文章编号:1001 - 9081(2011)03 - 0781 - 03
doi:10.3724/SP.J.1087.2011.00781

卫星网络基于信任的认证路由协议

潘艳辉,王　韬,吴　杨,王文豪
(军械工程学院 计算机工程系,石家庄 050003)
(yanhuipan@126.com)

摘　要:安全路由协议是保障卫星网络安全运行的一个重要因素。针对现有卫星网络路由大多缺少安全机制的问题,运用基于椭圆曲线的签名方案保证路由报文的合法性,通过改进的信任评估机制排除内部恶意节点参加选路,设计了适用于高空通信平台(HAP)/低轨道(LEO)结构的层次式安全路由协议。分析表明该协议能够抵御多种常见的路由攻击。

关键词:卫星网络;椭圆曲线密码;信任;认证路由;路由安全
中图分类号: TP393.08　　**文献标志码**:A

Trust-based authentication routing protocol for satellite network

PAN Yan-hui, WANG Tao, WU Yang, WANG Wen-hao
(*Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang Hebei* 050003, *China*)

Abstract: Security routing protocol is a key element to guarantee satellite network security. To solve the problem that most of routing protocols lack security scheme, the Elliptic Curve Pintsov-Vanstone Signature Scheme (ECPVSS) was used to attain confidentiality and authentication of packets, and trust evaluation scheme could exclude internal malicious node from the route path. Then a security routing protocol oriented to High Altitude Platform (HAP)/Low Earth Orbit (LEO) architecture was formed. The analysis results show that the proposed protocol can prevent network from some common routing attacks.

Key words: satellite network; Elliptic Curve Cryptography (ECC); trust; authentication routing; routing security

0　引言

我国目前已经完成了多星组网运行实验,理论上具备了雏形星座的组网控制能力[1]。然而,由于卫星网络节点暴露于公共的空间环境中,以及其无线移动通信所固有的脆弱性,使得卫星网络安全问题突出。与传统网络一样,卫星网络的路由安全必须确保可用性、机密性、完整性、安全认证和抗抵赖性[2]。而不同的是,卫星网络有其自身的特点(拓扑结构动态性、节点间距离较远、误码率高等),使得传统地面网络的安全路由协议无法直接适用于空中的卫星网络。如何在拓扑结构动态变化,节点处理与存储资源有限的卫星网络中,设计理想的安全路由协议是卫星网络研究领域内的一大难点。研究并不断改进卫星网络路由的安全方法和策略,对卫星星座联网运行尤为重要。目前,对卫星网络安全保障机制的研究主要集中于基于密码学方法的卫星网络链路层安全加密方案[3-5],以及密钥管理与安全认证协议[6-10],然而对卫星网络安全路由的研究还不太完善,现有卫星网络路由协议,在设计过程中一般都没有考虑安全问题。

结合卫星网络的特点与安全需求,本文引入轻量级高安全性的签名方案——Elliptic Curve Pintsov-Vanstone Signature Scheme (ECPVSS)[11],结合改进后的信任评估方法,设计了一种层次式卫星网络安全认证路由,为卫星网络提供路由安全保障的同时,避免因加解密操作的冗余占用过多的网络资源。

1　相关研究分析

现有的卫星网络安全路由主要有两种机制。李喆等人[12]提出了一种基于信任的路由安全机制,其突出贡献是打破了卫星网络拓扑节点总数固定不变的传统假设惯例,安全机制能够检测到节点遭受的恶意攻击;但其属于攻击事后检测,采取补救措施降低攻击范围的大幅度扩展。文献[13]中提出了事前攻击防御措施,采取基于身份的签密方案设计了适合低轨道(Low Earth Orbit, LEO)卫星网络特点的安全按需路由协议,来解决由于外部攻击而产生的各种路由安全问题,并采用"紧约束"与"松约束"结合的方案降低路由开销;但该协议是建立在卫星网络节点总数固定不变的基础之上的,仅适用于 LEO 卫星网络,其可靠性与扩展性有待完善。而且它们都针对单层卫星网络,虽然多层卫星网络可以应用单层卫星网络的安全方法,但由于涉及不同层次卫星节点之间的管理以及信息交互等问题。随着多层卫星网络技术的发展,有必要设计适用于多层卫星网络的安全协议。卫星网络路由研究者们取得的共识是卫星网络与移动自组织网络(Mobile Ad Hoc Network, MANAT)存在相似之处,借鉴 MANAT 先进的安全技术,结合应用环境进行改进以适用于卫星网络是一种有效的途径[14]。

2　信任度量与 ECPVSS 签名

2.1　信任度量方法

文献[12]中介绍了对路由信息信任的评价方法,由于认证路由主要是对路由协议的控制信息,如路由请求(Route Request, RREQ)报文、路由应答(Route Reply, RREP)报文、路由失效(Route Error, RRER)报文等,进行签名、认证和完整性校验来保证路由协议的正常工作,因此,本文对路由信息

收稿日期:2010 - 09 - 16;**修回日期**:2010 - 11 - 14。　**基金项目**:国家自然科学基金资助项目(60772082)。
作者简介:潘艳辉(1982 -),女,湖北广水人,博士研究生,主要研究方向:网络安全、卫星网络路由;　王韬(1964 -),男,河北石家庄人,教授,博士生导师,主要研究方向:网络安全;　吴杨(1985 -),男,四川成都人,硕士研究生,主要研究方向:卫星网络安全认证协议。

的评估进一步细分为:路由请求、路由应答、路由维护行为的评估,根据其对三类路由控制报文的处理行为进行评估,综合信任度的计算如式(4)所示:

$$R_{\mathrm{RREQ}}=\begin{cases}(NS_{\mathrm{RREQ}}-NF_{\mathrm{RREQ}})/(NS_{\mathrm{RREQ}}+NF_{\mathrm{RREQ}}), & NS_{\mathrm{RREQ}}+NF_{\mathrm{RREQ}}\neq 0\\ 0, & NS_{\mathrm{RREQ}}+NF_{\mathrm{RREQ}}=0\end{cases}\tag{1}$$

$$R_{\mathrm{RREP}}=\begin{cases}(NS_{\mathrm{RREP}}-NF_{\mathrm{RREP}})/(NS_{\mathrm{RREP}}+NF_{\mathrm{RREP}}), & NS_{\mathrm{RREP}}+NF_{\mathrm{RREP}}\neq 0\\ 0, & NS_{\mathrm{RREP}}+NF_{\mathrm{RREP}}=0\end{cases}\tag{2}$$

$$R_{\mathrm{RRER}}=\begin{cases}(NS_{\mathrm{RRER}}-NF_{\mathrm{RRER}})/(NS_{\mathrm{RRER}}+NF_{\mathrm{RRER}}), & NS_{\mathrm{RRER}}+NF_{\mathrm{RRER}}\neq 0\\ 0, & NS_{\mathrm{RRER}}+NF_{\mathrm{RRER}}=0\end{cases}\tag{3}$$

$$R=\frac{1}{3}(R_{\mathrm{RREQ}}+R_{\mathrm{RREP}}+R_{\mathrm{RRER}})\tag{4}$$

其中:R_{RREQ} 是评价节点转发路由请求报文行为的信任度,用于度量节点发送路由拥塞控制报文的行为;R_{RREP} 是评价节点转发路由应答报文行为的信任度,用于度量节点发送路由欺骗报文的行为,以用于度量节点发送路由“吸收报文”产生“黑洞”攻击的行为;R_{RRER} 是度量节点转发路由失效报文行为的信任度,检测节点发送伪失效数据包,引起源节点不断重新发送路由请求,从而进行路由破坏攻击;NS 是成功转发报文的次数;NF 是转发报文失败的次数。

2.2 ECPVSS 签名方案

ECPVSS 是基于椭圆曲线的具有消息恢复特性的签名方案,研究表明它是一种比传统方案安全性更高、轻量级的安全机制[16-17],因而能够适用于像卫星网络这样的特殊应用环境。文献[18]详细介绍了其签名与验证的方法,不在此赘述,本文用 $Sign_S$ 表示节点 S 基于 ECPVSS 的签名。

3 基于信任的卫星网络认证路由

3.1 HAP/LEO 卫星网络模型

相对卫星系统而言,高空通信平台(High Altitude Platform, HAP)是在平流层(距地高度一般为 17 ~ 22 km)使用的一种新的通信手段,具有往返延迟短、容量大、费用低等优点,特别适合应用于地面通信需求集中及有特殊任务需求的地区,是发展空间信息网络的重要组成部分[15]。鉴于此,本文采用了 HAP/LEO 结构的卫星网络模型,如图 1 所示,据此设计安全认证路由协议,为多层次卫星网络提供安全保障。但安全协议的引入,无疑会影响卫星网络的通信效率,卫星节点星上存储与计算资源有限性需要权衡安全与性能两方面的因素。

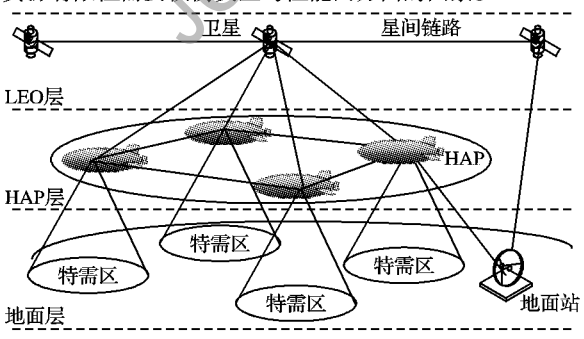

图 1 HAP/LEO 网络模型

本文假设系统具有安全的密钥管理协议;上层 LEO 卫星节点是完全可信的,承担对 HAP 的管理功能。符号说明:S 表示源节点;D 表示目的节点;$X1, X2, \cdots, Xn(n \in \mathbf{Z}^*)$ 表示 S 与 D 之间的中间节点;ID 表示节点的标示号。每个 HAP 节点进入网络之前,通过 LEO 卫星(假设为节点 C)进行认证后方可获得一个证书,证书格式如下:

$$Cert_A = Sign_C[ID_A, KP_A, t\_cur, t\_val]$$

其中:字段 t_cur 记录证书的生成时间,t_val 表示证书的有效期。

3.2 路由建立过程

1)源节点请求。

步骤 1 S 通过 D 的信任度 R_D 判断是否为恶意节点。如果是则继续,否则放弃路由请求。

步骤 2 S 生成 $RREQ$,包含:数据包的类型为路由发现数据包(Router Data Packet, RDP)、S 与 D 的标识 ID_D 与 ID_S、报文序号 N_S、证书 $Cert_S$,报文生成时间 t,定义如下:

$$RREQ:[RDP, ID_D, ID_S, Cert_S, N_S, t]$$

步骤 3 S 对 $RREQ$ 进行签名后向其邻居广播发送。

$$S \rightarrow Brdcst: Sign_S[RDP, ID_D, ID_S, Cert_S, N_S, t], Cert_A$$

2)中间节点处理。

步骤 1 $X1$ 验证。通过 S 的信任度 R_S 判断:是否为恶意节点 & 证书签名的正确性 & 证书是否过期 & 报文的新鲜性,若为真则记录其上游节点以建立反向路径,以便收到应答消息能转发回源,继续执行,否则丢弃报文。

步骤 2 $X1$ 对收到的 RDP 进行签名将自己的证书附在其后,并继续广播转发如下:

$$X1 \rightarrow Brdcst: Sign_{X1}[Sign_S[RDP, ID_D, ID_S, Cert_S, N_S, t], Cert_A], Cert_{X1}$$

步骤 3 $X2$ 对收到的 RDP 包进行步骤 1 的检验,如果通过检验则 $X2$ 将 $X1$ 的签名和证书移除,并进行步骤 2 的操作:

$$X2 \rightarrow Brdcst: Sign_{X2}[Sign_S[RDP, ID_D, ID_S, Cert_S, N_S, t], Cert_A], Cert_{X2}$$

步骤 4 重复步骤 3,直至到达目的节点。

3)目的节点应答。

步骤 1 D 通过 S 的信任度 Xn(假设其为 D 的上一个节点)判断:是否为恶意节点 & 证书签名的正确性 & 证书是否过期 & 报文的新鲜性。如果是则继续,否则丢弃该路由请求报文。

步骤 2 D 生成 $RREP$,包含:S 与 D 的标示、报文序号 N_D、证书 $Cert_D$,报文生成时间 t,定义如下:

$$RREP:[REP, ID_S, ID_D, Cert_D, N_D, t]$$

步骤 3 D 沿着相反的路径向源节点传送 REP 包,然后上游节点依序进行检测并向 S 方向转发。

$$D \rightarrow Xn: Sign_D[REP, ID_S, ID_D, Cert_D, N_D, t], Cert_D$$

3.3 路由维护过程

1)路由失效或链路发生断裂。

S 发现与某个邻居节点的链路中断后生成错误消息,签名后向其邻居广播发送,如果存在上游节点则继续广播,其处理与上述报文请求过程类似。

2)节点安全隔离。

该协议增加了安全隔离功能,当 S 发现其邻居节点 $X1$ 的信任度低于阈值时,也生成 ERR 消息,并进行签名后向其他节点广播,更新其他节点中 $X1$ 的信任度值。

4 算法安全性与性能分析

4.1 安全性分析

1)重放攻击。由于路由控制报文中有序列号保证报文的新鲜性,能够过滤掉重放的旧报文。

2)伪造及篡改攻击。基于 ECPVSS 签名的安全性保证报文不会被篡改和伪造。

3)拒绝服务攻击。信任值的度量能够检测数据报文非

正常的大量转发。

4)中断攻击。中断攻击者选择丢弃控制报文后其信任值会逐渐降低,系统将会隔离此类节点,从而在一定程度上遏制了这种攻击。

4.2　性能分析与仿真

1)对于路径的评价。

由于源节点按照收到的第一个 RREP 建立路径,因而能够保证选择时延最小的路径。同时说明,能够由 HAP 承担的业务不会经过卫星节点的转发,因为 HAP 之间的传输时延较小,而协议总是会选择时延较小的路径。这对于负载相对集中的地区来说,用费用相对低廉的 HAP 能够解决卫星网络的负载均衡问题。

2)仿真设计与分析。

现有仿真软件不直接支持 HAP/LEO 网络仿真,NS-2 的开源性使得它具有良好的可扩展性,而且能够支持卫星网络仿真。结合其中地面移动节点和卫星节点、链路的实现过程,实现 HAP 节点及链路。LEO 与 HAP 之间能够建立链路的条件是:

$$2\cdot\arcsin\left(\frac{|S'H|}{R_E+h_H}\right)\leqslant 90-\varepsilon_{\min}-\arcsin\left(\frac{R_E+h_H}{R_E+h_S}\cdot\cos(\varepsilon_{\min})\right)\quad(5)$$

其中:R_E 表示地球半径;h_H 是 HAP 节点的高度;h_S 是卫星节点的高度;S' 是卫星节点在 HAP 节点上覆盖区的抽象投影点,$\varepsilon_{\min}$ 是 HAP 节点的最小仰角。仿真场景采用 24 个 LEO 节点和 16 个 HAP 节点,以拒绝服务路由表溢出攻击为例,在不同攻击程度(攻击节点数不同)下对采用安全机制前后的网络性能进行仿真分析,如图 2 所示,安全机制能够有效遏抑攻击行为对网络性能的影响,保证数据的正常传输。

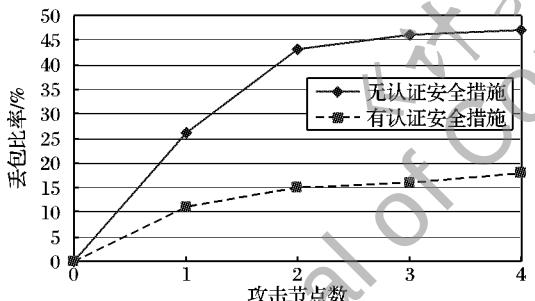

图 2　网络丢包率

5　结语

研究表明在卫星网络中信任机制和认证机制都能够提高卫星网络路由的安全性,是实现安全路由的保障,但它们能够抵御的攻击类型都存在局限性。本文通过信任机制与认证机制的结合,提出了适用于卫星网络,基于信任的认证安全路由协议,能够在一定程度上防止常见攻击的发生,但安全机制的引入(如加解密操作和信任的评估)不可避免地增加了路由开销,如何提高协议效率需进一步完善。

参考文献:

[1] 徐志博, 马恒太. 一种用于卫星网络安全认证的协议设计与仿真[J]. 计算机工程与应用, 2007, 43(17): 130 – 132.

[2] 吴举, 杜学绘, 钱雁斌, 等. 改进的空间网络密钥交换协议[J]. 计算机工程, 2009, 35(18): 113 – 115.

[3] 吴志军, 阚洪涛. 基于 ECC 的 TES 网络链路层安全协议的研究[J]. 通信学报, 2009, 30(11): 86 – 92.

[4] 向红权. 一种卫星通信链路的加密技术实现研究[D]. 西安: 电子科技大学, 2007.

[5] 杨揆. 应急系统中卫星通信椭圆曲线安全算法的研究[D]. 合肥: 合肥工业大学, 2007.

[6] ARSLAN M G, ALAGÖZ F. Security issues and performance study of key management techniques over satellite links [C]// Proceedings of the 11th Intenational Workshop on Computer-Aided Modeling, Analysis and Design of Communication Links and Networks. Trento: IEEE Press, 2006: 122 – 128.

[7] ROY-CHOWDHURY A, BARAS J S. A lightweight certificate-based source authentication protocol for group communication in hybrid wireless/satellite networks [C]// Global Telecommunications Conference. New Orleans: IEEE Press, 2008: 1 – 6.

[8] 张志强, 张永健, 王宇. 低轨卫星网络中基于轨道分簇的密钥更新算法[J]. 电子与信息学报, 2010, 32(3): 687 – 692.

[9] 冯涛, 马建峰. UC 安全的移动卫星通信系统认证密钥交换协议[J]. 宇航学报, 2008, 29(6): 1959 – 1964.

[10] 罗长远, 李伟, 邢洪智. 空间网络中基于身份的分布式密钥管理研究[J]. 电子与信息学报, 2010, 32(1): 183 – 188.

[11] PINTSOV L A, VANSTONE S A. Postal revenue collection in the digital age [C]// FC 2000: Proceedings of the 4th International Conference on Financial Cryptography, LNCS 1962. Berlin: Springer, 2001: 105 – 120.

[12] 李喆, 刘军. 卫星网络安全路由研究[J]. 通信学报, 2006, 27(8): 113 – 119.

[13] 彭长艳, 张权, 唐朝京. LEO 卫星网络中一种安全的按需路由协议[J]. 信号处理, 2010, 26(3): 337 – 346.

[14] 李喆, 李冬妮, 王光兴. LEO_MEO 卫星网络中运用自组网思想的动态路由算法[J]. 通信学报, 2005, 26(5): 50 – 57.

[15] 张登银, 刘升升. 基于 Mesh 的空间信息网体系结构研究[J]. 计算机技术与发展, 2009, 19(8): 69 – 74.

[16] 阚元平. 基于椭圆曲线的具有消息恢复特性的签名方案[J]. 计算机工程与科学, 2010, 32(2): 58 – 59.

[17] YAVUZ A A, ALAGÖZ F, ANARIM E. A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption [J]. Turkish Journal of Electrical Engineering and Computer Science, 2010, 18(1): 1 – 11.

[18] YAVUZ A A, ALAGÖZ F, ANARIM E. A new satellite multicast security protocol based on elliptic curve signatures [C]// Proceedings of the 2nd IEEE International Conference on Information Communication Technologies. Damascus: IEEE Press, 2006: 2512 – 2517.

(上接第 780 页)

[3] 王金朋. 工作流建模方法及模型验证方法的研究[D]. 秦皇岛: 燕山大学, 2009.

[4] 文俊浩, 饶锡如, 何盼, 等. 基于工作流的服务组合在电子政务中的应用[J]. 计算机应用, 2009, 29(9): 2512 – 2515.

[5] 魏立峰, 孟凯凯, 何连跃. 面向用户角色的细粒度自主访问控制机制[J]. 计算机应用, 2009, 29(10): 2809 – 2811.

[6] 王福, 沈寒辉, 邹翔. 基于 IRBAC 的跨域角色映射方法[J]. 计算机应用, 2010, 30(z1): 106 – 108.

[7] 李斓, 范磊, 回红. 行为驱动的基于角色的信任管理[J]. 软件学报, 2009, 20(8): 2298 – 2306.

[8] 宋春燕, 徐建良, 李申华. 基于角色的安全工作流模型[J]. 计算机工程, 2008, 34(21): 139 – 140.

[9] 王博, 张莉. 基于角色权限的业务过程协同建模方法[J]. 计算机工程, 2009, 35(13): 14 – 16.

[10] 单徐梅, 虞慧群. 基于 RBAC 的工作流管理系统授权约束方法[J]. 计算机工程, 2010, 36(4): 152 – 154.