能够有效减少协议的路由建立时间。下文首先分析协议的安全性,然后通过仿真实验具体分析协议的性能。

4　安全性分析

由于基于身份的签密方案本身的安全性已经有较为完整和充分的证明[16],本文认为该方案是安全的,并在此基础上分析 SOR 协议的安全性。

由于节点加入网络之前均已经从 PKG 获得了公私钥对(Q_i,D_i),在节点的私钥没有泄露的情况下,通过使用签密方案,只有预先设定的接收者才能够解密消息,从而保证了机密性,接收者进而通过消息签名的

验证,能够达到消息的认证性。此外,签密方案本身能够满足消息内容的完整性和不可否认性。因此,根据卫星网络按需路由的特点而设计的 SOR 协议,能够满足认证性、保密性、完整性和不可否认性等安全需求。另外,SOR 协议使用了逐跳认证的机制,因此任何非法的路由控制包都能够被排除在最终的路径之外。下面简要分析 SOR 协议如何防御几种典型的针对路由协议的外部攻击。

身份欺骗攻击。将节点标识与其在星座中的虚拟坐标绑定,使得 SOR 协议能够抵抗身份欺骗攻击。只有节点拥有与其标识和虚拟坐标相对应的私钥,才能够使经过其签密的消息通过其它节点的合法性验证。在对签密的消息进行验证时,首先检查消息源的实际位置是否与消息中声明的位置相一致,然后再根据节点的公钥(由标识和坐标计算得出)判断消息的合法性。这样一来,即使攻击者得到了节点的私钥,但是由于空间位置的不同,其发出的消息将无法得到其它节点的认可。

路由信息窃取、篡改和伪造攻击。由于所有路由请求和路由维护包均通过签密进行保护,外部节点无法获取包的内容。同样,签密方案的使用可以保证即使路由消息被外部节点篡改,也不能通过其它内部节点的验证。最后,只有内部节点才能发出路由建立或维护控制包,外部节点的伪造包将被下一跳节点识别并丢弃。

重放攻击。在路由发现和维护包中均使用了序列号机制,可以很容易地发现重放的路由控制包。另外,路由序列号 *Seq* 包含在经过签密的控制包中,外部节点由于没有合法的私钥而无法伪造,因此难以实施重放攻击。

SOR 协议本身不能抵抗外部节点的拒绝服务攻击,但是可以方便地通过与入侵检测和响应机制的结合,发现攻击并采取一定的防御措施。

采取 DVAP 机制以后,SOR 协议的安全性有所降低,可能导致伪造的或错误的路由控制包在网络中的传播,但是由于所有的控制包最终还是要经过合法性验证,因此最终选择的路径仍可认为是安全可靠的。

5 性能评价

5.1 评价指标和仿真环境

为了有效地比较基本的按需路由(BOR)、SOR 及其改进协议,本文使用如下性能指标进行分析评价:

平均路由建立时间:从源节点发出路由请求包到最后接收到路由应答包的平均时间,用于评价协议的时间开销。

端到端包传输率:网络中所有目的节点收到的数据包与源节点发送数据包的比率,用于评价协议的有效性。

归一化路由开销:传输的路由控制包的总量与数据包总量的比值,即平均传输一个数据包所需的控制包的个数,用于评价协议的效率。

其它的指标如平均端到端延迟、平均延迟抖动、平均路由跳数等也经常用于评价路由协议的性能,但由于 SOR 主要为路由建立和维护过程提供安全保护,在这几个方面的性能和 BOR 差别不大,因此本文主要分析安全机制影响较大的三个性能指标。

通过网络仿真工具 Opnet 14.5 对一个典型的极轨道 LEO 卫星网络在 BOR、SOR 和 SOR-DVAP 协议下的路由性能进行分析,卫星网络主要的仿真参数见表 2。

表 2 仿真参数表

参数	值	参数	值
星座轨道数	6	每个轨道的卫星数	11
轨道倾角	86.4°	轨道高度	780km
轨道内链路数	2	轨道间链路数	2
星间链路带宽	10Mbps	数据包尺寸	1500Byte
数据传输比特率		200~1200Kbps	

在仿真过程中,每一个卫星节点任意选择一个目的节点并以某一传输比特率发送数据包,路由发现过程中使用“松约束”机制。当节点位于两极区域时,轨道间链路关闭。为了更具体直观的分析单个路由的性能,在仿真 1 中以分别位于北京(40N,116E)和南美布宜诺斯艾利斯(35S,58W)上方的两个 LEO 卫星 *A* 和 *B* 进行数据通信为例。在使用 DVAP 机制时,参数分别为 $p_0=0$,$CV_1=0.1$,$CV_2=0.2$,$\alpha=0$。

5.2 仿真结果与讨论

5.2.1 平均路由建立时间

网络中的路由建立时间主要由星间链路传输延迟、节点队列延迟和路由包处理延迟三个部分组成。星间链路传输延迟由节点之间的距离决定,队列延迟取决于网络中的通信流量,而路由包处理延迟则来源于对各种路由控制包的处理所需时间。分别考虑网络路由正常运行情况下 *A* 和 *B* 之间以及整个网络的平均路由建立时间。在 10 分钟的仿真时间内,每个节点每一分钟以另一任意节点为目的节点开始完整的路由发现过程,分别统计三种路由协议的时间开销,结果如图 3 所示。

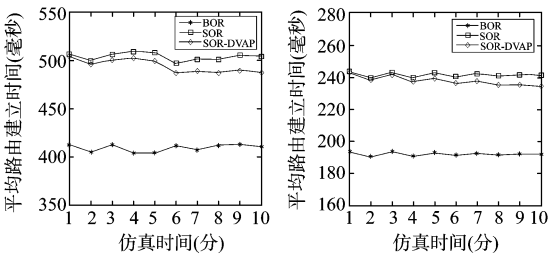

图 3　A 与 B 之间以及整个网络的平均路由建立时间

从图 3 可以看出,与基本的按需路由协议相比,SOR 协议的平均路由建立时间有所增加,其中 *A* 与 *B* 之间的路由发现时间大约增加了 22%,而整个网络的平均时间开销大约增加了 25%。这是因为 SOR 协议中的签密运算需要进行复杂的“对运算”操作,使得路由包处理时间显著延长,因此导致了平均路由建立时间的增长。在使用 DVAP 策略之后,两种情况下的时间开销比 SOR 分别减少 4% 和 3%,可见通过使用自适应概率性延迟验证,能够在一定程度上提高协议性能。

当卫星网络中的某条链路遭到外部攻击,比如注入了伪造的或者经过篡改的路由控制包,使用 BOR 协议可能导致经过该链路的路由发现无法完成或者得到错误的路径。而 SOR 及其改进协议由于能够抵抗外部攻击行为,因此路由发现时间基本不变或略微增加(外部的路由控制包的处理时间)。

5.2.2　端到端包传输率

路由协议正常运行时,安全机制的引入基本不会对端到端包传输率产生影响;但是当外部恶意攻击对路由发现或维护控制包进行操纵,从而使路由协议不能正常运行时,包传输率会显著降低。本文模拟恶意攻击伪造 *RREQ* 包情况下路由协议的性能。在网络中任意选择一个节点模仿外部节点,除了正常的路由功能以外,相比于正常的路由请求包,按照一定比例发送或转发伪造的 *RREQ* 包,仿真时间为 60 分钟。当伪造控制包的比率增加时,整个网络的平均端到端包传输率的变化情况如图 4 所示。

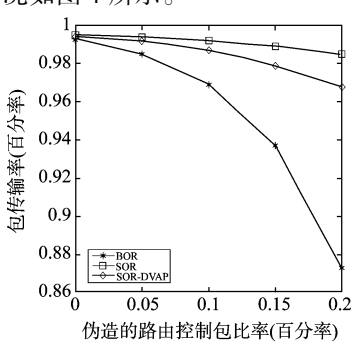

图 4　端到端包传输率

从图 4 可以看出,当网络中伪造的路由控制包的比率逐渐增大时,BOR 的端到端包传输率迅速下降,可见外部攻击影响了路由协议的正常运行,从而导致性能的剧烈下降。相反,SOR 协议由于能够识别出伪造的路由控制包,协议的正常运行基本没有受到外部攻击的影响,仍然能够得到较为稳定的高传输率。另外,因为可能存在的未验证的非法路由导致了数据包的少量丢失,运用 DVAP 机制的 SOR 协议的包传输率略微下降,但是下降幅度在可接受的范围之内。

5.2.3　归一化路由开销

路由开销包括用于路由发现和维护的所有 *RREQ*、*RREP* 和 *RERR* 控制包,体现了网络用于寻路的附加开销,通常用包开销和字节开销两种方式来衡量。图 5 显示了 60 分钟的仿真时间内不同伪造数据包比率情况下的归一化路由开销。

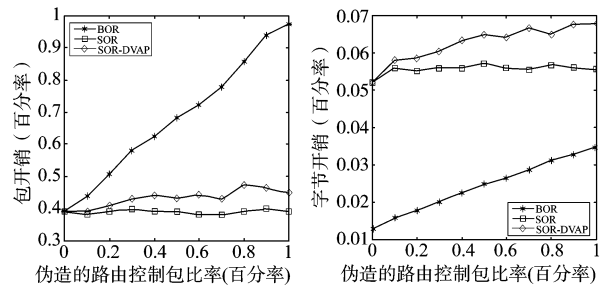

图 5　包开销和字节开销

如图 5 所示,在路由协议正常运行时,SOR 的包开销与 BOR 的包开销基本相同,这是因为 SOR 只是在 BOR 的基础上采取了安全措施,并没有增加路由控制包的数量;但是,由于使用的签密机制扩展了路由控制包的尺寸,将导致字节开销的增加,从图 5 中可以看出 SOR 的字节开销大约是 BOR 的 4 倍。另外,由于 BOR 的路由控制包的尺寸(不超过 100Byte)远小于网络数据包的尺寸(1500Byte),因此包开销和字节开销之间在数值上存在较大的差距。

当向网络中注入伪造的 *RREQ* 路由控制包时,SOR 协议由于能够及时将其识别出然后丢弃,包开销和字节开销基本不变,性能较为稳定;而 BOR 协议则会由于伪造路由请求包在网络中的不断扩散,从而导致包开销和字节开销迅速增加,不但消耗了可用的网络带宽而且降低了协议的有效性。从图 5 还可以看到,同 SOR 协议相比,使用 DVAP 机制后的协议在包开销和字节开销方面均有所增加,但增加的幅度非常有限,说明了 DVAP 机制对外部攻击的适应性,能够以少量的路由开销为代价,取得路由发现时间这一性能指标的

提升。

6 总结

针对 LEO 卫星网络按需路由面临的安全威胁,本文根据极轨道卫星网络拓扑和抽象出的星座系统模型的特点,通过引入基于身份的签密方案,设计了一种安全的按需路由协议 SOR,能够分别为协议的路由发现和路由维护提供安全保障。此外,为了减少协议的路由建立时间并同时提高对外部攻击的适应能力,本文在延迟验证方法的基础上提出了验证概率的自适应策略,并将其应用于 SOR 协议中。最后对协议进行了安全性分析和性能仿真实验,结果表明,虽然安全机制的引入带来了路由建立时间和路由开销的增加,但是 SOR 及其改进协议在外部攻击存在时仍然具有较高的安全性和稳定的包传输率,因此适合于 LEO 卫星网络。

参考文献

[1] Fatih Alagoz, Omer Korcak, Abbas Jamalipour. Exploring the routing strategies in next-generation satellite networks [J]. IEEE Wireless Communications,2007,14(3):79-88.

[2] 孙利民, 卢泽新, 吴志美. LEO 卫星网络的路由技术[J]. 计算机学报,2004,27(5):659-667.

[3] Evangelos Papapetrou, Stylianos Karapantazis, Fotini-Niovi Pavlidou. Distributed on-demand routing for LEO satellite systems[J]. Computer Networks, 2007, 51(15): 4356-4376.

[4] Stylianos Karapantazis, Evangelos Papapetrou, Fotini-Niovi Pavlidou. Multiservice on-demand routing in LEO satellite networks[J]. IEEE Transactions on Wireless Communications,2009,8(1):107-112.

[5] 万鹏,曹志刚, 王京林. LEO 星座网络动态源路由算法[J]. 宇航学报,2007,28(5):1295-1303.

[6] 李□, 刘军. 卫星网络安全路由研究[J]. 通信学报, 2006,27(8):113-118.

[7] Loay Abusalah, Ashfaq Khokhar. A survey of secure mobile ad hoc routing protocols[J]. IEEE Communications Surveys & Tutorials,2008,10(4):78-93.

[8] D. Bonh, M. Franklin. Identity-based encryption from Weil pairing[J]. Springer-Verlag LNCS, 2001(2139): 213-229.

[9] Hongmei Deng, Dharma P. Agrawal. TIDS: threshold and identity-based security scheme for wireless ad hoc networks[J]. Ad Hoc Networks,2004,2(3):291-307.

[10] Bok-Nyong Park, Wonjun Lee. ISMANET: A secure routing protocol using identity-based signcryption scheme for mobile ad-hoc networks[J]. IEICE Transactions on Communications,2005,88(6):2548-2556.

[11] Chuanrong Zhang, Zhonghai Yin, Yuqing Zhang. Secure AODV routing protocol using SL multi-signcryption[J]. Chinese Journal of Electronics,2007,16(2):311-314.

[12] 田野, 张玉军, 李忠诚. 使用对技术的基于身份密码学研究综述[J]. 计算机研究与发展,2006,43(10): 1810-1819.

[13] Eduardo Da Silva, Aldri L. Dos Santos, Luiz Carlos P. Albini, et al. Identity-based key management in mobile ad hoc networks, techniques and applications[J]. IEEE Wireless Communications,2008,15(5):46-52.

[14] P. S. L. M. Barreto, B. Libert, N. McCullagh and J. J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[J]. Springer-Verlag, LNCS,2005(3788):515-532.

[15] Fagen Li, Xiangjun Xin, Yupu Hu. Identity-based broadcast signcryption[J]. Computer Standards & Interfaces, 2008,30(1-2):89-94.

[16] Yong Yu, Bo Yang, Xinyi Huang, Mingwu Zhang. Efficient identity-based signcryption scheme for multiple receivers[J]. Springer-Verlag, LNCS,2007(4610):13-21.

[17] Manel Guerrero Zapata. Key management and delayed verification for ad hoc networks[J]. Journal of High Speed Networks,2006,15(1):93-109.

作者简介

彭长艳(1980-),男,博士研究生,主要研究方向为卫星网络和信息安全。
E-mail:pengchangyan@gmail.com

张 权(1974-),男,博士,副教授,硕士生导师,主要从事通信网络和信息安全领域的研究。

唐朝京(1962-),男,博士,教授,博士生导师,主要从事通信网络和信息安全领域的研究。