基于 CRC 的防污染网络编码方案①

周赵斌, 许 力, 李世唐

(福建师范大学 福建省网络安全与密码技术重点实验室, 福州 350007)

摘 要: 网络编码的直接应用容易遭受污染攻击, 我们针对这一安全性问题, 给出了一种基于 CRC 校验码的防污染网络编码方案. 该方案首先通过引入快速的并行 CRC 校验码和消息时间戳的设计理念, 然后结合具有同态性质的RSA签名算法, 来确保校验码和时间戳的安全. 从该方案的安全性方面和效率方面进行分析表明: 网络编码、并行逆序 CRC 检验码和消息时间戳三者的结合可以有效地抵抗污染攻击和重放攻击, 并且大大地降低节点的计算代价, 提高了网络的吞吐量.

关键词: 网络编码; 污染攻击; 并行 CRC 校验码; 时间戳

Pollution-Resistant Network Coding Based on CRC

ZHOU Zhao-Bin, XU Li, LI Shi-Tang

(Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: The direct application of network coding is vulnerable to pollution attack. In order to solve this security problem, we propose a network coding scheme to prevent it from pollution based on CRC check code. First, this protocol employs a fast parallel CRC check code and message timestamp to effectively resist pollution attack and replay attack. Secondly, by combining with the homomorphic properties of RSA signature algorithm, we ensure the security of CRC and timestamp. Security analysis and efficiency analysis show that applying network coding, parallel CRC check code and message timestamp together can greatly reduce the computational cost of the node and improve the network throughput.

Key words: network coding; pollution attacks; parallel CRC check code; timestamp

1 绪论

自 2000 年网络编码[1]被提出以来, 因为其允许中间节点对上游节点发送的消息数据流进行编码组合, 所以它彻底地改变了传统网络存储转发的数据通信方式, 成为 21 世纪信息通信领域的巨大突破之一, 极大地提高了组播通信网络的吞吐量和鲁棒性. 但是不可避免地, 网络编码作为一种新的安全数据传输方式, 却容易遭受污染攻击.

恶意节点的数据篡改和信道噪声是通信网络中数据污染的两大来源. 近年来, 针对恶意节点发起的污染攻击, 研究人员提出了许多的安全解决方案. Krohn 等人[2]基于同态 hash 函数的机制, 提出了一种抵抗网络编码污染攻击的方案. Kehdi 等人[3]主要利用网络编码的零空间来实现认证, 克服了 Krohn 等人方案中计算复杂度较大的缺点. Yu 等人[4]提出的基于数字签名的方法, 要求为每一个新文件分发新的公共密钥, 并且密钥的大小与文件大小成线性关系, 这一要求同样限制了其在大容量文件分发系统中的使用. Yu 等人[5]又利用对称密码的方法, 采取不同于哈希和数字签名的方法, 但带宽消耗大的问题依旧存在. 但是 Yun 等人[6]已经证明了 Yu 等人的方案不具有同态性质, 其网络安全性很弱. Liu 等人[7]利用一个动态的公钥密码技术, 提出了一种能抵抗污染攻击的同态签名网络编码方案, 该方案可以快速地为每个数据包生成签名消息

① 基金项目:国家自然科学基金(61072080);福建省高校产学合作科技重大项目(2011H6008);福建省 2013 年战略性新兴产业技术开发项目(闽发改高技[2013]266 号)

收稿时间:2015-04-10;收到修改稿时间:2015-06-03

对, 大大地减少了通信开销. Liu 等人[8]基于消息认证码(MAC)提出了一种检测网络编码污染攻击方案, 该方案通过在节点处引入身份认证系统来检测污染攻击, 仿真表明, 该方案具有较高的检测效率和较低的计算复杂度(包括身份验证信息的生成和验证), 有效地节省了计算开销. 因此, 对于资源受限的无线网络, 其更具有优势. Zhang 等人[9]结合同态消息认证码和同态签名设计出了一种混合加密方案, 周赵斌等人[10]提出一种抗窃听和污染攻击的网络编码方案, 该方案通过对数据进行编码, 使得对信道进行窃听的敌手无法得到原始数据信息, 进而有效地抵抗了窃听攻击, 并且利用列表译码算法有效地抵抗污染攻击.

目前基于数字签名的方案在抵抗污染攻击中得到了较好的应用, 虽然在安全性方面得到了有效地增强, 但是对于整个网络依旧存在计算代价和带宽消耗较大这两个主要的问题[11]. 随着智能终端设备朝着小型化的方向发展与普及, 人们不仅关心其安全性问题, 也会关心设备的通信计算代价. 对于无线网络中的节点来说, 由于其本身较小的体积原因, 所以无线网络存在着许多资源上的限制, 如计算能力有限、存储空间有限、通信的带宽有限和电池的容量等限制. 这些限制无不给无线网络的发展带来了阻碍, 为了无线网络有更好的发展和应用前景, 所以未来的重点研究将是如何降低计算代价, 提高节点的计算效率[12]. 梁海华等人[13]提出了一种并行 CRC 逆序校验方法, 该方案通过调整节点的移位寄存器初始状态能够提高 CRC 编码信道传输的安全性, 并且计算量较小和计算速度快. 本文提出了一种基于 CRC 的防污染网络编码设计方案, 源节点通过快速的 CRC 逆序校验方法生成消息校验码并使用数字签名技术对检验码进行加密, 目的节点解码组合数据包后通过校验码验证传输数据是否被篡改, 解决了网络编码的安全性. 又因为该方案具有计算快速的优点, 所以可有效地减小网络编码的同步问题对网络造成的影响.

2　预备知识

2.1　循环冗余校验码(CRC)的基本原理

循环冗余码检验(CRC, Cyclic Redundancy Check)技术自提出以来, 就被作为一种特殊的线性分组编码, 广泛地应用于计算机的数据通信和数据压缩等相关领域. CRC 计算是通过专用的硬件(如移位寄存器)来实现编译码, 且可以在通信过程中以较低的计算和通信花销提供可靠无差错的信息数据传输[14].

CRC 校验码的具体实现过程为: 假设发送的原始数据块用二进制多项式 $P(x)$ 表示, 大小为 k 位.

发送方编码方法: 将 $P(x)$ 二进制码序列左移 r 位, 得到 $P(x)\times x^r$, 然后除以 $G(x)$, 得到余式 $R(x)$, 即检验码. 用公式表示为 $T(x)=P(x)\times x^r+R(x)$.

接收方解码方法: 将 $T(x)$ 除以 $G(x)$, 得到的余数就是校验码, 如果得到余数是零, 则说明通信过程中数据传输正确, 否则说明数据传输不正确.

如果得到余数是零, 则说明通信过程中数据传输正确, 否则说明数据传输不正确.

图 1 为网络节点的寄存器中串行 CRC 编码过程示意图, 图 2 为网络节点的寄存器中串行 CRC 解码过程示意图, 其中这两个过程当中的移位寄存器中的初始状态都是零状态.

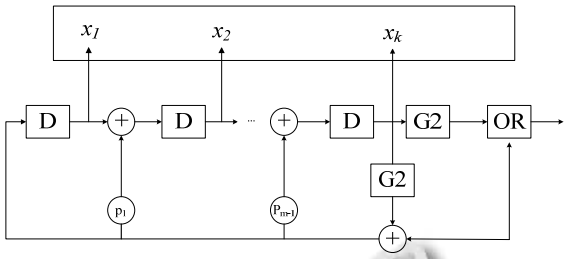

图 1　串行结构编码过程

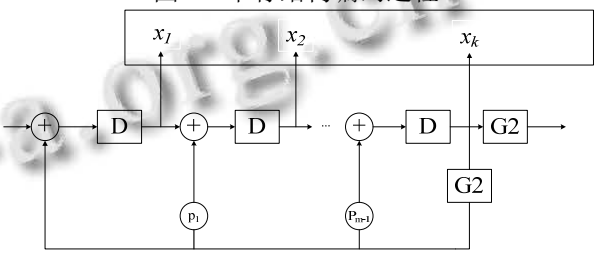

图 2　串行结构解码过程

目前基于上述原理实现的编解码器被广泛地应用, 文献[13]指出这种先进先出(First In First Out, FIFO)正序处理方式的 CRC 解码器存在一定的局限性, 该解码器虽然可以实现节点零初态的检验, 但无法在初始状态为非零态的环境下工作. 图 3 为 CRC 校验码的计算流程图.

2.2　系统模型

源和多源是目前主要的两种网络编码模型. 只有一个发送源节点的网络模型称之为单源模型, 有多个

发送源节点的称之为多源模型. 在本方案中我们设定的网络模型是单源多播. 我们用一个有向非循环的图 $G=(V,E)$ 表示, 其中 V 表示网络中节点集合, E 表示网络中边的集合. 其中 V={S, 1, 2, ...,8, t_1,...t_k}, E={e(S, 1),e(S, 2),e(S, 3),e(1, 5),e(2, 6,e(3,4),e(5, 7),e(6, 8),e(4, 8),..,e(7, t_1),...,e(8, t_k)}.

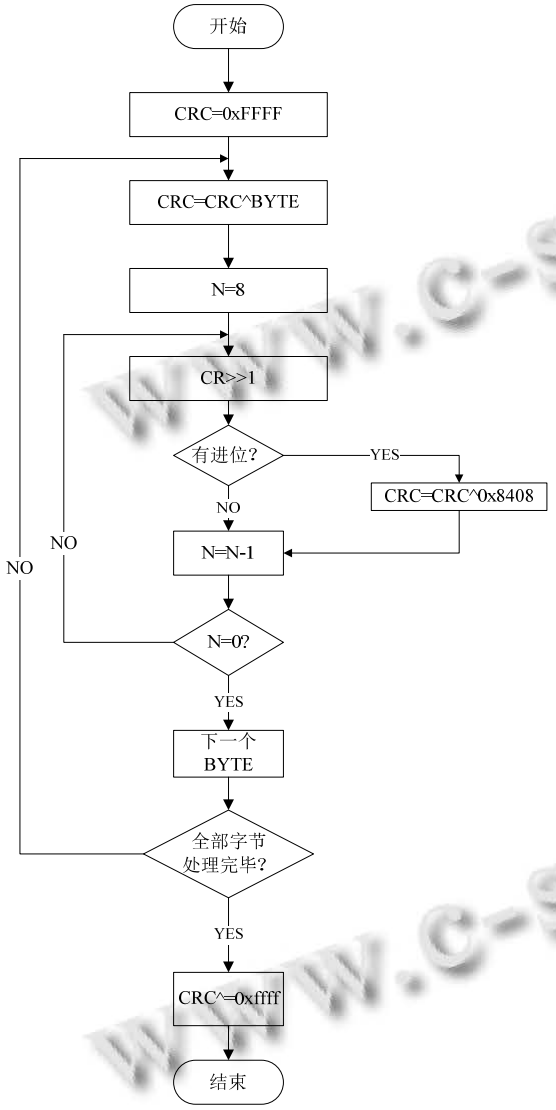

图 3 CRC 校验码的计算流程图

在本网络中, 系统模型如图 4 所示, 源节点 S 通过中间节点(模型中的节点 1, …, 8)同时发送 n 个消息 M_1, …, M_n 到目的节点 t1, …, t_k . 首先, 网络中的所有节点都具有线性网络编解码特性; 其次, 每个节点增加一个移位寄存器, 并调整其工作初始状态, 增强节点 CRC 编码信道传输的安全性.

3 基于并行CRC逆序校验的防污染攻击网络编码方案

3.1 串行的 CRC 逆序校验

串行的 CRC 逆序校验作为一种常用的数据校验方法, 能够对任意初始状态的 CRC 校验码进行数据判断, 但是随着网络的高速发展, 用户之间传输的数据量越来越大, 如何快速地检验数据在传输过程当中是否发生错误或者被敌手修改, 是我们目前急需解决的问题. 文献[14]通过在移位寄存器中预补零操作, 提出了一种的并行 CRC 正序校验(FIFO)算法, 但存在着处理的数据位宽较小的缺点, 数据的校验运算速度较慢. 针对节点对数据校验运算速度的问题, 梁海华等人基于串行算法, 提出了一种快速的并行 CRC 逆序校验算法[15]. 文献[15]与文献[16]中的处理算法对比, 其无须额外的通过对移位寄存器预补零操作就可以使得输入处理数据位宽几倍于并行处理位宽, 大大地简化了计算流程, 提高了节点的数据校验运算速度.

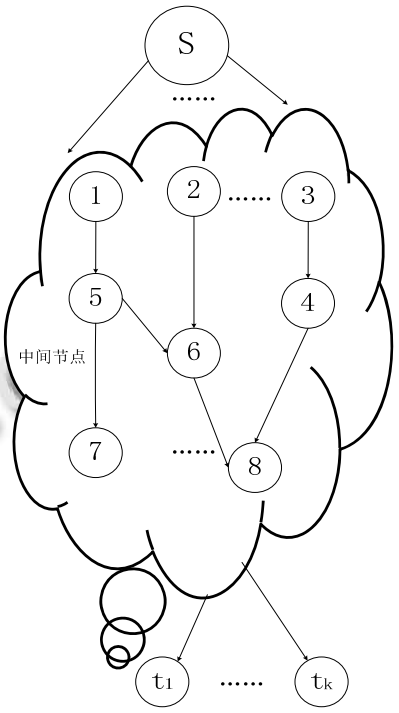

图 4 基于网络编码的多播网络模型

3.2 防污染攻击网络编码方案

将源节点发送的消息 F 按顺序分割为 m 个向量 $x_1,x_2,...,x_m \in F_q^n$, $x_i=(x_{i1},x_{i2},...,x_{in})$, F_q 是一个包含 q 元素的有限域, m, n, q 是预先设置的系统参数. 为了原始消息的安全性, 源节点在传播之前首先

必须对这些向量 x_i 进行编码，$i=1,2,...,m$. 为了便于信宿节点对编码消息解码并恢复出原始消息，更好地解决重放攻击，本方案在线性网络编码的基础上，引入消息时间戳和密钥预分配设计.

首先，网络中的各节点从密钥池 P 随机选择一个密钥并预存储在节点的存储器，分别记为 k_{id}，id 是节点的标识符；之后由可信中继节点 R 从密钥池 P 里面随机选取一个簇密钥 k_G，其中 $k_{id},k_G\in P$，节点 R 计算 $k_{id}\oplus k_G$，分别广播出去；节点 i 收到后各自计算 $k_{id}\oplus k_{id}\oplus k_G$. 各节点得到簇密钥 k_G 后对消息数据组合中生成的 CRC 校验码和添加的消息时间戳两部分进行加密处理.

同态 RSA 密码算法原理:

假设 (N,e) 和 (N,d) 分别是 RSA 的公钥和私钥，明文消息为 m，密文消息为 c，加密过程为 $c\equiv m^e(\bmod N)$，解密过程为 $m\equiv c^d(\bmod N)$.

对于明文消息 x 和 y 加密可分别得到，$E_e(x)=x^e(\bmod N)$ 和 $E_e(y)=y^e(\bmod N)$.

由于
$$\begin{aligned}E_e(x\cdot y)&=(x\times y)^e \bmod N\\&=(x^e(\bmod N))\times(y^e(\bmod N))\\&=E_e(x)\times E_e(y)\end{aligned},$$

所以 RSA 公钥密码算法满足乘法同态性质.

具体步骤如下:

1) 首先假设二进制多项式 $P(x)$ 的最高次幂是 k 位，由低到高的系数为 $(p_0,p_1,...,p_{k-1},1)$. 之后源节点生成 m 个扩展消息向量，把该条消息的时间戳信息 T_i 转换为属于 F_q^n 值域中的数值，并附在数据包结尾处，最后对 m 条扩展消息进行 CRC 编码处理，得到 CRC 校验码并使用簇密钥进行加密，为了便于下游节点解码，加密方式选择具有同态性的 RSA 算法.

2) 中间节点对收到的组合数据中的 CRC 校验码做解密处理，判断数据是否被篡改. 若被篡改就丢弃该数据，向上游节点发送一个信号，要求重新传输，直到数据安全正确地传输到该中间节点. 若传输过程当中未发生数据篡改或者传输错误情况，节点重新对数据进行 CRC 编码和加密处理，然后发送到下游节点.

3) 目的节点收到上游节点发送的消息，对数据进行线性解码，然后根据收到的二进制数据串，生成 CRC 校验码，最后与解密出的 CRC 校验码对比，判断数据是否被篡改. 如果签名验证通过，则节点接收消息签名对；如果验证失败，则拒绝接收.

3.3 基于并行CRC逆序校验的防污染攻击网络编码方案过程

CRC 逆序校验计算过程图，如图 5 所示，其中 $p_kx^k+p_{k-1}x^{k-1}+\cdots+p_1x^1+p_0$，$p_0=1,p_k=1$.

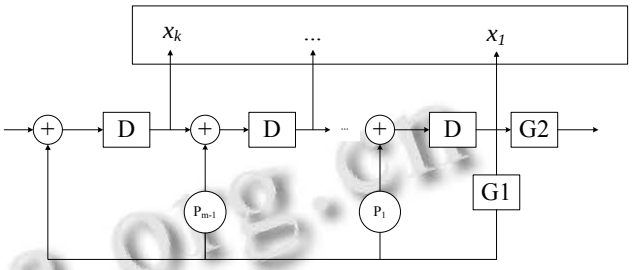

图 5　后进先出串行解码过程

假设寄存器 i 在 t 时刻的状态为 $x_i(t)$，$x(t)=\left[x_k(t),x_{k-1}(t),\cdots,x_1(t)\right]^T$，$M=\left[m(t)\quad 0\quad\cdots\quad 0\quad 0\right]^T$，

$$A=\begin{bmatrix}p_{k-1}&1&0&\cdots&0\\p_{k-2}&0&1&\cdots&0\\\vdots&\vdots&\vdots&\cdots&\vdots\\p_1&0&0&\cdots&1\\p_0&0&0&\cdots&0\end{bmatrix}$$

通过多矩阵 A 进行逆变换，可得 A 的逆矩阵

$$A^{-1}=\begin{bmatrix}0&\cdots&0&0&1\\1&\cdots&0&0&p_{k-1}\\\vdots&\vdots&\vdots&\cdots&\vdots\\0&\cdots&1&0&p_2\\0&\cdots&0&1&p_1\end{bmatrix}.$$

图 1 所示的串行结构编码算法过程:

$$x(t+1)=\begin{bmatrix}x_k(t+1)\\x_{k-1}(t+1)\\\vdots\\x_2(t+1)\\x_1(t+1)\end{bmatrix}$$

$$=\begin{bmatrix}p_{k-1}&1&0&\cdots&0\\p_{k-2}&0&1&\cdots&0\\\vdots&\vdots&\vdots&\cdots&\vdots\\p_1&0&0&\cdots&1\\p_0&0&0&\cdots&0\end{bmatrix}\otimes\begin{bmatrix}x_k(t)\\x_{k-1}(t)\\\vdots\\x_2(t)\\x_1(t)\end{bmatrix}\oplus\begin{bmatrix}m(t)\\0\\\vdots\\0\\0\end{bmatrix}\quad(1)$$

即 $x(t+1)=A\otimes x(t)\oplus M$，由公式(1)可计算

$x(t)=A^{-1}\otimes x(t+1)\oplus M$.

假设 $x(t)$ 的逆序 $x'(t)=\left[x_1(t),x_2(t),\cdots x_{k-1}(t),x_k(t)\right]^T$，$M$ 逆序为 M'，即 $M'=\left[0\quad 0\quad \cdots\quad 0\quad m(t)\right]^T$，

令 $B=\begin{bmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ p_{k-1} & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$

则: $x_k(t)=\begin{bmatrix} x_1(t) \\ x_2(t) \\ \vdots \\ x_{k-1}(t) \\ x_k(t) \end{bmatrix}$

$$=\begin{bmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ p_{m-1} & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}\otimes\begin{bmatrix} x_1(t+1) \\ x_2(t+1) \\ \vdots \\ x_{k-1}(t+1) \\ x_k(t+1) \end{bmatrix}\oplus\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ m(t) \end{bmatrix} \quad (2)$$

即 $x'(t)=B\otimes x'(t+1)\oplus M'$.

由上可知, 在节点编码寄存器的 t 时刻, 二进制码 $m(t)$ 生成的 CRC 校验码序列为 $x(t+1)$，由 $x(t+1)$ 可知其逆序为 $x'(t+1)$，然后通过公式(2)可以计算 $x'(t)$. 节点通过对比 $x(t)$ 的逆序与 $x'(t)$，若相同, 则信息序列 $m(t)$ 没有被篡改, 否则发生信息的篡改.

4 性能分析

4.1 安全性分析

4.1.1 抵抗污染攻击

C 逆序校验码和消息时间戳的安全性，而校验码在源节点处和中间节点处生成. 本方案同样假设源节点是可信任的，也就是说攻击者不可能在源节点处发起污染攻击，但是数据的污染可能会发生在传输过程当中，如信道噪声干扰. 其次对于中间节点来说，攻击者可以捕获网络中的任何节点并利用它发起攻击. 例如敌手可以利用该节点发送污染的数据或者伪造加密的 CRC 校验码并传输至下一个节点，但是它通过加密的 CRC 校验码来计算签名私钥是困难的，因为 $y=g^{-x}(\mathrm{mod}\ p)$，攻击者想通过该等式解出签名所使用的私钥 x 相当于解离散对数问题.

4.1.2 抵抗重放攻击

由于信源节点在发送的信息尾端添加了消息时间戳，中间节点和信宿节点可以通过组合信息中的消息时间戳来判断该消息数据是否被重放，若节点判断为重放消息则丢弃.

本方案定义的重放攻击有两种攻击模型: 1. 敌手通过捕获到的信息直接转发至下一节点; 2. 节点首先从捕获的消息组合提取里面的消息时间戳, 然后篡改该时间戳, 生成一个新的时间戳签名. 针对第一种重放攻击, 通过对比节点接收到的 k 条消息组合是否在给定的 Δt 时间内, 就可以判断是否存在重放攻击. Δt 是关于 v, c, d 三个变量的一个函数，即 $\Delta t=f(v,c,d)$，其中 v 表示网络中链路的传输速率, c 为节点编码(coding)时间, d 为节点解码(decoding)时间. 如果当前时刻信息 t_2 与消息组合中的时间信息 t_1 的差值小于 Δt，即 $|t_2-t_1|\le\Delta t$，那么该节点就对该组合信息进行解码处理. 若 $|t_2-t_1|>\Delta t$，则定义为重放攻击. 针对第二种重放攻击, 虽然敌手可以通过被捕获节点的簇密钥, 生成一个新的恶意签名信息, 但是由于源信息的消息签名对是对整个原始消息进行的签名操作, 而敌手只能得到链路上的部分信息, 所以敌手无法通过部分源信息生成一个完整有效的签名. 综上所述, 本方案可抵抗重放攻击者, 即原始组合信息中的 CRC 和消息时间戳的签名是安全的.

4.2 效率分析

由于本方案中的运算只涉及到了模指数运算和乘法运算并没有使用线性对运算, 移位寄存器中的并行 CRC 检验码生成的代价基本可以忽略, 因此根据运算的相似性, 可与文献[4]中 Yu 等人的 RSA 签名方案和文献[10]的 SCH 签名方案对比. 设 Tme 为模指数运算所需时间, Tmul 为乘法运算所需时间. 表 1 中对比模指数运算, 表 2 中对比乘法运算. 从表 1 和表 2 可以看出, 本文方案在效率上远远优于文献[4][10]. 而且本文考虑到了节点发送的消息的篡改问题, 采取了的加密防范措施, 确保了消息组合中的 CRC 校验码和消息时间戳的安全性, 有效地抵御了污染攻击. 同时因为在本文中引入了消息时间戳的设计理念, 节点可根据消息的时间信息戳, 判断消息是否被重放, 有效地抵抗了重放攻击.

表 1 模指数运算时间对比

方案	签名	验证
Yu 等人	(m+n+1)T_{me}	(m+2)T_{me}
SCH NC	(m+n)T_{me}	(m+2)T_{me}
CRC NC	(m+1)T_{me}	(m+1)T_{me}

表 2 乘法时间运算对比

方案	签名	验证
Yu 等人	(m+n)T_{mul}	(m+2)T_{mul}
SCH NC	(m+n)T_{mul}	(m+1)T_{mul}
CRC NC	(m+1)T_{mul}	(m+1)T_{mul}

5 小结

随着网络编码更加深入地研究与快速地发展, 污染攻击这个安全问题越来越引起网络编码研究者的关注, 本文针对这个问题设计出一种基于并行 CRC 校验码的防污染网络编码方案. 该方案中节点对接收消息组合采用快速地逆序校验算法解码, 能有效地降低节点数据编解码的延迟性, 并且其在抵抗污染攻击的同时, 还能有效地抵抗重放攻击. 但该方案需要在节点布置之前需要预存储一个在密钥池中的私钥, 可信的第三方再从密钥池中选取该节点的私钥和簇密钥做异或操作, 以便该节点能拥有一个签名的簇密钥, 增加了网络节点布置的难度. 同时, 由于该方案主要考虑抗污染和重放攻击, 对抗窃听攻击考虑较少, 所以在应用网络编码的无线网络中, 该方案无法抵抗窃听攻击.

参考文献

1 Ahlswede R, Cai N, Li SYR, et al. Network information flow. IEEE Trans. on Information Theory, 2000, 46(4): 1204–1216.

2 Krohn MN, Freedman MJ, Mazieres D. On-the-fly verification of rateless erasure codes for efficient content distribution. Proc. 2004 IEEE Symposium on Security and Privacy. IEEE. 2004. 226–240.

3 蒋铭勋,崔巍.随机线性网络编码污染数据的检测分析.Computer Engineering,2010,36(24):107–109.

4 Yu Z, Wei Y, Ramkumar B, et al. An efficient signature-based scheme for securing network coding against pollution attacks. Proc. of the 27th IEEE Conference on Computer Communications (INFOCOM). Phoenix, AZ, US. IEEE Press. April 13-18, 2008. 1409–1417.

5 Yu Z, Wei Y, Ramkumar B, et al. An efficient scheme for securing XOR network coding against pollution attacks. Proc. of IEEE INFOCOM. Rio de Janeiro, Brazil. IEEE Press. April 19-25, 2009. 406–414.

6 Yun A, Cheon JH, Kim Y. Brief contributions on homomorphic signatures for network coding. IEEE Trans. on Computers, 2010, 59(9): 1295–1296.

7 Liu GJ, Wang B. Secure network coding against Intra/Inter-generation pollution attacks. China Communications, 2013, 10(8): 100–110.

8 Liu J, Liu C, Liu H, et al. Pollution resistance network coding research for Ad hoc network. Proc. of International Conference on Computer Science and Information Technology. Springer India. 2014. 261–268.

9 Zhang P, Jiang Y, Lin C, et al. Padding for orthogonality: efficient subspace authentication for network coding. Proc. of IEEE INFOCOM. Shanghai, China. IEEE Press. April 10-15, 2011. 1026–1034.

10 周赵斌,许力,李世唐,罗晓晴.一种抗窃听和污染攻击的网络编码方案.福建师范大学学报(自然科学版),2014,30(2):41–48.

11 刘外喜,余顺争,蔡君.安全的网络编码所面临的挑战和对策.计算机科学,2011,38(6):20–27.

12 严鸣,汪卫,施伯乐.无线传感器网络中关键节点的节能问题.计算机应用与软件,2007,24(6):129–131.

13 梁海华,盘丽娜.快速 CRC 逆序校验方法.计算机应用,2013,33(7):1833–1835.

14 吕晓敏.嵌套循环冗余码(CRC)的优化与检验[硕士学位论文].杭州:浙江大学,2012.

15 梁海华,盘丽娜,赵秀兰,李克清.CRC 查询表及其并行矩阵生成方法.计算机科学,2012,39(B06):154–158.

16 李双喜.快速循环冗余校验编码方法及装置:中国,2009l0085524.4. 2010–12-01.