



基于统一通信技术的异构网络穿越安全算法研究

陈莹莹¹, 张庚², 翟明岳¹, 李杰³, 党美琳¹, 邢桂兰¹

(1. 华北电力大学 北京 100282; 2. 中国电力科学研究院 北京 100192;

3. 国网四川省电力公司资阳分公司 资阳 641300)

摘要:在统一通信异构网络环境中,由于统一的协议规范、加密以及防火墙等安全措施的存在,在网络环境内部进行的通信具有良好的可用性和安全性。当前的电力通信网,由于业务网络众多、网络层级明显,异构网络环境被广泛地应用在其通信的各个方面。但异构网络之间的通信,为了保证其可用性,安全性却被降低。在研究了异构网络穿越的问题和现状之后,又对对称密钥密码体制、非对称密钥密码体制进行了深入的研究,并且提出了一种基于 RSA 算法和改进型 DES 算法的混合加密算法。最后,运用实例分析表明,该算法具有很好的安全性。

关键词: UC 技术; 异构网络; RSA 算法; DES 算法

doi: 10.3969/j.issn.1000-0801.2013.12.008

Research on Security Algorithm for Crossing Heterogeneous Network Based on Unified Communication Technology

Chen Yingying¹, Zhang Geng², Di Mingyue¹, Li Jie³, Dang Meilin¹, Xing Guilan¹

(1. North China Electric Power University, Beijing 100282, China; 2. China Electric Power Research Institute, Beijing 100192, China; 3. Ziyang Branch of Sichuan Electric Power Corporation, Ziyang 641300, China)

Abstract: Due to the unified protocol specification, encryption, and firewalls and other security measures at present, communication within the network environment are in good usability and security in heterogeneous network environment. However, in order to guarantee the availability, safety of the communication between heterogeneous networks has been reduced. Based on the study of heterogeneous networks through the issues and the status quo on the symmetric key cryptography, asymmetric key cryptosystem in-depth research, an encryption algorithm based on the RSA algorithm and improved DES algorithm was proposed. Finally, the use of case study shows that the algorithm has good security.

Key words: universal communication technology, heterogeneous network, RSA algorithm, data encryption standard algorithm

1 引言

统一通信技术是把计算机技术与传统通信技术融于一体,将众多网络融合成一个网络平台,实现电话、传真、短信、数据传输、多媒体音视频会议、即时通信等众多通信服务的新型技术^[1]。统一通信将数据网络、语音网络和视频

网络融合在一起,通过基于 IP 的基础网络平台,实现数据、语音及视频等多业务的统一集成。数据网络、语音网络和视频网络之间彼此依存,互相影响,为用户提供了多种服务支撑。在这些异构的网络环境中,通过统一的协议规范、加密以及防火墙等安全措施,使得在网络环境内部所进行的通信,无论是可用性还是安全性,都得到了很好的

保证。但在异构网络之间通信,为保证异构网络穿越的可用性,理论上必须牺牲一定的安全性。因此,有必要对异构网络穿越的安全算法进行研究,以便于更好地提供网络服务。

2 异构网络现状

随着电力通信新技术的发展,电力通信网作为保持电力系统安全稳定运行的支柱之一,发挥着不可忽视的作用。电力通信网是由光纤、微波及卫星电路构成主干线,各支路充分利用电力线载波、特种光缆等电力系统特有的通信方式,并采用明线、电缆、无线等多种通信手段及程控交换机、调度总机等设备组成的多用户、多功能的综合通信网。电力通信网分为一级通信网、二级通信网、三级通信网和四级通信网。而电力通信业务网主要由行政交换网、数据通信网、电视电话会议系统、网管系统、时钟同步网组成。网络结构复杂,随着智能电网的发展,移动现场作业对无线网络的需求越来越大,各种业务交叉,应用广泛,使得网络的异构性成为了通信发展的必然趋势^[2]。

为保证电力通信网异构网络之间的安全穿越,在现有不同类型的网络的基础上,通过对各种网络进行融合、协同,并且通过统一的平台管理和交互访问来提供多种业务,满足用户的多种多样的需求。当前的异构网络,主要存在以下特点。

(1) 异构性

作为异构网络的核心特性,其主要表现在以下几点:

- 接入方式的异构性,如有线、无线等,而有线和无线也分别有多种不同的接入方式;
- 终端设备的异构性,当前的网络接入,除了传统的 PC 接入,更有 PDA、手机、平板电脑以及多种专用接入设备,这些设备不仅功能各异,运算和存储能力也有很大的差别,特别是随着云计算的发展,异构网络对终端设备的要求越来越低;
- 业务类型的异构性,不同的业务类型对应着不同的需求。

(2) 通信协议的统一性

为保证异构网络之间的安全穿越,进而保证网络之间的协同,统一的协议规范必须被应用到异构网络之间的通信中。另外,在通信系统中,无论是接入网、传输网还是核心网,都逐渐向 IP 化进行演变,基于 IP 传输已经成为业务传送的核心传输方式。通过将通信协议统一为 IP,可以

有效降低数据的传输成本,简化传输模式,增强 QoS^[3]。

(3) 异构网络的融合

异构网络的融合主要可以分为网络、业务和接入 3 个方面,3 方面共同构成了异构网络融合的主体。网络融合顾名思义,表示在网络层上保证异构网络之间的联通,为网络运行的畅通提供最基本的保证;业务融合通常在最高层(即应用层)实现,通过业务融合,消除业务之间的壁垒,使得在业务的应用上能够交叉使用,并且能够互相协同;而接入融合则强调异构网络之间的通信,应当无视接入技术的不同,保证不同的接入技术对网络畅通的影响达到最小。综合网络、业务、接入融合的要求和特点,都要求要实现无缝融合。异构网络的融合如图 1 所示。

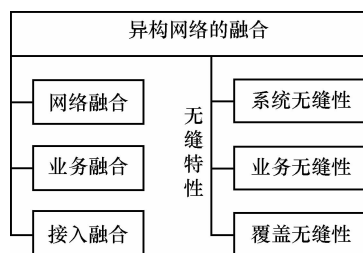


图 1 异构网络的融合

(4) 透明性和开放性

作为业务驱动的网络,异构网络的透明性和开放性是一个必然的发展趋势。透明性主要强调用户对业务的透明,即用户不需要关心网络状态、网络类型、接入方式、传输技术等,只需要关注具体的业务功能的实现。而开放性则强调了业务和网络的分离,也就是业务功能专注于业务的实现,而传输功能专注于网络的安全和可靠的传输,使得多种业务可以灵活扩展,也能进一步实现业务的协同^[4]。

3 密码体制

为保证异构网络间信息的安全传输,需要在传输过程中进行发方加密和收方解密过程。加密和解密算法的实现,通常是通过特定的密码体制和密钥共同完成的,密码体制即加密和解密的方法,而密钥是加密和解密的核心。安全传输的核心在于,保证攻击者在不知道密钥的情况下,无法根据加密和解密算法自己计算出密钥从而进行解密。

通常情况下,一个密码体制由 5 个部分组成:明文信息空间 M ; 密文信息空间 C ; 密钥空间 K ; 加密变换 $E_k: M \rightarrow C$, 其中 $k \in K$; 解密变换 $D_k: C \rightarrow M$, 其中 $k \in K$ 。



按加密和解密密钥的不同,主要分为对称密码体制(私钥密码体制)和非对称密钥密码体制^[4]。

3.1 对称密钥密码体制

对称密码体制,又称私钥密码体制。顾名思义,就是加密和解密方法是对称的,也就是加密和解密采用了相同的密钥,该密钥又称私钥。由于在加密和解密中,采用了共同的发方的私钥,因此收发双方必须拥有发方的私钥,并且通信双方都必须保证该私钥不被泄露,才能保证通信的安全。在这种场合下,必须强调发送报文的机密性和完整性。

由于对称密码体制要求双方具有相同的私钥,因此对于每2个用户,需要1个密钥,随着用户量的增加,由 n 个用户组成的网络中,为保证每2个用户之间拥有一个安全的密钥,一共则需要 $n(n-1)/2$ 个密钥,空间复杂度就成为 O^2 。这种指数级的空间复杂度,在用户数较小的情况下对整个网络的影响不大,但是,当用户量比较大时,会给管理带来极大的困难。

最经典的对称加密算法是DES (data encryption standard,数据加密标准)算法,由美国国家标准局提出,现在已经广泛应用于银行、网络传输等各种领域,密钥长度为56 bit。在DES加密算法的基础上,很多人对DES进行了变换,对其复杂度进行提高,通过增加复杂度,对算法的安全性也进行了增强,比较著名的有triple DES (三重DES)、GDES(广义DES)、IDEA、FEAL N、TC5等。

由于对称加密算法在每对用户之间只是用了一个相同的密钥且通常算法比较简单,容易实现,因此计算的开销很小,加密速度快,占用的空间也很小,成为当前加密的主要算法和基本算法。但是,由于在用户量比较大的情况下空间复杂度会急剧加大,并且不能进行数字签名,因此在应用中也受到很大的限制。

3.2 非对称密钥密码体制

非对称密码体制,又称公钥加密技术,该密码体制就是针对对称密码体制的缺陷提出的。不同于对称密码体制中收方和发方共用一个私钥,在非对称密码体制的加密和解密中,使用了不同的密钥。发方的加密密钥向公众公开,任何人都可以使用该加密密钥,但是解密的密钥只有收方知道,并且该解密的密钥无法通过加密密钥和加密算法推算出,因此保证了信息传输的安全性。在这种情况下,一个人只需要公开自己的公钥,其他人就可以用这个公钥对文件进行加密,然后给这个人发文件,而这个人自己掌握着私钥,因此只有他自己能够进行解密。通过公钥加密技术,

可以有效预防对称密码体制中通信双方的密钥被截获的可能,并且可以实现数字签名和认证^[5]。

在非对称密码体制中,当一个网络中有 n 个用户时,只需要 $2n$ 个密钥(公钥)就可以保证整个网络的安全传输,而不需要达到对称密码体制中的 n^2 个,空间复杂度大大降低。

当然,在保证安全性和密钥空间的同时,非对称密码体制通常算法复杂度较高,加密的效率也较低。

公钥密码体制的算法主要有3类:基于有限域范围内计算离散对数的难度的算法(如Diffie-Hellman算法(世界上第一个公钥加密算法)、ElGamal算法、数字签名算法)、椭圆曲线密码体制(如Diffie-Hellman算法、ElGamal算法和Schnorr算法等)和RSA公钥密码算法。

其中,RSA公钥密码算法经过多年的发展,成为当前最主要的公钥算法,并且由于其完备性较好,现在依然作为主流算法应用在各大领域。

4 基于RSA算法和DES算法的混合加密算法

4.1 混合加密的原理

对称加密体制具有运算开销少、速度快的优点,但面临通信双方安全密钥以及安全交换的局限性问题时,在网络传输中,密钥可能发生泄露,给安全性带来很大的隐患。此外,当多个用户之间需要进行加密传输时,随着用户量的增加,需要的密钥数量也随着增加,在密钥的分发和管理方面又面临了新的问题,并且增加了复杂度^[6]。

非对称加密体制下,安全性得到了很大的提高,并且能够适应异构网络的开放性、透明性等要求,但相对来说,加密算法更为复杂、速度较慢,特别是对大数据和密集型数据的加密,效率相对很低,通常只适合于对业务分离之后的密钥、数字签名等核心内容进行加密。

对于对称密钥和非对称密钥体制各自的特点,可以对其进行结合,互相弥补对方的缺陷。用对称密钥对数据进行加密,用非对称密钥加密采用对称加密算法加密所使用的密钥,既增强了安全性,又提高了加密效率,还能够满足业务分离的需求。

4.2 混合加密的实现

利用第4.1节提到的混合加密的思想进行加密,算法过程如下。

加密算法的过程如下。

(1)在发送方的 A 处产生一个随机数发生器,即一个 56 bit 的密钥 $D-Key$, 采用 DES 加密算法对明文 Q 进行加密,得到加密后的密文 P_1 ,并保存 $D-Key$ 。

(2)A 从密钥管理中心获取收方 B 的公钥,对 A 产生的 56 bit 的 DES 密钥 $D-Key$ 进行 RSA 加密,产生辅助密文 P_2 。

(3)将 P_1 和 P_2 组合,进行传输,完成了混合加密。
解密的过程与加密的过程相对应,介绍如下。

(1)收方 B 获取到密文 P_1 和 P_2 后,首先进行拆分,识别出 P_1 和 P_2 。

(2)B 用向密钥管理中心注册过的 RSA 私钥对 P_2 进行解密,恢复 A 的 DES 密钥 $D-Key$ 。

(3)B 利用 $D-Key$ 对 P_1 进行解密,恢复初始的明文 Q 。
加密解密步骤如图 2 所示。

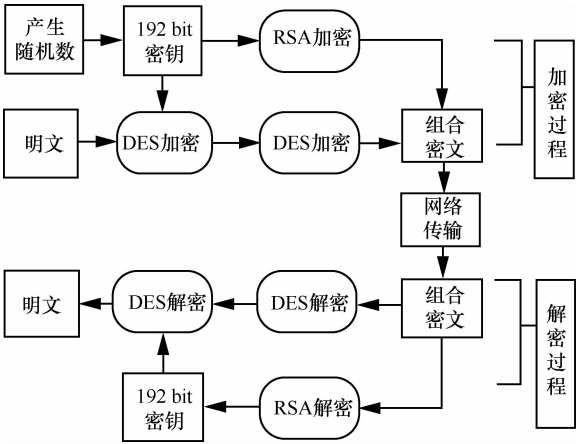


图 2 基于 RSA 算法和 DES 算法的混合加密算法

4.3 安全性分析

加密算法的安全性, 主要根据抵抗攻击的能力来判定。针对异构网络的通信传输进行攻击,主要采用的方法是密文攻击和算法攻击。

采用密文攻击, 根据第 4.2 节的设计, 假定攻击者 C 能够在通信过程中获取到传输的密文,并能成功获取到 B 的公钥,想通过攻击 RSA 算法来进行攻击。但是,RSA 算法的复杂度决定了 C 无法使用暴力破解的方法获取 DES 算法的密钥,进而无法获取明文信息 Q 。并且,混合加密在传输中对密文进行了组合,使得暴力破解的复杂度近似于 RSA 算法的复杂度与 DES 算法的复杂度之积, 安全性得到了极大的增强。

采用算法攻击,主要是针对 DES 的攻击。对 DES 的算法攻击主要有差分密码分析法和线性密码分析法,前者需

要知道 DES 的大量的(明文,密文)匹配对,后者则是一种已知明文攻击法。对于混合加密算法,由于明文的密钥采用了 RSA 算法加密,而明文本身进行了 DES 加密,因此上述两种算法对混合加密算法的攻击是无效的。

综上,针对密钥攻击,混合加密的安全性得到了很大的提高。

5 实例分析

通过一个例子, 对基于 RSA 算法和 DES 算法的混合加密算法进行分析和验证。测试环境如下:英特尔酷睿 2 双核处理器 P8600 2.4 GHz、内存 2 GB、Windows 7 操作系统、Eclipse 3.4.1 开发环境。表 1 为 DES 算法和 RSA 算法的密钥长度。

表 1 DES 算法和 RSA 算法的密钥长度比较

算法	DES 算法	RSA 公钥	RSA 私钥
密钥长度(bit)	56	1 024	1 024

由表 1 可得,RSA 算法的密钥长,加密的实现复杂,在内存和 CPU 中占用的时间、空间也多,复杂度很高。但区别于传统的全文加密, 只对 DES 算法加密后的密钥进行加密,因此所占的空间就很小,加密时间也很短。

因此,在实验中对加密时间进行比较,可以很好地对加密效率进行判断。

对一个 3 MB 的数据信息分别采用 DES 算法、RSA 算法和混合加密算法进行加密,得到加密时间见表 2。

表 2 3 种加密算法的加密时间对比

加密次数	DES 算法的加密时间(s)	RSA 算法的加密时间(s)	混合算法的加密时间(s)
1	13.32	294.45	23.38
2	13.23	301.41	24.03
3	14.19	308.74	24.18
4	13.85	303.85	23.99
5	13.06	299.83	24.10
平均	13.53	301.66	23.94

由表 2 可得, 采用 DES 算法的加密效率非常高,平均只需要 13.53 s,RSA 加密的时间则很长,平均需要 301.66 s,混合加密算法需要 23.94 s,所需时间比 DES 算法有所增加,但所需时间和 DES 算法处在同一个数量级。但是,通过混合加密,安全性得到了很大的提高。3 种算法时间和密钥长度数值比对结果如图 3 所示。

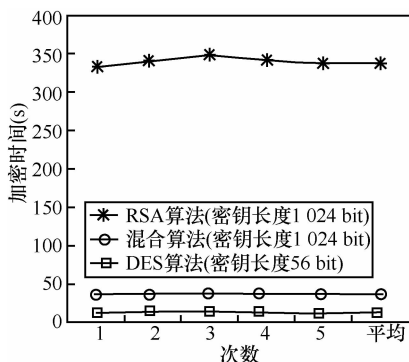


图3 时间和密钥长度数值比对结果

6 结束语

本文基于异构网络穿越问题和现状,对对称密钥密码体制和非对称密钥密码体制进行了研究,提出了基于RSA算法和改进型DES算法的混合加密算法。实例分析表明,采用通过RSA算法对DES的密钥进行加密的混合加密算法,极大地提高了安全性,并且具有良好的效率。

参考文献

- 1 张庚. 统一通信技术在电网中的应用. 电信科学, 2012(12): 243~247
- 2 袁伟. 基于Java的数据加密传输方案的研究. 天津大学硕士学位论文, 2009
- 3 周伟. 异构网络中的移动管理和安全机制研究. 中国科学技术大学硕士学位论文, 2009
- 4 王飞. 数据加密算法的分析改进及应用研究. 山东大学硕士学位论文, 2005

- 5 时华. 基于AES和ECC混合加密系统的算法研究. 西安工业大学博士学位论文, 2008
- 6 卜晓燕, 张根耀. 组合算法在软件加密系统中的实现. 计算机与数字工程, 2012(8): 21~23

[作者简介]



陈莹莹,女,华北电力大学硕士研究生,主要研究方向为电力系统通信。

张庚,男,中国电力科学研究院工程师,主要从事电力系统通信与物联网研究工作。

翟明岳,男,华北电力大学教授、教授级高级工程师,主要研究方向为信息通信。

李杰,男,国网四川省电力公司资阳分公司工程师,主要从事电力系统通信建设和管理工作。

党美琳,女,华北电力大学硕士研究生,主要研究方向为信息通信。

邢桂兰,女,华北电力大学硕士研究生,主要研究方向为信息通信。

(收稿日期:2013-08-01)

·简讯·

2013 亨通光电北京新品发布会 在京隆重举行

日前,江苏亨通光电股份有限公司(以下简称“亨通光电”)“引领智慧生活助力宽带中国”2013年新品发布会在北京隆重举行,20余款系列新品闪耀登场,覆盖4G通信、海洋工程等领域,全面展现其自主创新实力。

21世纪,海洋再度成为全球关注的焦点,在海洋工程领域,亨通光电是国内首家具备配套全套海洋通信系统的线缆企业,此次共发布跨洋海底光缆系列产品,如无中继系列Houc-1(LW、LWP、SAL、SA、DA)、有中继系列Horc-1(LW、LWP、SAL、SA、DA)以及无中继海底光缆系列

Houc-2新品。

创新是亨通光电发展的灵魂,其创新成果得益于长期投入和成熟的创新体系。亨通光电建立了国家级企业技术中心及博士后工作站、5个省级工程研究中心、3个院士工作站、6个研究生工作站等研发创新平台,参与国家与行业标准制订100多项,拥有国家授权专利720多项(专利总数列全国同行第一),在光纤光棒、智能电网、海底通信、电力传输等领域拥有最核心的研发技术及自主产权。

亨通光电以产品创新推动产业转型升级,为国际化战略实施提供保障,将以持续创新为引擎,实现产品与市场的全面突破,助推我国信息通信产业升级,持续促进信息消费,引领智慧生活,助力宽带中国。