

基于椭圆曲线的识别伪基站垃圾短信改进算法

孙旭敏, 刘彩霞

(内蒙古大学 计算机学院, 内蒙古 呼和浩特 010021)

摘要:随着公众移动通信的发展,不法分子为了牟取暴利,利用 GSM 网络自身的安全缺陷,多种机制的伪基站被应用于发送广告信息甚至诈骗短信,其带来的安全问题成为当前社会关注的一个重要问题。伪基站信号覆盖范围内下发垃圾短信和在正常基站信号覆盖范围内下发短信的机制有着根本的不同。合法短消息的转发需通过短消息服务中心,而伪基站垃圾短信是直接终端对终端进行的。通过分析伪基站信号特征和工作原理,提出了基于数字签名的识别伪基站下发的垃圾短信甚至诈骗短信的方法,并对用于数字签名的椭圆曲线算法进行改进,在签名与认证部分将算法的有效性提高大约 60%。将改进的基于椭圆曲线算法的数字签名应用于短信息合法性的识别中,能够达到百分之百识别垃圾短信的效果。

关键词:伪基站;垃圾短信;主动识别;数字签名;椭圆曲线

中图分类号:TP301.6

文献标识码:A

文章编号:1673-629X(2018)07-0121-04

doi:10.3969/j.issn.1673-629X.2018.07.026

An Improved Algorithm of Identifying Spam Message of Pseudo Base Station Based on Elliptic Curve

SUN Xu-min, LIU Cai-xia

(School of Computer, Inner Mongolia University, Hohhot 010021, China)

Abstract: With the development of the public mobile communications, in order to get a huge profit, criminals take advantage of the GSM network's security defects. A variety mechanisms of the pseudo base station are used to send advertising messages and even fraud messages, so security issues brought by spam messages of pseudo base station become a serious problem concerned by the society. The mechanism sending spam messages under signal covered by pseudo base station is fundamentally different from the mechanism covered by normal station. Legal short message should be forwarded through the short message service center, while the pseudo base station spam message is direct from terminal to terminal. By analysis of the pseudo base station signal feature and working principle, we propose an improved method based on digital signature to identify spam messages, and improve the elliptic curve cryptosystem used in digital signature. Therefore, the effectiveness of signature and verification process raises about 60%. The improved digital signature based on elliptic curve algorithm is applied to recognize the legality of short message, which can achieve the effect of one hundred percent identifying spam messages.

Key words: pseudo base station; spam messages; digital signature; elliptic curve

1 概述

1.1 伪基站

伪基站系统之所以能对用户发起进攻,是利用 GSM 网络单向鉴权的缺陷,即网络对用户的认证,用户终端对网络不进行鉴权以及空口信令完整性保护功能。GSM 基站在与用户终端通信的过程中,终端无法检测网络身份是否合法,也无法判断接受到的网络信令是否来自合法基站。当手机终端接收到网络发送的标准信令,就会进行响应以及处理。利用这一缺陷,伪

基站通过发出强于正常基站的信号,从而诱导移动用户手机的链接接入伪基站,获取覆盖范围内终端的手机串号 IMSI/IMEI 和电话号码,之后模拟任意号码向覆盖用户下发垃圾短信。在此期间,不仅手机会被强制接收垃圾短信,还会造成正常通信的阻断,伪基站覆盖区域内会出现大量掉话以及跨区频繁切换现象。

1.2 伪基站系统组成

伪基站系统主要是由信号处理子系统(伪基站和终端信号处理子系统)、用户操作平台和系统总控单

收稿日期:2017-05-23

修回日期:2017-10-27

网络出版时间:2018-03-07

基金项目:国家自然科学基金(61461037)

作者简介:孙旭敏(1993-),女,硕士,研究方向为网络通信;刘彩霞,博士,副教授,研究方向为嵌入式技术。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20180307.1416.008.html>

元、天线和电源等部分组成,如图 1 所示。终端信号处理子系统用来实现对目标所在区域移动系统无线参数的侦查。系统总控单元完成对各子系统的控制与调度、信令处理、内部通信等功能。用户操作平台提供人机界面,能够进行系统状态的显示,小区状态的显示,目标数据库的存储、系统维护等功能。

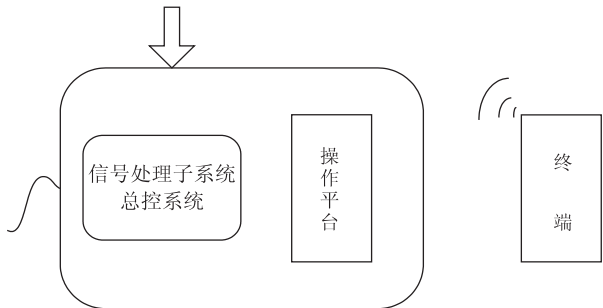


图 1 伪基站系统结构

2 伪基站的系统原理

2.1 强制接入原理

目前的 GSM 采用单向鉴权机制,伪基站利用移动通信网络这一漏洞,仿冒运营商移动网络发射射频信号。伪基站的 BCCH、功率参数与现网相同,LAC、CID 与现网不同。由于伪基站设置的 LAC 与用户当前网络的 LAC 值不同,移动终端会认为所在位置发生变化,然后基于 $C_2 = C_1 + CRO$ (C_1 为手机接收信号电平值)优先选择 C_2 值最大的信号快速重选到伪基站小区进行位置更新^[1]。

移动终端向伪基站发送位置更新请求,伪基站借机通过 MSC 和 BSC 的信令模拟,获取目标手机 IMSI、IMEI 串号以及手机号码,直接向用户下发位置更新接收消息,确认位置更新后向终端下发垃圾短信^[2]。此后伪基站为了避免因长时间驻留引起用户觉察,自动变换 LAC,移动终端再次发起位置更新请求后,伪基站会根据数据库存储信息将已下发垃圾短信的手机剔除,发回拒绝消息“Location update rejected”,终端手机脱网,回到运营商网络。期间 10 ~ 20 s,终端用户无法正常被叫,因手机被伪基站剔除后需要重新寻找网络,一般需要 15 s 左右才能重新驻留到 GSM 网络^[3]。

伪基站工作原理示意图如图 2 所示。

2.2 下发短信机制

在 GSM 机制中,短消息的发送要经由移动终端所在区域的短消息服务中心 (SMSC) 的存储和转发,经研究伪基站下发垃圾短信的流程中,并不会经过 SMSC 中转站^[4]。基于此漏洞,可以在短消息转发的过程中进行有效的数字签名,在接收终端上进行数字签名认证,在此过程选择合适的数字签名算法,确保其较高的安全在数据

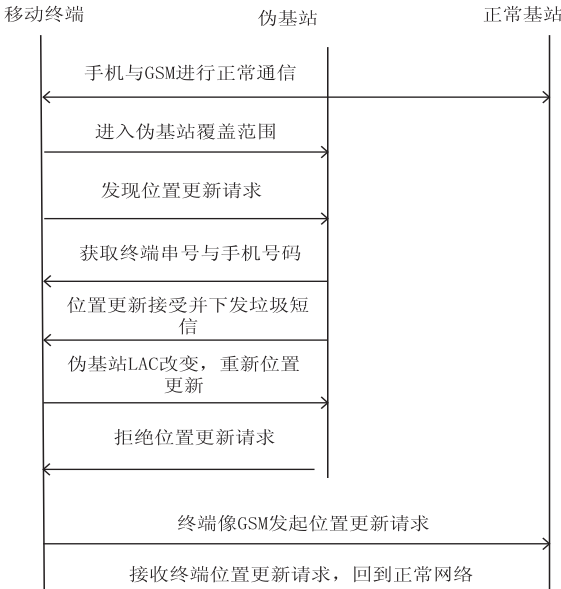


图 2 伪基站工作原理示意图

3 数字签名

3.1 数字签名简介

随着电子商务与电子政务的发展,对快速安全的加密算法有了新的需求。基于椭圆曲线的密码系统就以其卓越的安全性引起了专家学者的关注。椭圆签名算法的安全强度主要依赖于所选择的椭圆曲线^[6]。

与其他公钥密码 (如 RSA、DSA 等) 相比,椭圆曲线密码具有绝对的优势:高安全、存储空间少、处理速度快、占用带宽少、扩展性好。在伪基站发送诈骗短信的识别中,数字签名主要提供一个身份标识,证实终端接收的短消息来自运营商。

3.2 识别伪基站垃圾短信数字签名思路

基于上文提到的伪基站下发垃圾短信的机制,对其进行分析发现数字签名的思路。

当 SMCS 收到短消息后,对其内容进行 Hash 运算得到消息的摘要。然后,SMCS 用自己的私钥对消息摘要进行加密,将数字签名的摘要和短消息一起发送给用户的终端设备^[7]。

数字签名算法的签名过程如图 3 所示。



图 3 数字签名算法的签名过程

终端设备将收到的短消息采用相同的算法进行运算,得到一个短消息的摘要,并同时用 SMCS 的公钥对数字签名解密得到另一个短消息摘要,将两个消息摘要进行对比,识别其是否合法。若得到的两个摘要完全吻合,则短消息为合法消息^[8]。数字签名的演算过程如图 4 所示。

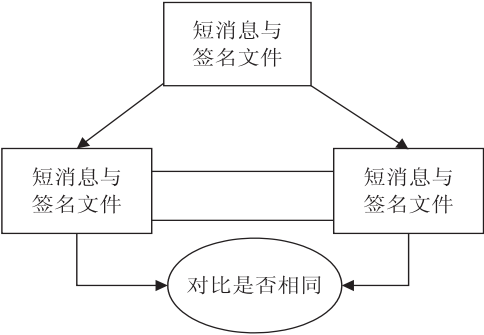


图4 数字签名的演算过程

3.3 基于椭圆算法的数字签名

ESDSA 是椭圆曲线加密体制 ECC 中应用的数字签名算法。实验表明,在椭圆曲线加密算法中采用 160 bit 密钥和 1 024 bit 密钥的 RSA 算法的安全性相当。由于椭圆曲线的加密算法密钥短,并且所基于的有限域的运算位数少于传统的运算位数,其加密算法很容易在计算机软硬件上实现^[9]。

在基本的二进制序列中,椭圆曲线的运算速度取决于点乘运算以及求逆运算。如果能缩短点乘运算中的序列长度,以及避免求逆运算,则算法速度就会提高。基于这种考虑,文中提出了快速点乘运算的改进的椭圆曲线算法。

3.3.1 点乘的基础算法

首先,将一些基本符号规定如下^[10]:
有限域 $K = Fq$,有限域 K 上的椭圆曲线 $E:y^2 + xy = x^3 + a_4x^2 + a_6$,其中 $x, y, a_i \in K$ 。椭圆曲线的基点为 G , G 不可任意改变, G 点的阶为 n ,辅助因子为 h 。曲线上的两个点 $P(x_1, y_1), Q(x_2, y_2)$, Q 不是无穷点 o_k , $-P_{(x_1, y_1+x_1)}$ 表示 P 的逆元。

定义 E 上的加法运算:
若 $Q = P$,则 $Q + P = 2p_{(x_3, y_3)}$,其中 $x_3 = \gamma^2 + \gamma + a_4$, $y_3 = x_1^2 + (\gamma + 1)x_3, \gamma = x_1 + y_1/x_1$ 。特别的,对 $\forall P \in E$,若 $Q = O_K$,则 $Q + P = P$,对于实数 0, $OP = O_K$ 。在有限域 K 上进行了 4 次乘法、1 次求逆和 5 次加法。
若 $Q \neq P$,且 $Q \neq -P, Q + P = 2p_{(x_3, y_3)}$,其中 $x_3 = \gamma^2 + \gamma + x_1 + x_2 + a_4, y_3 = \gamma(x_1 + x_2) + x_3 + y_1, \gamma = (y_1 + y_2)/(x_1 + x_2)$ 。在有限域 K 上进行了 3 次乘法、1 次求逆和 9 次加法。

设 P 为曲线 E 上的一个 t 阶点,且 $P \in E, 0 \leq s < t$ 且 $t \in N^+$ 。
点乘运算的一般情况为:
$$S = a_{n-1}m^{n-1} + a_{n-2}m^{n-2} + \cdots + a_1m^1 + a_0 \quad (1)$$
其中, $m > 1$ 且 $0 < a_j < m, a_j \in Z$ 。
当 $m = 2$ 时,则有:
$$SP = (a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_12^1 + a_02^0)P =$$

$$a_{n-1}2^{n-1}P + a_{n-2}2^{n-2}P + \cdots + a_12^1P + a_02^0P \quad (2)$$

由此可以看出要计算 2^iP ,共需 i 次倍乘运算,且:
$$a_i2^iP = \begin{cases} 2^iP, a_i = 1 \\ o_k, a_i = 0 \end{cases}, i = 0, 1, \cdots, n - 1 \quad (3)$$

基础算法需要在有限域 K 上进行 $7(n - 1)$ 次乘法以及 $2(n - 1)$ 次求逆^[11]。

3.3.2 点乘的改进算法

由上述基本算法可知,SP 的运算速度取决于 n 的大小,若选取适当的 $n = kN$,其中 $N \in N^+$ 。令 $M = 2^K (K > 1)$,有:

$$S = a_{n-1}(2^K)^{n-1} + a_{n-2}(2^K)^{n-2} + \cdots + a_1(2^K)^1 + a_0 \quad (4)$$
$$SP = (a_{n-1}(2^K)^{n-1} + a_{n-2}(2^K)^{n-2} + \cdots + a_1(2^K)^1 + a_0(2^K)^0)P = 2^K(2^K \cdots (2^K(O_K + a_{n-1}P) + a_{n-2}P) \cdots + a_1P) + a_0P = 2(2 \cdots (2(O_K + a_{n-1}P) + a_{n-2}P) \cdots + a_1P) + a_0P \quad (5)$$

改进的椭圆曲线算法如下:

Step1:
 $T_{[0]} = O_K$
for $i = 1$ to $2^K - 1$
 $T_{[i]} = T_{[i-1]} + p$
Step2:
 $T = O_K$
for $i = N - 1$ to 0 by -1
begin
for $h = 1$ to k
 $T = 2T$
for $j = 1$ to $2^K - 1$
if $j = a_{[i]}$ then $T = T + T_{[j]}$
end

在 Step1 中共需要进行 $(2^K - 1)$ 次加法运算,即需要做 $3(2^K - 1)$ 次乘法和 $(2^K - 1)$ 次求逆运算^[12];在 Step2 需要进行 N 次点的加法运算和 $K \times N$ 次倍点运算,即需要做 $(3 + 4k)N$ 次乘法运算和 $(k + 1)N$ 次求逆运算^[13]。

基础算法与改进算法在倍点运算上区别不大,比较结果见表 1。

表 1 两种算法的运算步数		
算法	加法运算	倍点运算
基础算法	$n - 1$	$n - 1$
改进算法	$2^K - 1 + n/k$	n

然而,在加法运算上面,当 k 与 n 满足 $n = 2^*k^2 \ln 2$ 时,可使得算法效果达到最佳。

下面给出实例,随机取 3 个大整数进行计算,结果 见表 2。

表 2 大整数的计算

序号	s 的十进制 序列长度	s 的二进制 序列长度	K 值	s 的 K 进制 序列长度	基础算法 加法次数	改进算法 加法次数	运算次数 减少量
1	23	76	4	19	75	34	55%
2	49	160	4	40	159	55	65%
3	106	352	5	71	351	102	71%

由此可以看出,改进算法的有效性比基础算法提高了 60%,考虑到短消息转发中心消息转发的及时性对用户的影响,改进的数字签名有助于加快签名和验证速度,能有效解决这一问题^[14]。

4 结束语

伪基站系统对运营商的影响巨大,会导致覆盖区域大量掉话以及跨区频繁出现,并且会导致网络拥塞。对此,提出了一种改进的基于椭圆曲线的数字签名方法,将其应用于伪基站垃圾短信识别,相对于其他防治伪基站的措施具有一定的优势。将数字签名应用于伪基站垃圾短信的识别^[15],对运营商网络不需进行修改;改进的椭圆曲线数字签名方法较其他算法具有较高安全性,且考虑到短消息转发中心要处理庞大的数据,改进算法的计算速度有所提高,而占用存储空间较小,便于在移动终端实现。

参考文献:

[1] 王 洗,陈 光,黄加波. 基于 Gb 信令分析的伪基站定位方法研究[J]. 电信技术,2014(9):73-76.

[2] 刘泽忠. 一种基于伪基站的 GSM 用户分选系统实现方案[J]. 通信技术,2013,47(6):127-129.

[3] 赵明伟,徐霖洲,石雷飞,等. 一种非法伪基站现场快速测量定位的方法[J]. 移动通信,2016,40(8):18-21.

[4] LEE W C Y. Effects on correlation between two mobile radio base station antennas[J]. IEEE Transactions on Communications,1973,21(11):1214-1224.

[5] 周之童,夏子焱,邢佳帅,等. 伪基站系统侦测识别及定位方法研究[J]. 信息网络安全,2014(9):196-198.

[6] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]//Advances in cryptology. Berlin:Springer-Verlag,1985:469-472.

[7] 严佳韵. 基于椭圆曲线的快速数字签名算法[D]. 成都:西南交通大学,2011.

[8] MILLER V S. Use of elliptic curves in cryptography[C]//Advances in cryptology. Berlin:Springer-Verlag,1985:417-426.

[9] 郝 林,罗 平. 椭圆曲线密码体制中点的数乘的一种快速算法[J]. 电子与信息学报,2003,25(2):275-278.

[10] GURA N,PATEL A,WANDER A,et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]//6th international workshop on cryptographic hardware and embedded systems. Cambridge,MA,USA:[s. n.],2004:119-132.

[11] 江志祥,蒯志青. 椭圆曲线密码体制[J]. 计算机研究与发展,2008,36(11):1281-1288.

[12] JOHNSON D,MENEZES A,VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security,2001,1(1):36-63.

[13] COHEN H,FREY G,AVANZI R,et al. Handbook of elliptic and hyperelliptic curve cryptography[M]. 2nd ed. [s. l.]: Chapman & Hall/CRC,2006.

[14] 张方国,王常杰,王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报,2001,22(8):22-28.

[15] 陈 勤. 数字签名算法的比较及其应用[J]. 计算机应用研究,1999,16(10):10-11.

(上接第 120 页)

of web services based on two-phase k-means clustering[C]//IEEE international conference on web services. New York,NY,USA:IEEE,2015:161-168.

[11] VU L H,HAUSWIRTH M,ABERER K. QoS-based service selection and ranking with trust and reputation management[C]//OTM confederated international conferences on the move to meaningful internet systems. Agia Napa, Cyprus: Springer,2005:466-483.

[12] ZHENG Zibin,ZHANG Yilei,LYU M R. Investigating QoS of real-world web services[J]. IEEE Transactions on Services Computing,2014,7(1):32-39.

[13] ZHENG Zibin,ZHANG Yilei,LYU M R. Distributed QoS evaluation for real-world web services[C]//IEEE international conference on web services. Miami,FL,USA:IEEE,2010:83-90.

[14] ZHENG Zibin,MA Hao,LYU M R,et al. Collaborative web service QoS prediction via neighborhood integrated matrix factorization[J]. IEEE Transactions on Services Computing,2013,6(3):289-299.

[15] ZHENG Zibin,MA Hao,LYU M R,et al. WSRec:a collaborative filtering based web service recommender system[C]//IEEE international conference on web services. Los Angeles,CA,USA:IEEE,2009:437-444.