应急通信的安全响应体系研究

陈延利[1],边巴旺堆[1],郭晋丞[2],李 鹏[3]
(1. 西藏大学 工学院 电子信息工程系,西藏 拉萨 850000;
2. 成都国腾电子技术股份有限公司,四川 成都 610041;
3. 国家 202 电台,西藏 拉萨 850000)

摘 要:文中基于中国剩余定理在广播方面的优势,通过对应急响应体系标准和架构需求的分析,将中国剩余定理用于应急响应体系中对信息进行组合,二次加密。加密时的模数是多项式随机数产生器实时产生的随机数,这种安全体系试图通过两种方式提高安全性。一方面通过中国剩余定理进行二次加密,另一方面每次通信时模数随机实时产生。应急体系以期达到抵抗穷尽攻击和时间上的差异化攻击。经过一系列的论证,应急通信的安全响应体系可以有效地为应急通信系统的安全性提供保障。

关键词:应急响应;应急通信;信息安全;中国剩余定理
中图分类号:TN918.91 **文献标识码**:A **文章编号**:1673-629X(2015)04-0108-04
doi:10.3969/j.issn.1673-629X.2015.04.025

Research on Security Response System of Communication Emergency

CHEN Yan-li[1], BIAN Ba-wangdui[1], GUO Jin-cheng[2], LI Peng[3]
(1. Department of Electronic Information Engineering, College of Technology, Tibet University, Lhasa 850000, China;
2. Chengdu GoldTel Electronical Technology Co., Ltd., Chengdu 610041, China;
3. 202 National Radio, Lhasa 850000, China)

Abstract: Based on the advantages of the Chinese Remainder Theorem (CRT) in broadcasting, through the analysis on the standards and frameworks of emergency response, CRT is applied to conduct the information combination and twice encryption. The module is generated in polynomial time in real-time and randomly. The security system attempts to make itself more security by two ways. On the one hand, it encrypts ciphertext by CRT, on the other hand, module is generated randomly and in real-time. It expects to resist exhaustive attack and differentiation time attack. After a series of arguments, the security response system of emergency communication can be effective to provide emergency communication system with protection.

Key words: emergency response; emergency communication; information security; CRT

0 引 言

我国目前的应急响应工作主要由国家计算机网络应急技术处理协调中心(CNCERT/CC)来承担,提供公益性的协调和支撑[1]。而企业的应急响应主要是靠自身,由系统所属单位负责,而专门针对互联网网络安全监控的工具和应急响应服务由安全厂商在提供。虽然各企业有自己的应急响应,但缺乏系统规范的应急响应服务支撑体系和平台来提供标准化、规范化的安全应急响应服务,企业只能提供局部的安全保障能力,无法延伸到其他行业,不具备覆盖全国、覆盖重要系统的安全保障能力。保障全社会整体的应急响应保障体系,成为学术界和企业一致关注的问题。

电信运营商具有较大规模的基础设施网络,承载了重要信息系统的数据,具备从事安全应急响应的天然优势。如果利用运营商的通信网络,结合政府的管理功能,建立完整的应急响应等级体系,可以为社会提供更广泛的互联网安全服务。目前信息在基础电信网中的安全问题已经越来越受到用户的关注,而应急响应体系的安全尤为重要,文中试图将同余理论的加密模型应用于应急响应体系,以期得到安全的应急响应

收稿日期:2014-06-13 **修回日期**:2014-09-17 **网络出版时间**:2015-02-23
基金项目:国家自然科学基金资助项目(61163013)
作者简介:陈延利(1981-),女,讲师,硕士,研究方向为移动通信系统安全、信号处理。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150223.1252.048.html

体系,抵抗网络中的不安全因素。

1　同余理论概念

定理[2](中国剩余定理):令 r 个正整数 $m_1, m_2, \cdots, m_r$ 两两互素,$M = m_1 m_2 \cdots m_r$,则同余方程组 $x = a_i \bmod m_i, 1 \leqslant i \leqslant r$。其中 $a_1, a_2, \cdots, a_r$ 是任意整数,有唯一解 $x = \sum_{i=1}^{r} a_i M_i y_i$,$M_i = M/m_i, y_i = M_i^{-1} \bmod m_i, 1 \leqslant i \leqslant r$。

由于中国剩余定理是 n 个同余方程有同一解,也就是说一种形式的信息可以转化成不同的表达形式。如果将这种方法运用于多用户的广播系统,发送方将不同的信息组合后以同样的形式发送给不同用户,这样对于选择明文攻击的攻击者来说无法从多个用户那里获得表达同样信息的密文,从而无法破解明文,降低了可攻击性。比如:用户 A 要发送 $x = b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3' \bmod n_1 n_2 n_3$ 给 B、C、D(n_1、n_2、n_3 是 B、C、D 用户的模数,$N_i = N/n_i, 1 \leqslant i \leqslant r$),其中只要求用户 B 知道 b_1 的内容,C 知道 b_2 的内容,D 知道 b_3 的内容即可。那么用户将此信息 $x = b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3'$ 与 n_1、n_2、n_3 求模即可得到 b_1、b_2、b_3。b_1、b_2、b_3 即是 m_B、m_C、m_D 的加密形式。并将 m_B、m_C、m_D 加密分别发送给 B、C、D 即可。

由 $x = b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3'$ 得到 b_1、b_2、b_3 的过程:

$$n_1 \mid N_2, n_1 \mid N_3$$

$$0 \equiv b_2 N_2 N_2' \bmod n_1, 0 \equiv b_3 N_3 N_3' \bmod n_1$$

$$b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3' \equiv b_1 N_1 N_1' \equiv b_1 \bmod n_1$$

$$b_1 = b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3' \bmod n_1$$

同理可得

$$b_2 = b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3' \bmod n_2$$

$$b_3 = b_1 N_1 N_1' + b_2 N_2 N_2' + b_3 N_3 N_3' \bmod n_3$$

2　基于同余理论的安全模型在应急响应中的应用

突发事件发生时,管理者应根据突发事件类型、通信网络受损状况、通信服务需求等级和通信保障的环境状态四类元素[3],才能对突发事件进行相应的响应,启动相应的预案级别。

2.1　模型架构

文中以省级应急响应体系为例进行说明。当发生突发事件时,由当地的应急指挥中心逐级向上一级进行报告,报告的内容包括事件类型、受损状况、通信服务需求等级和环境状态四要素,根据事件状况对应急响应初步判断 RE_0[4]。上一级应急中心接到报告后,对下一级应急中心的初判根据事件状况进行修正,并上报,直到可以对此事件进行处理的管理部门。具有决策权的应急中心根据突发事件四要素以及下一级应急中心对事件的初判,确定响应等级,并把响应等级和对各配合单位的通知利用同余理论对信息分别加密,经过中国剩余定理组合,以广播的形式发送给需要配合的通信运营商以及其他相关部门,各个接收单位得到信息后,按照需求启动相应等级,模型架构如图 1 所示。

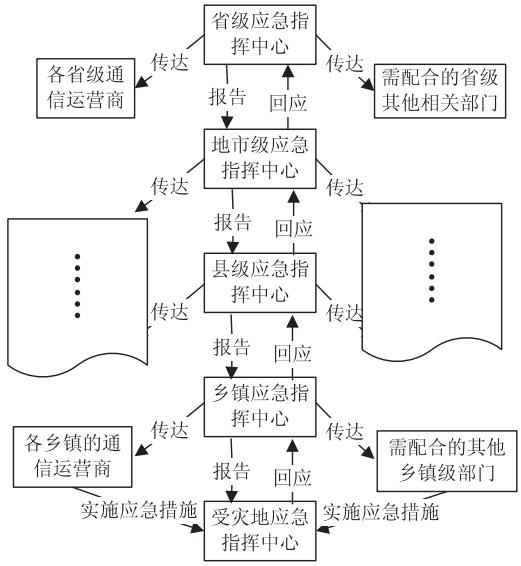

图 1　省级应急响应体系架构

在这个模型中各个事件集合定义[5-7]为:

(1)记突发事件集合为 E,$E = \{E_i, i = 0, 1, \cdots, n\}$,其中 E_0 为原生灾害事件,其他为次生灾害事件。这里将突发事件用 8 bit 的数据表示。

(2)通信网络受损集合记为 $NA(E) = \{NA_j(E), j = 1, 2, \cdots, m\}$,集合中各元素代表各网络设备与基础设备的受损状态。由于各种网络设备较多,将通信网络受损状况用 16 bit 数据表示。

(3)对于条件恶劣的自然环境,通信保障需要各部门的配合,应急响应等级应将环境因素考虑在内。记通信保障环境状态集合为 $EV(E) = \{EV_k(E), k = 1, 2, \cdots, s\}$,各元素代表道路、电力、能源等方面的环境状况,用 16 bit 数据表示。

(4)通信保障的服务需求记为 $SR(E) = \{SR_l(E), l = 0, 1, 2, 3\}$。其中,$l = 0$ 时集合中的元素代表政府应急指挥机构的应急保障需求;$l = 1$ 时集合中的元素代表抢险救援人员的应急保障需求;$l = 2$ 时集合中的元素代表媒体志愿者及相关人员的通信保障需求;$l = 3$ 时集合中的元素代表事发地群众对通信的保障需求。用 8 bit 数据表示,每种保障需求用 2 bit 数据表示。

(5)根据《国家通信保障应急预案》,将应急响应

分为四级,因此,将应急响应启动级别记为 RE(E),用 3 bit 数据表示,第一位备用,第二、三位表示应急响应的级别。

当受灾地应急中心向上一级应急中心报告信息时,有用信息的数据方式为:突出事件类型(8 bit)+通信网络受损状况(16 bit)+通信保障环境状态(16 bit)+通信保障的服务等级(8 bit)+应急响应级别初判(3 bit),共 51 bit,另外留出 13 bit 作为其他备用数据,用于系统的其他开销。同样高一级应急中心向低级应急中心、各通信运营商以及需要配合的其他单位传达相关命令时,使用同样的数据格式,但可根据不同的需要进行相应的调整,调整占用的各种数据。这些数据形式通过同余理论的安全方案进行传输。

2.2 基于同余理论的安全应急响应体系

在上一节的应急响应模型中,上级应急中心向下一级应急中心及相关部门传达通知时,将向不同部门发送的信息分别加密后,通过剩余定理将它们组合成一个消息,通过广播的形式发送。接收方接到信息后,可以通过自己的模数对信息进行分解得到自己的信息,并进一步解密,得到上级发送给自己的明文。如省级应急中心向下一级应急中心及相关单位和通信运营商发送通知数据,设向下一级应急中心的数据为 R,向通信运营商发送的数据为 T(如果有多个运营商,则分别为 $T_1,T_2\cdots$),向其他需要配合的部门发送的数据为 P(如果有多个运营商,则分别为 $P_1,P_2\cdots$),可通过以下过程完成。

(1)系统初始化。

安全应急响应中设定一个随机数管理中心,当有用户之间需要通信时,通信的发起方向管理中心索要随机数,随机数作为传输数据时各用户的模数,若省级应急中心向下一级应急中心 R、通信运营商 T 及其他各单位 P 发送数据时,管理中心产生四个模数均为素数 n_R、n_T、n_P,令 $n=n_Rn_Tn_P$。那么用户得到自己的模数后进行保存。

在该方案中,每次加密时模数只能使用一次,即每次用户间通信时,都需要向管理中心索要模数。每次产生的模数是由管理中心随机产生的,模数只对本次通信的用户公开,不对外公开。

(2)信息的发送和接收过程。

设省级应急中心 RC 分别发送信息 M_R、M_T、M_P 给接收方 R、T、P,如上所述,T 和 P 可是多个,这里以一个为例。首先用户 RC 把要发送给 R、T、P 的信息 M_R、M_T、M_P 通过文献[8] K 次剩余的加密方案,得到密文 C_R、C_T、C_P。利用中国剩余定理将 C_R、C_T、C_P 组合成 RC 要发送的信息 C_i,然后以广播的形式发送。

省级应急中心 RC 将 C_R、C_T、C_P 组合成要发送的信息:

$$C_i=C_RN_RN_R'+C_TN_TN_T'+C_PN_PN_P'$$

其中,$n=N_in_i$,$N_iN_i'\equiv 1\bmod(n_i)$,$i=R,T,P$。

接收方收到信息后,得到密文后利用系统已有的解密算法解密得到明文,这里以 R 获取信息的方法为例进行说明。用户 R 得到密文 C_i 后,R 通过求模计算自己的密文:

$$C_R=C_i(\bmod n_R)=(C_RN_RN_R'+C_TN_TN_T'+C_PN_PN)\bmod n_R$$

$$n_R\mid N_T,n_R\mid N_P$$

$$C_R=(C_RN_RN_R'+C_TN_TN_T'+C_PN_PN)\bmod n_R\equiv C_RN_RN_R'(\bmod n_R)$$

$$N_RN_R'\equiv 1(\bmod n_R)$$

$$C_R\equiv C_RN_RN_R'(\bmod n_R)\equiv C_R$$

得到密文后,R 通过系统的解密算法得到密文,用户 T、P 通过同样的方法得到密文,再经过自身的私钥进行解密得到明文。

2.3 安全性分析

应急响应是在发生突发事件时做出的响应,不法分子可能会利用突发事件制造事端。为了避免此类事件的发生,必须建立安全的应急响应体系,保障信息的安全性[9]。

基于同余理论的应急响应体系的安全性主要表现在以下几方面。

(1)应急响应体系的安全性首先是基于系统本身的加解密体制。公钥密码系统和概率密码安全性都是多项式安全的。

文献[8]中,对每个用户来说存在一个随机数 n_i 和加密算法 E,其中 n_i 是素数。通过随机数和加密算法,元素 x(定义在 $\{1,2,\cdots,N\}$ 上)映射到 $x^E\bmod n$ 上。下面证明 $x^E\bmod n$ 是一单向函数类。首先给出三个算法 (I,D,E)。

当系统产生一随机数 1^n 时,对算法 I 输入 1^n,那么算法 I 均匀地在系统的密钥空间中选取公钥 K 及与其对应的模数 n。算法 I 以输出 (n,K) 而结束。而公钥 K 和模数 n 均为集合,其元素为每个用户的公钥和模数。

对算法 D 来说,当输入 (n_i,k_i) 时,它在集合 $\{1,2,\cdots,N\}$ 中选择一个元素 x,即明文。当对算法 E 输入 $((n_i,k_i),x)$ 时,算法 E 输出 $x^k\bmod n$。

由于在方案中,大模数(各用户模数的积)和公钥是公开的,因此攻击者对算法进行解密时需要对大数 N 进行分解,而这是一个未决难题。

因此 CPES 函数是基于一个未决难题的单向函数类,也就是说基于同余理论的密码体制具有可证明的

安全性。因此应急响应体系本身的安全性也是多项式安全的。

(2)从上文可知发送方对信息加密后,对信息进行组合再发送,接收方得到信息后需要利用模数对信息进行运算,这一过程相当于对信息进行二次“加密”,对于攻击者来说,只有得到随机产生的模数才能得到密文并进行解密,得到明文。而每个用户的模数是实时随机产生的,只对一次通信有效,因此攻击者要想得密文,需要实时得到模数。目前随机数产生器都是多项式安全的,密文也是多项式安全的。

(3)发送方发送信息时,给不同接收方的信息是同时进行的,不需要逐个发送信息,为应急响应可以节省时间,同时也降低了攻击者在时间上的差异化攻击。

(4)密钥丢失时的安全性。

对于任何一个密码系统来说,如果用户丢失了私钥,即使在得到正确的密文条件下也无法解密密文。因此密码系统应该有一个措施防止此类事情的发生。本节介绍文中提出的基于同余理论的概率密码系统的应急安全性。

假定在一次应急事件处理中某一用户将自己的私钥丢失。由于时间紧迫,事件重要,已经来不及让发送方再重新发送,这时候就可以启用应紧措施。丢失密钥的用户,可以向系统中心申请索要其他用户的模数,系统对该用户的身份进行验证,若该用户是此次通信系统的用户,那么 CPES 通过他的申请并将发送该用户索要的数据。丢失私钥的用户得到其他用户的模数后,再结合这些用户的公钥解密出明文。

假定用户 B 丢失了自己的公钥。那么他从 CPES 中得到其他用户的模数 n_A 、n_C 、n_D 以及公钥(加密密钥) E_A 、E_C 、E_D ,通过下面的计算可以从密文 C_B 解密出明文 M_B 。

(1)计算大模数 $N = n_A n_B n_C n_D$;

(2)由 $N_i N_i^{'} \equiv 1 \bmod(n_i)$ 系统参数的生成过程可以看出,任一用户的公钥与其他用户公钥的积是关于大模数互逆的。因此有:

$$C_B^{k_A k_C k_D} (\bmod N) = (M_B^{E_B})^{E_A E_C E_D} (\bmod N) = M_B^{E_A E_B E_C E_D} (\bmod N)$$

$$E_A \cdot E_B \cdot E_C \cdot E_D \equiv 1 (\bmod \varphi(N))$$

$$M_B^{E_A E_B E_C E_D} (\bmod N) = M_B$$

3　结束语

通过对应急响应的需求和标准进行分析,构架了应急响应的体系结构[10-11]。并利用中国剩余定理对信息进行二次“加密”,同余理论对体系的安全性进行了改进,保证了信息传输的安全性,满足应急通信中的安全需求[12-13]。

参考文献:

[1] 张新跃,刘志勇,赵进延,等. 基于电信运营商的安全应急响应体系研究[J]. 信息网络安全,2011(8):76-78.

[2] 柯　召,孙　琦. 数论讲义[M]. 北京:高等教育出版社,2001:41-45.

[3] 王　谦,易　武,田晓东,等. 企业通信保障应急响应等级设定模型研究初探[J]. 现代电信技术,2012(1):60-64.

[4] 戚建刚. 突发事件管理中的“分类”、“分级”与“分期”原则—《中华人民共和国突发事件应对法(草案)》的管理学基础[J]. 江海学刊,2006(6):133-137.

[5] 张子民,周　英,李　琦,等. 基于信息共享的突发事件应急响应信息模型(I):模型定义[J]. 中国安全科学学报,2010,20(8):154-160.

[6] Wang Wenjun, Zhang Xiankun, Dong Cunxian, et al. Emergency response organization ontology model and its application [C]//Proc of fourth international symposium on information science and engineering. [s. l.]:[s. n.],2009:50-54.

[7] Han Fuyou, Zhang Hailong, Dong Liyan. Research on evaluation model of emergency response plans[C]//Proc of international conference on mechatronics and automation. Changchun: IEEE,2009:5117-5122.

[8] 林建辉. 基于日志技术的网络安全应急响应处置研究[J]. 湖北警官学院学报,2009(5):10-12.

[9] Symons L C, Pavia R, Hodges M. Emergency response in national marine sanctuaries[C]//Proc of OCEANS2005. Washington:[s. n.],2005:1-6.

[10] Boukerche A, Zhang Ming, Pazzi R W. An adaptive virtual simulation and real-time emergency response system[C]// Proc of international conference on virtual environments, human-computer interfaces and measurements systems. Hong Kong: IEEE,2009:360-364.

[11] 王海涛. 应急通信发展现状和技术手段分析[J]. 电力系统通信,2011,32(2):1-6.

[12] 张若英. 国内外突发公共事件应急响应典型案例[J]. 世界电信,2009(9):51-51.

[13] 罗　平,李　强. 网络安全应急响应体系研究[J]. 农业网络信息,2011(2):5-7.

应急通信的安全响应体系研究

作者： 陈延利， 边巴旺堆， 郭晋丞， 李鹏， CHEN Yan-li， BIAN Ba-wangdui， GUO Jin-cheng， LI Peng

作者单位： 陈延利,边巴旺堆,CHEN Yan-li,BIAN Ba-wangdui(西藏大学 工学院 电子信息工程系,西藏 拉萨,850000)， 郭晋丞,GUO Jin-cheng(成都国腾电子技术股份有限公司,四川 成都,610041)， 李鹏,LI Peng(国家202电台,西藏 拉萨,850000)

刊名： 计算机技术与发展 ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2015(4)