第 45 卷第 1 期
2013 年 2 月

南 京 航 空 航 天 大 学 学 报
Journal of Nanjing University of Aeronautics & Astronautics

Vol. 45 No. 1
Feb. 2013

一种新的赛博空间安全交互方法

周 未 张 宏 李千目 郭 萍
(南京理工大学计算机科学与技术学院,南京,210094)

摘要:现有的网络协议无法满足赛博空间的安全交互的需求,特别是节点的证书变更和移动性会造成安全交互的失败。本文针对传统体系中证书变更较慢的缺陷提出一种适合于赛博空间组网的扩散式证书变更方案。对传统协议中的私钥分量生成、数据安全传输方案进行优化,完善了传统协议中的证书撤销协议和节点定期通告存在协议,弥补了以往在分布式安全交互过程中由于节点的强移动性而导致的安全交互失败问题,提高了安全交互的成功率。最后,对新方法的安全性、性能等问题进行了对比分析。

关键词:赛博空间;协议设计;安全交互;证书
中图分类号:TP393.02 **文献标志码**:A **文章编号**:1005-2615(2013)01-0116-08

New Security Interaction Method for Cyberspace

Zhou Wei, *Zhang Hong*, *Li Qianmu*, *Guo Ping*
(College of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing, 210094, China)

Abstract: Existing network protocols can not meet the demand of the interaction of cyberspace security, in particular, the certificate change and mobility of the nodes cause the failure of the security interaction. A suitable diffusion certificate change program for networking of cyberspace is given to solve the defect of slower certificate change in the traditional networks system. The program optimizes the mode of private key generation and data security transmission scheme, improves the traditional protocol of certificate revocation protocol and node regularly notice, and solves the interaction of security failures in distributed security interaction due to the strong mobility of the nodes, improves the success rate of the security interaction. Finally, comparative analysis on security, performance and other issues of new method are given.

Key words: cyberspace; protocol design; security interaction, certificate

信息安全的重要性越来越突出。近年来,震网、火焰蠕虫等由于其高度的复杂性、攻击的针对性引起学术界的广泛关注,信息安全学科进入了全新的阶段,其中赛博空间的安全问题越来越引起人们的重视。美国政府先后公布了总统令:国家 Cybersecurity 全面倡议与 Cyberseurity 研究路线图等文件指导美国学术界、产业界的研究工作,也反映了美国政府对该问题的高度重视。赛博空间的控制、攻击、防御能力,既反映了一个国家对信息空间的控制管理能力,也是一个国家国防能力的一个重要方面[1-2]。

导弹作为一种攻击作用巨大的武器,从战术打击到战略打击以及战略威慑都有着不可低估的能力,一直以来都处于各国武器装备发展的尖端地位。现代战争是体系与体系对抗的信息化战争,因此,美军提出传统意义上的作战体系构成元素可以由导弹自身代替,可以根据作战任务的不同,将导弹组成的攻击体系划分为指挥控制系统、电子对抗系统、通信

基金项目:国家自然科学基金(60903027)资助项目。
收稿日期:2012-05-23;**修订日期**:2012-09-12
通信作者:周未,男,博士研究生,工程师,1979 年出生,E-mail:zhou_ziheng@126.com。

保障系统和战场信息侦察系统等,最终这些系统便构成了一种全新的导弹智能作战体系。在这种全新的导弹智能作战体系概念引导下,赛博空间组网系统需求应运而生。该技术要能够使得多攻击武器系统在脱离了我方作战支援系统有效范围情况下自成攻击体系,这就需要提高所有攻击系统之间的通信能力,并且调动每个攻击系统的计算能力,实现高度信息共享,将传感器网络与信息融合相结合,为作战决策提供更为准确的战场态势评估。

在需求层面,赛博空间组网系统中,由于导弹节点身份和位置信息同时暴露的意义远大于单独的身份信息或者位置信息暴露,因此保护导弹的位置隐私就是要保证敌方不能获得特定导弹节点的身份和位置信息。另外,为了保障路由安全,相关数据必须是可验证和仲裁的[3-4]。因此,也可以说赛博空间的安全也包含了它独特规则或者说法律[5]。在研究层面,Zhou 和 Hass[6]提出了基于公钥基础设施(Public key infrastructure,PKI)技术的密钥管理服务体系的概念模型,给出不信任分散原理的思想,但是在这种方式下,单个 dealer 拥有认证权威(Certrfication authority,CA)的完整私钥信息,如果其被暴露将危及整个网络的安全。Yi 和 Kravets[7]提出了一种通用的移动认证权威(Mobile certification authority,MOCA)架构,其本质上与 Hass 模型类似,只是进一步阐明服务节点的选择标准,以提高体系的可用性,同时该方案也存在与 Hass 模型相似的问题。Capkin 等人[8]提出了不同于前面两种分布式安全交互机构的结构方案,称为自组织 PKI,这是一种完全自组织形式的方案,它与 Zimmermann[9]在完美隐私(加密系统)(Pretty good privacy,PGP)的官方指导手册中的方法不完全相同,它没有采用集中式或分布式安全交互机构(CA)的概念,而是由用户自己担任 CA,完成公钥/私钥对的产生和各种证书服务。此外,这个方案没有集中式的证书目录服务器,而是由每个用户自己维护一个本地证书库,包括该用户颁发给其他用户的证书及其他用户颁发给该用户的证书等,证书的颁发是基于用户之间的信任。当两个没有预先关系的用户希望进行安全通信时,通过组合双方自己的本地证书库,并从中找出一条连接两个用户的证书链,利用中间用户作为推荐代理,完成双方公钥的获取和验证,从而建立起双方之间的信任关系。该方案具有较高的可伸缩性,可适应网络规模的动态变化。在网络形成初期,由于已颁发证书数量的不足可能造成在两个用户之间无法找到一条可信证书链,使体系可用性受到影响。Mosco 和 Deibert 等人[10-12]更加全面的研究了包括赛博空间组网和宏观层面的访问控制策略的修剪规则。

本文针对性地研究了赛博空间的安全交互方法和模型。主要贡献包括对传统协议中的私钥分量生成、数据安全传输方案进行了优化,针对传统体系中体系证书变更较慢的缺陷提出一种适合于赛博空间组网的扩散式证书变更方案,完善了传统协议中的证书撤销协议和节点定期通告存在协议,给出了一套适合赛博空间组网通信的无中心自组织安全交互方案。

1　赛博空间组网的安全交互

2006 年 12 月,美国参联会发布赛博空间行动国家军事战略,提出赛博空间是"通过网络化系统及相关的物理基础设施,利用电子和电磁频谱存储、修改并交换数据的领域。而关于赛博空间最新定义则描述赛博空间是一个物理域,该域通过网络系统和相关的物理性基础设施,使用电子和电磁频谱来存储、修改或交换数据。

从目前对赛博空间定义可以看到,赛博空间已从单纯的计算机网络扩展到无形的电磁频谱,是处于电磁环境中的一种物理领域。因此,在赛博空间中的战斗并非创造虚拟效果或在某种虚拟现实中攻击敌人,而是包括了物理作战,将产生非常真实的作战效果。其中的安全问题至关重要,本节主要从以下几个方面讨论赛博空间组网的安全问题。对比现有的伪名变更方法,本文方法可以让关系链的存储更加平均化,可以避免某个分布式节点存储过长的关系链。此外改进变更方法可以防止由于某个分布式节点被攻破而导致完整的伪名关系链泄露。在性能方面的改进则主要体现在,一方面新协议对数据安全传输的方法进行了优化,相比较传统协议省去了一次解密运算的开销,提高了速度。另一方面新的扩散式证书变更方案,相比较传统协议中一个接着一个顺序申请证书部分签名的方案,加快了证书变更的速度。

(1)证书变更

在赛博空间组网安全交互中,每张证书都有有效期,所以每个节点都会定期变更自己的证书。这里包括两类证书的变更:①节点用自己的私钥签发的对信任节点的证书,即形成信任链的证书,这些证书到期后需变更;②分布式 CA 签发给节点的证书,称之为节点安全交互证书,其中包含节点的公

钥等信息,这些证书到期后也需要变更。

第一类证书的变更:即形成信任链的证书变更。因为这类证书是节点自己签署并发放给其他节点的,所以由发放者自己定期变更,并保存证书变更记录。每隔一段时间,节点检查自己签署的证书的有效期,如果发现有即将过期的证书,就对证书重新签名,并变更它的有效期。当收到其他节点发来的证书变更请求时,发放者将已变更的相应证书发放给请求者就可以了,如图1所示。

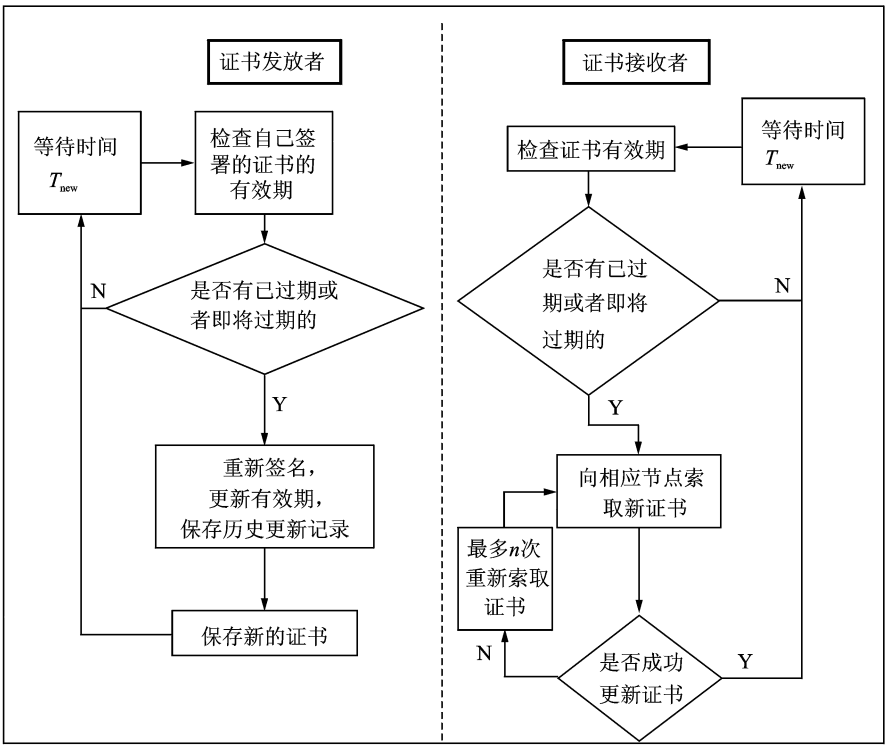

图1 形成信任链的证书变更

第二类证书的变更:即节点安全交互证书,用于确认节点身份的证书。该证书是通信域对节点身份的确定,证书的变更需要分布式CA节点的重新签名。流程图示意如图2所示。

(2)伪名变更

在"证书变更"中,节点 N 体系证书变更过程中,会收到多个分布式CA节点返还的包含部分签名的报文。在这些报文中,实际上还会包含一个值,表示该CA节点当前存储的伪名关系链的长度。伪名关系链就是用来记录某个节点新旧伪名之间的关系。N 在完成体系证书变更后,也会知道参与部分签名的分布式CA节点中伪名关系链的长度。选取其中伪名关系链最短的 n 个节点(n 可由管理员在体系中配置),例如 $n=3$。首先选取3个中的某一个,例如选取 CA_1,通过匿名双向安全交互建立信任关系,由 CA_1 根据新证书中公钥 PK_N 的若干位计算生成新的压缩布隆过滤器(Compressed bloom filter)值,并广播给域内所有节点,同时存储新的伪名关系链。接着 N 与剩余两个节点通过匿名双向安全交互建立信任关系,告知其需要存储新的伪名关系链。

(3)邻近节点通告

为了确认通信域内节点的真实存在,及时发现失效节点,并防止节点被俘获后冒充原节点混在通信域内,尽可能地保证通信域的安全性,节点必须周期性地向相邻节点广播报文,通告其存在。由于是在赛博空间组网中,节点间通信靠的是报文的转发。所以相邻节点指的是在 r 跳以内的节点,r 可以设置,若设置为1,则节点的报文仅能发送给与发送者直接相邻的节点。每个节点保存有一张节点活跃度列表。列表的存储结构如下:

条目序列号	节点历史伪名	节点当前伪名	节点最近活跃时间

其中

条目序列号:节点活跃度列表的条目序列号,类似于ID的作用,不可重复。

节点历史伪名:定期通告存在的节点若更改了

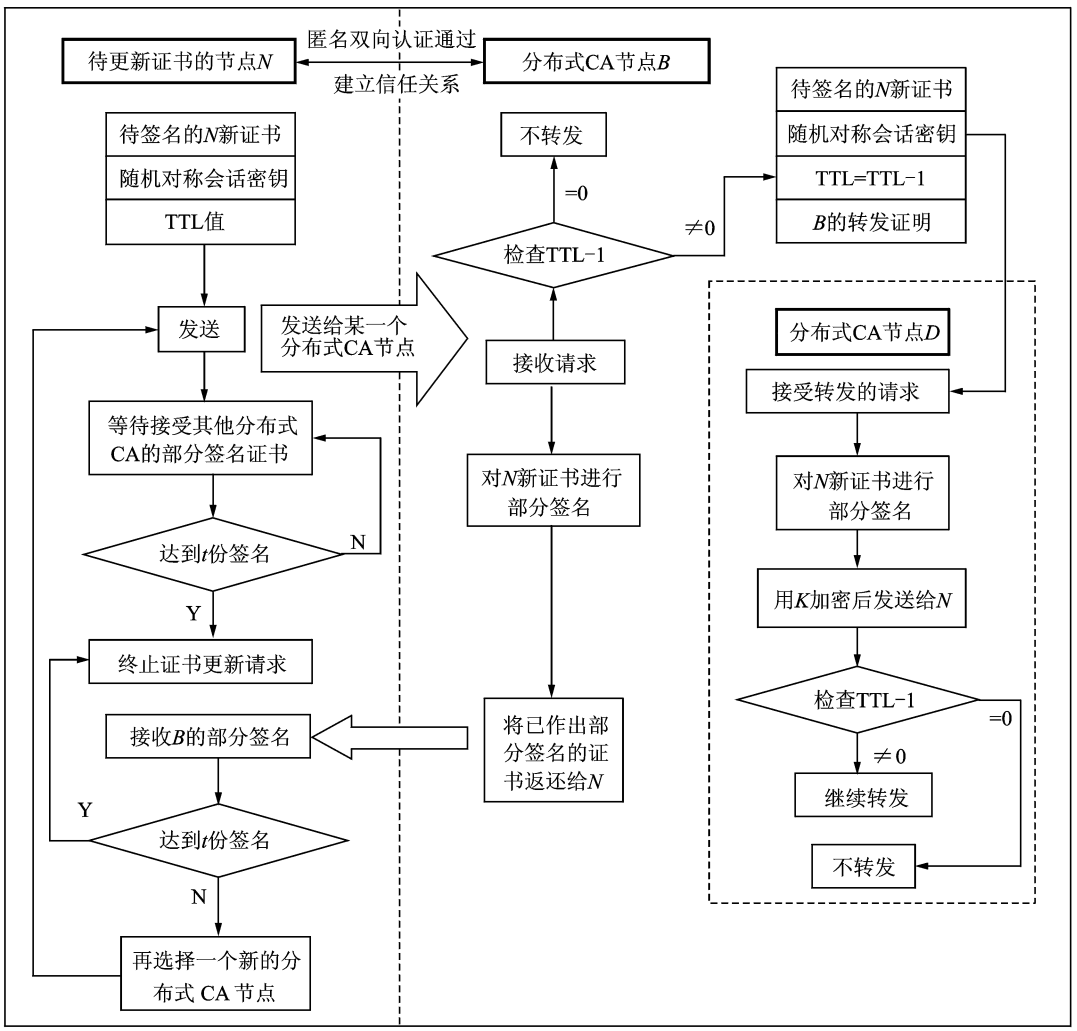

图 2　节点安全交互证书变更流程图

伪名,此条目存储该节点的历史伪名。历史伪名的存储个数应进行限制,一般 2～3 个即可。

节点当前伪名:存储定期通告存在的节点当前伪名。

节点最近活跃时间:节点上一次通告其存在的时间。

上述内容在广播前,必须由节点进行数字签名:即对所有内容执行散列函数运算得出摘要,再用节点的私钥加密,以防止传播过程中被篡改。假定有某节点接收到 A 的广播报文,则该节点首先使用 Compressed bloom filter 验证该 A 的伪名。验证通过后用域公钥 PK 验证 A 的证书。最后验证该报文内容的数字签名,确保报文未被篡改。然后根据报文内容中的"当前伪名"查找节点活跃列表,若有该条目,则变更节点最近活跃时间;若没有,则用报文内容中的"前一次使用的伪名"查找节点活跃列表。若有该条目,说明节点在两次通告的时间间隔里有变更过伪名,则变更列表中节点当前伪名和历史伪名两项,变更节点最近活跃时间;若没有,则用证书中的伪名创建一个新条目,记录该节点最近活跃时间。其过程详见算法 1。

算法 1　邻近节点通告算法

广播通告其存在的节点 A

While TRUE

SysCertificate=GetSystemCertificate(A)　//体系证书

PrevPseudoName=GetPreviousPseudoName(A)　//前一次伪名

CurPseudoName = GetCurrentPseudoName(A)　//当前伪名

DigitSign=CreateDigitalSignature(A)　//数字签名

BroadMessage = CreateMessage(SysCertificate, PrevPseudoName, CurPseudoName, DigitSign)　//生成广播报文

Broadcast(BroadMessage)//广播该报文

Sleep(t)//间隔时间 t

```
End While
报文接收者节点 B
ReceiveBroadMessage(&BroadMessage) //接收报文
If CBFVerify(BroadMessage.CurPseudoName) And CBF-
Verify(BroadMessage.PrevPseudoName) And PKVerify
(BroadMessage.SysCertificate,PK) And Verify(Broad-
Message.DigitSign)//CBF、A 的证书验证以及数字签字验
证
Then//通过验证
  CurActList=FindActivityList(BroadMessage.CurPseud-
oName) //查找节点活跃列表
  If ! Empty(CurActList)//非空,表示条目存在
  Then
    UpdateActivityTime() //更新最近活跃时间
  Else
    PrevActList=FindActivityList(BroadMessage.PrevP-
seudoName)
    If ! Empty(PrevActList)
    Then
      UpdatePseudoName(BroadMessage.PrevPseud-
oName,BroadMessage.CurPseudoName)//更新伪名
      UpdateActivityTime()
    Else
      CreateNewItem(BroadMessage.PrevPseudoName,
BroadMessage.CurPseudoName,ActivityTime)
    End If//End If ! Empty(PrevActList)
  End If//End If ! Empty(CurActList)
Else
  Abandon(BroadMessage);//丢弃该报文
End If//End If CBFVerify…
```

(4)节点消亡

节点自身会周期性地检查节点活跃列表,假定为节点 A,A 发现存在某些条目已经很久没有变更,即长时间未收到该条目对应节点通告其存在的报文,则广播一条信息,向其他节点征询是否有该节点的信息。若等待一段时间后,无来自其他节点的反馈信息,A 判定该条目对应节点已消亡,则 A 向邻近的一个分布式 CA 节点通告有节点消亡的信息。具体步骤如下所述:

(1)节点 A 周期性地检查节点活跃列表。若发现有条目很久没变更,则广播报文,向其他节点查询该节点是否存在。报文内容包括:待检查伪名,A 的体系证书和伪名。报文还应附上 A 对报文内容的数字签名,防止传输过程中被篡改。若不存在长时间未变更的节点,则等待一定时间后重复检查列表。

(2)节点 B 收到 A 广播的查询信息。首先使用 Compressed bloom filter 验证 A 的伪名。验证通过后用域公钥 PK 验证 A 的证书。最后验证该报文内容的数字签名,确保未被篡改。

(3)节点 B 根据广播报文中的待检查伪名检查自己的节点活跃列表。

(4)节点 A 等待接收反馈报文。

若未收到任何反馈信息,则 A 向邻近的分布式 CA 节点通告有节点消亡的信息。节点消亡协议详见算法 2。

算法 2 节点消亡算法

```
  节点 A
If CheckUpdate(ActivityList)//检查,有条目未更新?
Then
  ToCheckPseudoName=GetToCheckPseudoName()
  SysCertificate=GetSystemCertificate(A)//体系证书
  PseudoName=GetCurrentPseudoName(A)//伪名
  DigitSign=CreateDigitalSignature(A)//数字签名
  BroadMessage=CreateMessage(ToCheckPseudoName,
SysCertificate,CurPseudoName, DigitSign)//生成广播报
文
  Broadcast(BroadMessage)//广播该报文
  DealFeedback();//调用处理反馈的线程
  Wait(t) //等待时间 t
Else
  Wait(t) //等待时间 t
End If//End if Check…
处理反馈的线程 DealFeenback
While TRUE
  If TimeOut()
  Then//超时
    CANode=GetNearCANode()
    DeadMessage=CeateDeadMessage()
    Notify(CANode,DeadMessage) //联系 CA,告知节点
死亡
    Break//中断循环,超时退出
  End If//End If TimeOut…
  FeedbackMessage=ReceiveMessage()
If ! Empty(FeedbackMessage) //非空,收到反馈
Then
  If CBFVerify(FeedbackMessage.PseudoName) And PK-
Verify(FeedbackMessage.SysCertificate,PK) And Verify
(FeedbackMessage.DigitSign)
  Then//通过验证
    If FeedbackMessage.Type==NodeUnDead
    Then DeleteItem(ActivityList)//删除该条目
    Else If FeedbackMessage.Type==PseudoNameUp-
date Then
      UpdateItem(ActivityList, PseudoName, Activity-
Time)
```

```
    End If//End If FeedbackMessage…
    Break;//反馈处理结束,中断循环
  Else Abandon(FeedbackMessage) //丢弃该报文,继续等待接收反馈
      End If//End If CBFVerify…
    End If//End If ! Empty…
  End While
节点 B
ReceiveBroadMessage(&BroadMessage) //接收报文
If CBFVerify(BroadMessage.PseudoName) And PKVerify(BroadMessage.SysCertificate, PK) And Verify(BroadMessage.DigitSign)//CBF、A 的证书验证以及数字签字验证
Then//通过验证
  CurPseudoNameItem=CheckList(BroadMessage.PseudoName) //检查节点 B 列表"节点当前伪名"一项
  If ! Empty(CurPseudoNameItem)//非空,表示对应条目存在
  Then
    If Expire(CurPseudoNameItem)//过期
    Then
      DeleteItem(CurPseudoNameItem)
      Close()//结束通信,不返回任何信息
    Else
      SysCertificate=GetSystemCertificate(B)//体系证书
      PseudoName=GetCurrentPseudoName(B)//伪名
      DigitSign=CreateDigitalSignature(B) //数字签名
      FBMessage=CreateFeedbackMessage(SysCertificate, PseudoName, DigitSign, NodeUnDead)
      Send(FBMessage)
    End If//End If ! Expire…
    Else
      PrevPseudoNameItem=CheckList(BroadMessage.PseudoName) //检查节点 B 列表"节点历史伪名"一项
      If ! Empty(PrevPseudoNameItem) //存在对应历史条目
      Then
        SysCertificate=GetSystemCertificate(B)//体系证书
        NewPseudoName=GetNewPseudoName(B)//获得节点新伪名
        LastActivityTime=GetLastActivityTime(B)//获得最近活跃时间
        DigitSign=CreateDigitalSignature(B)//数字签名
        FBMessage=CreateFeedbackMessage(SysCertificate, NewPseudoName, LastActivityTime, DigitSign, NodeUpdate)
        Send(FBMessage)
      Else
        Close() //结束通信,不返回任何信息
      End If//End If ! Empty(PrevPseudoNameItem)
  End If//End If ! Empty(CurPseudoNameItem)
Else
  Abandon(BroadMessage);//丢弃该报文
End If//End If CBFVerify…
```

(5)证书撤销

无论设计得多么充分或"完美",使密钥无效总是存在可能的,且是不可预测的。在某些情况下,一个攻击或者通讯实现问题都将导致密钥泄露。另一方面,证书拥有者可能离开通信域,而颁发给用户的身份将用户和通信域联系在了一起,这时必须使该身份无效。

证书撤销协议只能由分布式 CA 来启动,在以下情况将启动该协议:

(1)通过上一节描述的节点消亡协议,发现某个节点已不存在,分布式 CA 收到撤销该节点证书的请求,经核实无误后。

(2)节点发现自己的私钥泄露,通知分布式 CA。

(3)节点出现恶意行为,经分布式 CA 核实无误后。

这些情况下,CA 必须采取行动,撤销节点证书或者使它无效,并警告证书使用者,该证书不再代表一个可信身份。本体系用来公布已更改的证书状态的机制是一个撤销证书列表 CRL。证书撤销列表包括已被撤销证书的序列号与撤销日期,还有标识撤销原因的状态。

CRL 由通信域的私钥进行签名,以保证列表不能被修改。每个节点都会保存一份 CRL。CRL 以增量的方式变更。节点 E 在收到该条广播报文后,首先确认自己没有缺失 CRL 记录。若也缺失,则同 D 一样广播报文索要缺失的记录。若 CRL 记录是完整的,则 E 向 D 请求通信,发送缺失的 CRL 记录给 D。这样,最终每个节点均维护一份完整的 CRL 列表。

2　安全交互方法的性能分析

本文提出的安全交互体系与传统协议相比,性能方面的改进主要体现在两方面:一是新协议对数据安全传输的方法进行了优化,相比较传统协议省去了一次解密运算的开销,提高了速度。二是提出了新的扩散式证书变更方案,相比较传统协议中一个接着一个顺序申请证书部分签名的方案,加快了

证书变更的速度。因此,更加适应于高速赛博空间组网需要。

(1)数据安全传输对比分析

传统的数据安全传输中加密方案如图3所示,散列函数的运算是在明文被加密之前,也就是说是对明文进行散列函数运算,生成摘要。

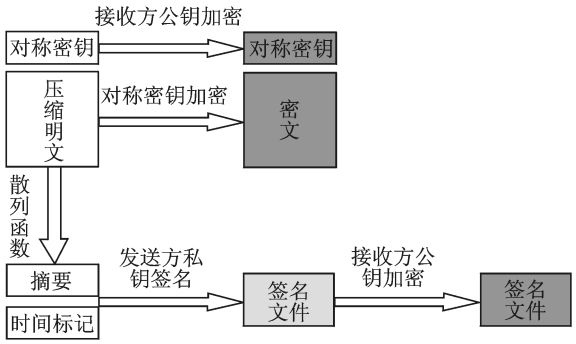

图3 传统的数据安全传输中加密方案

新协议则将散列函数的运算放在了明文加密之后,如图4所示,也就是对加密后的密文进行了散列函数运算。

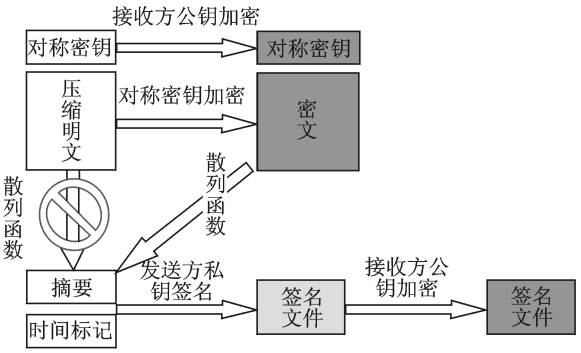

图4 新协议数据安全传输中加密方案

在加密过程中,均要经过对明文的加密、散列函数运算生成摘要等操作,性能并未提升。但是在解密时则减少了相应操作。新协议由于是对密文进行散列函数生成摘要的,所以在解密过程的第一步是直接对接收到的密文进行了散列函数运算,生成摘要,然后与签名文件中的摘要进行对比。新协议对比传统协议,少了一次解密密文的过程,接收到的信息的摘要直接由密文生成。如果摘要对比通过,则新协议与传统协议在效率上没什么差异。但是如果摘要对比不通过,则传统协议要比新协议多了一次解密密文的操作,这其中具体涉及到一次非对称加密算法的解密过程和一次对称加密算法的解密过程。

不论是新协议还是传统协议,签名文件在发送者传输前都是用接收方的公钥加密过的,所以在安全性方面这两者是接近的。但是在摘要对比验证失败的情况下,新协议省去了一个解密密文的操作,提高了系统的运行效率。

(2)证书变更协议对比分析

传统的证书变更协议采用的是申请节点依次向 t 个分布式CA节点申请证书部分签名,最后合成一份新的证书。而新的证书变更协议是一种扩散式的证书变更方案,在申请证书变更的节点向邻近的分布式CA提出证书变更请求后,分布式CA在做出部分签名的同时,会将该请求转发给其信任的其他分布式CA节点,接收到请求的其他分布式CA节点也会帮助进行证书变更,这个过程不需要申请证书变更的节点参与,提高了证书变更的速度。

假定节点间通信的延时均为 m,分布式CA节点生成一份证书部分签名的时间均为 c,节点需要向 t 个分布式CA申请部分签名。那么传统证书变更方案所需要的证书变更时间为:$T_{\text{old}} \approx (2m+c)\cdot t$。同样的环境下,设定分布式CA仅转发一次证书签名请求,每个分布式CA节点与其他 n 个分布式CA节点建立了信任关系。新的证书变更协议所需要的证书变更时间为:$T_{\text{new}} \approx (3m+c)\cdot\left(\frac{t}{n+1}\right)$。当延时 m 远小于分布式CA生成部分签名的时间 c 时,则有 $\frac{T_{\text{old}}}{T_{\text{new}}} \approx n+1$。

由此可以看出,若 $n=1$,则新的证书变更协议在时间上比传统证书变更协议节省了50%;若 $n=3$,则节省了75%。因此,新的证书变更协议比较传统证书变更协议效率的提高是确定的。

3 结束语

赛博空间组网能使战区空中一定范围内导弹群自动地组织成一个网络,提高单一数据链覆盖范围,使得各导弹在网络内部能够进行安全、高效的信息交流。各种信息按照规定的信息格式,实时、自动、保密地进行传输与交换,从而实现信息资源共享,为指挥系统迅速、正确地决策提供整个战区统一、及时和准确的态势感知。这是信息化战争的内在要求。本文对匿名安全交互体系各项关键协议进行了设计、优化,详细设计了各个阶段的协议内容,并提出了一种高效的证书变更方案,从而构造了一个可靠的赛博空间组网通信模型。

参考文献:

[1] 李昊, 龙晓波. 赛博行动与电子战[J]. 中国电子科学研究院学报,2011, 6(3):240-242;247.
LI Hao,Long Xiaobo. Cyber operations and electronic warfare[J]. Journal of CAEIT, 2011,6(3):240-242;247.

[2] 方剑. 赛博空间的挑战与机遇[J]. 国际电子战, 2009, 11(5):22-24.
Fang Jian. Cyberspace: challenges and opportunities [J]. International Electronic Warfare, 2009, 11(5): 22-24.

[3] 张建辉,于婧,汪斌强,等. 可重构路由协议构件研究[J]. 信息工程大学学报,2009,10(1):109-114.
Zhang Jianhui, Yu Jing, Wang Binqiang, et al. Research on reconfigurable routing protocol software [J]. Journal of Information Engineering University, 2009,10(1):109-114.

[4] 于永娇. 基于数据接入类型和节点负载的移动自组织网络 QoS 按需路由协议[D]. 长春:吉林大学,2011.
Yu Yongjiao. A QoS support on-demand routing protocol based on data access types and node load[D]. Chang Chun:Jilin University,2011.

[5] Spinello[R]. Cyberethics: Morality and law in cyberspace[M]. 6th edition. Canada: Jones & Bartlett Learning Computer Science, 2010.

[6] Zhou L, Hass Z. Securing Ad Hoc networks[J]. IEEE Network Magazine,2003, 13(6):751-765.

[7] Yi S, Kravets R. MOCA:mobile cetification authority for wireless Ad Hoc networks[C]// The 2nd Annual PKI Research workshop(PKI 03). NIST Gaithersburg MD,USA:[s. n.], 2003.

[8] Capkin S, Buttyan L, Hubaux J. Self-organized public-key management for Mobile Ad Hoc Networks [J]. IEEE Transactions on Mobile Computin, 2009, 8(1):651-660.

[9] Zimmermann P. The official PGP user's guide[M]. MA:MIT Press, 2005.

[10] Mosco V. The digital sublime: myth, power, and cyberspace cambridge[M]. MA: MIT Press, 2004.

[11] Deibert R, J G Palfrey, R Rohozinski. Access controlled: the shaping of power, rights, and rule in cyberspace[M]. MA:MIT Press, 2010.

[12] 李千目,刘凤玉. 战略互联网风险检测与故障分析方法[J]. 计算机研究与发展,2008, 45(10):1718-1723.
Li Qianmu, Liu Fengyu. A risk detection and fault analysis method for the strategic Internet[J]. Journal of Computer Research and Development 2008, 45 (10):1718-1723.