基于网络编码的ECC验证方案在WSN中的研究

朱雪寒,夏卓群,刘品超,谢立通
(长沙理工大学 计算机与通信工程学院,湖南 长沙 410114)

摘 要:网络编码在无线传感器网络应用,改善了无线传感器网络的性能。虽然与之前相比,其安全性有所提高,但当面临安全攻击(被动攻击和主动攻击)时,整个网络系统的安全性仍然亟待提高。提出了一种改进方案,该方案结合密码学中椭圆曲线加密算法,并基于应用网络编码的无线传感器网络,采用加密验证方案。使传感器节点在电量受限的情况下,传输更多的有效数据。同时,增强了无线传感器网络节点之间通信的安全性,以及WSN其鲁棒性和容错性。

关键词:无线传感器网络;网络编码;安全性;椭圆曲线加密算法;加密验证
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)02-0173-04

Research of ECC Verification Based on Network Coding in WSN

ZHU Xue-han, XIA Zhuo-qun, LIU Pin-chao, XIE Li-tong
(Department of Computer and Communication Engineering, Changsha University of Science & Technology, Changsha 410114, China)

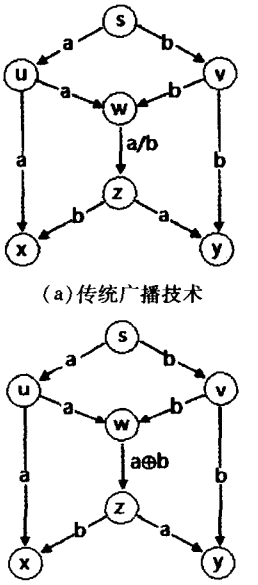
Abstract: With the application of network coding in wireless sensor networks, it has improved the performance of wireless sensor networks. Although compared with the previous, improved their safety, but when faced with security attacks (passive attacks and active attacks), the whole network system security still needs to be improved. An improved scheme is proposed. The scheme combines elliptic curve cryptography (ECC), encryption algorithm, and based on application of network coding for wireless sensor networks using encryption verification. Because electricity constrained sensor nodes, it requires more effective data transmission. At the same time, it enhances communication between the wireless sensor network node security, as well as the system robustness and fault tolerance.

Key words: wireless sensor networks; network coding; security; elliptic curve encryption algorithm; encrypted authentication

0 引 言

集成了传感器、微机电系统和网络三大技术而形成的传感器网络(Wireless Sensor Networks, WSN)是一种全新的信息获取和处理技术[1]。随着无线传感器网络的广泛应用,其信息传输对安全性的要求也越来越高。当前,如何通过无线传感器网络更加安全地传输关键和敏感的信息,已成为研究的热点。

网络编码(Network Coding)[2]是21世纪初在信息论领域中的一个重要突破。它是一种融合编码和路由的信息交换技术,在传统存储转发的路由方法基础上,通过允许对接收的多个数据包进行编码信息融合,增加单次传输的信息量(见图1)。如今,网络编码已成为一项融合信息论、代数学、图论、网络流理论和优化理论等多学科的交叉技术,且日益引起更多研究者的关注,其对现有的网络体系结构、协议设计方法、信息交换方式和网络管理模式带来了革命性的变化。



(a)传统广播技术

(b)网络编码技术

图1 网络编码的基本原理

网络编码最早是在2000年由R. Ahlswede等人[3]首先提出的,他们提出网络编码可以实现网络流

收稿日期:2010-06-16;**修回日期**:2010-09-19
基金项目:教育部国家创新性实验支持项目(091053604)
作者简介:朱雪寒(1989-),男,湖南长沙人,研究方向为无线传感器和网络编码;夏卓群,博士生,研究方向为无线网络、网络编码。

量的最大化。2003 年,Li,Yeung 和 Cai 通过线性网络编码对这个观点加以证明[2]。随后随机网络编码(Random Network Coding,简称 RNC)理论由 T. Ho 等人[4,5]提出。他们指出在数据传输过程中,传输经过的网络节点在某一个足够大的有限域中随机选择一个元素,作为随机组合系数,然后对其输入数据进行随机线性组合后输出,接收节点能以很大的概率正确恢复出信源所发送的信息。文中所提出的方案就是在随机网络编码与 WSN 结合的基础上实现的。

虽然网络编码在无线传感器网络中的应用大大提高了网络的性能,但是其安全性仍然亟待提高。其中三种典型的安全威胁是窃听、伪造和篡改。在这里,文中假设:

Alice:数据传输的源发送端。

Bob:数据传输的接收端。

Carol:攻击者。

Eve:数据传输的中间节点(也可以是接收端)。

Mallory:Eve 的临近节点(可以是发送端或接收端),能够直接通信。

WSN 的广播特性使其数据传输过程中受到窃听的威胁也大于普通的有线网络。例如,Alice 发送数据到 Bob,Carol 计划对 Eve 进行窃听。Carol 通过获取到线性网络编码的系数和其相对应的密文,就能够对数据进行窃听。

当 Carol 得到线性网络编码的系数并且成功加入 WSN 后,Carol 就可以将数据进行编码,并和其他 WSN 中的节点进行通信。当 Carol 伪造一份数据发送给 Bob,或者通过 Eve 发送到 Bob 端,Bob 会认为这个数据是从 Alice 端发送来的。这就是最常用的伪造的方式。Carol 利用伪造还能和 Bob 进行后续通信,获取重要数据。这是 Carol 利用身份欺骗对 WSN 进行攻击。

当 Alice 发送数据给 Bob 时,如果其中某一数据包被 Carol 截获后篡改,再通过 Eve 等节点发给 Bob。被修改的数据包在 Eve 节点无法被检测出,甚至在 Bob 端也无法被及时检测。只有当 Bob 收到了所有数据后,进行解码转换后,才能发现。导致了节点能量损耗、计算浪费,而这对于 WSN 是致命的。

1 相关知识

关于椭圆曲线公钥密码算法(ECC)相关知识,在 IEEE P1363 中有具体规定。其中定义了公共密钥加密技术,以及生成基于 GF(p)域的椭圆曲线参数,而且能够生成足够的信息能使其他人验证这样的曲线的确是随机生成的[6]。

Lun 等人提出了分组网络可靠的通信编码方式[7]。尽管能够使得网络流量达到最大化,但是该方案不能应对窃听和篡改等安全攻击。周业军等提出了一种防窃听的网络编码算法[8]。该编码算法仅是在原随机编码体制的基础上对信源和信宿进行了改变,中间节点编码保持不变。虽然修改不大,但是其效果还是比较明显的。算是一种有益的改进。但是,这个方法有一个缺点,就是需要在信源和信宿之间建立一种安全信道,这个对于 WSN 来说,是不合适的。蒲保兴等[9]针对随机线性网络编码,提出点到点检错和端到端重传相结合的差错控制方法。并采用三维奇偶校验码进行检错,让有错的数据包不参与编码。当宿点不能解出源点播出的信息时,通过反馈重传策略让源点重传信息。作者的实验结果表明其能以较低的重传率完成信息传输,对于无线传感器网络有些不适,因为其计算量过大,这会导致节点能量的过度损耗。

Cai 等[10]提出了一种安全网络编码。文中指出了安全网络编码在防止窃听时的一些必要的条件。但是这种方案仍然不能解决篡改攻击。同时,Carol 通过监控 Bob 附近的信道,能够获取到保密数据。M. Krohn 等[11]提出了一种实时验证,确保有效内容尽快发布。这个方案需要路由器和目的节点 刚一接收到数据就使用同态散列法确认数据的完整性。但是,作者没有考虑到 hash 值的安全传输。K. Bhattad 等提出了一种弱安全网络编码[12]。这样的一种新的安全信息理论模型定义了弱安全,在这样的系统中,Carol 窃听不到任何关于 Alice 有价值的信息。这个方案要求编码方式是 Carol 所不知道的,并且窃听信道是固定的。T. Ho 等提出一种 Byzantine 修改检测协议[13]。在该方案中,Alice 在每个数据包中插入经过多项式函数计算出的 hash 值。Bob 对收到的数据包进行检测,并决定该数据包是否已经被修改。这个协议中涉及到了最小附加计算量,它是用没有加密的函数介绍的。同样的,当数据包没有到达 Bob 时,Carol 可以对数据包进行 Byzantine 攻击。这样会消耗大量的节点能量用于传输污染数据,这对 WSN 来说是致命的。

文中提出了一种基于密码学中的 ECC,提出了一种基于 WSN 的椭圆曲线加密算法验证方案。在第二部分进行详细介绍。

2 基于网络编码的 ECC 的研究与设计

椭圆曲线(Elliptic Curve)是代数几何中研究的重要问题。椭圆曲线公钥密码算法(ECC)是由 Neal Koblitz 和 Victor Miller 在 1985 年分别独立提出的。椭圆密码体制是基于椭圆曲线离散对数问题(ECDLP)。它是目前已知的公钥体制中,对每一比特所提供加密强度最高的一种体制。它具有安全性高、密钥量小、灵

活性好的特点,受到了国际上的广泛关注。

文中所提出的方法就是将网路编码与密码学相关理论相结合,提出一种基于椭圆曲线加密算法的验证方案。鉴于传感器传输信息要比执行计算更消耗电能,传感器传输 1 位信息所需要的电能足以执行 3000 条计算指令,文中增加了 WSN 节点的计算量。显而易见,适当增大其节点的计算量,远比大量传输受污染的信息更为节能。文中认为在通过 WSN 传输重要信息时,其安全性远比效率更为重要。因此文中在设计时,将数据的 Hash 值的计算放到了经过 ECC 加密之前完成,而不是在完成 ECC 加密后计算其 Hash 值。文中的目标是在有限的能量范围内传输更多有效的数据。

2.1　基于网络编码的 ECC 的基本框架

Alice 要发送 n 个数据报文,$m_1,m_2,m_3,\cdots,m_n$。Alice 经过随机线性网络编码来产生他们的输出信息,记作 M。根据输出信息 M 计算出其 Hash 值为 $H(M)$。Alice 将 $H(M)$ 附加到 M 尾部,并使用密钥 K 进行 ECC 加密,生成密文,并发送。

Eve 接收到后,首先使用密钥 K 对进行 ECC 解密,得到数据报文。分离出 $H(M)$ 和编码后的报文 M 后,Eve 对编码后的报文自行计算其 Hash 值 $H_2(M)$。将 $H_2(M)$ 与分离出的 $H(M)$ 进行比较。如果一致,将 M 与接收到的其他数据报文 M_2 进行随机线性编码。按照与 Alice 相同的方法,将数据进行发送,直到数据包正确发送至 Bob。若 Eve 接收到的数据报文的 Hash 值 $H_2(M) \neq H(M)$,则证明数据传输过程中出现差错或存在安全隐患,将该数据包直接丢弃。加密和验证的过程如图 2,3 所示。

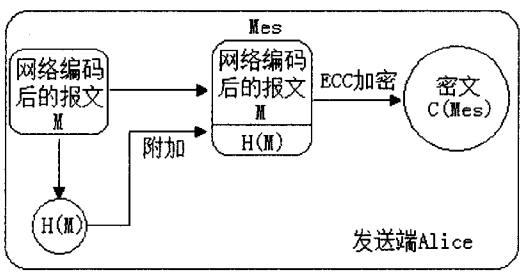


图 2　Alice 端数据加密发送

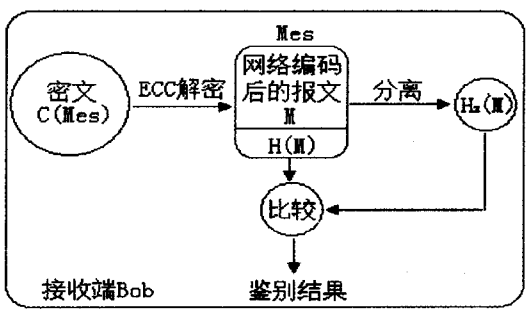


图 3　Bob 端数据接收验证

2.2　基于网络编码的 ECC 实现

1)Hash 值的计算与比较。

采用 MD5 算法计算 M 的 Hash 值,即 $H(M)=\mathrm{MD5}(M)$。

2)椭圆曲线域的参数。

实现基于 ECC 的加密和解密,必须首先确定椭圆曲线域并确定一条椭圆曲线。根据 IEEE P1363 标准[6],定义一个七元组:

$T=(q,F_R,a,b,G,n,h)$

其中,

q 表示某个素数幂即素数或 2^m;

F_R 为域的表示法,表示为含有 R 个元素的有限域;

当 q 为素数时,曲线的方程为:$y^2=x^3+ax+b$;

当 $q=2^m$ 时,方程为:$y^2+xy=x^3+ax^2+b$;

其中 a,b 为方程的系数;

G 为基点;

n 为大素数并且等于点 G 的阶;

h 是小整数称为余因子且 $h=\dfrac{\#E(F_q)}{n}$。

其中 n 为主要的安全参数,因此 ECC 密钥的长度为 n。

3)椭圆曲线密码的密钥。

选取基域 F_q 和椭圆曲线后,即可得到曲线 E 在有限域 F_q 的具体形式,即上述的椭圆曲线域参数的一个七元组。每个用户选取一个整数 $d(1\leqslant d\leqslant n-1)$ 作为其私钥,而以点 $Q=dG$ (G 为基点) 作其公钥,这样形成一个椭圆曲线公钥密码系统。在这个密码体制中,具体的曲线、基域、基点 G 及其阶 n,以及每个用户的公钥都是该系统的公开参数,每个用户的私钥是保密的。也就是说,对于 Eve 而言,其公开参数为:$E(F_q,G,n,Q_E)$。

4)WSN 中节点 ECC 密钥交换。

WSN 中节点 Eve 能够接收 Mallory 节点的相关信息。Eve 要向 Mallory 发送数据包前,需要两节点达成协议,提前将其公开参数 $E(F_q,G,n,Q_E)$ 告知 Mallory,同样 Mallory 也将其公开参数告知 Eve。

文中规定,当 Eve 得知 Mallory 信息后,称 Mallory 对于 Eve 是已知的。这种通信方式仅仅在有新节点加入且需要与新节点进行数据传输时,才会进行。当 Eve 与已知节点 Mallory 在数据传输过程中,不会进行二次密钥交换。

5)基于椭圆曲线密码体制的加解密。

WSN 中,Alice 将随机线性编码后的数据 M 和其 Hash 值 $H(M)$ 一起通过 Eve 发送给 Bob。文中将 M 与 $H(M)$ 合称为 Mes。Alice 须执行以下操作,见表 1。

表 1 Alice 对 Mes 加密

a	获取 Eve 的公开信息 $E(F_q, G, n, QE)$ 中的公钥
b	将 Mes 表示成一个 F_q 域中的元素，即 Mes $\in F_q$
c	在区间[1, $n-1$] 内选取一个随机数 k
d	计算点 $kG = (x1, y1)$
e	依据 Eve 的公钥 QE，计算点 $k\,QE = (x2, y2)$，若 $x2 = 0$，则返回 c)
f	计算 C = Mes × $x2$
g	将加密后的数据 $(x1, y1, C)$ 发送给 Eve

Eve 收到 Alice 的密文 (x_1, y_1, C) 后，解密步骤如表 2 所示。

表 2 Eve 对 Mes 解密

a	使用私钥 dE，计算点 $(x2, y2) = dE(x1, y1)$
b	计算 F_q 中的 $(x_2)^{-1}$
c	计算 $C(x_2)^{-1}$ 便可得明文 Mes，Mes = $C(x_2)^{-1}$

6) 验证消息完整性。

Eve 在收到 Mes 后进行如下操作，见表 3。

表 3 Eve 对 Mes 验证

a	将其拆分为 M 和 $H(M)$
b	计算 $H_2(M)$ = MD5(M)
c	若 $H_2(M) = H(M)$，则确认接收并转发数据；若 $H_2(M) \neq H(M)$，则直接丢弃

3 算法评估

当传送数据被窃听时，Bob 必须在 Alice 发送数据之前，先将公钥告知 Alice，Alice 再对编码后的数据用 Bob 的公钥进行再加密，发送即可。Carol 为了能窃听成功，必须要在获取到线性网络编码的系数和其相对应密文的同时，计算出 Bob 的私钥。此时 Carol 再试图窃听，对于采用一种安全的加密方案来说，是徒劳的。

当数据受到伪造和篡改这些攻击时，易想到采用源节点身份认证的方式是理所当然的，但是在数据传输时，经过网络编码，数据进行融合，源节点的身份验证有效信息会受到破坏。

因此文中提出在防止伪造和篡改这些攻击时，考虑到 WSN 节点能量受限，为了在有限的能量范围内传输更多有效的数据，采取节点加密验证的方式。因为适当增大其节点的计算量，远比大量传输受污染的信息更为节能。在传统方案中，数据传输时受到污染，只有到了接收端才能被发现。而点能量损耗、计算浪费，而这对于整个 WSN 是致命的。因此提前进行数据验证是更加有效的。

文中之所以选用 ECC 加密算法，而不是其他像等 RSA 算法。因为 ECC 的具有以下 4 个主要优点：密钥尺度小；参数选择比较灵活；具有由数学难题保证的安全性；实现速度较快。用国际上公认的对于 ECC 算法最有效的攻击方法--Pollard rho 方法去破译和攻击 ECC 算法，它的破译或求解难度基本上是指数级的。正是由于 RSA 算法和 ECC 算法这一明显不同，使得 ECC 算法的单位安全强度高于 RSA 算法，也就是说，要达到同样的安全强度，ECC 算法所需的密钥长度远比 RSA 算法低。将 ECC 加密算法与基于 WSN 的网络编码相结合大大提升了 WSN 的鲁棒性和容错性。

4 结束语

文中结合密码学中验证和签名概念，针对网络编码在无线传感器网络中应用时出现的三种典型的安全威胁，提出了一种基于 WSN 的椭圆曲线加密算法验证方案，大大增强了无线传感器网络节点之间通信的安全性。鉴于传感器网络能量受限，网络中的传感器由于电源能量的原因经常失效或废弃。传感器网络要利用有限的电源能量来处理和传输更多的有效信息。与此同时，经过数据加密后的 WSN 其鲁棒性和容错性也有大幅度的提升。

参考文献：

[1] 任丰原，黄海宁，林 闯. 无线传感器网络[J]. 软件学报，2003，14 (7)：1282-1291.

[2] Li S Y R，Yeung R W，Cai N. Linear network coding[J]. IEEE Trans. Info. Theory，2003，49(2)：371-381.

[3] Ahlswede R，Cai N，Li S Y R. et al，NetWork Information Flow [J]. IEEE Transaction on Information Theory，2000，46(4)：1204-1216.

[4] Ho T，Karger D，Medard M，et al. The benefits of coding over routing in a randomized setting[C]//IEEE International Symposium on Information Theory. Yokohama：[s. n.]，2003.

[5] Ho T，Medard M. On randomized network coding[C]//In：Proceeding of 41st Annual Allerton Conference on Communication Control and Computing. Monticello，IL：[s. n.]，2003.

[6] IEEE Standard Specifications for Public-Key Cryptography [S]. New York：[s. n.]，2000：146-147.

[7] Lun D S，Medard M，Effros M. On coding for reliable communication over packet networks[C]//Conference on Communications，Control and Computing. Allerton：[s. n.]，2004.

[8] 周业军，李 晖，马建峰. 一种防窃听的随机网络编码[J]. 西安电子科技大学学报(自然科学版)，2009，36(4)：696-701.

[9] 蒲保兴，杨路明，王伟平. 随机线性网络编码的一种差错控制方法[J]. 小型微型计算机系统，2009，30(6)：1108-1112.

[10] Cai N，Yeung R W. Secure network coding[C]//In International Symposium on Information Theory (ISIT). Lausanne，Switzerland：[s. n.]，2002.

(下转第 180 页)

```
var temp="";
for(var i=0;i<valueNum;i++){
    values[i]=($(":input:eq("+i+")").val());
    temp+=values[i];
}
var sql_post_inj=new Array("'",";"," ","--","or","and",
"not","select","updte","insert","drop","sp_","create",
"function","grant","revoke","union");//JSON 数据或 XML 可
以代替数组,直接用 $.getJSON()来获取数据更方便
var htmlbj="<div class='postcontain'>+"temp+"</div>"
$("body").append(htmlbj);
$(".postcontain").hide();
for(var i=0;i<sql_post_inj.length;i++){
if(($(".postcontain").html().indexOf(sql_post_inj[i].toString
(),0))>0){
$("form").remove();//破坏 DOM 的结构
$.sqlInject.sqlDialog("锁定","text:you are attrack my website",
"400","150","cssClassName");
break;}
}
}
};
```

在任何的网页中只要导入这个插件就能实现过滤敏感 SQL 语句实现防止 SQL 注入,同时锁定网页,为了保持页面的简洁性,可以让其保存为一个页面在其他的页面中通过 include 指令来包含该页面。导入的方法如下:

```
<script language="javascript" src="jquery-1.3.2.min.js"></
script>
<script language="javascript" src="jQuery.sqlInject.js"></script
>
<script language="javascript">
$(function(){
$.sqlInject.sqlPostInj();
$.sqlInject.sqlgetInj();
});
</script>
```

jquery-1.3.2.min.js 是 jQuery 类与对象的封装,jQuery.sqlInject.js 是本插件。插件两个全局函数可以任何需要防止 SQL 注入的事件处理中。

4 结束语

文中对 SQL 注入攻击的原理、方法进行了阐述,提出了从客服端解决 SQL 注入攻击的方案,同时利用插件可扩展接口使用者只要提出自己的处理方案(或利用本插件处理方案)就能方便的把插件效果改变,但其实质是不变的,提出了 SQL 注入攻击的一种开放性解决方案,无论动态网页采用那种语言只要导入本插件就能实现保护。伴随 EXTJS 的发展,可以利用 js 的线程技术(TaskRunnner)和集合来改装本插件使其更趋轻便灵活。

参考文献:

[1] 张 楠.基于规则的检测 SQL 注入攻击方法的研究[J].陕西科技大学学报,2007,25(2):121-123.

[2] 钱林红.部分加密防御 SQL 注入攻击[J].中国科技信息,2008(24):101-102.

[3] 崔学冰. 基于 URL 重写技术的 SQL 注入攻击防御方法[J]. 河南城建学院学报,2009,18(3):63-69.

[4] 田 鼎.病毒与黑客攻防[M].北京:清华大学出版社,2006:198-203.

[5] 曾 顺. 精通 jQuery+javascript[M]. 北京:人民邮电出版社,2009:373-389.

[6] SQL Server 安全回顾[EB/OL]. 2004. http://www.microsoft.com/china/ctc/Newsletter/04/ctc2.htm.

[7] Anley C. Advanced SQL injection in SQL server applications [EB/OL]. 2002. http://www.creangel.com/papers/advanced_sql_injection.pdf. An NGS Software Insight Security Research(NISR) Publication.

[8] 陈小兵,张汉煜,骆力明. SQL 注入攻击及其防范检测技术研究[J]. 计算机工程与应用,2007(11):150-152.

[9] Sam M S. NG,SQLBlock:SQL injection protection by variable nor-malization of SQL statement [EB/OL]. 2010. http://www.iem.pw.edu.pl/~kozlowk3/biblioteczka/www_SQL/SQL_Injection_Protection_by_Variable_Normalization_of_SQL_Statement.pdf.

[10] 徐 陋,姚国祥. SQL 注入攻击全面预防办法及其应用[J]. 微计算机信息,2006(9):18-20.

[11] Finnigan P. SQL injection and Oracle[EB/OL]. 2002-11-21. http://www.oracledeveloper.nl/newforum/files/2002_11_21%20SecurityFocus%20SQL%20Injection%20and%20Oracle.pdf.

[12] Cerrudo C. Manipulating Microsoft SQL server using SQL injection[EB/OL]. 2010. http://injection.rulezz.ru/Manipulating_SQL_Server_Using_SQL_Injection.pdf.

(上接第 176 页)

[11] Krohn M, FreedMan M, Mazieres D. On-the-Fly Verification of Rateless Erasure Codes for Efficient Content Distribution [C]//IEEE Symposium on Security and Privacy. Berkeley, CA:[s.n.], 2004.

[12] Bhattad K, Nayayanan K P. Weakly secure network coding [C]//In:Proc. First Workshop on Network Coding, Theory, and Applications (NetCod). Hanover, USA:[s.n.],2005.

[13] Ho T, Leong B, Koetter R, et al. Byzantine modification detection in multicast networks using randomized network coding [C]//In International symposium on Information Theory (ISIT). Chicago, USA:[s.n.],2004.