西安电子科技大学
XIDIAN UNIVERSITY

电力系统视频监控网络安全接入协议研究

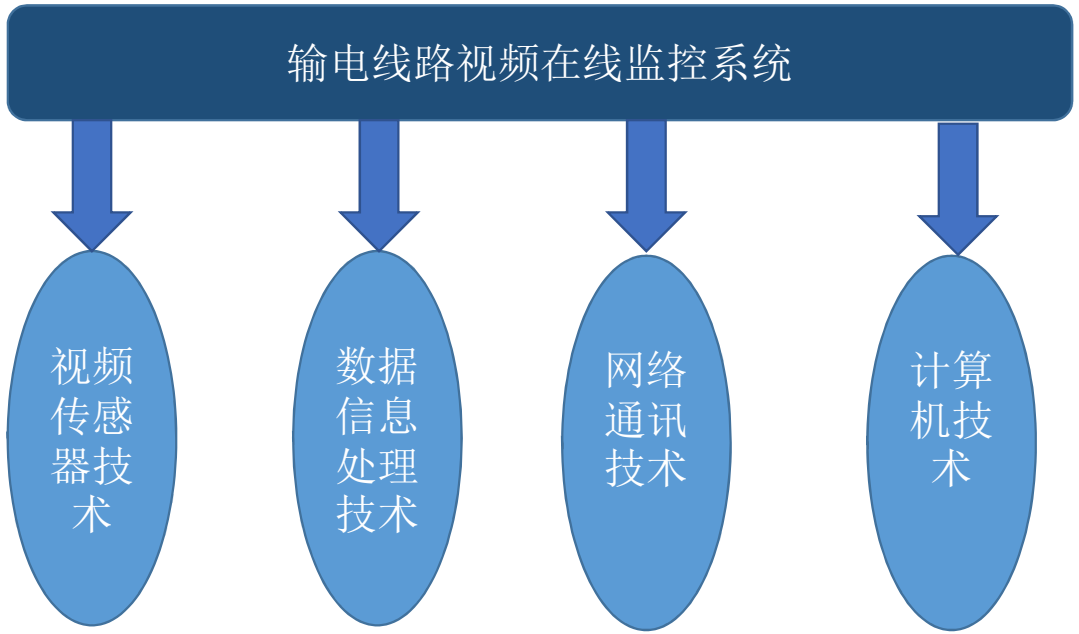
刘渊峰

目录

一 研究意义和主要工作
二 电力LTE系统网络架构和解决方案
三 电力LTE接入侧信息加密机制设计
四 电力LTE网络侧安全接入机制设计
五 电力LTE网络安全接入测试

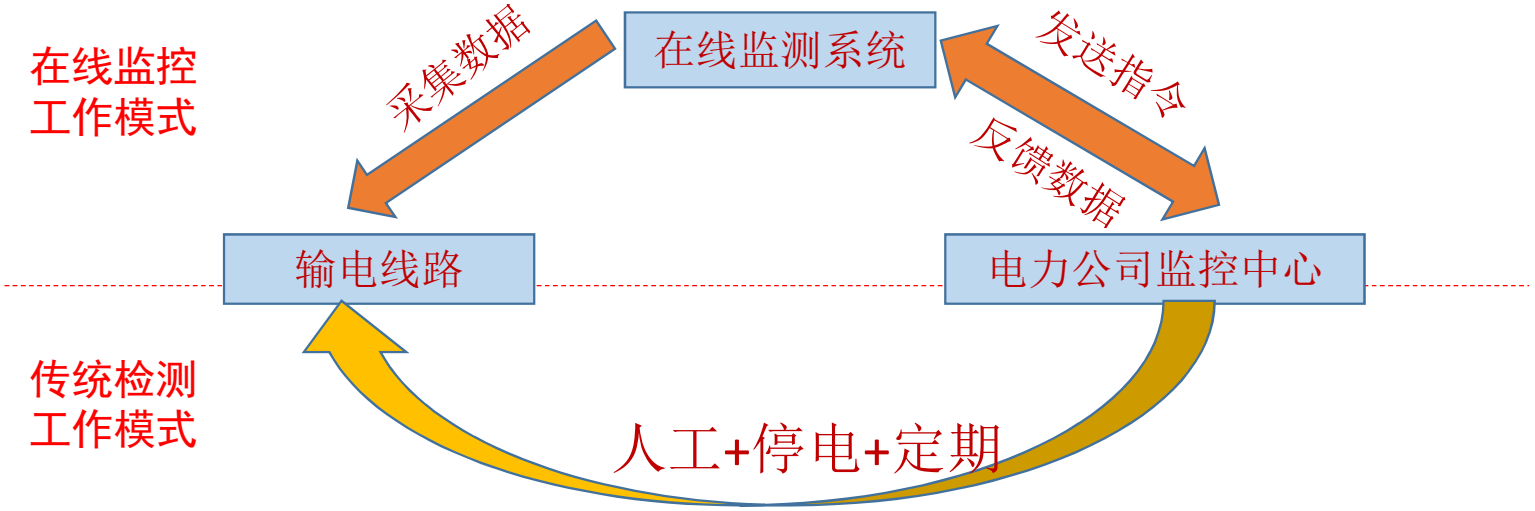
一、研究意义和主要工作

➢ 关键技术



一、研究意义和主要工作

➢ 输电线路在线监控工作模式

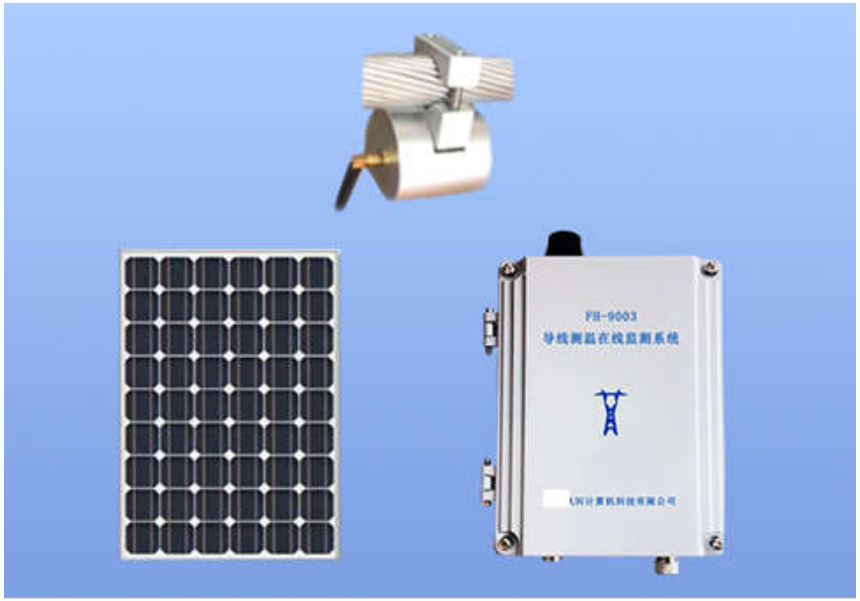


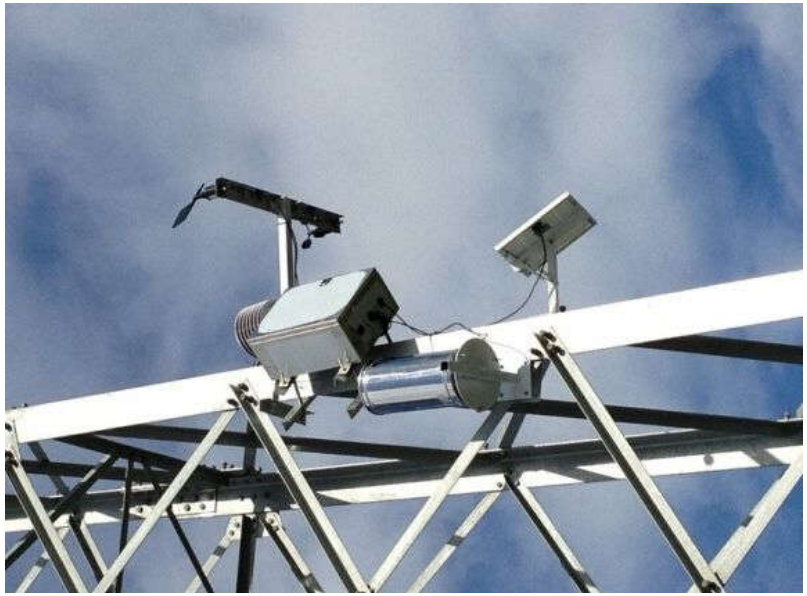
一、研究意义和主要工作

➢ 输电线路在线视频监控图

一、研究意义和主要工作

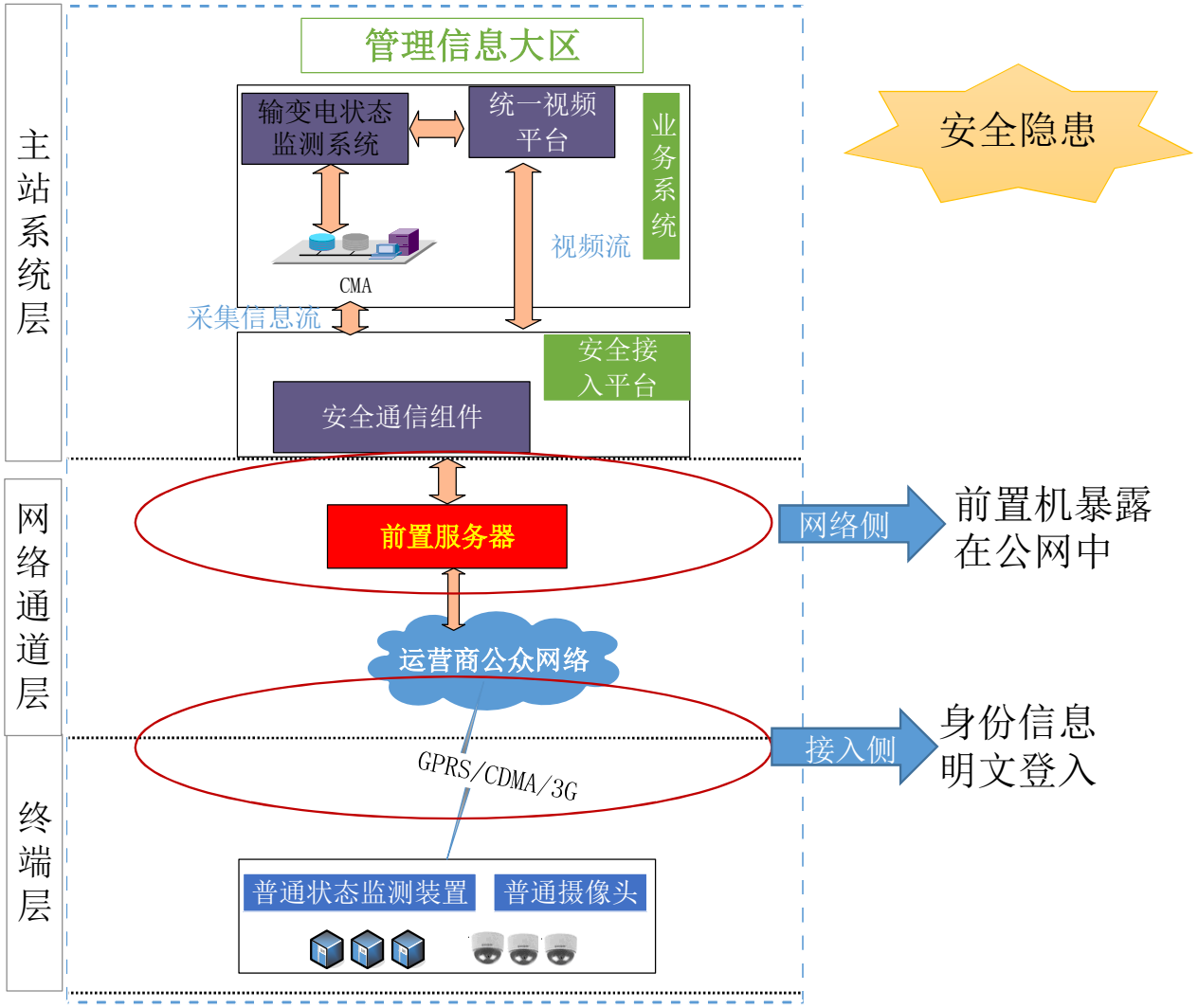
在线监测装置设备





一、研究意义和主要工作

➢ 课题现状



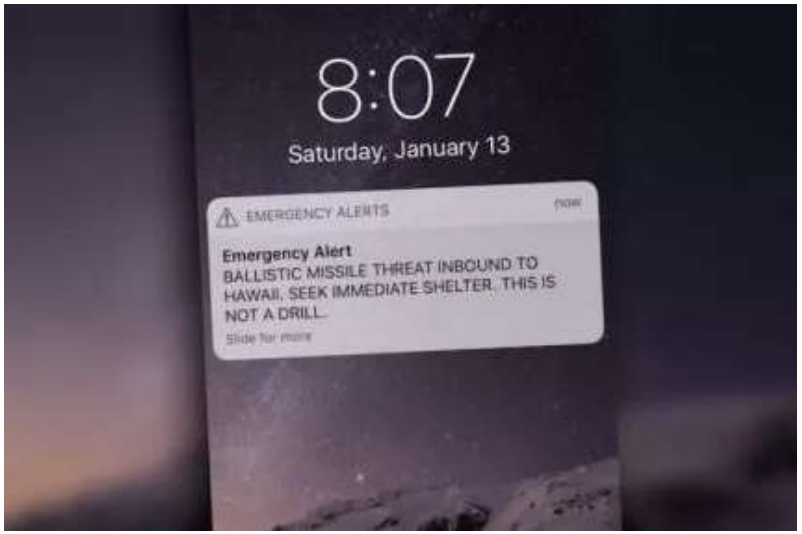
一、研究意义和主要工作

输电线路在线监测安全问题

- 2015年12月23日，乌克兰电力部门遭受恶意代码攻击，以邮件发送恶意代码载荷为攻击的直接突破口，侵入远程控制SCADA系统，下达指令切断电力供应，最终造成大面积数小时的停电事故。

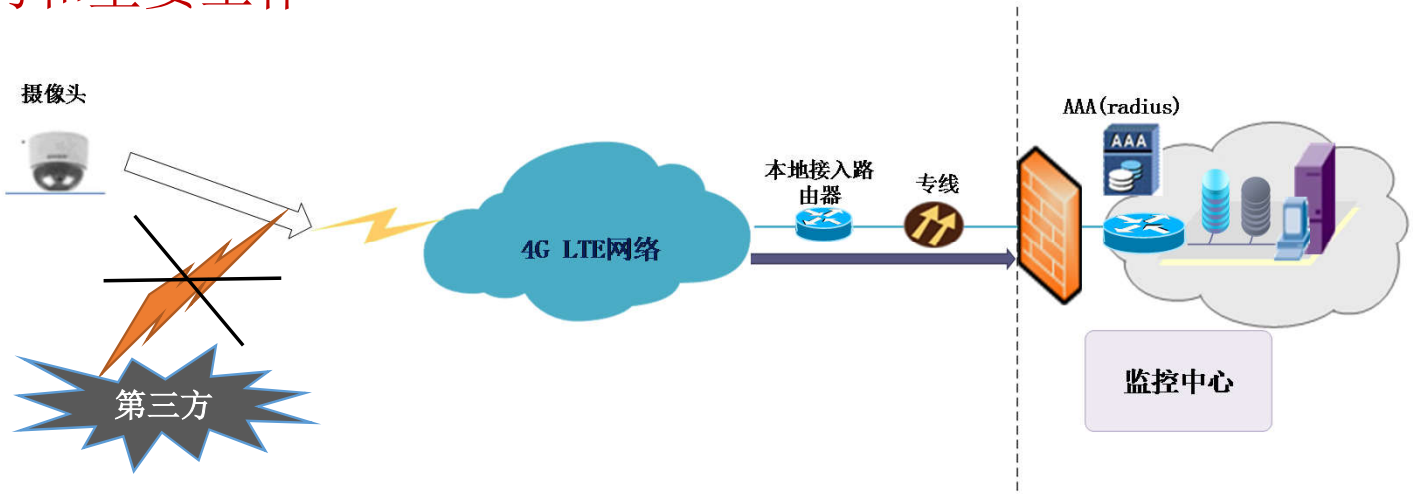
- 2014年11月，土耳其国家电力系统被入侵，总价值约6700亿美元（约合4.1万亿人民币）的账单信息被删除。

- 2019年3月，美国研发人员，使用LTE Inspector工具发现了漏洞：易导致用户信息被窃或拦截、电话遭遇窃听、中断网络连接、让设备脱机、锁定用户位置以及发出虚假报警等安全威胁。



一、研究意义和主要工作

➢研究目的和主要工作



- 针对电力LTE网络过程中的接入侧：提出改进的，适应海量终端接入请求的、高认证效率、安全的接入认证协议。

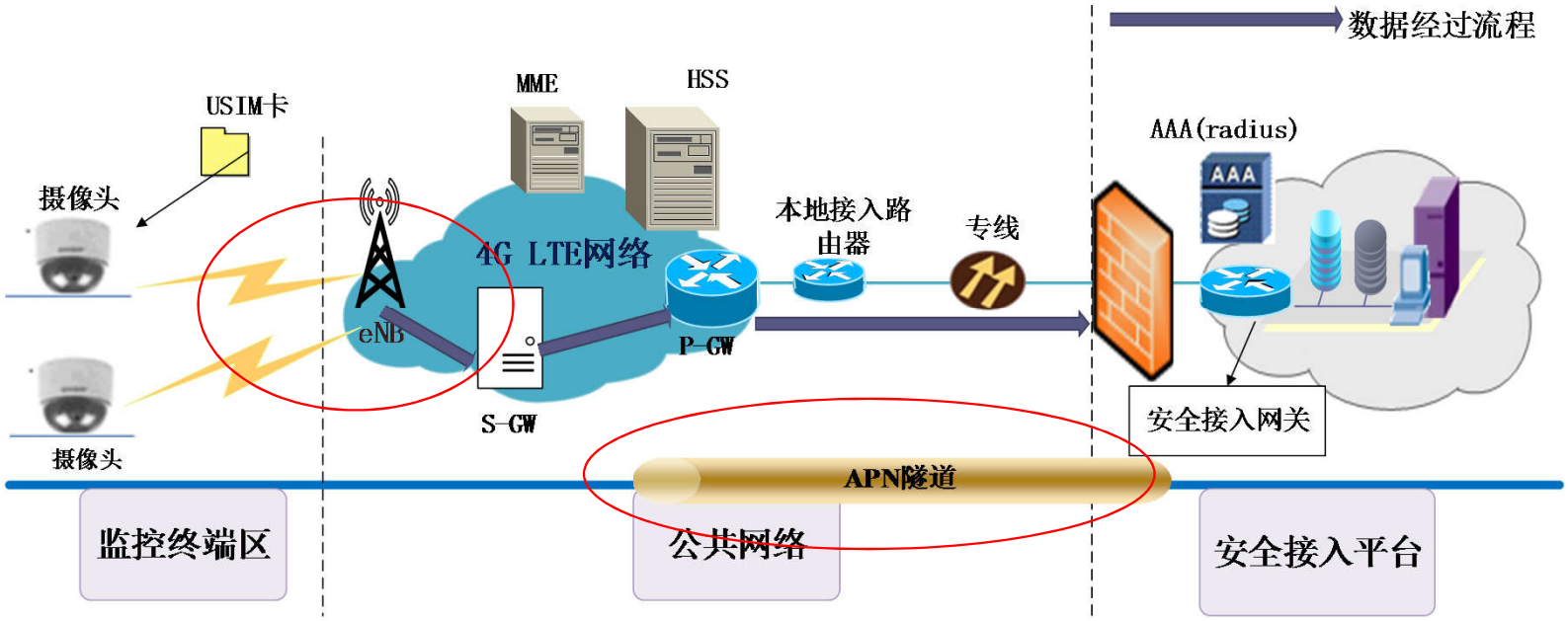
- 针对终端请求接入电力信息网络中的网络侧：分析现有的基于PKI密钥管理体系，提出安全的虚拟传输通道。

国家电网公司于2013年11月出台了《输电线路在线监测代理安全接入技术规范》，提出加强在线监测系统的安全性。

二、电力LTE系统网络架构和解决方案

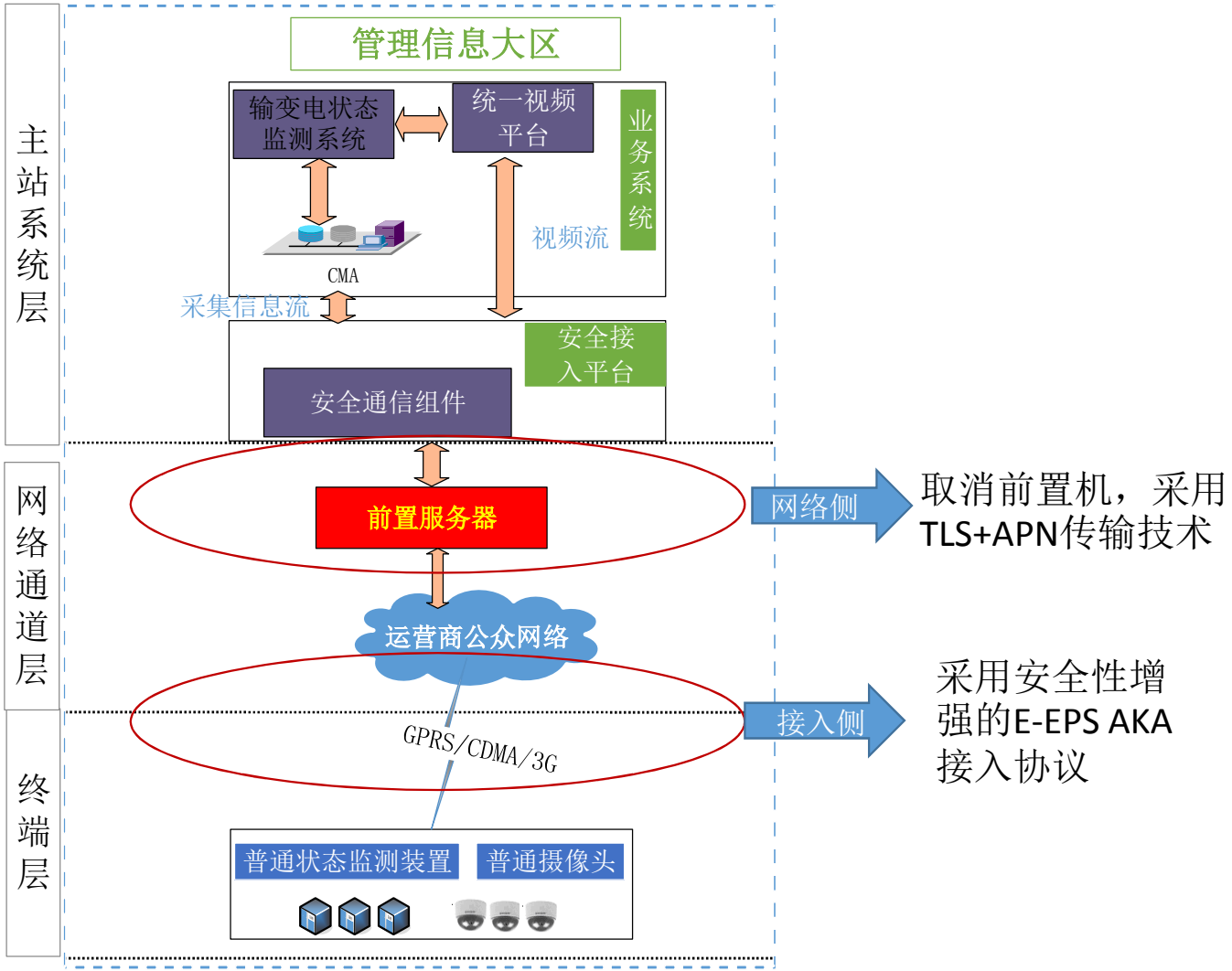
➢ 远程视频监控网络架构图

- 可信接入
- 安全传输
- 安全管理



二、电力LTE系统网络架构和解决方案

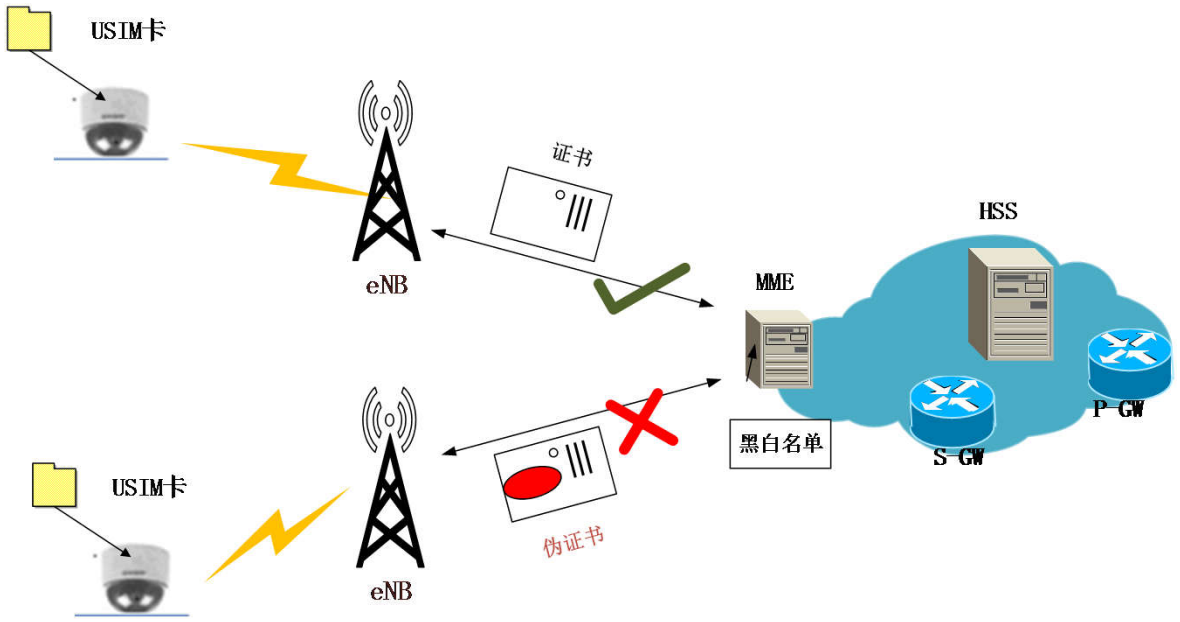
➢解决方案



二、电力LTE系统网络架构和解决方案

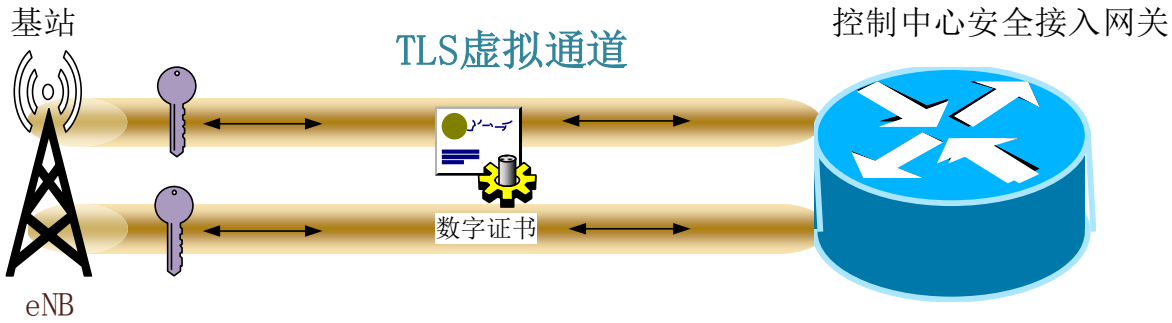
(1) 可信接入。

- 加密身份信息
- 数字证书



二、电力LTE系统网络架构和解决方案

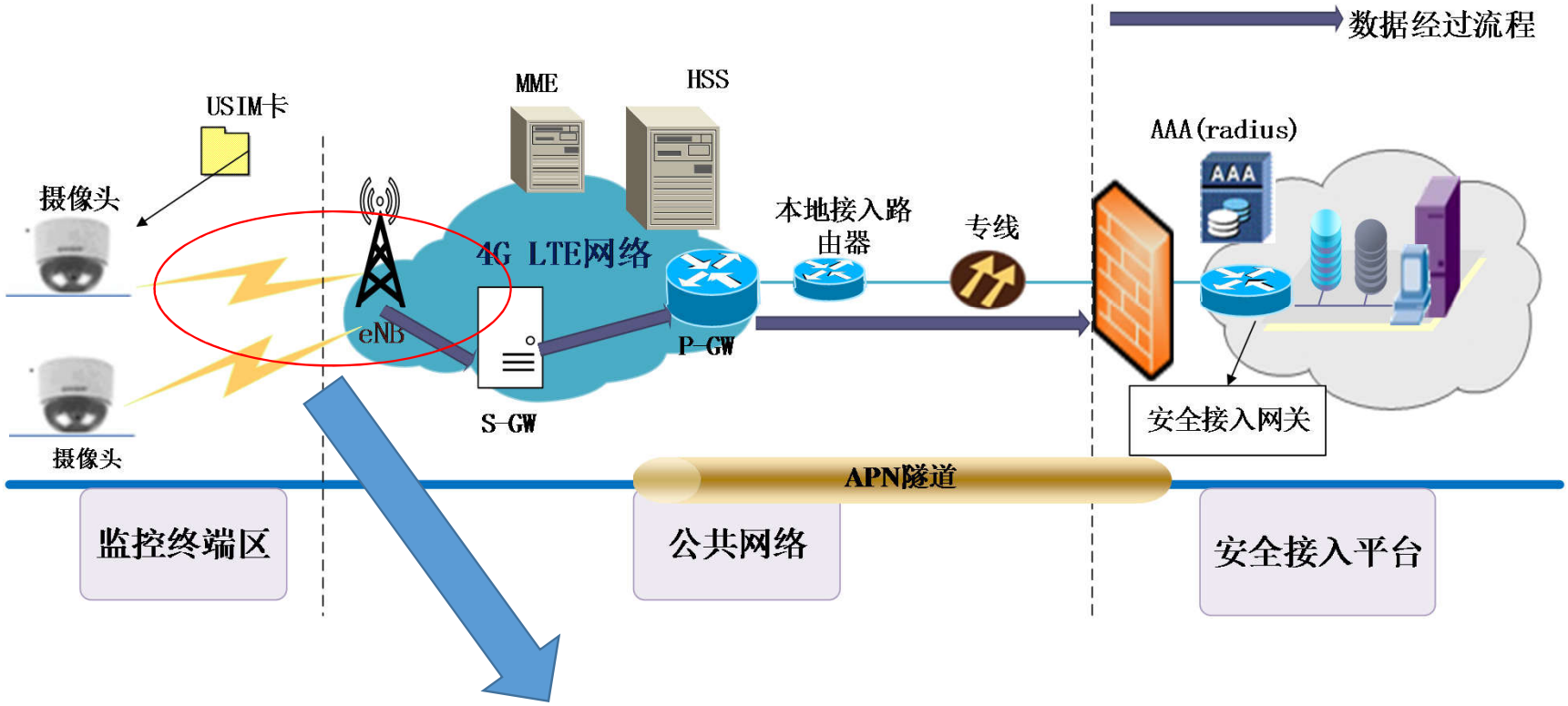
（2）安全传输



（3）安全管理

基站与安全接入网关，基站与电力控制中心管理系统之间都需要基于证书建立加密连接，保证接入及传输安全。本方案提供了基于PKI系统的证书统一管理体系，数字证书在输电线路监测终端安装前已经装在设备内部。

三、电力LTE接入侧信息加密机制设计

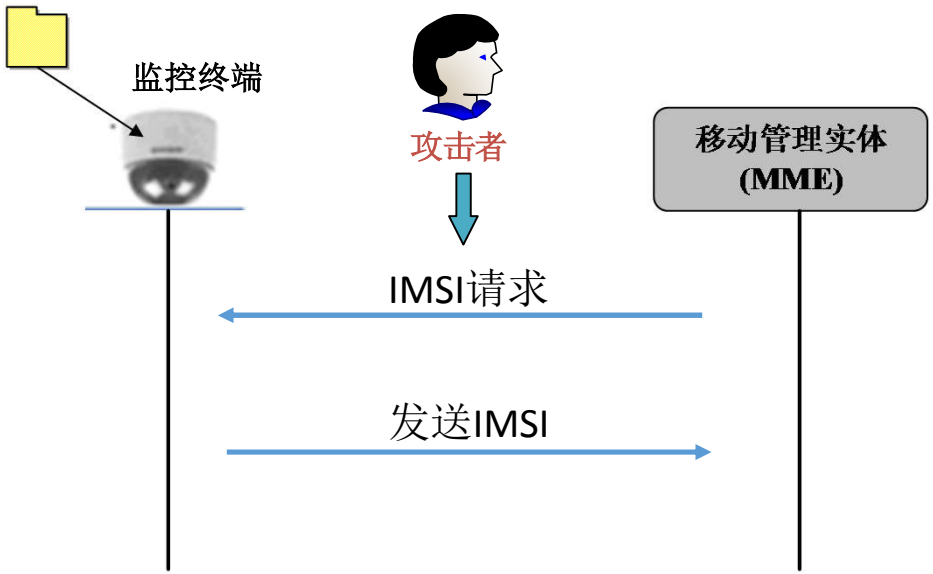


EPS AKA接入协议

三、电力LTE接入侧信息加密机制设计

➢ 攻击方式

(1) 拒绝服务攻击（DoS）



◆ 终端上传IMSI条件：

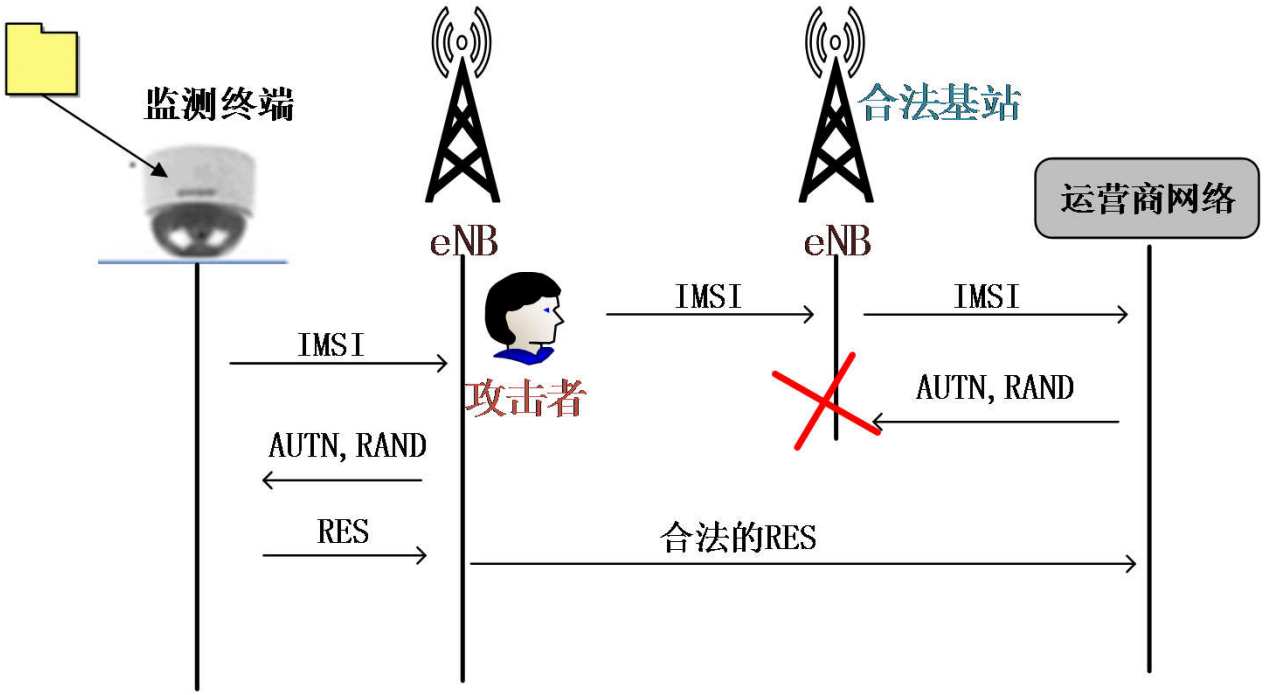
① 首次接入运营商网络或移动到其它MME覆盖范围内。

② 伪基站强行要求终端发送

③ 网络侧由于某些原因删除了保存的 TMSI（比如用户很长一段时间与网络失去联系）

三、电力LTE接入侧信息加密机制设计

（2）伪基站



（3）重放攻击

攻击者可以截获和保存输电线路在线终端和运营商网络之间的身份信息认证，并在间隔一段时间后再次发送进行干扰正常终端的请求接入。

三、电力LTE接入侧信息加密机制设计

➢ 传统的防范措施

- 对于明文IMSI

采用临时代替IMSI在网络中进行传递，这就是TMSI（临时移动用户标识）。

- 缺点

（1）攻击者可利用大量TMSI推导出可能的IMSI；

（2）计算产生负荷，分配TMSI时，也会消耗带宽。

三、电力LTE接入侧信息加密机制设计

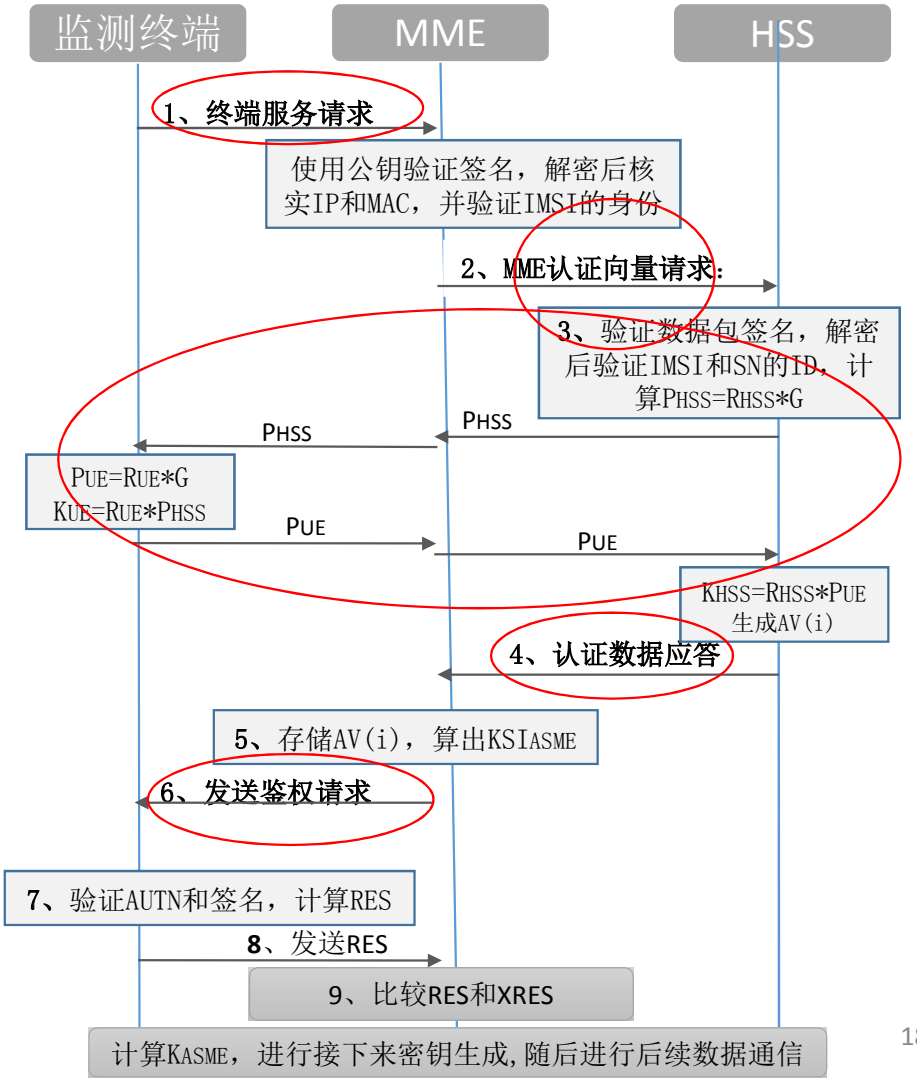
➢ 安全性增强的SE-EPS AKA

- 改进的接入过程如右：

1. 使用公钥算法ECC加密IMSI等身份信息

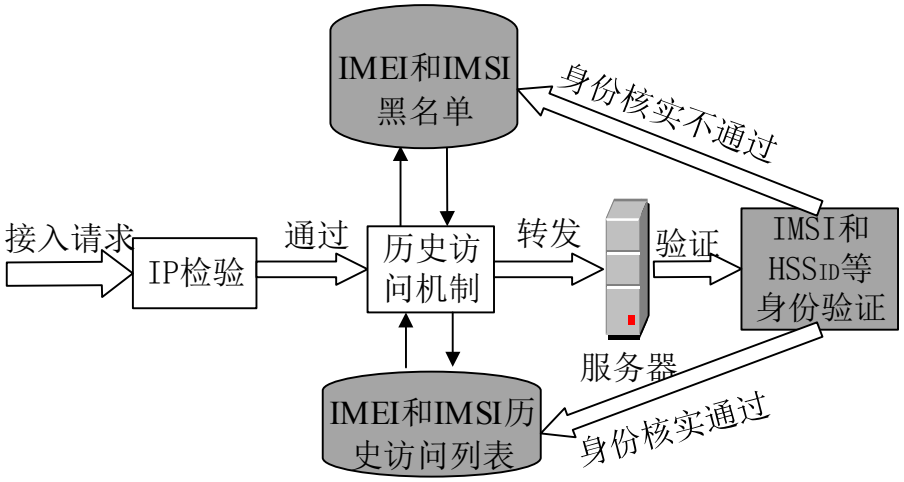
2. 使用TLS协议的椭圆曲线密钥(ECC)交换算法解决公共密钥长期共存而导致的密钥泄露问题

3. 在MME中建立MAC的历史访问机制和黑名单IMSI的白名单和访问记录机制



三、电力LTE接入侧信息加密机制设计

➢ MME中历史访问记录表



作用：可有效的防止攻击者恶意发送大量接入请求而导致网络服务器瘫痪或者拒绝服务，提高认证效率。

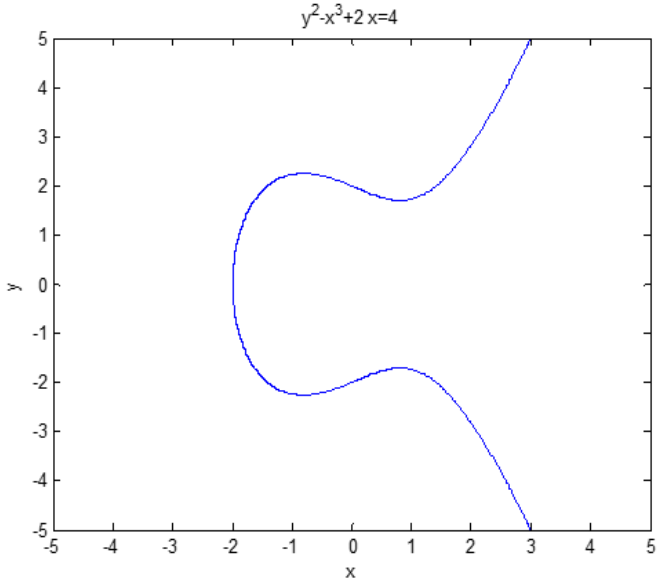
➢ ECC公钥加密算法

ECC，Elliptic curve cryptography，即椭圆加密算法。其椭圆曲线一般方程如下：

$$y^2 = ax^3 + bx^2 + cx + d$$

其中，a≠0，$ax^3+bx^2+cx+d=0$没有重根，a，b，c，d代表系数，是定义在某个域上。

例如，当a=1,b=0,c=-2,d=4时，如右图所示。



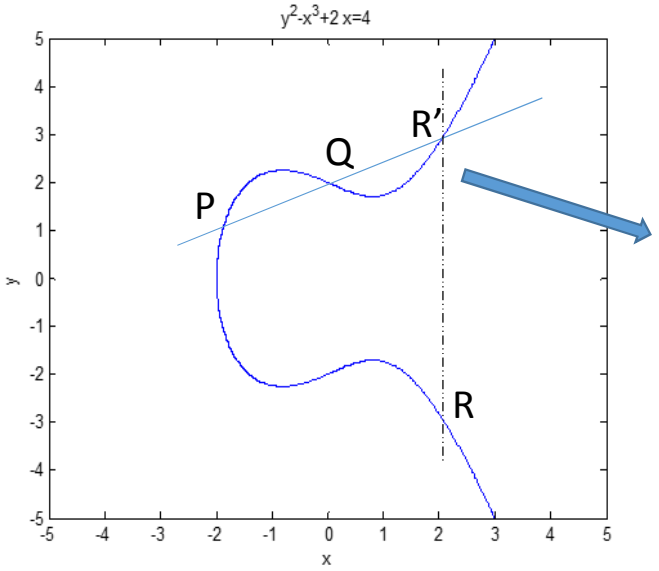
➢ 椭圆曲线离散对数问题(ECDLP)

ECC公开密钥算法基于一个关于离散对数的数学上难题，考虑如下等式：

$$K = N \times G$$

其中K , G为曲线$E_p(a,b)$ 上的点，G称为基点，N（N<n的整数，n为基点G的阶）称为私钥，K称为公钥。

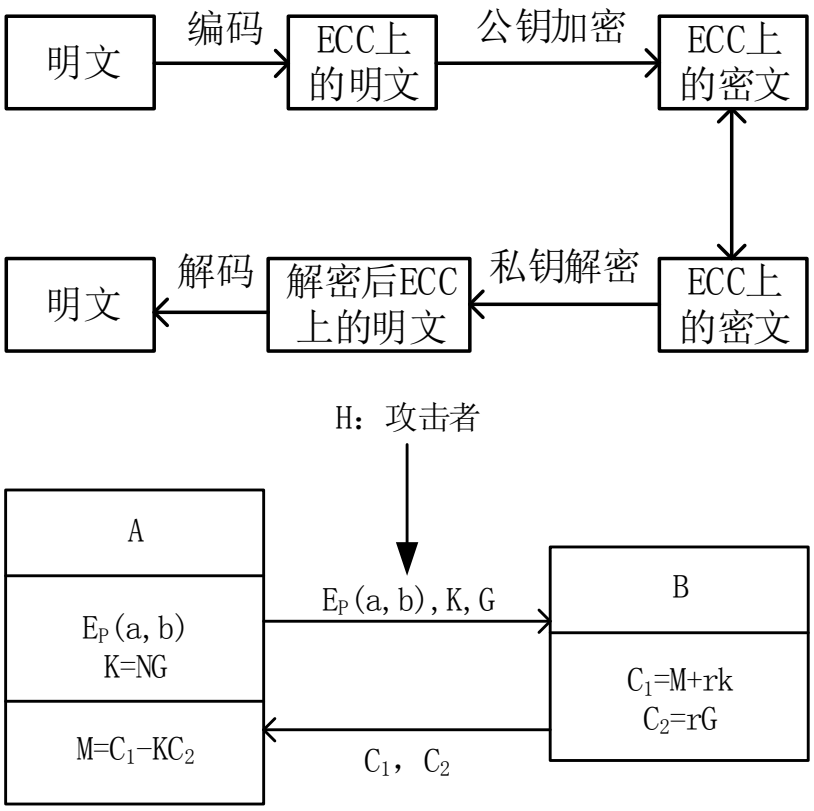
给定N和G，根据有限域的性质，计算出K很容易；但已知K和G，就很难求解出N。被称为椭圆曲线离散对数问题(ECDLP)



椭圆曲线的加法：定义P+Q=R

三、电力LTE接入侧信息加密机制设计

➢ 椭圆曲线密码体制的工作流程如下



①A选择一条椭圆曲线，并随机选取一点基点G。

② A可以选择一个私钥N，计算出公钥K=NG。

③ A将数据、点K和G传给B。

④ B接到数据信息后，然后把明文数据编码到曲线 上一点M，与此同时随机产生一个整数 r；

⑤ B算出点 C_1=M+rK; C_2=rG；

⑥ B将C1、C2传给A。

⑦ A接到消息后，算出 C_1-KC_2，

$$C_1 - kC_2 = M + rK - k(rG) = M + rK - r(NG) = M$$

三、电力LTE接入侧信息加密机制设计

➢ ECC的安全性

ECC的安全性取决于求离散对数问题的难解性，而对ECC的攻击，也就是对 ECDLP的攻击。

攻击方法

➢ 穷尽搜索法：

计算P的倍乘，一直搜索到我们想要的结果K。但是一般对n的定义$n>2^{191}$。

➢ 小步-大步算法:

通过牺牲空间来换取时间上的缩短，需要保存$n^{1/2}$点，最糟糕的情况下运算量有$n^{1/2}$步。

➢ pollard rho算法:

是小步-大步方法的一种随机版本,运算量有√（πn/2）步，忽略算法所带来的存储空间。

➢ 并行pollard rho算法：

使用r个处理器进行并行运算的话， pollard rho算法的运算量就是： √（πn）/2r

三、电力LTE接入侧信息加密机制设计

➢ECC公钥挑战

- 1999年9月28日，Certicom宣布97位的椭圆曲线离散问题被成功解决，花费了代价包括法国、美国、澳大利亚等国的760台计算机，共做了130000亿次ECC点加上的运算，计算量相当于RSA（512位）公钥算法的两倍。

- 在2000年4月9日，Robert Harley等人宣告使用pollard rho方法，求解出Certicom的挑战，花费九千五百台计算机，并且全部运行四个多月，世界各地的总共大约250个研究团队参与这次挑战，实验得到了238015条椭圆曲线。

- 2002年10月15日，由Notre Dame大学数学研究中心的Chris Monico博士后领队的数学家，花费了549天，总共使用全国10000台计算机每天24小时运行，以此解决了Certicom 的ECC挑战，被人叫做这个挑战开创了数学史上一个记录。

三、电力LTE接入侧信息加密机制设计

➢ECC与RSA的对比分析

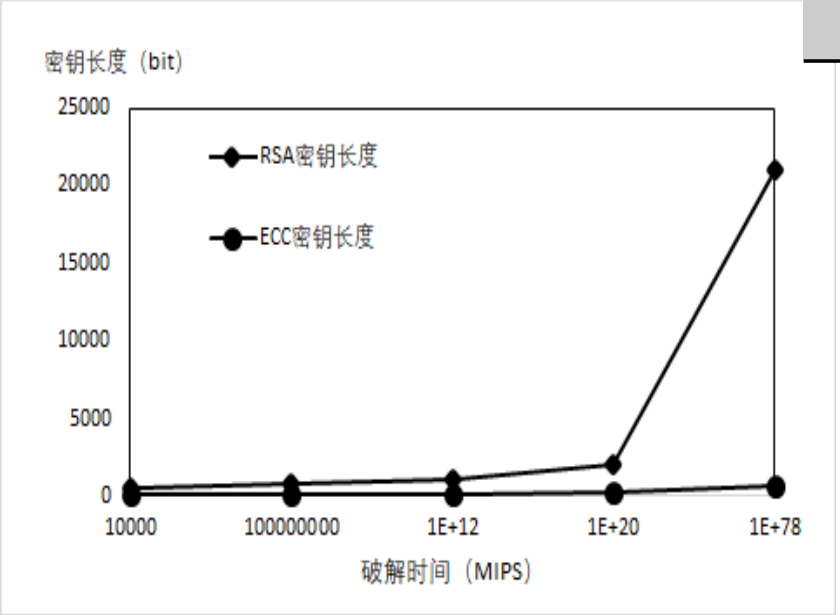
	RSA	ECC
数学理论	欧拉定理	离散对数
安全性分析	大整数分解的困难性（2个大素数）	椭圆曲线离散对数问题的困难性
安全的密钥长度	1024位	160位
作用	数字签名，加密	数字签名，加密

结论：可看出对于ECC还是RSA作用几乎相同的，不同之处就是其数学分解难度不同导致的密钥安全长度的不同。

三、电力LTE接入侧信息加密机制设计

➢ECC与RSA的对比分析

破解时间(MIPS)	RSA密钥长度(Bit)	ECC密钥长度(Bit)	密钥长度比
1.0×10^4	5.120×10^2	1.060×10^2	4.8:1
1.0×10^8	7.680×10^2	1.320×10^2	5.8:1
1.0×10^{12}	1.024×10^3	1.600×10^2	6.4:1
1.0×10^{20}	2.048×10^3	2.100×10^2	9.8:1
1.0×10^{78}	2.100×10^4	6.000×10^2	35.0:1



注：MIPS表示每秒执行100万条指令的计算机运行一年

ECC比RSA的优点：

- 安全性高
- 效率高
- 代价低

三、电力LTE接入侧信息加密机制设计

➢协议安全性能分析

对比传统身份认证协议，改进后的基于ECC公钥算法的E-EPS AKA认证协议在安全性上的优点：

五大优点

01 身份加密

IMSI和认证向量组AV(i)采用加密传输

02 相互认证

监测终端与MME身份会进行相互核实

03 认证高效率

IMEI和IMSI历史访问状态表可快速删除非法攻击者

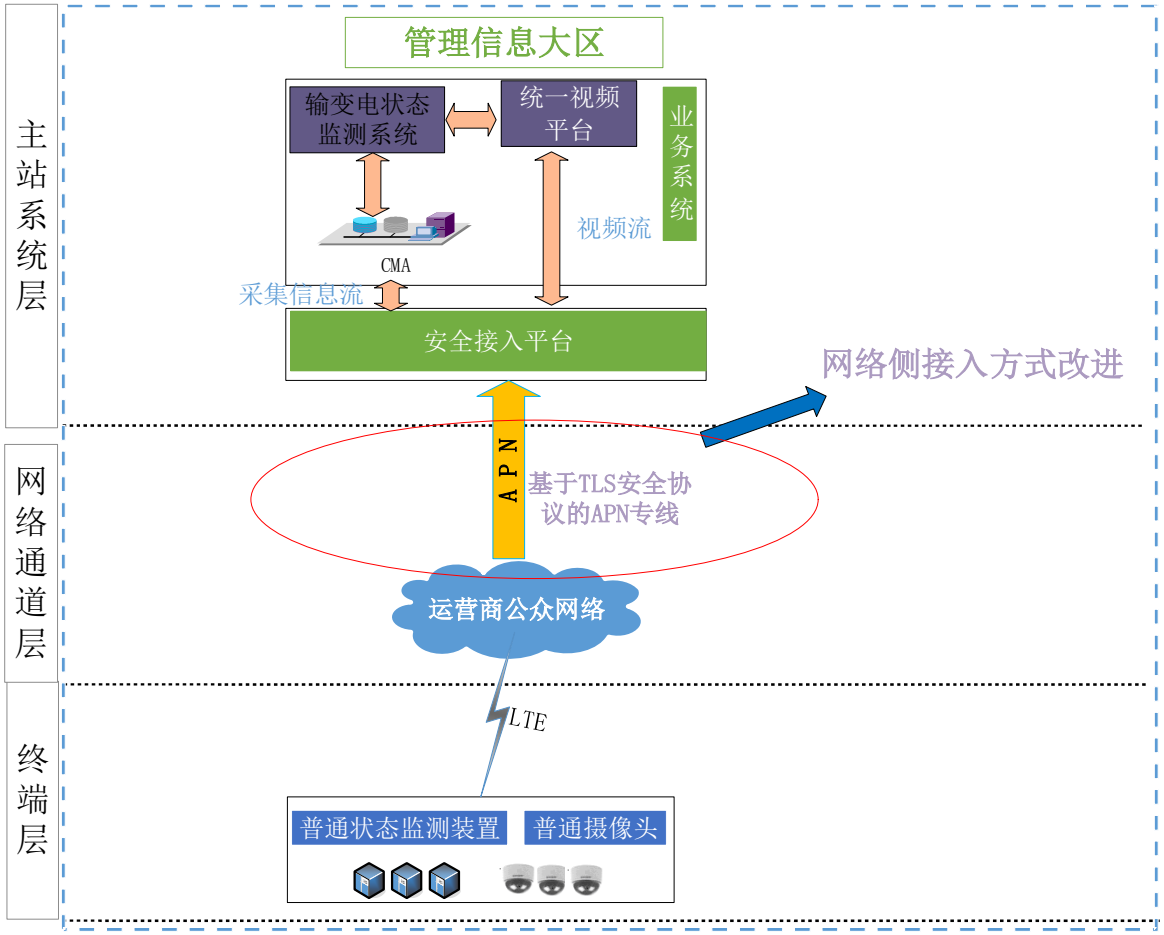
04 数据完整性

SHA-512算法验证数据来源和数据包是否被破坏

05 更安全

有效抵御伪基站和OS攻击

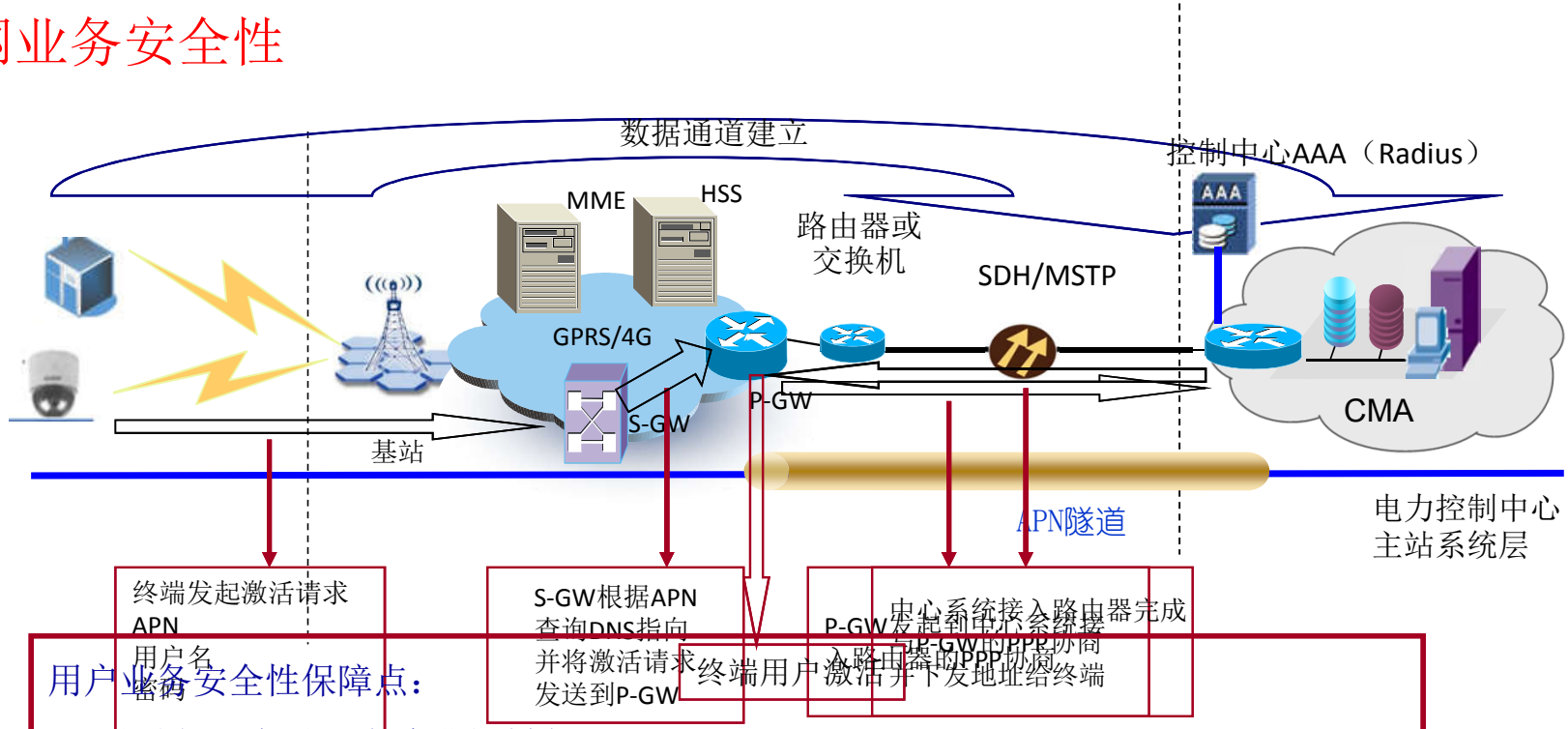
四、电力LTE网络侧安全接入机制设计



APN是由运营商分配给其他机构的，同时拥有公网的便捷和专网的安全，是一种介于公网与专网之间的虚拟专网（VPN）的业务。对于本文的输电线路在线监测系统的APN业务就是采用TLS APN技术，通过Internet或建立的 GRE专线，为电力信息网络提供准确的、安全的、稳定的加密传输业务。

四、电力LTE网络侧安全接入机制设计

➢APN组网业务安全性



用户业务安全性保障点：

1、移动侧对卡是否合法进行判定；

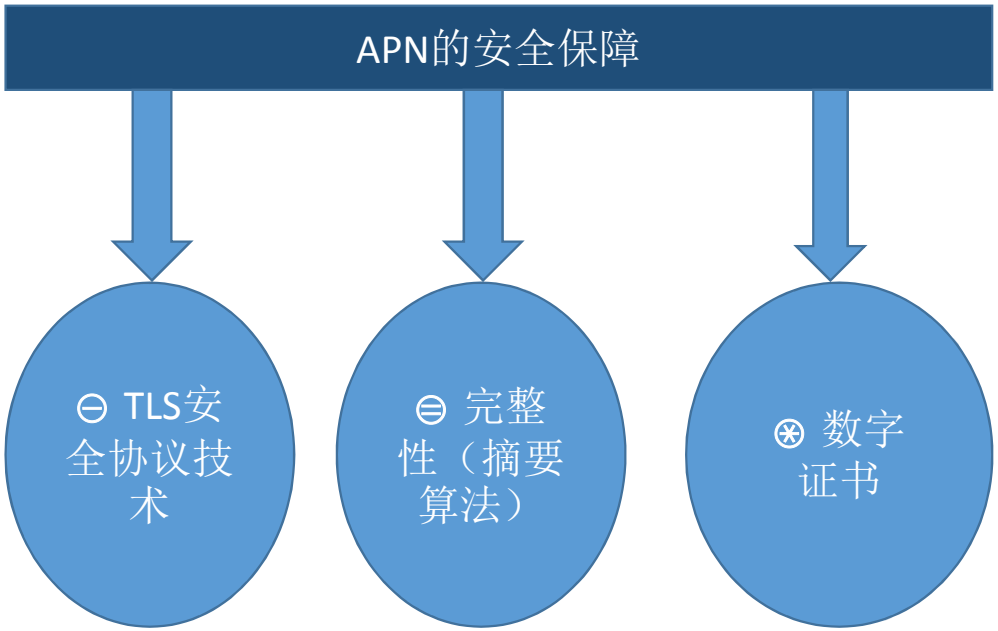
2、网络侧对于卡使用的APN是否合法进行判定

3、控制中心AAA对于用户号码或IMSI是否合法进行判定（路由器无法使用该项）；

4、控制中心AAA对于用户名、密码是否合法进行判定

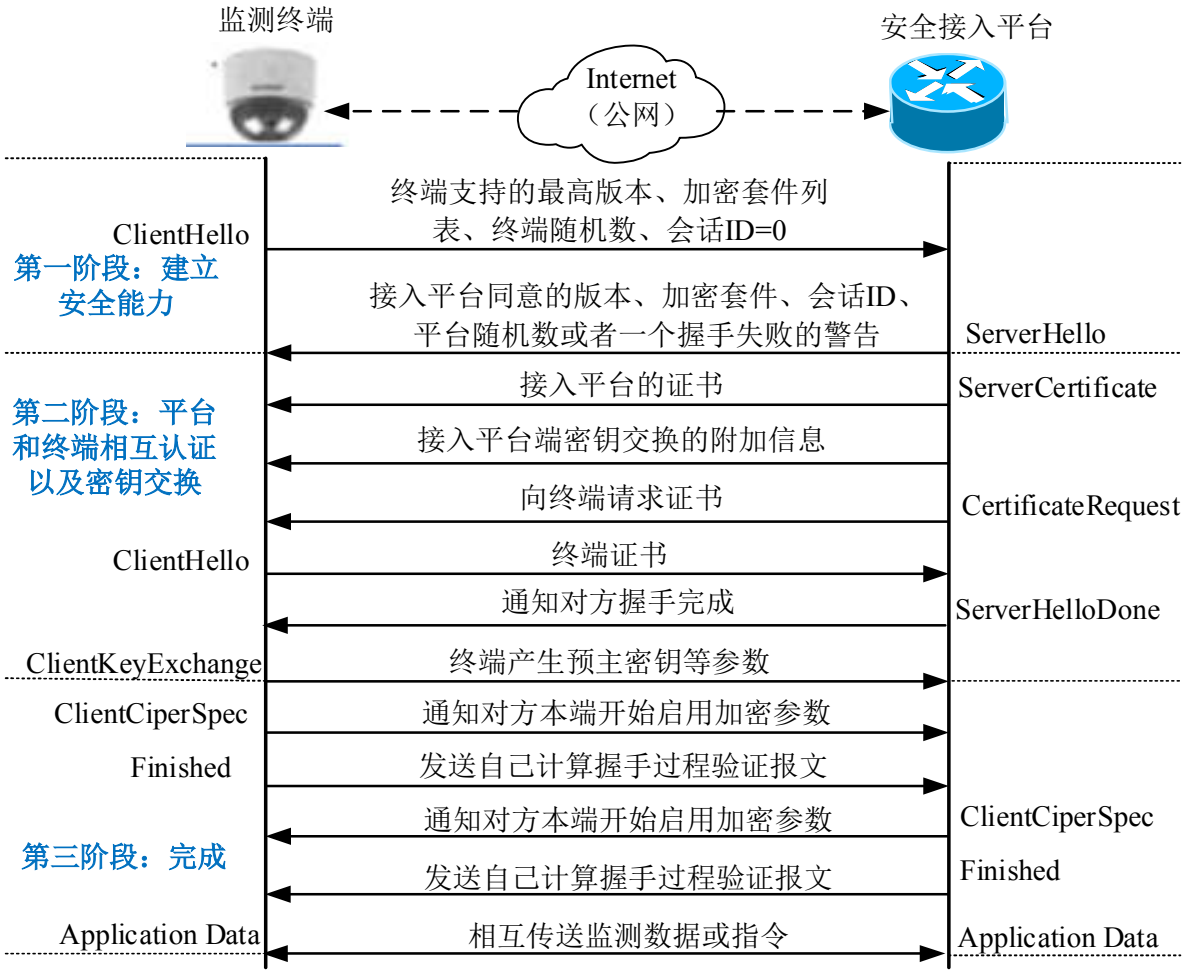
四、电力LTE网络侧安全接入机制设计

➢ APN专用通道关键技术



四、电力LTE网络侧安全接入机制设计

① TLS安全协议



四、电力LTE网络侧安全接入机制设计

TLS安全协议的特点

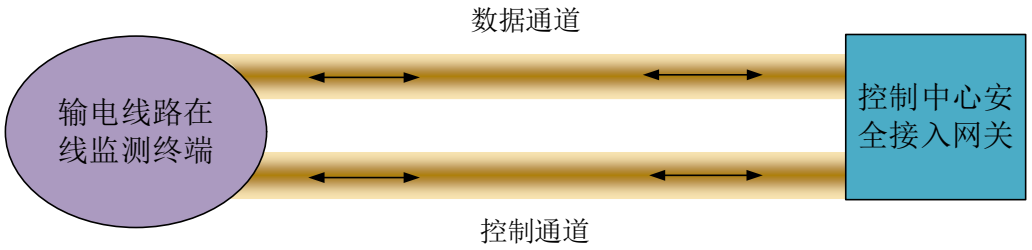
a) 运营商对终端的USIM卡是否合法进行判定；

b) 运营商判定终端的USIM卡所使用的APN是否合法，随后自行将认证信息由路由器转向控制中心的AAA；

c) 控制中心AAA判定用户卡号和IMSI是否合法（路由器无法使用该项）；

d) 控制中心AAA对于用户名、密码是否合法进行判定。

终端和电力控制中心的安全接入网关双隧道模型



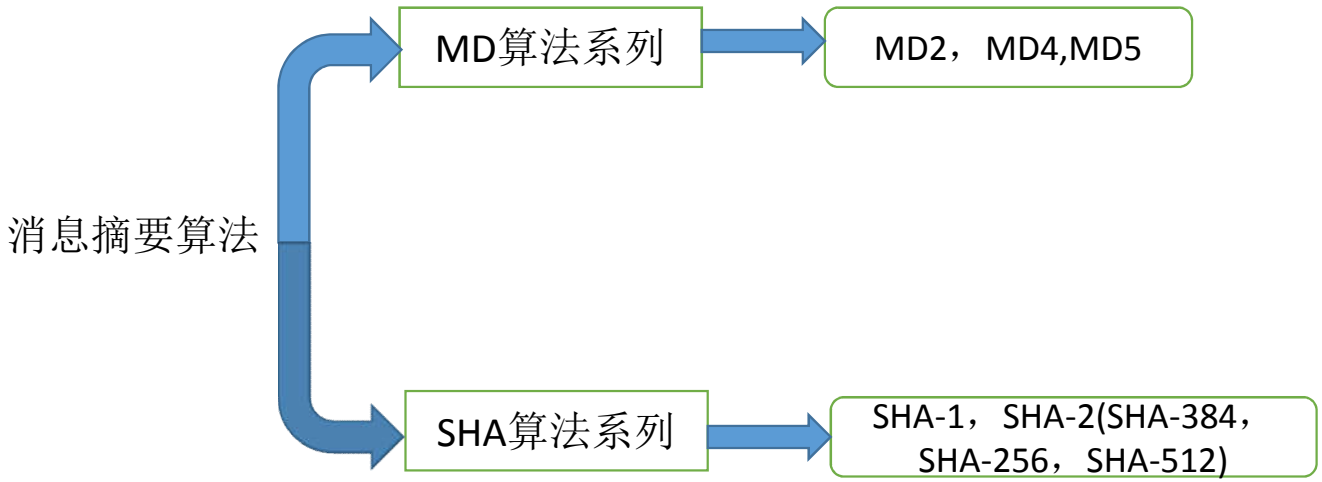
② 摘要算法

消息摘要（Message Digest）又称为数字摘要(Digital Digest)。将长度**不固定**的消息（message)作为输入参数，运行特定的Hash函数,生成**固定长度**的输出，这个输出就是Hash.也称为这个消息的消息摘要（Message Digest）.

文本　　固定长度的hash值

四、电力LTE网络侧安全接入机制设计

- 消息摘要算法分类



四、电力LTE网络侧安全接入机制设计

- 摘要算法的特点：

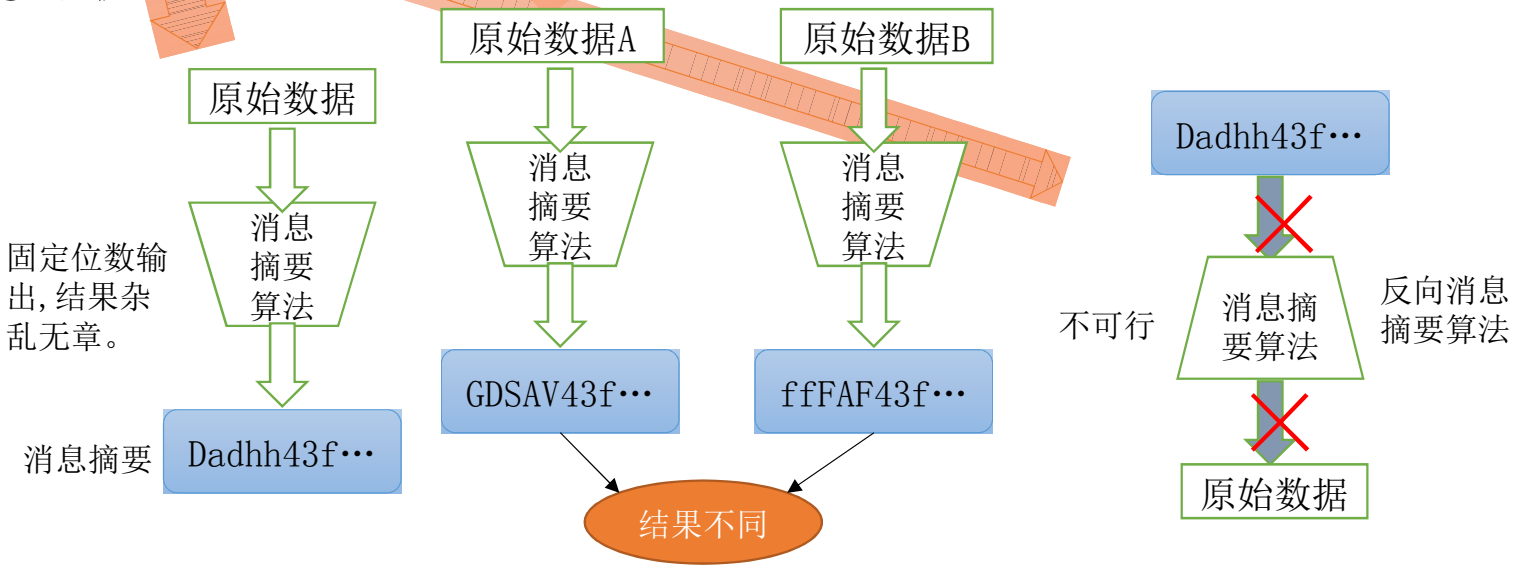
① **固定输出**：消息的输出长度总是固定的；

② **无序输出**：消息摘要看起来是“随机的”，像是胡乱的杂凑在一起的；

③ **相同输入相同输出**：一般地，只要输入的消息不同，对其进行摘要以后产生的摘要消息也必不相同（潜在意识是可以相同）；但相同的输入必会产生相同的输出；

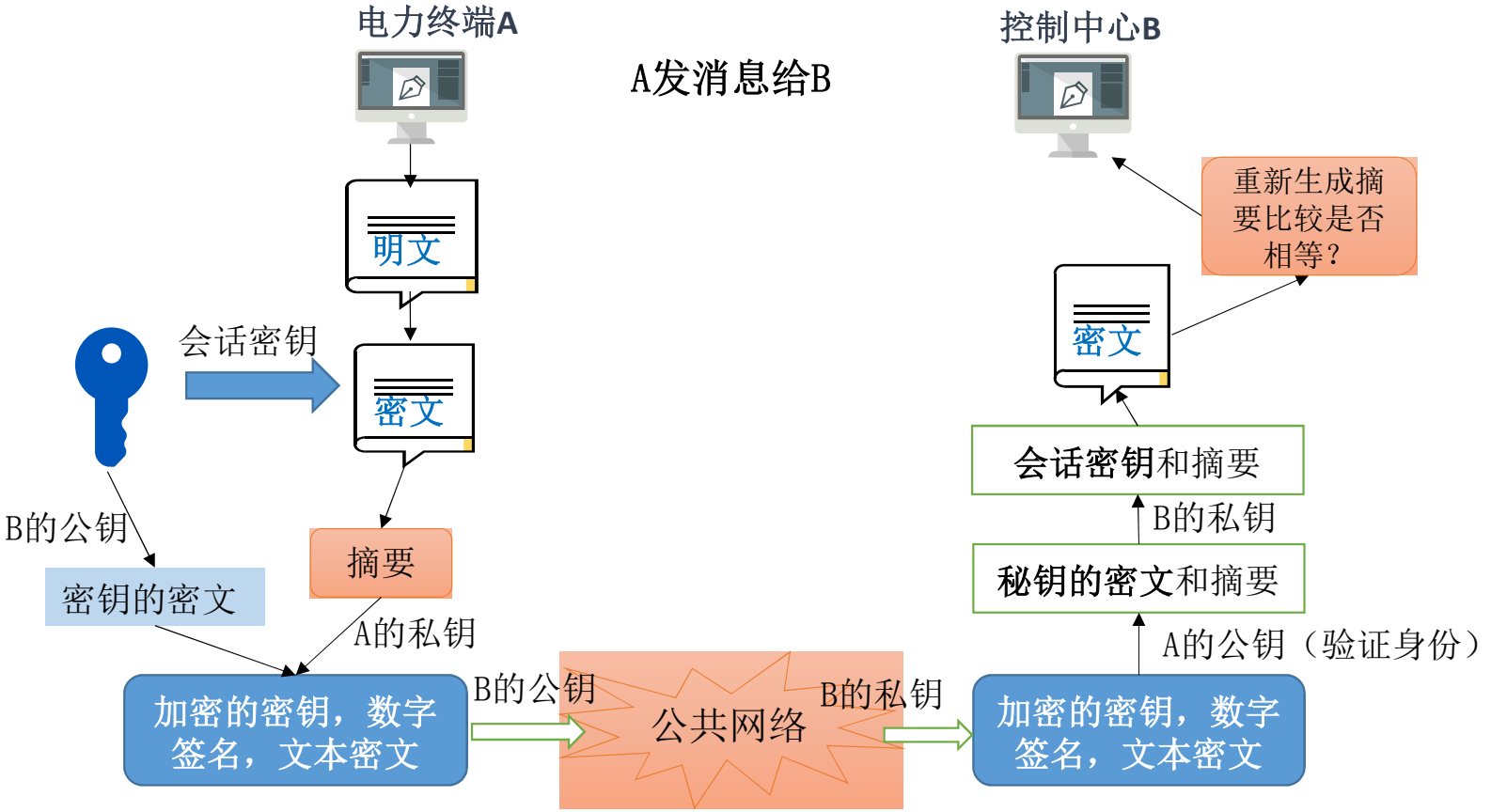
④ **单向导出**：消息摘要函数是无陷门的单向函数；

⑤ **强抗碰撞**：好的摘要算法，无法从中找到“碰撞”，但是“碰撞”是肯定存在的。



四、电力LTE网络侧安全接入机制设计

- 摘要算法与公钥算法在输电线中应用

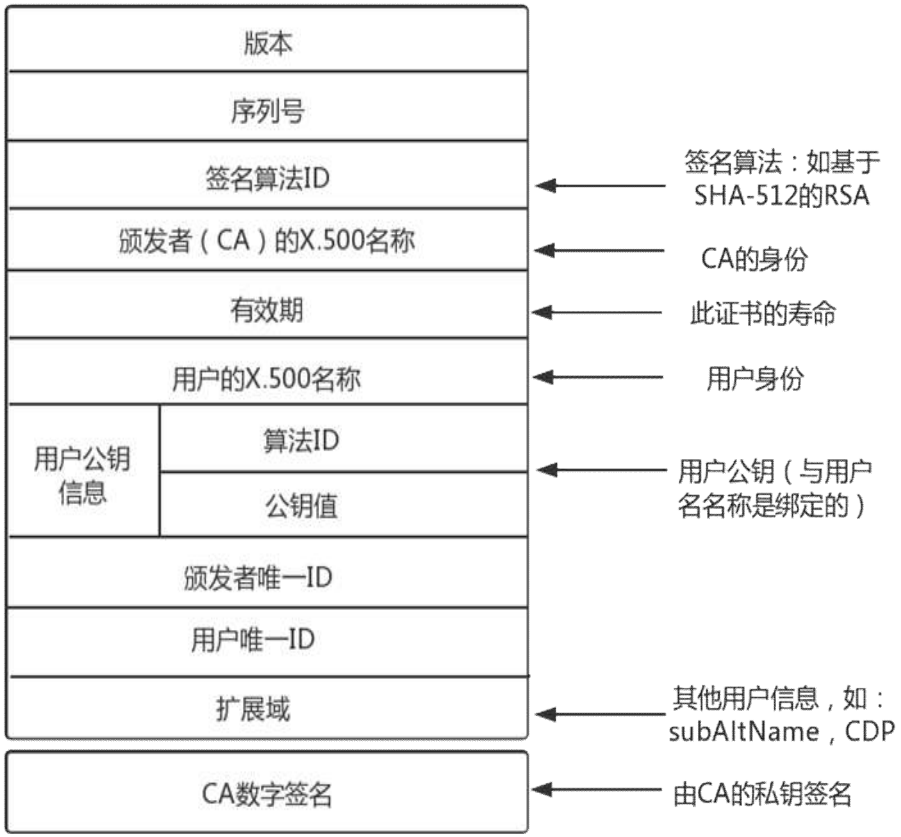


四、电力LTE网络侧安全接入机制设计

③ 数字证书

- 数字证书简介

在电力终端请求接入认证的机构中，需要有一个值得信赖的第三方，用于判定、颁发数字证书和管理某些私密信息，即CA认证中心，以此确认某个公开密钥的终端的真实身份。（X.509数字证书如右：）



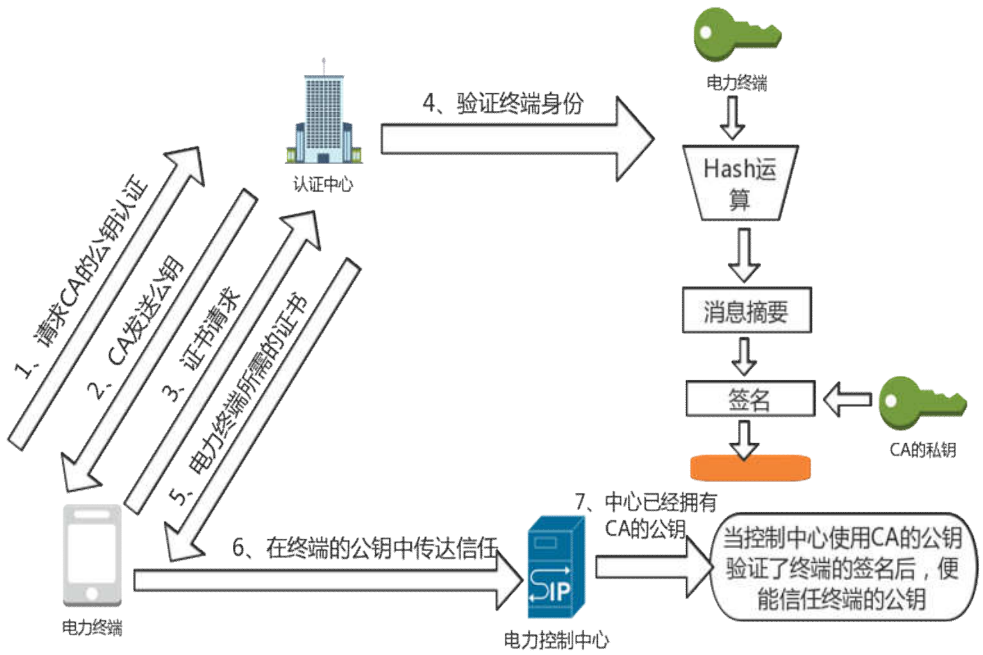
四、电力LTE网络侧安全接入机制设计

1）数字证书获取（方法一）

带好认证材料，直接去数字证书认证管理中心有限公司申请。

四、电力LTE网络侧安全接入机制设计

2）数字证书获取（方法二）



① 终端首先请求CA的证书。

② CA中心发送自己的根证书给电力终端。

③ 终端产生一个证书请求，其中包含终端的身份信息和公钥，然后电力终端用CA公钥签名此证书请求。

④ CA中心获得证书请求，验证电力终端的身份，并产生一个数字证书，绑定其身份和公钥，由此产生的数字证书签名。

⑤ CA认证中心向终端颁发证书。

⑥ 当终端收到身份证书后，便将其呈递给中心。

⑦ 中心将验证此数字签名，以确认终端的证书，以传达信任。随后便对终端的公钥建立信任。

五、电力LTE网络安全接入测试

1 软件平台开发参数

参数	说明
系统版本	Windows7（64）操作系统
处理器	Intel(R) Core(TM) i3−3220 CPU @3.30GHz
内存	4.00GB
Eclipse版本	Oxygen-R

2 硬件平台开发参数

参数	说明
系统版本	Ubuntu16.04 LTS
处理器	Intel®Core™i3−2350 CPU @323.30GHz x 4
内存	3.8 GB
软件无线电平台	HackRF One

五、电力LTE网络安全接入测试

实验1：E-EPS AKA接入协议加密算法性能测试

基于ECC算法的E-EPS AKA认证协议比现有EPS AKA认证协议增加了部分算法，包含公钥算法ECC、完整性算法SHA-512等。使用Java语言对算法进行测试。实验数据统一512比特。

（1）公钥算法RSA和ECC测试：

1）ECC运行 测试1000次时间（单位ms）

测试次数	1	2	3	4	5	1000	平均值
加密耗时	226.352	234.257	226.963	229.824	228.571	227421	227.421
解密耗时	0.515	0.527	0.412	0.479	0.505	506	0.506

1）RSA运行测试1000次时间（单位ms）

测试次数	1	2	3	4	5	1000	平均值
加密耗时	482.011	384.627	513.494	478.552	517.127	414285	414.285
解密耗时	4.391	4.794	4.592	3.251	4.268	4186	4.186

五、电力LTE网络安全接入测试

（2）完整性算法MD5和SHA-512测试如下：

1）MD5运行测试1000次时间（单位ms）

测试次数	1	2	3	4	5	1000	平均值
加密耗时	5.930	5.120	4.892	5.729	5.184	4843	4.843

2）SHA系列运行测试1000次时间（单位ms）

测试次数	1	2	3	4	5	1000	平均值
SHA-1	0.620	0.673	0.531	0.672	0.584	586	0.612
SHA-256	0.518	0.597	0.612	0.520	0.536	524	0.524
SHA-384	0.507	0.561	0.518	0.602	0.509	518	0.518
SHA-512	0.298	0.327	0.276	0.392	0.294	284	0.284

五、电力LTE网络安全接入测试

(3)E-EPS AKA协议与EPS AKA协议安全性能和复杂度（效率）对比

1）接入认证性能比较

协议	身份保密	AV保密	双向认证	认证效率	密钥更新
EPS AKA	否	否	否	否	否
SE-EPS AKA	是	是	是	是	是

2）接入认证效率对比

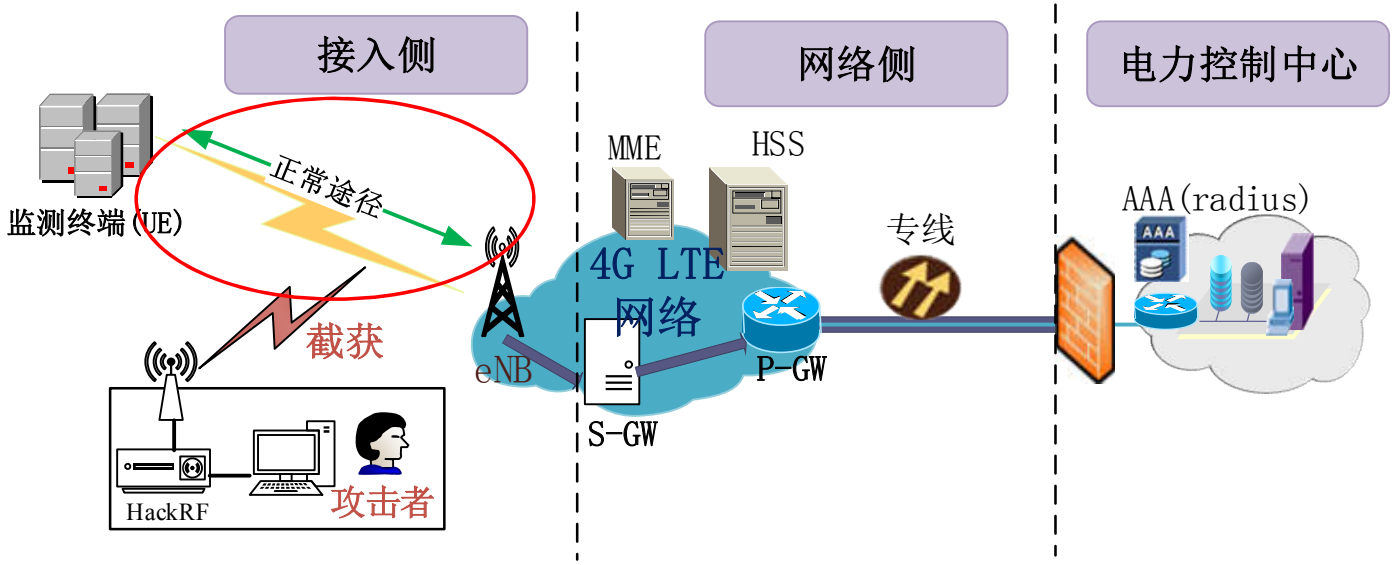
	EPS AKA	E-EPS AKA
传输次数	5	10
加密次数	0	5
验证次数	3	8

总结：

尽管新方案多增加几个算法的运行时间，但是公钥算法和完整性算法加解密耗时并不长，并且身份信息的多次验证有利于智能电网的安全。因此，对于SE-EPS AKA认证协议中少量的身份核实消息来说，这些加密算法仅在接入时才用到，并不影响实时监控建立终端。

实验2 电力LTE网络接入侧仿真系统实验

- 截获IMSI等身份信息



五、电力LTE网络安全接入测试

- 实验准备

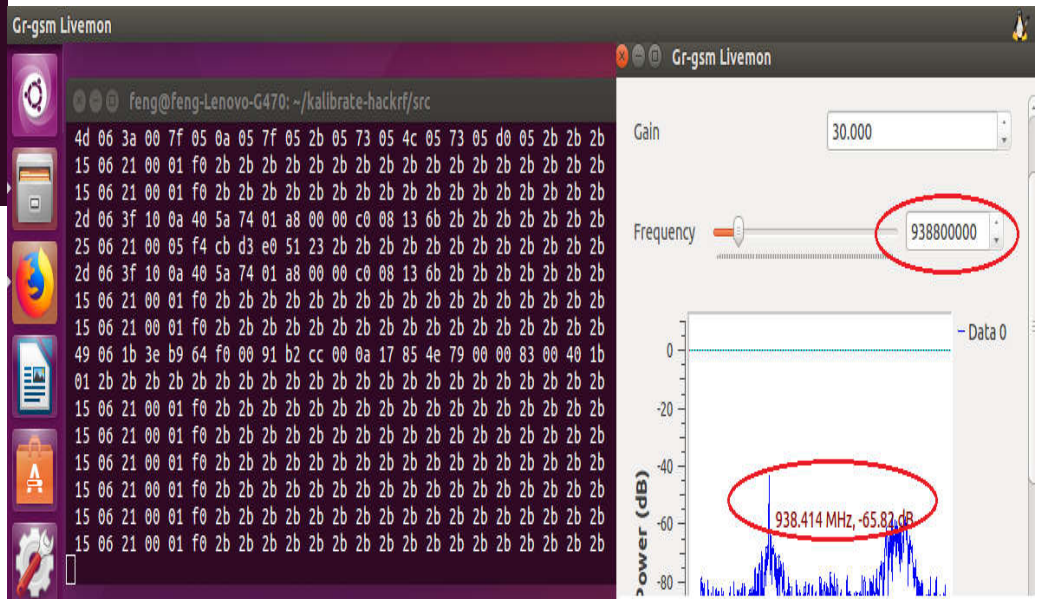
终端设备IMEI和IMSI

攻击身份信息的仿真平台

五、电力LTE网络安全接入测试

```
root@feng-Lenovo-G470: ~/kalibrate-hackrf/src
root@feng-Lenovo-G470:~/kalibrate-hackrf/src# ./kal -s GSM900 -g 40 -l 40
kal: Scanning for GSM-900 base stations.
GSM-900:
        chan:     7 (936.4MHz - 11.985kHz)        power:  613342.34
        chan:     8 (936.6MHz - 37.742kHz)        power:  667097.05
        chan:    13 (937.6MHz + 27.859kHz)        power:  603803.93
        chan:    14 (937.8MHz + 12.398kHz)        power:  545184.68
        chan:    15 (938.0MHz - 10.471kHz)        power:  649645.38
        chan:    21 (939.2MHz - 30.814kHz)        power: 1088970.44
        chan:    39 (942.8MHz + 37.999kHz)        power: 1064855.50
        chan:    41 (943.2MHz - 20.252kHz)        power:  909523.72
        chan:    42 (943.4MHz - 20.183kHz)        power:  992699.61
        chan:    47 (944.4MHz + 27.379kHz)        power: 1706136.38
        chan:    48 (944.6MHz + 2.404kHz)         power: 1558773.93
        chan:    49 (944.8MHz - 22.724kHz)        power: 1681605.25
        chan:    50 (945.0MHz - 32.386kHz)        power: 1735192.87
        chan:    78 (950.6MHz + 7.725kHz)         power:  536463.62
        chan:    83 (951.6MHz + 38.232kHz)        power: 1444200.37
        chan:    84 (951.8MHz + 34.203kHz)        power: 1396595.63
        chan:    85 (952.0MHz + 10.945kHz)        power: 1533028.29
        chan:    86 (952.2MHz - 14.419kHz)        power: 1635271.17
        chan:    87 (952.4MHz - 37.967kHz)        power: 1398376.32
        chan:    90 (953.0MHz + 36.843kHz)        power: 1513206.10
root@feng-Lenovo-G470:~/kalibrate-hackrf/src#
```

信号搜索



选取938.8MHz频率截获终端信息

五、电力LTE网络安全接入测试

- IMSI-catche捕获

```
正在处理用于 libc-bin (2.23-0ubuntu10) 的触发器 ...
feng@feng-Lenovo-G470:~/IMSI-catcher$ sudo python simple_IMSI-catcher.py --sniffWARNING: No route found for IPv6 destination :: (no default rou
te?)
Nb IMSI ; TMSI-1     ; TMSI-2     ; IMSI             ; country      ; brand      ; operator             ; MCC  ; MNC   ; LAC    ; CellId
1       ;            ;            ; 460 02 0743790927 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
2       ;            ;            ; 460 00 9229075973 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
3       ;            ;            ; 460 02 3290084007 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
4       ;            ;            ; 460 02 7105562297 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
        ; 0xb50e77a8 ;            ; 460 02 7105562297 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
        ; 0xb50e77a8 ; 0xd381d087 ; 460 02 7105562297 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
5       ;            ;            ; 460 02 7404627492 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
6       ;            ;            ; 460 02 6918544203 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
7       ;            ;            ; 460 04 1156204049 ; China        ;            ; Global Star Satellite ; 460  ; 00    ; 37298  ; 16057
8       ;            ;            ; 460 02 0744617337 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
9       ;            ;            ; 460 00 1904953201 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
10      ;            ;            ; 460 02 3029268440 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
11      ;            ;            ; 460 00 2452746968 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
12      ;            ;            ; 460 02 7894149338 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
13      ;            ;            ; 460 07 8029496482 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
14      ;            ;            ; 460 07 8618215005 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
15      ;            ;            ; 460 02 6918861966 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
16      ;            ;            ; 460 02 0883171444 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
        ; 0xc2da4804 ;            ; 460 02 0883171444 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
17      ;            ;            ; 460 02 5851292398 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
18      ;            ;            ; 460 02 7929958830 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
19      ;            ;            ; 460 02 6203053150 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
20      ;            ;            ; 460 02 6918143390 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
        ; 0x3e08bb34 ;            ; 460 02 6918143390 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
21      ;            ;            ; 460 02 7929995926 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
22      ;            ;            ; 460 04 0825802289 ; China        ;            ; Global Star Satellite ; 460  ; 00    ; 37298  ; 16057
23      ;            ;            ; 460 00 1824983926 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
24      ;            ;            ; 460 02 1914578295 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
25      ;            ;            ; 460 02 0846389772 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
26      ;            ;            ; 460 04 1023408480 ; China        ;            ; Global Star Satellite ; 460  ; 00    ; 37298  ; 16057
27      ;            ;            ; 460 04 1154903392 ; China        ;            ; Global Star Satellite ; 460  ; 00    ; 37298  ; 16057
28      ;            ;            ; 460 00 1933988674 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
29      ;            ;            ; 460 02 0846337783 ; China        ; China Mobile ; China Mobile         ; 460  ; 00    ; 37298  ; 16057
```

TMSI：国际移动识别码的临时身份信息；

Country：终端设备所属的国家地区，

brand：运营商类别；

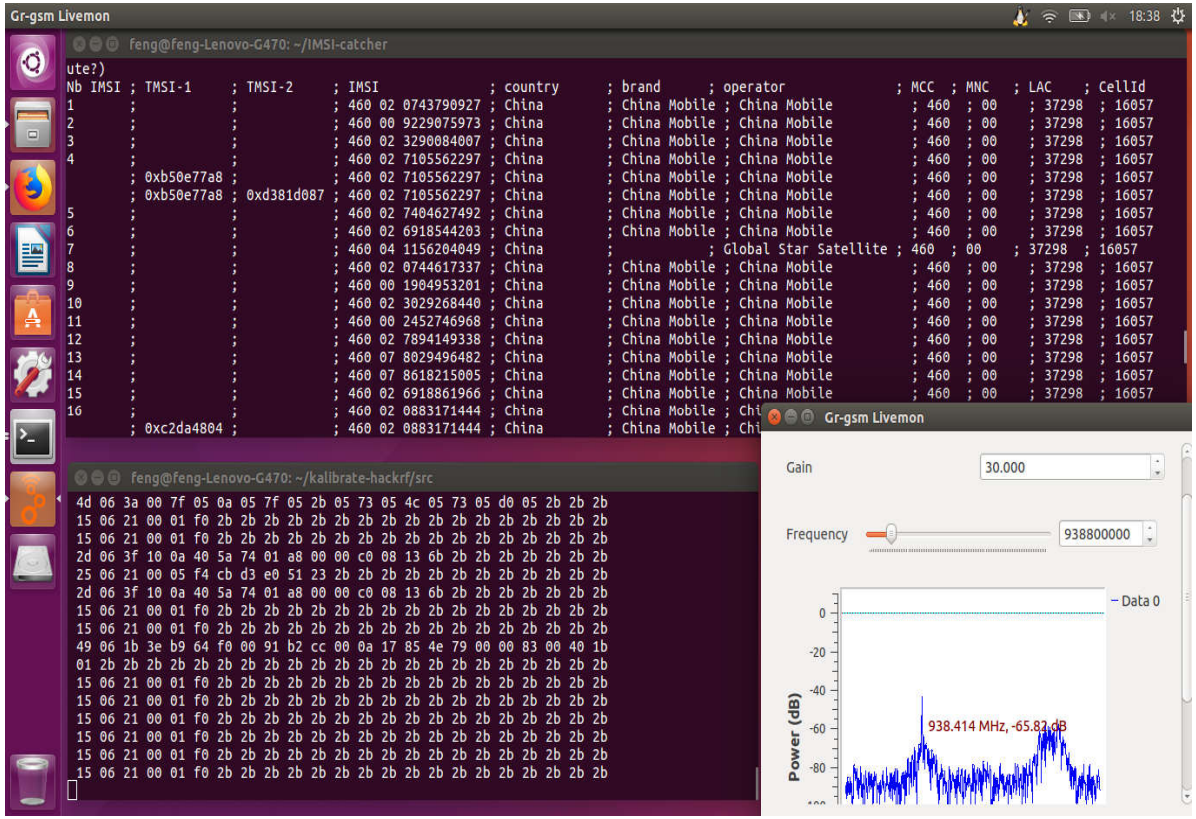
MCC：移动国家代码；

MNC：移动网络代码；

LAC和CellId：终端设备的物理地址。

五、电力LTE网络安全接入测试

- IMSI-catche捕获



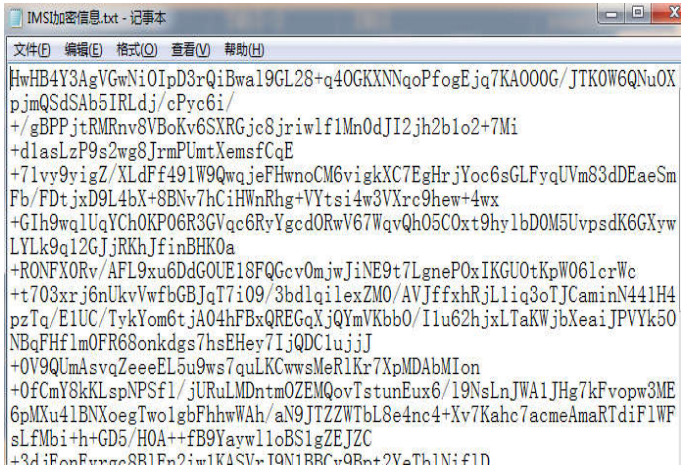
针对：LAC=37298，CellId=16057

五、电力LTE网络安全接入测试

- 身份信息加密

加密前

加密后



五、电力LTE网络安全接入测试

➢实验3：电力LTE网络接入侧仿真系统实验

- 明文信息安全漏洞危害

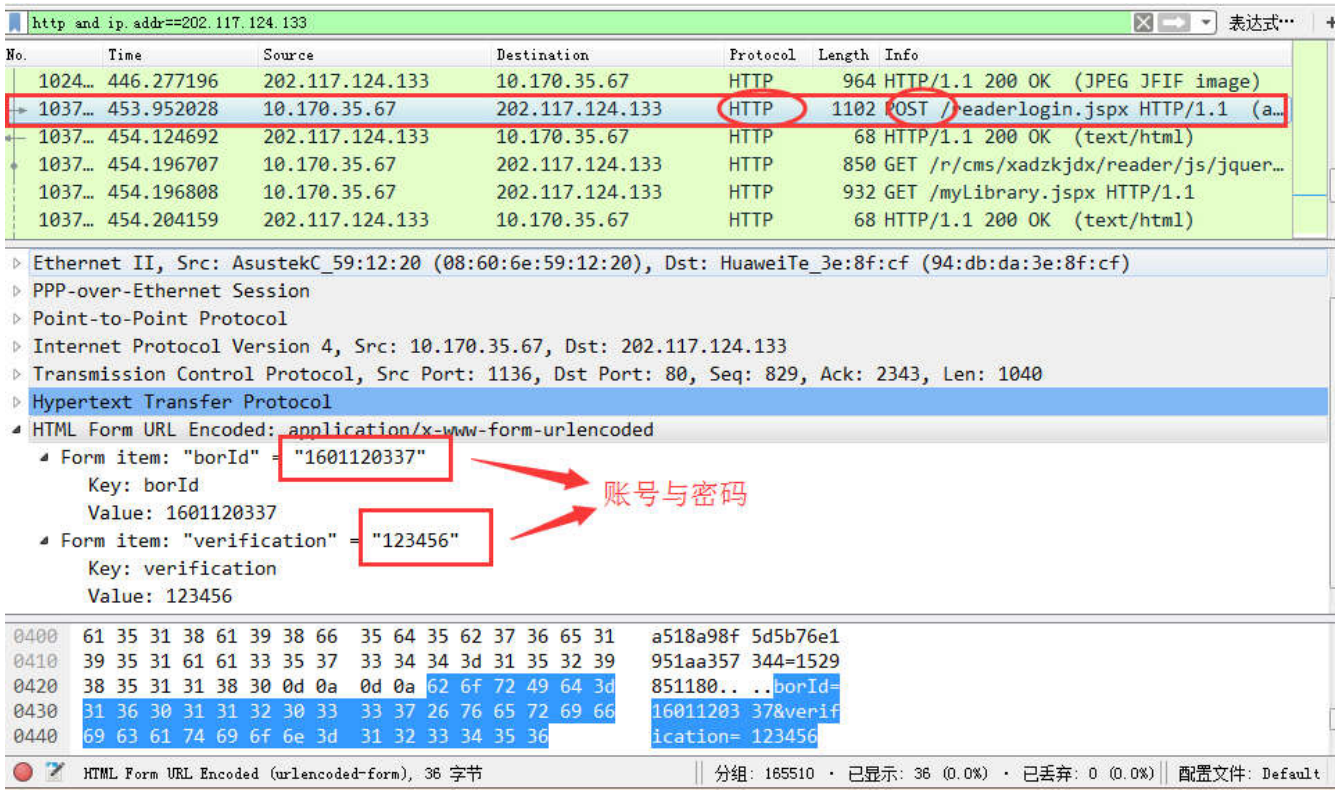
在实验室中通过个人用户请求接入没有加载TLS安全协议的服务器中心网站过程，并通过wireshark工具进行针对个人终端用户的身份信息捕获的环境下，以此模拟输电线路在线监测终端请求接入电力信息网络中网络侧接入电力控制中心实验。

下图是显示的是执行账号密码登录前后的界面。（认证与通信）

五、电力LTE网络安全接入测试

- 明文信息安全漏洞危害

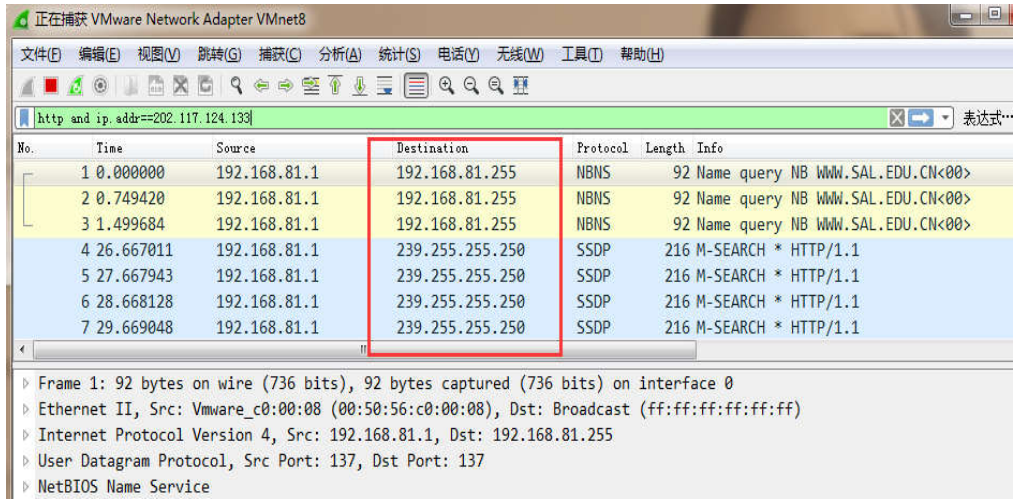
利用wireshark捕获数据包。在此捕获信息中发现post登录信息，点击进入查看详细的登录信息。



五、电力LTE网络安全接入测试

- 明文信息安全漏洞危害

一旦对这些网站添加信任，即增加TLS安全协议，在网址接入部分添加数字证书，再次捕获终端身份信息时结果如图所示：



多谢指导！