



## (12)发明专利申请

(10)申请公布号 CN 108600173 A

(43)申请公布日 2018.09.28

(21)申请号 201810249430.5

H04L 12/24(2006.01)

(22)申请日 2018.03.22

H04L 9/06(2006.01)

(71)申请人 中国南方电网有限责任公司超高压  
输电公司检修试验中心

地址 510507 广东省广州市萝岗区广州科  
学城科学大道181号A4第7层

申请人 山东山大电力技术股份有限公司

(72)发明人 张怿宁 齐曙光 朱诚 王越杨  
孟令军

(74)专利代理机构 济南圣达知识产权代理有限  
公司 37221

代理人 李圣梅

(51)Int.Cl.

H04L 29/06(2006.01)

H04L 29/08(2006.01)

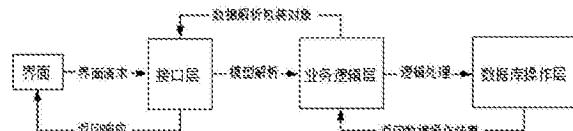
权利要求书2页 说明书7页 附图2页

### (54)发明名称

一种具备加密安全性的分布式行波测距系  
统与方法

### (57)摘要

本发明公开了一种具备加密安全性的分布  
式行波测距系统与方法，包括：界面请求模  
块，在前端界面发起向后台查询操作请求并  
进行加密；模型解析模块，用于对前端界面请  
求数据进行解密并传输至业务逻辑层；逻辑处  
理模块，用于对解密后的数据进行逻辑处理并  
传输至数据库操作层，从数据库操作层获取数  
据查询结果并返回至业务逻辑层；数据解析包  
装对象模块，用于将查询结果数据加密并返  
回至前端接口层；返回响应模块，用于将查询  
结果数据进行解密并展示。  
本发明通过在Web应用层对前端的交互数据进  
行数据加密，使网络结构更健全，达到有效杜绝  
恶意原因造成的数据破坏、更改、泄露的目的，保  
证行波测距系统数据及网络服务的安全性。



1. 一种具备加密安全性的分布式行波测距系统，其特征是，所述分布式行波测距系统的Web应用层对前端的交互数据进行数据加密，具体包括：

界面请求模块，用于在前端界面发起向后台查询操作请求并进行加密，将加密数据通过接口层进行数据传输；

模型解析模块，用于对前端界面请求数据进行解密并传输至业务逻辑层；

逻辑处理模块，用于对解密后的数据进行逻辑处理并传输至数据库操作层，从数据库操作层获取数据查询结果并返回至业务逻辑层；

数据解析包装对象模块，用于将查询结果数据加密并返回至前端接口层；

返回响应模块，用于将查询结果数据进行解密并展示。

2. 如权利要求1所述的一种具备加密安全性的分布式行波测距系统，其特征是，所述具备加密安全性的分布式行波测距系统还包括请求判断模块，用于对界面请求模块中的查询操作请求数据进行分析判断，如果请求的是非敏感数据量查询操作时，使用3DES算法和SM3算法进行加解密；如果请求的是敏感数据，使用非对称的安全级别高的SM2算法和SM3算法进行加解密，并且双方产生的SM2算法的公钥使用3DES进行加密，在会话期间传给对方。

3. 如权利要求2所述的一种具备加密安全性的分布式行波测距系统，其特征是，针对非敏感的数据，所述界面请求模块中对查询操作请求加密的过程：

将需要加密的数据先转json字符串；

传数的时候，数据以令牌形式传输，由两部分组成：3DES加密的数据和SM3生成的校验码。

4. 如权利要求2所述的一种具备加密安全性的分布式行波测距系统，其特征是，针对非敏感的数据，所述模型解析模块中解密的过程：

取出需要解密的整个字符串；

将字符串的加密数据和校验码分别取出来，计算字符串的SM3值，比较两部分计算SM3值是否相同，不相同就返回，相同就进行下一步；

使用会话产生的钥匙，对字符串进行3DES解密。

5. 如权利要求2所述的一种具备加密安全性的分布式行波测距系统，其特征是，针对非敏感的数据，所述数据解析包装对象模块加密的过程：

把要返回的数据转换成json字符串；

使用会话产生的钥匙，对json字符串进行3DES算法加密；

对加密后的密文计算SM3，生成校验码；

将加密后的密文和SM3生成的校验码作为令牌进行传输；

针对非敏感的数据，所述返回响应模块中解密的过程：

先验证校验码的SM3跟加密数据的SM3值是否相同，判断数据完整性；

如果不同，直接返回，如果相同，就使用会话钥匙对加密数据进行3DES解密。

6. 一种具备加密安全性的分布式行波测距系统的方法，其特征是，所述分布式行波测距系统的Web应用层对前端的交互数据进行数据加密，具体包括：

在前端界面发起向后台查询操作请求并进行加密，将加密数据通过接口层进行数据传输；

对前端界面请求数据进行解密并传输至业务逻辑层；

对解密后的数据进行逻辑处理并传输至数据库操作层,从数据库操作层获取数据查询结果并返回至业务逻辑层;

将查询结果数据加密并返回至前端接口层;

将查询结果数据进行解密并展示。

7. 如权利要求6所述的一种具备加密安全性的分布式行波测距系统的方法,其特征是,所述具备加密安全性的分布式行波测距系统还包括请求判断步骤,对查询操作请求数据进行分析判断,如果请求的是非敏感数据量查询操作时,使用3DES算法和SM3算法进行加解密;如果请求的是敏感数据,使用非对称的安全级别高的SM2算法和SM3算法进行加解密,并且双方产生的SM2算法的公钥使用3DES进行加密,在会话期间传给对方。

8. 如权利要求7所述的一种具备加密安全性的分布式行波测距系统的方法,其特征是,针对非敏感的数据,对查询操作请求加密的过程:

将需要加密的数据先转json字符串;

传数的时候,数据以令牌形式传输,由两部分组成:3DES加密的数据和SM3生成的校验码。

9. 如权利要求7所述的一种具备加密安全性的分布式行波测距系统的方法,其特征是,针对非敏感的数据,所述对前端界面请求数据进行解密的过程:

取出需要解密的整个字符串;

将字符串的加密数据和校验码分别取出来,计算字符串的SM3值,比较两部分计算SM3值是否相同,不相同就返回,相同就进行下一步;

使用会话产生的钥匙,对字符串进行3DES解密。

10. 如权利要求7所述的一种具备加密安全性的分布式行波测距系统的方法,其特征是,针对非敏感的数据,所述将查询结果数据加密的过程:

把要返回的数据转换成json字符串;

使用会话产生的钥匙,对json字符串进行3DES算法加密;

对加密后的密文计算SM3,生成校验码;

将加密后的密文和SM3生成的校验码作为令牌进行传输;

针对非敏感的数据,所述将查询结果数据进行解密的过程:

先验证校验码的SM3跟加密数据的SM3值是否相同,判断数据完整性;

如果不同,直接返回,如果相同,就使用会话钥匙对加密数据进行3DES解密。

## 一种具备加密安全性的分布式行波测距系统与方法

### 技术领域

[0001] 本发明涉及数据安全技术领域,特别是涉及一种具备加密安全性的分布式行波测距系统与方法。

### 背景技术

[0002] 目前,行波测距项目,以快捷、强大、丰富、可定制的人机界面给予用户高效、丰富的体验;并提供稳定持久的故障数据、运算步骤、故障文件存储功能,快速了现场排除故障,有效提高了电网运行效益和设备管理水平。

[0003] 随着网架结构更加合理也更加复杂,与传统的行波测距装置相比,分布式行波测距系统具有更高的定位精度和更强的适应性。其故障定位装置分布安装于输电线路的导线上,将采集到的数据经分析处理后通过GPRS无线网络上传到测距监控中心,测距监控中心接受到现场监测装置上传的故障数据后,进行智能分析诊断,并将诊断结果通过短信方式发送给相关线路维护人员。系统还能实现对现场监测终端进行各种参数的实时读取和设置,包括监测终端的实时运行状态和故障时刻的故障信息。

[0004] 随着信息化和数字化社会的发展,信息交互日益频繁,信息安全的重要性毋庸置疑,人们对信息安全和保密的重要性认识不断提高。目前,多数行波测距技术支持系统,均忽略了对安全性能的加强处理,导致测距主站系统受到外来攻击,影响电网系统的安全运行,所以,安全技术越来越成为行波测距系统的重点关注内容之一。为了防止数据泄露或被篡改,往往需要对数据进行加密,敏感数据要求的安全性更高,因此,数据加密技术作为信息安全技术的重要手段得到了广泛的应用。

[0005] 3DES对称加密算法占用资源少,安全性高,在信息安全系统设计方面得到了广泛应用。它是DES加密算法的一种模式,使用3条64位的密钥对数据进行三次加密。SM2椭圆曲线公钥密码算法是我国自主设计的公钥密码算法,基于椭圆曲线上点群离散对数难题,256位的SM2密码强度已经高于2048位RSA算法。SM3摘要算法属于哈希算法,消息分组长度为512位,摘要值长度为256位。其压缩过程不可逆,在SHA-256基础上改进实现,算法设计更复杂。现今为止,SM3算法的安全性相对较高,被广泛应用在数字签名,消息认证,数据完整性检测等领域。但是如何将上述加密算法应用至分布式行波测距系统还没有相关技术。

[0006] 综上所述,现有技术中对于分布式行波测距系统中的数据安全问题,尚缺乏有效的解决方案。

### 发明内容

[0007] 为了解决现有技术的不足,本发明提供了一种具备加密安全性的分布式行波测距系统,应用层的数据传输中,进行认证与密匙管理机制的建立,令分布式行波测距系统应用层的安全更为稳固,有效杜绝恶意原因造成的破坏、更改、泄露,保证了分布式行波测距系统数据及网络服务的安全性。

[0008] 一种具备加密安全性的分布式行波测距系统,所述分布式行波测距系统的Web应

用层对前端的交互数据进行数据加密,具体包括:

- [0009] 界面请求模块,用于在前端界面发起向后台查询操作请求并进行加密,将加密数据通过接口层进行数据传输;
- [0010] 模型解析模块,用于对前端界面请求数据进行解密并传输至业务逻辑层;
- [0011] 逻辑处理模块,用于对解密后的数据进行逻辑处理并传输至数据库操作层,从数据库操作层获取数据查询结果并返回至业务逻辑层;
- [0012] 数据解析包装对象模块,用于将查询结果数据加密并返回至前端接口层;
- [0013] 返回响应模块,用于将查询结果数据进行解密并展示。
- [0014] 进一步的,所述具备加密安全性的分布式行波测距系统还包括请求判断模块,用于对界面请求模块中的查询操作请求数据进行分析判断,如果请求的是非敏感数据量查询操作时,使用3DES算法和SM3算法进行加解密;如果请求的是敏感数据,使用非对称的安全级别高的SM2算法和SM3算法进行加解密,并且双方产生的SM2算法的公钥使用3DES进行加密,在会话期间传给对方。
- [0015] 进一步的,针对非敏感的数据,所述界面请求模块中对查询操作请求加密的过程:
- [0016] 将需要加密的数据先转json字符串;
- [0017] 传数的时候,数据以令牌形式传输,由两部分组成:3DES加密的数据和SM3生成的校验码。
- [0018] 进一步的,针对非敏感的数据,所述模型解析模块中解密的过程:
- [0019] 取出需要解密的整个字符串;
- [0020] 将字符串的加密数据和校验码分别取出来,计算字符串的SM3值,比较两部分计算SM3值是否相同,不相同就返回,相同就进行下一步;
- [0021] 使用会话产生的钥匙,对字符串进行3DES解密。
- [0022] 进一步的,针对非敏感的数据,所述数据解析包装对象模块加密的过程:
- [0023] 把要返回的数据转换成json字符串;
- [0024] 使用会话产生的钥匙,对json字符串进行3DES算法加密;
- [0025] 对加密后的密文计算SM3,生成校验码;
- [0026] 将加密后的密文和SM3生成的校验码作为令牌进行传输。
- [0027] 进一步的,针对非敏感的数据,所述返回响应模块中解密的过程:
- [0028] 先验证校验码的SM3跟加密数据的SM3值是否相同,判断数据完整性;
- [0029] 如果不同,直接返回,如果相同,就使用会话钥匙对加密数据进行3DES解密。
- [0030] 一种具备加密安全性的分布式行波测距系统的方法,所述分布式行波测距系统的Web应用层对前端的交互数据进行数据加密,具体包括:
- [0031] 在前端界面发起向后台查询操作请求并进行加密,将加密数据通过接口层进行数据传输;
- [0032] 对前端界面请求数据进行解密并传输至业务逻辑层;
- [0033] 对解密后的数据进行逻辑处理并传输至数据库操作层,从数据库操作层获取数据查询结果并返回至业务逻辑层;
- [0034] 将查询结果数据加密并返回至前端接口层;
- [0035] 将查询结果数据进行解密并展示。

[0036] 进一步的,所述具备加密安全性的分布式行波测距系统还包括请求判断步骤,对查询操作请求数据进行分析判断,如果请求的是非敏感数据量查询操作时,使用3DES算法和SM3算法进行加解密;如果请求的是敏感数据,使用非对称的安全级别高的SM2算法和SM3算法进行加解密,并且双方产生的SM2算法的公钥使用3DES进行加密,在会话期间传给对方。

[0037] 进一步的,针对非敏感的数据,对查询操作请求加密的过程:  
[0038] 将需要加密的数据先转json字符串;  
[0039] 传数的时候,数据以令牌形式传输,由两部分组成:3DES加密的数据和SM3生成的校验码。

[0040] 进一步的,针对非敏感的数据,所述对前端界面请求数据进行解密的过程:  
[0041] 取出需要解密的整个字符串;

[0042] 将字符串的加密数据和校验码分别取出来,计算字符串的SM3值,比较两部分计算SM3值是否相同,不相同就返回,相同就进行下一步;

[0043] 使用会话产生的钥匙,对字符串进行3DES解密。

[0044] 进一步的,针对非敏感的数据,所述将查询结果数据加密的过程:

[0045] 把要返回的数据转换成json字符串;

[0046] 使用会话产生的钥匙,对json字符串进行3DES算法加密;

[0047] 对加密后的密文计算SM3,生成校验码;

[0048] 将加密后的密文和SM3生成的校验码作为令牌进行传输。

[0049] 进一步的,针对非敏感的数据,所述将查询结果数据进行解密的过程:

[0050] 先验证校验码的SM3跟加密数据的SM3值是否相同,判断数据完整性;

[0051] 如果不同,直接返回,如果相同,就使用会话钥匙对加密数据进行3DES解密。

[0052] 与现有技术相比,本发明的有益效果是:

[0053] 本发明通过在Web应用层对前端的交互数据进行数据加密,使网络结构更健全,达到有效杜绝恶意原因造成的数据破坏、更改、泄露的目的,保证行波测距系统数据及网络服务的安全性。

[0054] 本发明在分布式测距系统上增加了对数据进行加密处理。在对数据进行加密处理的过程中是将现有的加密方法直接应用,在将加密方法应用至本申请的安全性上时所用的手段是根据需要传输信息的敏感性,区分使用不同的加密方法。普通大量数据的传输使用的加密方法是3DES和SM3,敏感信息(比如登录密码)的传输使用的加密方法是SM2和SM3,其中SM2算法使用的公钥在传输过程中使用3DES进行加密。这样即保证数据传输的安全,又兼顾系统响应速率。

[0055] 本分布式行波测距系统网络结构健全,在软件方面配备3DES、SM2和SM3加密算法及多层企业级监听单元与过滤单元,加强网站和程序的安全性。应用层的数据传输中,进行认证与密匙管理机制的建立,令分布式行波测距系统应用层的安全更为稳固,有效杜绝恶意原因造成的破坏、更改、泄露,保证了分布式行波测距系统数据及网络服务的安全性。

[0056] 使用加密算法加密之后的数据,在网络中进行传输的时候,由前端到后台的过程中,经过了软件部分的监听单元和过滤单元进行的处理。此处具体为:对加密数据进行请求接口的响应和转发处理。这是软件框架里的工作机制。

## 附图说明

[0057] 构成本申请的一部分的说明书附图用来提供对本申请的进一步理解,本申请的示意性实施例及其说明用于解释本申请,并不构成对本申请的不当限定。

[0058] 图1是本发明的系统运行架构图;

[0059] 图2是Web应用服务器的业务逻辑架构图;

[0060] 图3是3DES算法示意图;

[0061] 图4是国密SM2算法示意图。

## 具体实施方式

[0062] 应该指出,以下详细说明都是例示性的,旨在对本申请提供进一步的说明。除非另有指明,本文使用的所有技术和科学术语具有与本申请所属技术领域的普通技术人员通常理解的相同含义。

[0063] 需要注意的是,这里所使用的术语仅是为了描述具体实施方式,而非意图限制根据本申请的示意性实施方式。如在这里所使用的,除非上下文另外明确指出,否则单数形式也意图包括复数形式,此外,还应当理解的是,当在本说明书中使用术语“包含”和/或“包括”时,其指明存在特征、步骤、操作、器件、组件和/或它们的组合。

[0064] 本申请的一种典型的实施方式中,提供了分布式行波测距系统,分布式行波测距系统包括测距监控中心和通讯数据网连接,通讯数据网与分布式行波装置连接。

[0065] 利用行波在输电线路有固定传播速度这一特点,根据线路两侧装置感受到行波暂态分量的绝对时间之差进行故障点定位。

[0066] 分布式行波测距系统,通过通讯数据网向分布式行波装置检索行波录波记录,并将行波录波数据文件上传到数据库服务器,然后对行波录波数据进行故障分析、计算,将测距结果和录波数据文件上送到监测控制中心。

[0067] 通过接口从测距监控中心获取相应的录波数据文件;然后从这些录波数据中提取有效信息;最后本系统进行分析计算,得到故障测距结果,并生成测距报告。

[0068] 如图1所示,整个系统采用四层架构:数据采集层、通讯程序数据处理层、数据存储层和Web应用层。

[0069] 上述分布式行波测距系统在硬件架构上,至少包括多台分布式行波装置,通讯服务器、数据服务器、Web应用服务器。

[0070] 分布式行波装置作为数据采集终端,利用分布和多点采集高频故障暂态电流(电压)的行波,形成故障录波数据文件,提供故障数据,来间接判定故障点的距离。

[0071] 分布式行波装置通过通信网络传输给通讯服务器,通讯服务器根据获取的故障数据,得到故障波形,并将设备采集的数据传送给测距监控中心;

[0072] 测距监控中心,包括:Web服务器,用于管理系统台账信息和查询数据,数据库服务器,保存故障数据、告警数据、通信数据以及行波录波文件等信息。

[0073] 测距监控中心的逻辑架构分为数据存储层、中间接口层、业务处理层和应用展现层;

[0074] 数据存储层,获取故障简报、故障波形和行波录波数据文件;

- [0075] 中间接口层是数据访问接口,数据存储层采用分布式数据库集群技术,使用接口层可以对上层应用提供统一的调用接口函数;
- [0076] 业务处理层,进行行波数据分析和故障测距计算;
- [0077] 应用展现层,进行数据检索和系统前端的故障展示。
- [0078] 获取故障录波数据过程:通讯服务器通过通讯程序根据约定好的通信规约获取故障简报、故障波形、故障录波数据文件等最新数据。
- [0079] 测距计算,根据首波头时间,对行波录波数据文件进行分析,计算行波暂态分量的绝对时间之差,最终得到测距结果及其它相关分析报告。
- [0080] 系统前端故障数据检索,面对海量数据,提供多种检索条件,方便不同用户根据需要和习惯查询不同的关注内容。
- [0081] 具备3DES、SM2和SM3加密安全性的分布式行波测距系统,所述分布式行波测距系统的Web应用层对前端的交互数据进行数据加密,具体包括:
- [0082] 界面请求模块,用于在前端界面发起向后台查询操作请求并进行加密,将加密数据通过接口层进行数据传输;
- [0083] 模型解析模块,用于对前端界面请求数据进行解密并传输至业务逻辑层;
- [0084] 逻辑处理模块,用于对解密后的数据进行逻辑处理并传输至数据库操作层,从数据库操作层获取数据查询结果并返回至业务逻辑层;
- [0085] 数据解析包装对象模块,用于将查询结果数据加密并返回至前端接口层;
- [0086] 返回响应模块,用于将查询结果数据进行解密并展示。
- [0087] 上述系统的工作方法,具体步骤包括:
- [0088] (1)发生故障后,分布式行波装置记录故障数据,然后通过通讯网络将数据送到通讯服务器;
- [0089] (2)测距监控中心通过通讯网获得故障数据,对故障进行分析得到故障波形,再通过计算,得出测距结果,判断出故障位置,得出分析报告;测距监控中心获取行波录波数据,然后对故障数据中的行波暂态分量信息进行分析。
- [0090] (3)将分布式行波测距系统对故障数据的分析结果上传给数据库服务器;
- [0091] (4)数据安全传输:前端使用加密数据与后台做相关查询时,Web服务器从数据库服务器获取数据,并将数据加密后通过网络送到前端进行展示。
- [0092] 所述步骤(2)中,对故障数据进行分析,从获得的通讯信息中找到首波头时间,计算行波暂态分量的绝对时间之差,根据这个公式和判断标准,分析得出故障位置。
- [0093] 数据安全传输的具体工作流程为:
- [0094] 如图2所示,前端使用加密数据向后台发相关查询操作(对应于界面请求环节);数据和应用服务器将前端数据解密(对应于模型解析环节)后,根据条件(界面上用户输入或选择的查询条件,比如时间、测距类型、公司等等)从数据库服务器获取查询结果;
- [0095] 后端将查询结果数据加密(对应于数据解析包装对象环节)后返回前端,前端将后台返回的结果进行解密(对应于返回响应环节),展示给分析该次故障的相关人员。
- [0096] 本申请中的前端具体是指用户的计算机浏览器端。后端是指系统的web服务器端。
- [0097] 前端如果请求的是非敏感的大数据量查询操作时,使用高效率的3DES算法和SM3算法进行加解密;如果请求的是敏感数据,如对用户名之类的数据进行操作时,使用非对称

的安全级别高的SM2算法和SM3算法进行加解密，并且双方产生的SM2算法的公钥使用3DES进行加密，在会话期间传给对方。其中SM3摘要算法用来进行数据完整性检测。以下步骤，以3DES算法和SM3算法加解密为例，进行说明，如图3-4所示。

[0098] 具体的，在敏感数据的判断上，由于不同查询使用不同接口，根据请求的接口就可以区别请求的是不是敏感数据。

[0099] 上文中的双方是加密方和解密方，即指前端数据的发送方和接收方。发送方加密，接收方解密。前端同时都可以是发送方和接收方。前端同时都可以是发送方和接收方。当前端是发送方时，后端是接收方（对方）；当后端是发送方时，前端是接收方（对方）。

[0100] 上述算法中，3DES用于数据加解密，SM3用于验证数据完整性。

[0101] 前台加密的过程：

[0102] 1、将需要加密的数据先转json字符串。

[0103] 2、传数的时候，数据以令牌形式传输，由两部分组成：3DES加密的数据和SM3生成的校验码。

[0104] 后台解密的过程：

[0105] 1、取出需要解密的整个字符串。

[0106] 2、将字符串的加密数据和校验码分别取出来，计算字符串的SM3值，比较两部分计算SM3值是否相同，不相同就返回，相同就进行步骤3。

[0107] 3、使用会话产生的钥匙，对字符串进行3DES解密。

[0108] 后台加密的过程：

[0109] 1、后台把要返回的数据转换成json字符串。

[0110] 2、使用会话产生的钥匙，对json字符串进行3DES算法加密。

[0111] 3、对加密后的密文计算SM3，生成校验码。

[0112] 4、将加密后的密文和SM3生成的校验码作为令牌进行传输。

[0113] 前台解密的过程：

[0114] 1、先验证校验码的SM3跟加密数据的SM3值是否相同，判断数据完整性。

[0115] 2、如果不同，直接返回。如果相同，就使用会话钥匙对加密数据进行3DES解密。

[0116] 本发明通过在Web应用层对前端的交互数据进行数据加密，使网络结构更健全，达到有效杜绝恶意原因造成的数据破坏、更改、泄露的目的，保证行波测距系统数据及网络服务的安全性。

[0117] 在安徽电科院、山东电科院均部署一套具备3DES、SM2和SM3加密安全性的分布式行波测距系统，实现以下功能：

[0118] 1、部署1套“输电线路分布式故障监测与智能诊断系统”软件系统。

[0119] 2、输电线路发生故障后，监测控制中心获得分布式行波装置的行波故障录波数据。

[0120] 3、通信程序获取并分析所有启动的分布式行波录波数据，计算得出故障位置、故障类型、故障相别等信息，给出故障告警，并保存到实时数据库服务器中。

[0121] 4、前端通过加密数据进行测距故障查询功能的操作时，后端查询结果经数据加密返回前端展示，供工作人员参考。

[0122] 本申请在分布式测距系统的应用层上对数据传输使用加密方法，本申请更注重的

是数据在传输过程中的安全处理,即数据逻辑上的安全,并且加密算法的使用根据实际需要即信息的敏感程度进行不同区分和选择。

[0123] 以上所述仅为本申请的优选实施例而已,并不用于限制本申请,对于本领域的技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

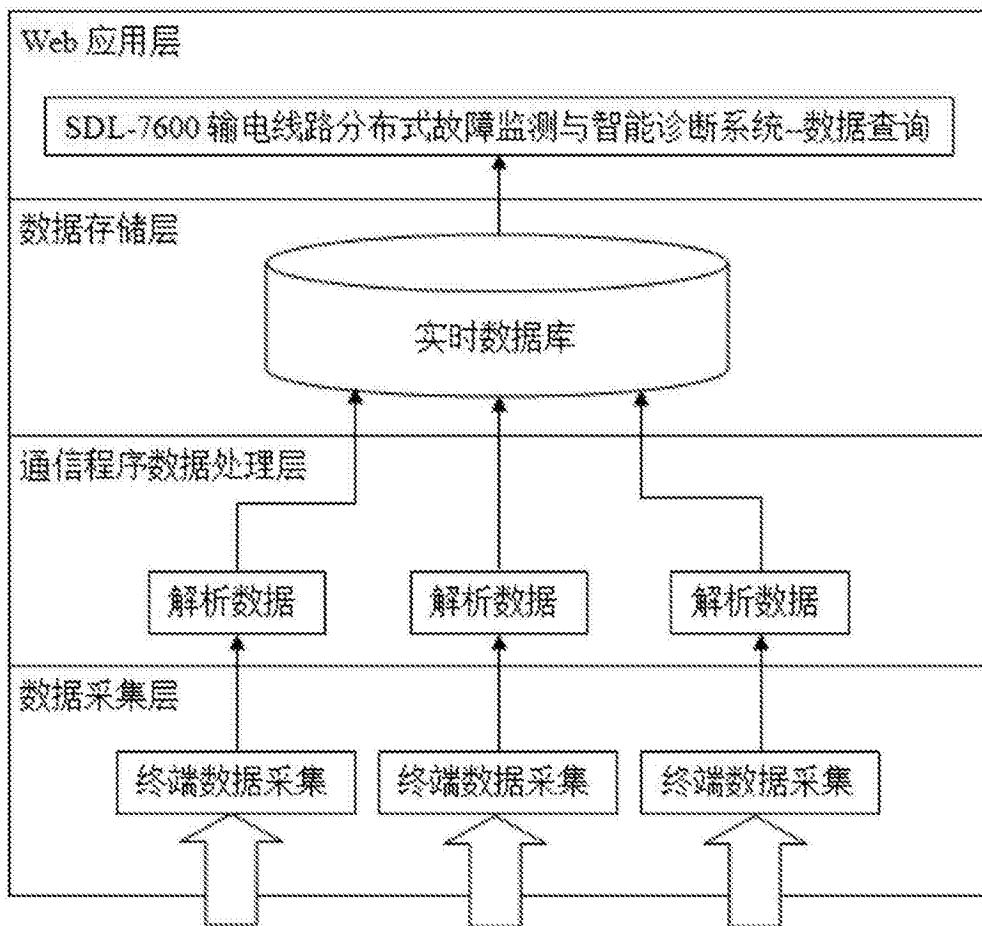


图1

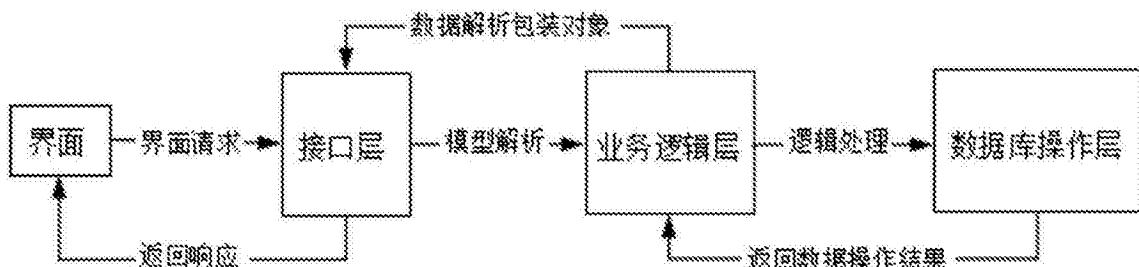


图2

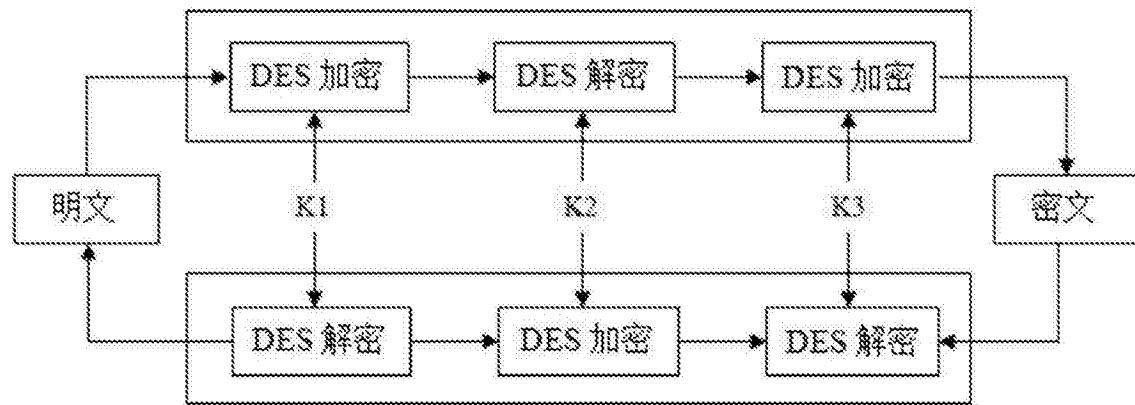


图3

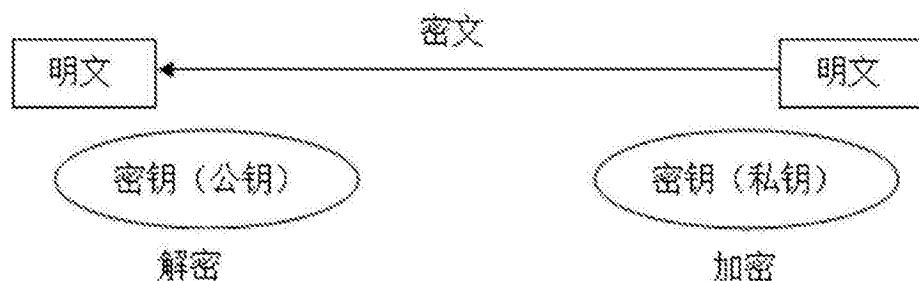
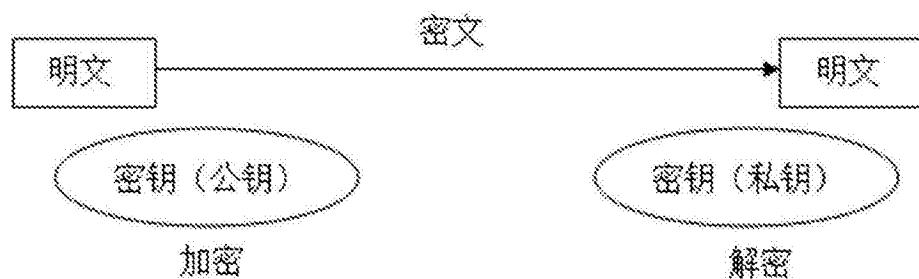


图4