文章编号:1005-0523(2019)04-0131-06

一种适用于WSN数据实时加密传输的超轻量级流加密方案

汤鹏志[1,2],康文洋[1,2],张 捧[1,2],左黎明[1,2]

(华东交通大学 1.理学院;2.系统工程与密码学研究所,江西 南昌 330013)

摘要:对于电力无线传感器网络实时数据传输中缺乏数据机密性保护以及设备计算能力较弱、带宽受限等问题,提出了一个超轻量级流加密方案。该方案由密钥创建、加密和解密3部分组成,并进一步基于该方案设计了一套适用于电力无线传感器网络的数据加密传输协议,给出了关键实现和仿真。仿真结果表明相比其它算法,效率有极大提高,实现难度低,适用于电力无线传感器网络设备计算能力较弱的应用场景下数据安全传输。

关键词:智能电网;无线传感器网络;流密码;哈希算法

中图分类号:TP309.2 **文献标志码**:A

随着电力系统智能电网的发展,无线传感器网络(wireless sensor network,WSN)技术[1-2]在发电、输变电、配电和用电等各电力系统环节[3-5]得到广泛的应用。当前的研究主要集中在WSN负载均衡路由优化算法[6]和网络性能的跨层控制方案[7-8],很少考虑数据的安全传输问题。为了解决电力系统无线传感器网络中数据实时传输的安全问题,一些学者[9-12]采用AES算法芯片加强传感器,虽然可以解决电网无线传感器网络数据传输的机密性问题,但需要大幅增加硬件成本,也很难满足现有计算能力差的设备的实时性要求。本文提出了一种基于哈希算法的超轻量级流加密方案,与使用AES算法的方案相比,只需要简单的与或非逻辑运算,计算性能较弱的设备也可以很好的运行; 因此可以低成本的方式大大提高电力系统数据实时传输的安全性。

1 电力无线传感器网络数据传输过程[13]

如图1所示,电力无线传感器网络系统架构可以分为电网应用层、网络层和感知层。传感器节点是信息采集终端,也是网络连接的起始点,各类传感器节点和路由节点通过各种网络拓扑形态将感知数据传送至无线传感器网络网关。无线传感器网络网关是感知数据向网络外部传递的有效设备,通过网络适配器转换连接至网络层,再通过网络层连接至电力无线传感器网络应用层。电力无线传感器网络采集的数据具有数据量大,实时性高等特点。从感知层到电网应用层传输很多时候需要经过公网,各种网络数据采集封包和控制封包存在明文泄露和被篡改的风险。

收稿日期:2019-01-28

基金项目:国家自然科学基金项目(11361024);江西省教育厅科技项目(GJJ170386);江西省研究生创新项目(YC2018-S250)

作者简介:汤鹏志(1961—),男,教授,研究方向为信息安全。

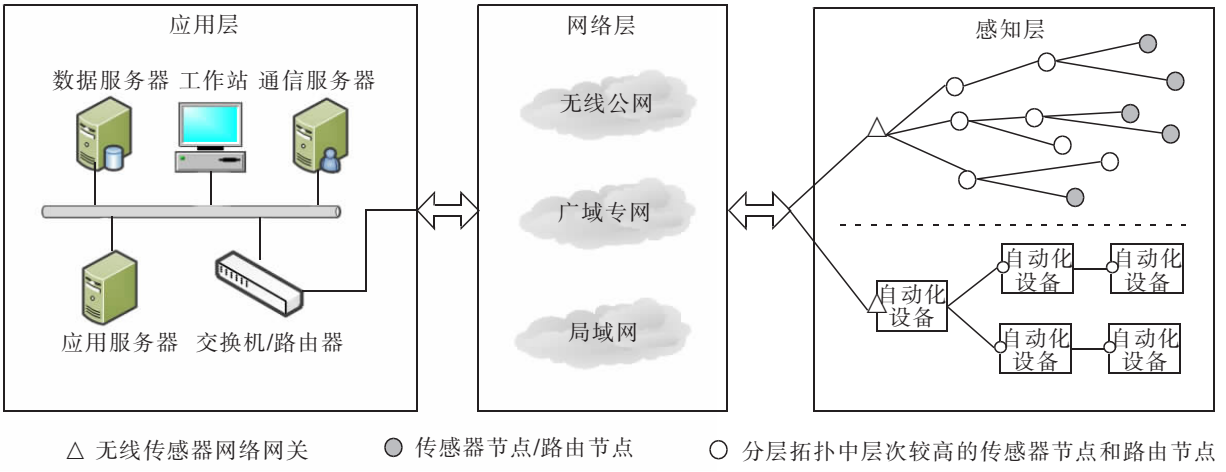


图1 电力系统中应用无线传感器网络系统架构图

Fig.1 Application of wireless sensor network architecture in power system

2 基于超轻量级的流加密方案设计

本文的超轻量级流加密方案由密钥创建、加密和解密3部分组成,具体设计过程如下:

2.1 密钥创建

密钥安全是流加密安全的保障,数据加密方A的密钥由设备*ID*和设备秘密值*Key*组成,其中设备*ID*是每台设备出厂的唯一标识码,设备秘密值*Key*是由数据解密方B统一生成的一串字符。数据加密方A与数据解密方B均通过对设备*ID*和设备秘密值*Key*不同的组合方式*Hash*获得h_1与h_2,并将h_1与h_2异或得到初始向量$\boldsymbol{IV}$

$$\begin{cases} h_1=Hash(ID,Key) \\ h_2=Hash(Key,ID) \\ \boldsymbol{IV}=h_1\oplus h_2 \end{cases} \tag{1}$$

2.2 加密

密钥创建完成后,数据加密方A使用加密算法对密钥流K_i的哈希值和明文流M_i做异或运算加密得到密文流C_i,并发送密文流C_i至数据解密方B解析,具体加密算法公式如下

$$\begin{cases} K_i=C_{i-1}\oplus Hash(M_{i-1}\oplus Key) \\ C_i=Hash(K_i)\oplus M_i \end{cases} \quad i=1,2,3,\cdots,n \tag{2}$$

其中密钥流$K_1=C_{i-1}\oplus Hash(M_{i-1}\oplus Key)$的产生分为两种情况:

1) 当i=1时,表示数据加密方A初次发送消息至数据解密方B,此时取$C_0=Hash(\boldsymbol{IV})$和$M_0=\boldsymbol{IV}$,得到密钥流$K_1=Hash(\boldsymbol{IV})\oplus Hash(\boldsymbol{IV}\oplus Key)$;

2) 当i>1时,表示设备数据加密方A非初次发送消息至数据解密方B,此时取上次发送的密文流C_{i-1}和明文流M_{i-1}经过运算得到密钥流K_i。

2.3 解密

数据解密方B收到数据加密方A发送来的密文流C_i之后,使用数据解密方B产生的密钥流K_i的哈希值和接收到的密文流C_i做异或运算解密得到明文流M_i,并验证明文流M_i中的标志位判断是否解密成功,具体解密算法公式如下

$$\begin{cases} K_i=C_{i-1}\oplus Hash(M_{i-1}\oplus Key) \\ C_i=Hash(K_i)\oplus C_i \end{cases} \quad i=1,2,3,\cdots,n \tag{3}$$

同样，密钥流 $K_i=C_{i-1}\oplus Hash(M_{i-1}\oplus Key)$的产生也分为两种情况，数据解密方 B 接收到密文流 C_i 之后，首先在设备列表中寻找该设备的最近一条密文流 C_{i-1} 与明文流 M_{i-1} 记录：

1）如果未找到任何密文流 C_{i-1} 或者明文流 M_{i-1} 记录，则表示数据解密方 B 初次接收数据加密方 A 发送来的消息，此时 i=1，数据解密方 B 生成初始向量 $\boldsymbol{IV}$，并取 $C_0=Hash(\boldsymbol{IV})$和 $M_0=\boldsymbol{IV}$，得到密钥流 $K_1=Hash(\boldsymbol{IV})\oplus Hash(\boldsymbol{IV}\oplus Key)$；

2）如果找到密文流 C_{i-1} 或者明文流 M_{i-1} 记录，则表示数据解密方 B 非初次接收数据加密方 A 发送来的消息，数据解密方 B 取上次接收到的密文流 C_{i-1} 和明文流 M_{i-1} 经过运算得到密钥流 K_i。

3　安全性分析

流密码的安全性完全取决于密钥流生成器所生成的密钥流的不可预测性和随机性。方案中，密钥流 K_i 通过上一次密文流 C_{i-1}，上一次明文流 M_{i-1} 以及设备秘密值 Key 一起来生成，将密钥流的哈希值与本次明文流 M_i 异或加密得到本次密文流 C_i，每次异或加密之后的密文流都不一样，这就保证了对不同明文流的加密密钥流也都不一样，从而本方案具有一次一密（One-Time-Pad）的安全性。由于本方案用于加密的密钥流是由前面三部分异或与哈希运算生成的，所以即使破解了一个密文流 C_i 对应的密钥流 K_i 及明文流 M_{i-1} 与秘密值 Key 的哈希值，也无法获得设备秘密值 Key，保证了本方案的保密性。

4　基于流加密方案的数据加密传输协议

在电力无线传感器网络体系中，感知层中的无线传感器负责对电网铁塔周围各环境信息数据采集，使用 $Hash$ 函数与异或运算对采集数据进行迭代加密操作后获得密文流 C，并通过在网络层中建立的 TCP 连接发送密文流 C 至应用层，应用层中的通信服务器接收到密文流 C 后，使用 $Hash$ 函数与异或运算对密文流 C 进行迭代解密操作获得明文流 M。

如图 2 所示，为基于超轻量级流加密方案的电力无线传感器网络数据传输流程图，其具体的数据处理步骤如下：

Step1：系统初始化参数建立过程中，首先无线传感器根据设备 ID 和设备秘密值 Key 哈希得到 h_1 与 h_2，且 h_1 与 h_2 经过异或处理得到初始向量 $\boldsymbol{IV}$。

Step2：无线传感器参数建立完成后，使用 $Hash$ 函数对设备 ID 进行哈希处理得到 $H_{ID}=Hash(ID)$，并发送至通信服务器。

Step3：通信服务器将维护一张由 n 个无线传感器设备 ID 哈希值组成的列表 $List=\{H_{ID_1},H_{ID_2},H_{ID_3},\cdots,H_{ID_k},\cdots\}$，其中 $k\in\{1,2,3,\cdots,n\}$。通信服务器收到 H_{ID_j} 后，将 H_{ID_j} 与 $List$ 中的元素一一对比，直到找到 $H_{ID_k}=H_{ID_j}$，记录此时的 ID_k，通过该 ID_k 在数据库中找到该设备秘密值 Key_k，并建立该设备的系统初始化参数，建立过程与 Step1 一致。

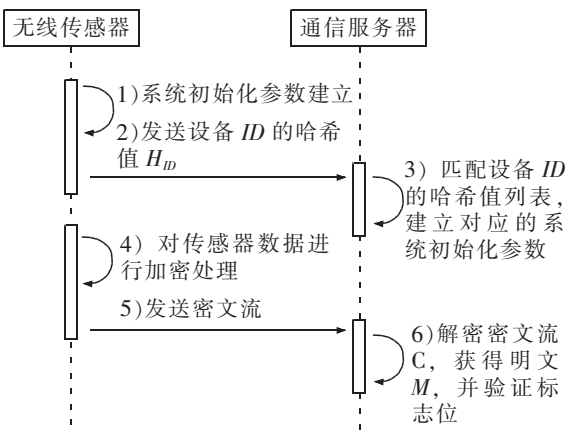


图 2　数据传输流程图

Fig.2　Data transmission flow chart

Step4：无线传感器采集电网铁塔周围各环境信息数据并加入 $true$ 标志位，组合为明文流 M_i，取设备秘密值 Key 与上一次的明文流 M_{i-1} 异或后做哈希运算，再与上一次的密文流 C_{i-1}（若 i=1，取 $C_0=Hash(IV)$和 $M_0=IV$）异或得到密钥流 K_i，最后将 K_i 的哈希值与本次传输的明文流 M_i 做异或运算加密得到密文流 C_i。

Step5：无线传感器通过在网络层中建立的 TCP 连接发送密文流 C_i 发送至应用层

$$\begin{cases} K_i=C_{i-1}\oplus Hash(M_{i-1}\oplus Key) \\ C_i=Hash(K_i)\oplus M_i \end{cases} \quad i=1,2,3,\cdots,n$$

Step6:通信服务器接收到密文流 C_i 之后,根据 ID_k 取出该设备秘密值 Key_k,并与上一次接收的密文流 C_{i-1} 和明文流 M_{i-1}(若 C_0 与 M_0 不存在,取 C_0=$Hash$(***IV***)和 M_0=***IV***)运算得到密钥流 K_i=C_{i-1}⊕$Hash$(M_{i-1}⊕Key),最后将 K_i 的哈希值与本次接收的密文流 C_i 做异或运算解密得到明文流 M_i。通信服务器验证明文流 M_i 中的标志位判断是否解密成功,若解密不成功,返回失败提示消息,通知无线传感器重新发送密文流 C_i。

5 关键代码与实验仿真

5.1 无线传感器数据加密过程

无线传感器首先采集获取被检测电网铁塔周围各环境信息数据 M_i, 然后获取上一次密文流进行判断,如果不存在, 则通过初始向量 ***IV*** 与设备秘密值 Key 进一步计算得密钥流 K_i。得到密钥流之后, 先进行sha256 哈希操作,最后与加入标志位的明文流进行异或处理的得到本次密文流。数据加密过程使用 Python 语言编写,其部分核心代码如下:

```
//获取上一次密文流 Cpi
Cpi = GetPreviousCipherText()
//如果上一次密文流 Cpi 不存在
if Cpi == "":
//获得初始向量 IV
IV = GetInitIV()
//计算得上一次密文流 Cpi
Cpi = sha256(IV)
//计算得上一次明文流 Mpi
Mpi = IV
//计算得到密钥流 Ki
Ki = GetKeysText(Cpi,Mpi)
Hi = sha256(Ki)
//明文消息增加标志位
Mi = Mi + ",true"
Ci = xor_encrypt(Mi,Hi)
//保存本次密文流 Ci
SaveCipherText(Ci)
```

5.2 无线传感器数据解密过程

通信服务器接收到无线传感器发送来的密文流 C_i 之后, 然后获取最近一次密文流与明文流进行判断,如果不存在,则通过初始向量 ***IV*** 与设备秘密值 Key 进一步计算得密钥流 K_i。得到上一次密钥流之后,先进行 *sha256* 哈希操作,最后与接收的密文流 C_i 进行异或处理得到本次明文流 M_i,并判断 M_i 是否含有标志位信息,含有则解密成功;否则返回失败提示消息,通知无线传感器重新发送密文流 C_i。数据解密过程使用 C# 语言编写,其部分核心代码如下:

```
//获取上一次密文流 Cpi
string Cpi = GetPreviousCipherText();
//如果上一次密文流 Cpi 不存在
If(Cpi == "")
{
//获得初始向量 IV
IV = GetInitIV()
//计算得上一次密文流 Cpi
Cpi = sha256(IV)
//计算得上一次明文流 Mpi
```

```
Mpi = IV
}
//计算得到密钥流 Ki
Ki = GetKeysText(Cpi,Mpi)
string Hi = sha256(Ki);
string Mi = xor_decrypt(Ci,Hi);
//获取明文消息标志位
string flag = Mi.Split(',').Last();
if(flag == "true")
{
//保存本次密文流 Ci
SaveCipherText(Ci);
}
```

5.3　实验仿真与性能对比

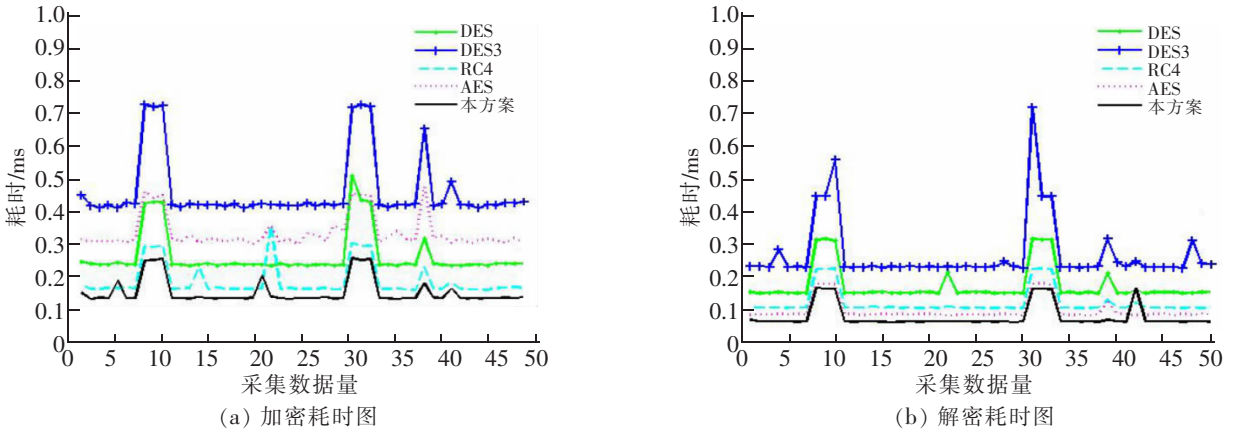
本实验仿真平台环境分为应用层与感知层两部分，应用层的仿真环境为:Windows Server 2008 R2 Enterprise 操作系统,处理器为 Intel(R) Xeon(R) CPU E5-2682 v4 @ 2.50 GHz、RAM 2.0 GB。感知层的无线传感器模拟环境为:Raspberry Pi 2B,操作系统为 Raspbian,处理器为 ARM Cortex-A7 CPU、RAM 1G(LPDDR2)。

在实验仿真过程中,通过无线传感器模拟采集了 50 条仿真数据，分别为导线温度值，电压值,电流值,导线振动频率,风偏和标志位,得到明文流为 M_i。同时选择 AES、DES、DES3 和 RC4 加密解密方案与本方案进行实验仿真对比,得到无线传感器在不同方案下对该 50 条明文数据的加密耗时,以及通信服务器在不同方案下对该 50 条明文数据的解密耗时。如图 3 所示,本方案加密耗时最短平均为 0.155 ms,DES3 方案加密耗时最长平均为 0.468 ms;本方案解密耗时最短平均为 0.095 ms,DES3 方案加密耗时最长平均为 0.281 ms。各方案加密与解密平均耗时如表 1 所示。本实验仿真表明,无线传感器可以高效快速地对采集的各类数据进行加密处理。

表 1　各方案加密与解密平均耗时

Tab.1　Average time taken by each scheme to encrypt and decrypt

方案	平均加密耗时/ms	平均解密耗时/ms
本方案	0.155	0.095
RC4	0.186	0.134
DES	0.266	0.190
AES	0.338	0.115
DES3	0.468	0.281



(a) 加密耗时图　　(b) 解密耗时图

图 3　数据加密与解密耗时图

Fig.3　Time consuming diagram of data encryption and decryption

6 结论

本文提出了一个超轻量级流加密方案，密钥生成器采用上一次的密文流做哈希生成下一次的密钥流，使得每一次生成的密文都与上一次的密文产生关联，一旦数据被篡改将导致后续数据解密失败。并将该方案应用到了电力无线传感器网络中，实现计算能力较弱的传感器节点也可以实时的对采集数据加密进行数据机密性传输保护。与采用AES和三重DES等方案的对比实验可知，本文方案效率有优势，适合设备计算能力弱、实时要求高的场合。

参考文献：

[1] KOCAKULAK M，BUTUN I. An overview of wireless sensor networks towards internet of things[C]//Las Vegas，NV，USA：IEEE 7th Annual Computing and Communication Workshop and Conference(CCWC). IEEE，2017：1-6.

[2] GUNGOR V C，LU B，HANCKE G P . Opportunities and Challenges of Wireless Sensor Networks in Smart Grid[J]. IEEE Transactions on Industrial Electronics，2010，57(10)：3557-3564.

[3] 刘建明，赵子岩，季翔. 物联网技术在电力输配电系统中的研究与应用[J]. 物联网学报，2018，2(1)：88-102.

[4] MAHMOOD A，JAVAID N，RAZZAQ S. A review of wireless communications for smart grid[J]. Renewable and Sustainable Energy Reviews，2015，41：248-260.

[5] EROL-KANTARCI M，MOUFTAH H T. Wireless Sensor Networks for smart grid applications[C]// Electronics，Communications & Photonics Conference. IEEE，2011.

[6] 戚攀，包开阳，马晶源. 基于模糊C均值聚类及群体智能的WSN分层路由算法[J]. 计算机应用，2018，38(7)：1974-1980.

[7] 薛雪，王建平，孙伟. 微电网数据通信无线传感器网络性能的跨层控制方法研究[J]. 电子测量与仪器学报，2018，32(10)：15-25.

[8] 武涛，应怀樵，简献忠，等. 基于WSN的电站电气设备监测系统设计[J]. 电站系统工程，2018，34(6)：51-53.

[9] LIU Y，OTA K，ZHANG K，et al. QTSAC：An Energy-Efficient MAC Protocol for Delay Minimization in Wireless Sensor Networks [J]. IEEE Access，2018，6(99)：8273-8291.

[10] LUO X Q，QI YUE，WAN Y D，et al. Low-cost and Fast AES Encryption method for industrial wireless network[J]. Journal of Beijing University of Posts & Telecommunications, 2015 (1): 55-60.

[11] VANGALA A，PARWEKAR P. Encryption model for sensor data in wireless sensor networks[M]. Springer：Information Systems Design andIntelligent Applications.2018：963-970.

[12] 左黎明，王露，张梦丽，等. 基于高效短签名的自动售货机安全交易协议[J]. 制造业自动化，2018，40(10)：4-7.

[13] 方如举，王建平，孙伟. 智能配电网无线传感器通信网络的跨层协作控制[J]. 电子测量与仪器学报，2018，32(2)：128-136.

A Super Light-Weight Stream Encryption Scheme for Real-Time Encryption of WSN Data

Tang Pengzhi[1,2]，Kang Wenyang[1,2]，Zhang Peng[1,2]，Zuo Liming[1,2]

(1.School of Science; 2.SEC Institute，East China Jiaotong University，Nanchang 330013, China)

Abstract：Aiming at the problems of lacking data confidentiality protection, weak computing ability and limited bandwidth in real-time data transmission of power wireless sensor networks, an ultra-lightweight stream encryption scheme was proposed. It consists of three parts: key creation, encryption and decryption. Furthermore, a data encryption transmission protocol for power wireless sensor networks was designed. Besides, the key implementation code and simulation were given. The simulation results show that compared with other algorithms, the efficiency is greatly improved and the difficulty of implementation is lower, and it is suitable for the secure transmission of data in the application scenarios where the computing power of power wireless sensor network devices is relatively weak.

Key words：smart power grid; wireless sensor network; stream cryptography; hash algorithm