WSN 中一种轻量级和高安全性的密钥管理方案*

曾 萍，张 历，杨亚涛，刘宇新，储 旭
（北京电子科技学院 通信工程系，北京 100070）

摘 要：提出了一种基于 ECC 和 ElGamal 的轻量级高安全性密钥管理方案。该方案采用汉密尔顿算法构造密钥池，采用分区域管理模型，每一区域设有一个服务器和控制中心，协议结合 ElGamal 进行通信双方的会话密钥协商。性能分析和仿真结果表明，该方案与传统的密钥管理方案相比，方案中节点的计算开销和通信开销得到了大大的降低，具有良好的网络连通性，比较适合于无线传感器网络。

关键词：无线传感器网络；通信协议；汉密尔顿回路算法；密钥管理；安全
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2014)01-0199-04
doi:10.3969/j.issn.1001-3695.2014.01.046

Lightweight and high security key management for wireless sensor networks

ZENG Ping, ZHANG Li, YANG Ya-tao, LIU Yu-xin, CHU Xu
(*Dept. of Communication Engineering, Beijing Electronic Science & Technology Institute, Beijing* 100070, *China*)

Abstract: This paper proposed a lightweight and high security key management based on ECC and ElGamal. In the scheme, the key pool was structured by the Hamilton algorithm, in which a layer network model was given, each lay had a servicer and control center, and session key was generated by ElGamal key agreement. The performance and simulation analysis shows, this scheme is superior to the traditional key pre-distribution schemes, not only computation cost and communication cost could be decreased, but good network connectivity is suitable for wireless sensor networks.

Key words: wireless sensor networks; communication protocol; Hamilton algorithm; key management; security

无线传感器网络(wireless sensor networks,WSN)是一种典型的分布式移动网络，其资源受限，网络中节点电量、计算能力和存储量都较小。传统网络的密钥管理方案并不完全适用于 WSN，为此需要寻找一种安全高效的密钥管理方案满足 WSN 对资源和安全的要求。近些年一些学者提出的密钥管理方案通常是在节点认证环节采用公钥密码体制，通信则采用对称密码体制。在这些方案中密钥分配和节点身份认证的安全性完全由公钥密钥体制来保证，通信的保密等安全特性则由对称密码体制完成。然而这些方案带来的结果是增加了节点的存储量和计算量。

1 相关工作

目前国内外关于 WSN 密钥管理方案的研究主要集中于对称密钥的预分配方案和基于公钥密钥的管理方案。基于对称密钥的预分配方案主要有两种：a)主密钥方案，所有节点在部署之前预分配一个主密钥，节点部署之后，任意两个节点利用主密钥产生会话密钥，实现安全通信；b)方案是对称密钥方案，假设节点规模为 N，每个节点保存 $N-1$ 个节点的对称密钥，但随着 WSN 规模的扩展，其资源占用率很大，网络没有扩展性。为了同时兼顾安全性和存储量，随后又产生了随机密钥预分配方案[1,2]、多项式的密钥预分配方案[3]和基于网络部署知识的密钥预分配方案[4]。

Eschenauer 等人在 WSN 中最先提出随机密钥预分配方案。该方案由三个阶段组成：a)密钥预分配阶段，部署前，部署服务器首先生成一个密钥总数为 P 的大密钥池及密钥标志，每一节点从密钥池中随机选取 $k(k<<P)$ 个不同密钥；b)共享密钥发现阶段，随机部署后，两个相邻节点如果存在共享密钥，就随机选取其中的一个作为一个双方的配对密钥，则进入阶段 c)；c)密钥路径建立阶段，节点通过与其他存在共享密钥的邻居节点经过若干条后建立双方的一条密钥路径。随后 Chan 等人[2]提出 q-Composite 随机密钥预分配方案，该方案从密钥池中预随机选取 m 个不同的密钥，部署后两个相邻节点至少需要共享 q 个密钥才能直接建立配对密钥。

Diffie 和 Hellman 提出第一个两方的密钥协商协议，自 Shamir 提出基于身份的密钥系统以来，研究人员利用 Shamir 的密钥构造方法结合 DH 协议，提出了一些基于身份的密钥协商协议，2001 年 Boneh 等人[5]利用双线性对提出基于身份的加密方案。然而，这些协议都不能满足完善前后安全性，虽然 Shim 的协议[6]满足了完善前后安全性，但是对于中间人攻击是脆弱的。McCullagh 等人[7]提出了一种有效的密钥协商协议，但他们的协议无法抵抗密钥泄露伪装攻击。Chen 等人[8]的协议首次在随机预言机模型下证明其安全性，但是他们的协议也不满足前后向安全性。

针对上述存在的问题，本文提出了一种 WSN 网络模型，运用计算量较小的 ECC 认证机制，采用 AES 的 ECB 模式进行密钥分配和传输信息，结合汉密尔顿算法建立密钥池。该方案中

收稿日期：2013-02-16；**修回日期**：2013-06-04 **基金项目**：中央办公厅信息安全重点实验室基金资助项目(YZDJ1004,YZDJ0805)；北京电子科技学院重点实验室学术科研基金资助项目(YZDJ1101)；中央高校基本科研业务费专项资金资助项目(YZDJ1101)

作者简介：曾萍(1969-)，女，广东潮安人，教授，硕导，博士，主要研究方向为无线通信与安全(zp@besti.edu.cn)；张历(1988-)，男，江苏淮安人，硕士，主要研究方向为无线通信与安全.

节点的身份认证和密钥协商采用 ECC 密码体制,弥补了节点计算能力有限、存储量小、电源能量、通信范围存在限制的缺点。

2 基于区域的密钥管理方案

2.1 网络模型

该方案将 WSN 网络分为管理层、服务层、用户层三层。管理层具有能量充足、计算能力强大、有足够的存储空间和通信范围的特点,称做控制中心(S);服务层有较强的能量、计算能力和一定的存储量;用户层,即用户传感器节点(U_{ij}),数量巨大,计算能力弱,能量、存储空间和通信范围有限。网络模型如图 1 所示。

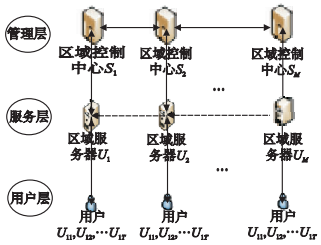

图1 网络模型图

2.2 密钥初始化

1)系统参数建立阶段 本方案采用椭圆曲线密码体制。设素数域中的椭圆曲线方程为 $E:y^2=(x^3+ax+b)\bmod p$,曲线参数为 $E:\{a,b,G,N,P\}$。其中,G 是椭圆曲线 $E/F(P)$ 上的基点,N 为 G 的阶。用 $G=(x_G,y_G)$ 来表示 G,设系统私钥为 s。则对应的系统公钥为椭圆曲线上的 $sG=(x_S,y_S)$,其中 $s\in Z_P$。系统参数由离线密钥分配中心管理和更新。

2)节点初始化阶段 此阶段在节点部署前进行。假设无线传感器网络中有 $T\times M$ 个传感器节点。将整个网络分成 M 个区域。设 U 为任意单元(包括控制中心、服务器、普通传感器节点),其完整的身份信息 ID_u 如图 2 所示。其中,区域号为节点 U 所在的区域,每一节点都有唯一的身份标志,编号为节点在该区域中的代号。

节点ID_u

区域号	身份标志	编号

图2 节点身份信息

节点密钥初始化:ID_u,公钥 uID_usG,私钥 u,其中 $u\in Z_P$,$ID_u\in Z_p$ 为节点随机选取的整数。

3)区域密钥初始化阶段 区域密钥的初始化在节点部署之前进行。采用 AES 对称密钥进行加密传输,每次进行 128 bit 分组加密,加密方式为 ECB。每一节点存储 128 bit 的对称密钥 K 作为区域初始密钥。

2.3 密钥协商和通信协议

设用户 A 和用户 B 进行通信,具体通信过程如图 3 所示。

具体的密钥协商协议(协议 1)[10] 如下所示:

$1:A\rightarrow B:ID_A\ ||\ R_A\ ||\ (x_1ID_A,y_1R_A)$

$2:B\rightarrow A:ID_B\ ||\ R_B\ ||\ E_K(R_A\ ||\ ID_A\ ||\ bsGy_2\ ||\ (x_1ID_B,y_1R_B))$

$3:A\rightarrow B:E_K(R_B\ ||\ ID_B\ ||\ asGy_2)$

$4:B\rightarrow A:E_K(L\ ||\ \text{start})$

$5:A\rightarrow B:E_K(M\ ||\ ID_A\ ||\ L)$

A 的私钥为 a,公钥为 aID_AsG,$R_A=F_AsG$,F_A 是新鲜随机数。

B 的私钥为 b,公钥为 bID_BsG,$R_B=F_BsG$,F_B 是新鲜随机数,$a,b,F_A,F_B\in Z_P$。

L 为通信计数器,每通信一次,L 值 +1,当 L 达到阈值时,更新密钥。

start 为通信正式开始标志,会话密钥为 K。

E_K 的加密密钥从 x_2 提取,y_2 作为签名密钥。

认证协商过程如下:

a)A 首先计算 $abID_BsG\times ID_B^{-1}=absG=(x_1,y_1)$,并对 ID_A,R_A 进行加密。

b)B 开始计算 $baID_AsG\times ID_A^{-1}=basG=(x_1,y_1)$,验证 ID_A,R_A 是否被窜改,若被窜改就放弃会话,否则计算$(x_2,y_2)=F_AF_BsG=F_AR_B=F_BR_A$,会话密钥 K 从 x_2 提取,采用 AES 分组加密技术,同时计算 $bsGy_2$ 进行加密传输。

c)A 首先计算$(x_2,y_2)=F_AF_BsG=F_AR_B=F_BR_A$,对密文进行解密,然后验证 ID_B,R_B 是否被窜改,若被窜改则放弃会话;否则验证等式 $bsG=bsGy_2\times y_2^{-1}$ 是否成立,成立说明会话密钥协商成功,否则放弃会话。

d)B 验证 $asG=asGy_2\times y_2^{-1}$ 是否成立。若成立,则发送 L 和通信标志 start,否则放弃会话。

e)A 发送明文 M,L 和身份信息进行通信。

2.4 密钥池生成

设 WSN 中有 $t\times M$ 个节点,分成 M 个区域,每个区域 t 个节点。初始化阶段,服务器存储该区域内所有节点的身份信息,然后服务器对每个节点进行随机编号,每个节点设定完编号后,采用汉密尔顿算法对编号进行随机排序,区域密钥的选取根据排序选择每一节点的子密钥,构成完整的区域密钥。具体操作工作如表 1 所示。

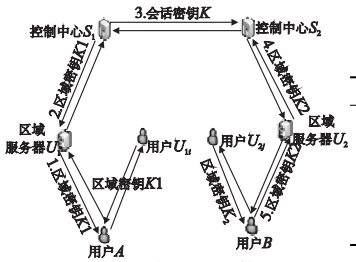

表 1 区域密钥池构造

身份信息	编号	密钥信息
ID_1	1	K_1
ID_2	2	K_2
ID_3	3	VK_3
⋮	⋮	⋮
ID_T	T	K_T

图3 物联网设备节点通信协议过程

其中,$ID_1,ID_2,\cdots,ID_T$ 为该区域内所有节点的身份信息,1,2,3,$\cdots$,T 为服务器对区域内节点进行的随机编号 $K_1,K_2,\cdots,K_T$ 取自每个节点身份信息的 L bit。设节点的身份信息为 K bit,则每一节点共有 C_K^L 种取法,完整的区域密钥长度为 LT bit。

2.5 密钥更新

密钥更新也分为三个阶段:a)周期性更新密钥; b)节点加入/离开;c)系统密钥更新。本方案根据 ECC 协议的更新体制,节点自身的私钥 s 和会话密钥从数域 Z_P 中随机选取的。

1) 周期性密钥更新

本方案中节点的密钥与身份一一对应,可采取在节点初始化后,设定身份 ID 中的前 n 位作为周期更新时间,节点临时更新密钥时采用在通信协议中加入时间戳来完成。

2) 节点加入

网络结构如图 4 所示。

具体协议如下:

当有新节点加入时,首先控制中心 S_1 检查该节点的身份,

假设该节点为 U_{1J},进行如下通信:

1:$U_{1J}\rightarrow S_1$:$\mathrm{ID}_{U_{1J}}$ || join || ($x_{S1}\mathrm{ID}_{U_{1J}}$,$y_{S1}R_{1J}$)

2:$S_1\rightarrow U_{1J}$:ID_{S_1} || R_{S1} || E_{KS}(R_{1J} || $\mathrm{ID}_{U_{1J}}$ || $csGy_{S2}$ || ($x_{S1}\mathrm{ID}_{S_1}$,$y_{S1}R_{S1}$))

3:$U_{1J}\rightarrow S_1$:E_{K_S}(R_{S1} || ID_{S_1} || $dsGy_{S2}$)

4:$S_1\rightarrow U_1$:join || $\mathrm{ID}_{U_{1J}}$ || time

其中:join 为加入标志,验证过程遵循协议 1。

然后区域服务器 U_1 进行区域号、编号以及区域密钥分发,区域密钥由节点向服务器申请。假设新加入节点为 U_{11},则申请过程如下:

1:$U_1\rightarrow U_{11}$:joinID || time

2:$U_{11}\rightarrow U_1$:$\mathrm{ID}_{U_{11}}$ || ($x_1\mathrm{ID}_{U_{11}}$,y_1R_{11})

3:$U_1\rightarrow U_{11}$:ID_{U_1} || R_1 || E_K(R_{11} || $\mathrm{ID}_{U_{11}}$ || $bsGy_2$ || ($x_1\mathrm{ID}_{U_1}$,y_1R_1))

4:$U_{11}\rightarrow U_1$:E_K(R_1 || ID_{U_1} || $asGy_2$)

5:$U_1\rightarrow U_{11}$:E_K(L || start || K_1)

验证过程遵循表 1 协议。其中区域服务器为 U_1,私钥为 b,区域内某一节点为 U_{11},私钥为 a。控制中心 S_1 的私钥为 c,$R_{S1}=F_{S1}sG$,F_{S1} 为 S_1 的新鲜随机数。离开节点为 U_{1J},私钥为 d。

$R_{1J}=F_{1J}sG$,F_{1J}为 U_{1J}的新鲜随机数。E_{K_S}的加密密钥从 x_{s2} 提取,K_S 作为会话密钥。

L 为通信计数器,每通信一次,L 值 +1,当 L 达到阈值时,更新密钥。

E_K 的加密密钥从 x_2 提取,y_2 作为签名密钥。最后的协商密钥即会话密钥为 K。

K_1 为该区域的区域密钥,E_{K_1}使用区域密钥加密。

start 为通信正式开始标志(即身份验证和会话协商完毕)。

time 是工作站为离开节点设置的暂停时间。

3)节点离开/撤销

网络结构如图 5 所示。

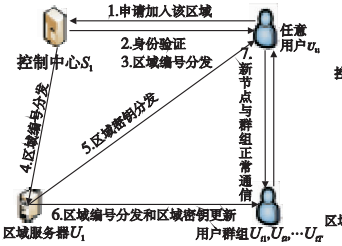

图4 区域新节点加入过程

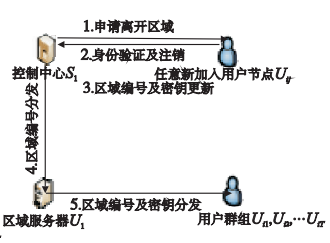

图5 物联网设备节点离开过程

具体协议内容如下:

假设节点 U_{1J}离开该区域,控制中心 S_1 使用密钥协商协议对 U_{1J}的身份进行验证。

1:$U_{1J}\rightarrow S_1$:E_{K_1}(leave || $\mathrm{ID}_{U_{1J}}$)

2:$S_1\rightarrow U_{1J}$:ID_{S_1} || ($x_{S1}\mathrm{ID}_{S_1}$,$y_{S1}R_{S1}$)

3:$U_{1J}\rightarrow S_1$:$\mathrm{ID}_{U_{1J}}$ || R_{1J} || E_{KS}(R_{S1} || ID_{S_1} || $dsGy_{S2}$ || ($x_{S2}\mathrm{ID}_{U_{1J}}$,$y_{S2}R_{1J}$))

4:$S_1\rightarrow U_1$:deleteID$_{U_{1J}}$ || time

其中:leave 为离开标志,E_{K_1}使用区域密钥 K_1 加密,验证过程遵循协议 1。

然后区域服务器 U_1 广播给区域内其他节点,并进行区域密钥更新,设区域内某一节点为 U_{11},则

1:$U_1\rightarrow U_{11}$:deleteID || time

2:$U_{11}\rightarrow U_1$:$\mathrm{ID}_{U_{11}}$ || ($x_1\mathrm{ID}_{U_{11}}$,y_1R_{11})

3:$U_1\rightarrow U_{11}$:ID_{U_1} || R_1 || E_K(R_{11} || $\mathrm{ID}_{U_{11}}$ || $bsGy_2$ || ($x_1\mathrm{ID}_{U_1}$,y_1R_1))

4:$U_{11}\rightarrow U_1$:E_K(R_1 || ID_{U_1} || $asGy_2$)

5:$U_1\rightarrow U_{11}$:E_K(L || start || K_1)

其中:delete 为删除标志。验证步骤遵循协议 1。

4)系统密钥更新

当系统密钥使用了一段时间后,为了防止敌手进行明密文、穷举法等攻击行为,需要定期地对系统参数 $\{E_p(a,b),a,b,p,N,G,sG,s,K\}$进行更新。

具体步骤:在系统初始化阶段有一个临时离线密钥分配中心负责系统参数的更新工作,并分发给每个控制中心,再由控制中心分发给各自区域内的节点。

3　性能分析

设网络规模为 $M\times T$,分为 M 个区域,每个区域 T 个节点。节点类型分为控制中心、服务器、传感器节点。

1)存储量

控制中心 S 存储 WSN 中所有控制中心以及该区域内所有节点的身份、公钥信息,控制中心负责节点跨区域通信消息的转发,需要存储该区域的区域密钥池。存储复杂度为 $O(M+T)$。

服务器 U 存储该区域的区域密钥池、节点身份公钥信息,存储复杂度为 $O(T)$。节点 U_{ij}存储自身和区域控制中心的身份公钥信息、区域密钥,存储复杂度为 $O(3)$。

2)计算时间复杂度

在 Tseng 方案[9]和本方案中,普通节点只存储一个群密钥。而在 Steiner 方案中每两个节点都有交换密钥用于通信。群密钥由这些通信密钥联合生成,因此存储在普通节点中的密钥要比前两种方案的密钥多。有新节点加入时,本方案只需要更新区域密钥,并且只有该区域内的节点数量发生变化,对其他区域没有影响,而在 Tseng 方案和 Steiner 方案中一旦有新节点加入,则必须生成新的密钥发放给所有区域内的节点,时间复杂度为 $O(MT)$。表 2 给出不同方案的时间复杂度比较。

表 2　不同方案的时间复杂度对比

方案	群首节点的密钥存储量	普通节点的密钥存储量	新节点加入时间复杂度	节点离开时间复杂度	群内部通信时间复杂度
Steiner 方案	$O(MT)$	$O(MT)$	$O(MT)$	$O(MT)$	$O(MT)$
Tseng 方案	$O(1)$	$O(1)$	$O(MT)$	$O(MT)$	$O(MT)$
本方案	$O(1)$	$O(1)$	$O(1)$	$O(1)$	$O(1)$

从表 2 可以看出,本方案存储在用户节点中的密钥信息明显比 Tseng 方案和 Stentiner 方案少。新节点加入时,本方案只需要更新区域编号和区域密钥,对其他区域没有影响,而在上述其他两种方案中,一旦有新节点加入,则必须生成一个新的群密钥并分发给所有剩余的节点。节点离开时,Tseng 方案和 Stentiner 方案中整个网络都必须生成新的群密钥并分发给所有的节点,而本方案只需要对离开节点进行身份注销并更新对应区域编号和密钥,而不影响其他区域。

为了进一步描述物联网用户节点的网络特性,本方案就节点计算复杂度和通信复杂度等特性与 E-G 方案[1]、q-Composite 方案[2]、PIKE 方案[10]、LEAP 方案[11]以及 CPKS 方案[4]作了比较。E-G 方案中用户节点需要存储 K 个密钥组成自身的密钥环用于共享密钥发现,因此节点的计算复杂度和存储复杂度都为

$O(m)$;q-Composite 方案中节点随机密钥中选取 m 个密钥构成自身的密钥环,类似于 E-G 方案,节点计算复杂度和存储复杂度为 $O(m)$。上述两个方案中节点通信都只需要密钥发现和会话密钥两个阶段,其复杂度都为 $O(2)$。同样可以分析出 PIKE 方案、LEAP 方案和 CPKS 方案对应的复杂度,比较结果如表3所示。

表3 密钥管理方案和协议的性能比较

密钥管理方案	计算复杂度	通信复杂度	存储复杂度
CPKS 方案	0	0	$O(c)$
E-G 方案	$O(k)$	$O(2)$	$O(k)$
q-Composite 方案	$O(m)$	$O(2)$	$O(m)$
PIKE 方案	$O(2)$	$O(\sqrt{n})$	$O(\sqrt{n})$
LEAP 方案	$O(d^2/N)$	$O(\log N)$	$O(d+L)$
本方案	$O(2)$	$O(2)$	$O(2)$

从表3中可以看出,本方案的用户节点只需要进行两次协商密钥的计算,两次通信以及存储自身的公私钥和区域密钥,与传统的密钥管理方案相比,通信成本以及存储成本得到了大大的降低。

4 仿真分析

4.1 通信开销

为了比较通信双方在不同区域的开销,假设节点 A 和 B 在同一区域的概率为 P,一次通信的开销为 $\lg q$ 。

本方案中,同一区域的节点通信至少需要进行3次会话通信,不同区域的节点至少需要16次会话通信。故节点的通信开销期望为 $E(p)=3p\log_2 q+16p\log_2 q$,$q$ 的取值范围为[2,20],单位为 KB,通过取不同的概率 P 来模拟网络节点的通信开销。仿真结果如图6所示。从图6可以看出,随着概率的增加,节点的通信开销期望值也随之增加,即节点通信的开销期望值随着通信区域的变化而不同。

4.2 网络连通性

假设网络规模为 $T\times T$,分为 T 个区域,每个区域 T 个节点。由于无线传感器网络中节点在传输信息的过程中存在丢包现象,丢包率的大小与整个网络的规模存在一定的关联,设丢包率为 $L=0.1$,考察节点密钥更新开销的期望值与网络规模的关系。条件满足以下假设:a)若信息在传输途中丢失,则由上一次负责传输的节点进行重发(此时密钥需要更新),同时区域服务器广播区域内所有节点进行区域密钥更新;b)信息丢失在可控的范围内,即至少有相邻的节点可以进行信息重发,未丢失的节点只需更新一次区域密钥,密钥更新一次的开销为 $\lg q$。

若区域内有 T 个节点,丢包率为 L,结合上述的假设,该区域内节点密钥更新开销的期望值 $E(q)=2TL\lg q+T(1-L)\lg q$。通过选取不同的 T 值进行比较,使用 MATLAB 编程,仿真结果如图7所示。

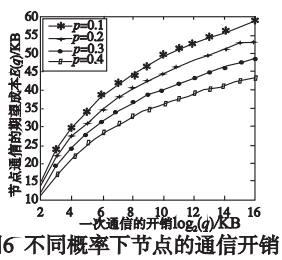

图6 不同概率下节点的通信开销

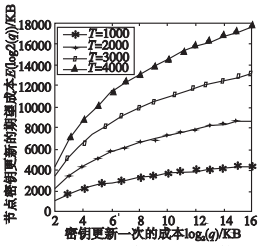

图7 不同网络规模下的密钥更新开销

图7仿真结果表明,随着网络节点数量的不断增加,节点密钥更新的开销不断增大,但增长的幅度是多项式阶的,并不会对整个网络的连通性造成太大的影响。

5 安全性分析

本方案中网络模型按区域进行划分,每个区域都有一个区域控制中心和一个区域服务器,同一区域中的节点通信只需采用区域密钥进行会话密钥协商,节省了通信开销和计算开销。不同区域的节点通信需要通过各自的区域控制中心进行身份验证和加密处理,提高了通信安全性并可以较好地防范外部网络的攻击。方案采用文献[12]中已证明安全性的密钥协商协议,协商协议满足前/后向安全性和 PKG 安全性,即当有节点加入或离开时,区域密钥会由服务器更新,各节点的会话密钥也会更新,故新加入的节点和离开后的节点无法获取区域密钥和会话密钥。由于各节点在密钥协商时自动生成自己的秘密密钥,所以 PKG 无法计算出协商的会话密钥。除此之外,该协议可以抵御常见的中间人攻击、重放攻击,满足已知密钥安全、未知密钥共享安全等安全性。方案中的密钥池根据汉密尔顿算法构造,敌手破获密钥池的复杂度为 $O(n!)$,远大于 2^n。

6 结束语

针对 WSN,本文提出了一种基于椭圆曲线密码体制的密钥管理方案和通信协议,该模型能提供简洁、安全的密钥协商、身份认证和更新方法,同时由于椭圆曲线的计算特性,节点在通信过程的存储量、计算量与传统的密钥管理方案相比很小,更易于实现。本方案使用的通信协议具有更高的安全性,任何节点在受到攻击时,受影响的仅仅是该节点及其对应的链路信息,对网络中的其他节点和链路不会造成影响。在下一步研究工作中,将重点研究 WSN 环境中具体的算法和方案实现。

参考文献:

[1] ESCHENAUER L,GLIGOR V. A key management scheme for distributed sensor networks[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York:ACM Press,2002:41-47.

[2] CHAN H,PERRIG A,SONG D. Random key predistribution schemes for sensor networks[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society,2003:197-213.

[3] LIU Dong-yang, NING Peng . Establishing pairwise keys in distributied sensor network[C]// Proc of the 10th ACM Conference on Computer and Communications Security. New York:ACM Press, 2003:51-61.

[4] LIU Dong-yang, NING Peng. Location-based pairwise key establishments for static sensor networks[C]//Proc of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks. New York:ACM Press, 2003:72-82.

[5] BONEH D,FRANKLIN M. Identity based encryption from the Weil pairing[C]//Proc of Advances in Cryptology—Crypto. Berlin: Springer-Verlag,2001:213-229.

[6] SHIM K. Efficient ID-based authenticated key agreement protocol based on the Weil pairing[J]. IEE Electronics Letters,2003, 39(8): 653-654.

(下转第205页)

3.2　条件熵计算选择

将 X_1、X_2 交换,求出 X_2 关于 X_1 的加权条件熵 $H(X_1|X_2)$,如图 3 所示。由图中可以看出,该熵值在正常流量中表现不稳定,与异常流量区分度不大。这是由于正常情况下,相同的主机连接一般进行的是相同服务,而提供相同服务的主机却不一定是相同的,所以相同服务关于相同主机的条件熵波动较大。由实验可以看出,同一组网络特征属性计算不同条件熵对网络特征的反映不同。

3.3　与其他信息熵对比

相对熵可以反映两个分布的相似程度,其公式为

$$H(X_1,X_2) = -\sum_{i=1}^{q} P(a_i)\log\frac{P(a_i)}{Q(a_i)} \tag{7}$$

其中:$P(a_i)$ 和 $Q(a_i)$ 分别表示两个特征属性的概率分布。运用相对熵处理上述实验的两个属性,分别计算在正常网络和异常网络中的相对熵值,如图 4 所示。由图中可以看出,相对熵仅仅描述两个属性分布的相对情况,由于缺乏考虑攻击发生特征属性内在联系,不能准确反映正常网络与异常网络的差别。

最后根据本文提出的异常检测方法,除上述特征属性外,引入网络服务类型关于数据包大小,root 用户次数关于程序执行次数的两组条件熵对五种攻击类型进行综合异常检测,检测方法与传统信息熵理论对比,实验结果如表 3 所示。

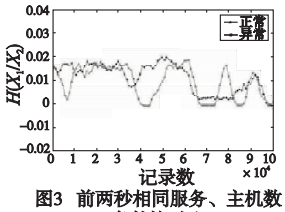

图3　前两秒相同服务、主机数条件熵对比

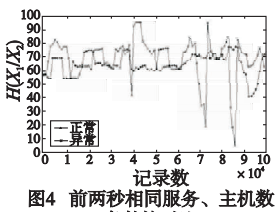

图4　前两秒相同服务、主机数条件熵对比

表 3 综合检测结果

攻击	加权条件熵检测		信息熵检测	
类型	检测次数	检测率/%	检测次数	检测率/%
Probe	9/11	81.8	6/11	54.5
DoS	32/33	96.9	30/33	90.9
U2R	13/16	81.2	5/16	31.2
R2L	21/28	75.0	7/28	25.0
unknow	5/9	55.5	1/9	11.1

由表 3 可看出,由于 DoS 攻击中有大量流量记录,两种算法均能较好地检测出异常状态,其他三种攻击模式中其流量记录较少,仅有单一特征属性检测成功率很低,而条件熵可以反映某种属性条件下另一属性分布情况,对于端口扫描,非法访问等攻击手段具有良好的检测效果。而对于未在训练过程中出现的未知攻击,加权条件熵也表现出较好的识别效率。通过实验对比说明,加权条件熵能在特征属性和计算方法选择合理的前提下,其异常检测效果比传统信息熵理想。

4　结束语

在已有信息熵理论的基础上,分析条件熵固有特性,提出了加权条件熵在异常检测中的应用。由于条件熵既包括一般信息熵特性,也反映事件发生之间的内在相关性,考虑到实际中网络特征属性之间也存在一定的相关性,将该方法引入异常检测是一种行之有效的方法。通过实验,证明其在异常检测方面的有效性和适用性。

在实验过程中也发现一些问题,属性选择和熵值计算方法的不同将对异常检测的性能造成明显的影响,所以如何选取更有效的特征属性和应用于实际网络中检测其效果将是下一步研究的方向。

参考文献:

[1] WAGNER A, PLATTNER B. Entropy based worm and anomaly detection in fast IP net works[C]//Proc of IEEE International wordshop on Ensbling Technolgies. 2005:172-177.

[2] LALL A, SEKAR V, XU Jun, *et al*. Data streaming algorithms for estimating entropy of net work traffic[J]. ACM SIGMETRICS Performance Evaluation Review,2006,34(1):145-156.

[3] 朱应武,杨家海,张金祥. 基于流量信息结构的异常检测[J]. 软件学报,2010,21(10):2573-2583.

[4] 王海龙,杨岳湘. 基于信息熵的大规模网络流量异常检测[J]. 计算机工程,2007,33(18):130-133.

[5] 陈锶奇,王娟.基于信息熵理论的教育网异常流量发现[J]. 计算机应用研究,2010,27(4):1437-1436.

[6] 刘军,程光.异常检测中信息熵灵敏度分析[J]. 广西大学学报,2011,36(1):161-164.

[7] 张亚玲,韩照国,任姣霞.基于相对熵理论的多测度网络异常检测方法[J]. 计算机应用,2010,30(7):1771-1774.

[8] ALTAHER A, RAMADSS S, ALMOMANI A. Real time nework anomaly detection using relative entropy[C]// Proc of the 8th International Conference on High-Capacity Optical Networks and Emerging Technologies. [S. l.]: IEEE Press,2011:258-260.

[9] 张登银,廖建飞.基于相对熵的网络流量异常检测方法[J]. 南京邮电大学学报,2012,32(5):26-31.

[10] 徐久成,孙林,马媛媛.基于新的条件熵的决策表约简方法[J]. 计算机工程与设计, 2008, 29(9): 2313-2316.

[11] 易胜蓝.利用互信息进行网络异常检测的熵特征优选[J]. 电讯技术,2012,52(6):1018-1021.

[12] GUIASU R. Information theory with application [M]. New York: McGraw-Hill, 1997.

[13] 傅祖云. 信息论[M]. 北京:电子工业出版社,2005.

(上接第 202 页)

[7] McCULLAGH N, BARRETO P. A new two party identity-based authenticated key agreement[C]// Proc of RSA Conference. Berlin: Springer-Verlag,2005:262-274.

[8] CHEN L, KULDA C. Identity based authenticated key agreement protocols from pairing[C]//Proc of the 16th IEEE Computer Security Foundations Workshop. 2003:219-233.

[9] TENG Y M, YANG C C, LIAO D R. A secure group communication protocol for Ad hoc wireless networks[C]//Proc of Advances in Wireless Ad hoc and Sensor Networks and Mobile Computing. [S. l.]: Springer,2007:385-390.

[10] CHAN H, PERRIG A. PIKE: peer intermediaries for key establishment in sensor networks[C]//Proc of IEEE INFOCOM . Piscataway: IEEE Communication Society,2005:524-535.

[11] ZHU S, SEYIA S, JAJODIA S. LEAP: efficient security mechanisms for large-scale distributed sensor networks [C]//Proc of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press,2003:62-72.

[12] 曾萍,张历,胡荣磊,等. WSN 中基于 ECC 的轻量级认证密钥协商协议[J]. 计算机工程与应用,2012,49(10).