在无线双向通信中基于 CRC-NC 抵抗污染攻击方案

罗晓晴[1,2] 李世唐[1,2] 许 力[1,2]
(1. 福建师范大学数学与计算机科学学院，福州 350007；2. 福建省网络安全与密码技术重点实验室，福州 350007)

摘 要： 本文提出一种在无线双向通信中基于 CRC-NC（Cyclic Redundancy Check-Network Coding）抵抗污染攻击方案。在无线双向通信网络中，该方案通过结合网络编码和循环冗余校验码技术，对接收到的消息进行可信度检测，有效地降低目的节点解码差错概率，并抵抗污染攻击。该方案中节点 A 与节点 B 在中继节点的辅助下相互发送消息，并利用对方节点和中继节点发送的消息解码。若节点直接从对方节点获得的消息中有 S 个消息正确，该节点将对方节点发送的消息和中继节点发送的消息进行组合，并计算组合消息的汉明重量，从中选择 $K-S$ 个最小的汉明重量所对应的由中继节点发送的消息解码。通过仿真结果表明，与基于随机选取方案和加密方案相比，该方案能有效的降低节点解码差错概率。

关键词： 网络编码；污染攻击；循环冗余校验编码；汉明重量
中图分类号： TP393.08 **文献标识码：** A **文章编号：** 1003-0530(2014)11-1357-06

A CRC-NC Scheme Against Pollution Attack in Wireless Two-Way Communication

LUO Xiao-qing[1,2] LI Shi-tang[1,2] XU Li[1,2]
(1. School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China;
2. Fujian Provincial key Lab of Network Security and Cryptology, Fuzhou 350007, China)

Abstract: We propose a CRC-NC(Cyclic Redundancy Check-Network Coding) scheme against pollution attack that exploit network coding and cyclic redundancy check code approach to detect the trustworthiness of the packets and decrease the probability of decoding error in the presence of pollution attack in the wireless two-way communication. In this paper, two nodes send packets to each other with the assistance of a relay node, and one node decoding packets which received from the other node and the relay. If S packets are correctly received from the other node directly, then $K-S$ packets for which the Hamming weight are smallest are selected from all combination packets' Hamming weight for decoding. We show that the CRC-NC scheme provides a significantly lower probability of decoding error than the random selection scheme and cryptographic scheme that require computational and bandwidth overheads.

Key words: network coding; pollution attacks; cyclic redundancy check code; Hamming weight

1 引言

Ahlswede[1]等人于 2000 年提出了网络编码概念，并指出网络编码可以提高网络吞吐量，增强网络鲁棒性和可靠性。但是，由于网络编码允许中间节点参与编译码，因此可能会发生恶意中间节点添加垃圾消息或破坏消息，从而污染整个网络，导致目的节点无法正确译码[2-3]。为了提高网络通信的安全性，有效地阻止污染攻击，越来越多的人采用加密、签名或认证编码与网络编码相结合的方法来解决污染攻击问题。Yu 等人[4]提出一种基于签名技术有效抵抗污染攻击的网络编码方案。Oggier 在文章[5]中提出利用认证编码与网络编码相结合生成标签的方法抵抗污染攻击。随着无线通信的广泛应用，由于其广播的特性，敌手可以很容易获得通信内容，因此如何提高无线通信的安全性成为如今最急需解决的问题。而与网络编码相比，物理层网络编码可以提高百分之五十的吞吐率[6-7]。因此，近来越来越多的研究人员利用物理层网络编码的方法解决无线网络通信的安全性问题。Yoon 等

收稿日期：2014-06-18；修回日期：2014-09-30
基金项目：福建省自然科学基金项目(2013J01222)；福建师范大学“网络与信息安全关键理论和技术”校创新团队(IRTL1207)

人[8]提出一种在双跳中继网络中,利用物理层的信息检测编码数据包的可信度,降低解码错误率的方案。为了使目的节点检测出接收到的消息是否经过恶意篡改,Kim 等人[9]提出一种数据恢复的方案,利用物理层的信息,将污染的数据恢复从而正确译码。Jasper 等人[10]提出一种利用随机存取和物理层网络编码相结合的方法,恢复原始数据。

本文提出一种 CRC-NC (Cyclic Redundancy Check-Network Coding)抵抗污染攻击方案,即在无线双向通信网络中利用网络编码和循环冗余校验编码技术检测消息的可信度,抵抗污染攻击。节点 A 与节点 B 在中继节点的帮助下互相传送消息,若其中一个节点直接从对方节点获得的消息中有 S 个消息正确,该节点计算由中继节点发送的消息和对方节点发送的消息的线性组合消息的汉明重量,并从中选择 $K-S$ 个最小的汉明重量所对应的由中继节点发送的消息解码。通过仿真结果表明,与基于随机选择接收到的消息解码而不计算组合消息的汉明重量的方案或传统的加密方案相比,该方案能有效的降低译码错误率。

2 系统模型与攻击模型

2.1 系统模型

考虑图 1 所示的无线双向通信模型,节点 A 与节点 B 在中继节点 R 的辅助下,将文件$\vec{a}$与文件$\vec{b}$发送给对方节点。其中,文件$\vec{a}$与文件$\vec{b}$由 K 个矢量$\vec{a}=[a_1,a_2,\cdots,a_K]^{\mathrm{T}}$,$\vec{b}=[b_1,b_2,\cdots,b_K]^{\mathrm{T}}$ 组成,且 $a_i=(a_{i,1},a_{i,2},\cdots,a_{i,N})$,$b_i=(b_{i,1},b_{i,2},\cdots,b_{i,N})$,$i=1,2,\ldots,K$,T 为转置运算符。

2.2 攻击模型

在无线网络中,敌手可以通过窃听或捕获节点获得消息,并向网络中添加恶意消息污染整个网络,造成节点无法正确译码。本文考虑在通信过程中,敌手能捕获中继节点,并且当中继节点发送消息时,敌手可以某个概率向将要发送的消息中添加垃圾消息,造成污染攻击。而节点 A 与中继节点之间,节点 B 与中继节点之间的通信过程敌手不加以干涉,即节点 A 与中继节点之间,节点 B 与中继节点之间的通信是无噪声的。节点 A 与节点 B 在对方发送消息时可以接收到对方发送的消息,但节点 A 与节点 B 之间的通信存在噪声。

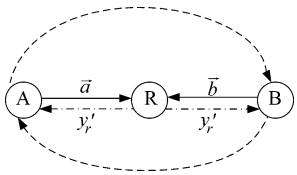

图 1 系统模型

Fig. 1 System model

3 CRC-NC 方案

本文提出一种 CRC-NC 方案,即在无线双向通信网络中,节点 A 与节点 B 在中继节点的辅助下利用网络编码与循环冗余校验码相结合的技术来抵抗污染攻击的方案。

第一步,节点 A 与节点 B 将文件$\vec{a}$与文件$\vec{b}$发送给中继节点。中继节点接收到消息后随机选取编码系数对消息编码,编码后的消息为:

$$y_r=\sum_{i=1}^{K}\alpha_{i,r}a_i+\sum_{i=1}^{K}\beta_{i,r}b_i,\ r=1,2,\ldots,K$$

其中编码系数 $\alpha_{i,r},\beta_{i,r}\in GF(q)$,$i=1,2,\ldots,K$,$GF(q)$是一个有限域。Médard 等人[10]提出,当 $GF(q)$足够大,节点采用随机网络编码得到的任意 K 个编码数据包都能以较高概率解码成功,即节点可以以高概率解码中继节点发送的消息。本文的所有操作都是在有限域 $GF(q)$上进行。

在无线通信中,当节点 A 将文件$\vec{a}$发送出去时,节点 B 可以收听到消息:

$$y_{b_i}=a_i+e_{sa_i},\ i=1,2,\ldots,K$$

其中 $e_{sa_i}=(e_{sa_i,1},e_{sa_i,2},\ldots,e_{sa_i,N})$表示节点 A 将消息发送给节点 B 时的信道噪声。假设,节点 A 与节点 B 之间的信道是 q 维对称信道且交叉概率为 p_s,则

$$P(e_{sa_i,n}=j)=\begin{cases}1-p_s, & j=0\\ \dfrac{p_s}{(q-1)}, & j=1,2,\ldots,q-1\end{cases}$$

同理,当节点 B 将文件$\vec{b}$发送出去时,节点 A 可以收听到消息:

$$y_{a_i}=b_i+e_{sb_i},\ i=1,2,\ldots,K$$

其中 $e_{sb_i},i=1,2,\ldots,K$ 表示节点 B 将消息发送给节点 A 时的信道噪声。

由攻击模型可知,敌手捕获中继节点,并且向将要发送的消息 $y_r,r=1,2,\ldots,K$ 中添加垃圾消息以达到污染整个网络的目的,篡改后的消息为:

$$y_r'=\sum_{i=1}^{K}\alpha_{i,r}\alpha_i+\sum_{i=1}^{K}\beta_{i,r}b_i+f_r,\ r=1,2,\ldots,K$$

其中 $f_r=(f_{r,1},f_{r,2},\ldots,f_{r,N})$为敌手加入的错误信息。若 $f_r=\vec{0}$,表示消息没有被篡改,反之,则消息经过了篡改。假设消息被篡改的概率为 p_f,即 $P(f_r\neq\vec{0})=p_f$。概率 p_f 对节点 A 与节点 B 而言是未知的。

第二步,中继节点将消息 y_r'广播给节点 A 与节

点 B,则节点 A 与节点 B 收到消息:

$$y'_r=\sum_{i=1}^{K}\alpha_{i,r}\alpha_i+\sum_{i=1}^{K}\beta_{i,r}b_i+f_r,\ r=1,2,\ldots,K$$

由上述可知,在第二步后,节点 A 与节点 B 分别接收到消息 y_{a_i},y_r'与 y_{b_i},y_r',$i=1,2,\ldots,K$,$r=1,2,\ldots,K$。通过利用 CRC 校验码,节点 A 可以对来自节点 B 直接广播的消息进行正确性验证,同理节点 B 进行同样操作验证节点 A 发送的消息的正确性。

对节点 A 而言,若经过 CRC 检验,在第一步当中 $y_{a_i}=b_i$,$i=1,2,\ldots,K$,则节点 A 可以直接得到文件 $\vec{b}$而不需要利用到消息 y_r'。反之,节点 A 计算:

$$y_{A,r}=y'_r-\sum_{i=1}^{K}\alpha_{i,r}a_i=\sum_{i=1}^{K}\beta_{i,r}b_i+f_r,\ r=1,2,\ldots,K \tag{1}$$

令 $y_A=\begin{pmatrix}y_{A,1}\\y_{A,2}\\\vdots\\y_{A,K}\end{pmatrix}$

则

$$y_A=\begin{pmatrix}\beta_{1,1}&\beta_{2,1}&\cdots&\beta_{K,1}\\\beta_{1,2}&\beta_{2,2}&\cdots&\beta_{K,2}\\\vdots&\vdots&\ddots&\vdots\\\beta_{1,K}&\beta_{2,K}&\cdots&\beta_{K,K}\end{pmatrix}\cdot\begin{pmatrix}b_1\\b_2\\\vdots\\b_K\end{pmatrix}+\begin{pmatrix}f_1\\f_2\\\vdots\\f_K\end{pmatrix}$$

令

$$M=\begin{pmatrix}\beta_{1,1}&\beta_{2,1}&\cdots&\beta_{K,1}\\\beta_{1,2}&\beta_{2,2}&\cdots&\beta_{K,2}\\\vdots&\vdots&\ddots&\vdots\\\beta_{1,K}&\beta_{2,K}&\cdots&\beta_{K,K}\end{pmatrix}$$

由文献[10]可知,当 $GF(q)$ 足够大,节点采用随机网络编码得到的任意 K 个编码数据包都能以较高概率解码成功,即采用线性网络编码(随机线性网络编码)时,传递矩阵(编码系数矩阵)可逆。故上述编码系数矩阵 M 是可逆的。

节点 A 计算:

$$\begin{pmatrix}\hat{b}_1\\\hat{b}_2\\\vdots\\\hat{b}_K\end{pmatrix}=\begin{pmatrix}\beta_{1,1}&\beta_{2,1}&\cdots&\beta_{K,1}\\\beta_{1,2}&\beta_{2,2}&\cdots&\beta_{K,2}\\\vdots&\vdots&\ddots&\vdots\\\beta_{1,K}&\beta_{2,K}&\cdots&\beta_{K,K}\end{pmatrix}^{-1}\cdot y_A$$

$$=\begin{pmatrix}b_1\\b_2\\\vdots\\b_K\end{pmatrix}+\begin{pmatrix}\beta_{1,1}&\beta_{2,1}&\cdots&\beta_{K,1}\\\beta_{1,2}&\beta_{2,2}&\cdots&\beta_{K,2}\\\vdots&\vdots&\ddots&\vdots\\\beta_{1,K}&\beta_{2,K}&\cdots&\beta_{K,K}\end{pmatrix}^{-1}\cdot\begin{pmatrix}f_1\\f_2\\\vdots\\f_K\end{pmatrix}$$

定义节点 A 正确解码当且仅当

$$\begin{pmatrix}\hat{b}_1\\\hat{b}_2\\\vdots\\\hat{b}_K\end{pmatrix}=\begin{pmatrix}b_1\\b_2\\\vdots\\b_K\end{pmatrix}\quad\text{即}\quad\begin{pmatrix}f_1\\f_2\\\vdots\\f_K\end{pmatrix}=\vec{0}$$

本文利用求组合消息 $y_{A,r}$ 的汉明重量,检测节点接收到的消息的可信度。对节点 A 而言,令

$$\begin{aligned}Z_r&=y_{A,r}-\sum_{i=1}^{K}\beta_{i,r}y_{a_i}\\&=\sum_{i=1}^{K}\beta_{i,r}b_i+f_r-\sum_{i=1}^{K}\beta_{i,r}(b_i+e_{sb_i})\\&=f_r-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i},\ r=1,2,\ldots,K\end{aligned} \tag{2}$$

为组合消息的线性差。

令 Z_r 的汉明重量为 $W_H(Z_r)$。因此由等式(2)可知

$$W_H(Z_r)=W_H(f_r-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i}) \tag{3}$$

敌手通过添加垃圾消息改变了消息的汉明重量,使 $f_r\neq\vec{0}$ 时的汉明重量大于 $f_r=\vec{0}$ 时的汉明重量。因为汉明重量约等于矢量元素中非零元素的个数,本文的矢量元素都选自 $GF(q)$。若攻击者添加了垃圾消息 $f_r=(f_{r1},f_{r2},\ldots,f_{rN})$,当 $GF(q)$ 足够大时,

中继节点接收的消息:

$$y_r=\sum_{i=1}^{K}\alpha_{i,r}a_i+\sum_{i=1}^{K}\beta_{i,r}b_i,\ r=1,2,\ldots,K$$

攻击者添加垃圾消息后:

$$y'_r=\sum_{i=1}^{K}\alpha_{i,r}a_i+\sum_{i=1}^{K}\beta_{i,r}b_i+f_r,\ r=1,2,\ldots,K$$

可知攻击者添加垃圾消息 $f_r=(f_{r1},f_{r2},\ldots,f_{rN})$ 后很有可能将中继节点原始消息矢量中的非零元素个数减少,则消息的汉明重量增加。

由(3)可知,即 $W_H(f_r-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i})\geqslant W_H(-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i})$。对于从中继节点接收到的任一消息所对应的 Z_r,$r=1,2,\ldots,K$ 的汉明重量 $W_H(Z_r)$ 越小,敌手添加垃圾消息的可能性越小,消息来源越可信。因此,对节点 A 而言,若直接从节点 B 获得的消息中有 S 个正确的消息,则节点 A 只需从 $W_H(Z_r)$ 中选择 $K-S$ 个最小的汉明重量所对应的由中继节点发送的消息 $y_{A,r}$ 解码。若 Z_r 的汉明重量都相等,则随机的选择 $K-S$ 个由中继节点发送的消息 $y_{A,r}$ 解码。

同理,节点 B 也做同样的操作。

4 解码差错概率

4.1 CRC-NC 方案

本文利用网络编码与循环检验编码相结合的方法抵抗污染攻击。节点计算接收到的消息的线性差的汉明重量,若从对方节点直接发送的消息中有 S 个消息是正确的,则节点只从 $W_H(Z_r)$ 中选择$K-S$个最小的汉明重量所对应的中继节点发送的消息解码。

对节点 A 而言,定义 y_a 为节点 A 接收到节点 B 发送的消息,y_A 为节点接收到来自中继节点的消息后对消息进行(1)式处理后的消息。T_{y_a}表示节点 A 收到由节点 B 直接发送的消息没有出错,T_{y_A}表示中继节点发送的消息没有被污染,F_{y_a}表示节点 A 收到由节点 B 直接发送的消息有出错,F_{y_A}表示中继节点发送的消息有被污染。$P(T)$表示解码成功的概率。令 $y_a=S$ 表示节点 A 收到由节点 B 直接发送的消息中有 S 个消息是正确的,$y_A=S'$表示节点 A 收到中继节点发来的消息中有 S'个消息未被篡改。则 CRC-NC 方案解码差错概率为:

$$\begin{aligned}P_E &= 1-P(T)\\ &= 1-P(T\mid y_a=T_{y_a},y_A=T_{y_A})P(y_a=T_{y_a})P(y_A=T_{y_A})\\ &\quad -P(T\mid y_a=T_{y_a},y_A=F_{y_A})P(y_a=T_{y_a})P(y_A=F_{y_A})\\ &\quad -P(T\mid y_a=F_{y_a},y_A=T_{y_A})P(y_a=F_{y_a})P(y_A=T_{y_A})\\ &\quad -P(T\mid y_a=F_{y_a},y_A=F_{y_A})P(y_a=F_{y_a})P(y_A=F_{y_A})\end{aligned} \tag{4}$$

且 $P(y_A=T_{y_A})=(1-p_f)^K$,

$P(y_a=T_{y_a})=(1-P_e)^K$,

$P(y_a=F_{y_a})=C_K^S P_e^{K-S}(1-P_e)^S$,

$P(y_A=F_{y_A})=C_K^{S'} p_f^{K-S'}(1-p_f)^{S'}$

其中 P_e 为由节点 B 直接发送的消息经编码错误概率,且 $P_e=\sum_{i=1}^{N} C_N^i p_s^i (1-p_s)^{N-i}$。

又因为

$P(T\mid y_a=T_{y_a},y_A=T_{y_A})=1$,

$P(T\mid y_a=T_{y_a},y_A=F_{y_A})=1$,

$P(T\mid y_a=F_{y_a},y_A=T_{y_A})=1$

因此等式(4)等价于

$$\begin{aligned}P_E &= 1-P(T)\\ &= 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K} P(T,y_a=S,y_A=S')\\ &= 1-\sum_{S=0}^{K-1}\sum_{S'=K-S}^{K-1} P(T,y_a=S,y_A=S')\\ &\quad -\sum_{S=0}^{K} P(T,y_a=S,y_A=K)-\sum_{S'=0}^{K} P(T,y_a=K,y_A=S')\\ &= 1-\sum_{S=0}^{K-1}\sum_{S'=K-S}^{K-1} P(T\mid y_a=S,y_A=S')P(y_a=S)P(y_A=S')\\ &\quad -\sum_{S=0}^{K} P(T\mid y_a=S,y_A=K)P(y_a=S)P(y_A=K)\\ &\quad -\sum_{S'=0}^{K} P(T\mid y_a=K,y_A=S')P(y_a=K)P(y_A=S')\\ &= 1-\sum_{S=0}^{K-1}\sum_{S'=K-S}^{K-1} P(T\mid y_a=S,y_A=S')P(y_a=S)P(y_A=S')\\ &\quad -\sum_{S=0}^{K} P(y_a=S)P(y_A=K)-\sum_{S'=0}^{K} P(y_a=K)P(y_A=S')\\ &= 1-\sum_{S=0}^{K-1}\sum_{S'=K-S}^{K-1} P(T\mid y_a=S,y_A=S')P(y_a=S)P(y_A=S')\\ &\quad -(1-p_f)^K\underbrace{\sum_{S=0}^{K} C_K^S P_e^{K-S}(1-P_e)^S}_{=1}\\ &\quad -(1-P_e)^K\underbrace{\sum_{S'=0}^{K} C_K^{S'} p_f^{K-S'}(1-p_f)^{S'}}_{=1}\\ &= 1-\sum_{S=0}^{K-1}\sum_{S'=K-S}^{K-1} P(T\mid y_a=S,y_A=S')P(y_a=S)P(y_A=S')\\ &\quad -(1-p_f)^K-(1-P_e)^K\end{aligned} \tag{5}$$

同理,节点 B 也做同样的操作。

4.2 随机方案

假设节点 A 收到由节点 B 直接发送的消息中有 S 个消息是正确的。在随机方案中,节点 A 随机从中继节点发来的消息中选择 $K-S$ 个,而不通过计算每个消息差的汉明重量。由与文献[8]类似计算可得随机方案的解码差错概率为:

$$\begin{aligned}P_E &= 1-P(T)\\ &= 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K} P(T,y_a=S,y_A=S')\\ &= 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K} P(T\mid y_a=S,y_A=S')P(y_a=S)P(y_A=S')\\ &\approx 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K}\frac{C_{S'}^{K-S}C_{K-S'}^{0}}{C_K^{K-S}}P(y_a=S)P(y_A=S')\\ &= 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K}\frac{C_{S'}^{K-S}}{C_K^{K-S}}C_K^S P_e^{K-S}(1-P_e)^S C_K^{S'} p_f^{K-S'}(1-p_f)^{S'}\\ &= 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K}\underbrace{\frac{C_{S'}^{K-S}C_K^{S'}}{C_K^{K-S}}}_{(\mathrm{I})}p_f^{K-S'}(1-p_f)^{S'}C_K^S p_e^{K-S}(1-p_e)^S\\ &= 1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K}\underbrace{C_{K-(K-S)}^{K-S'}}_{(\mathrm{II})}p_f^{K-S'}(1-p_f)^{S'}C_K^S p_e^{K-S}(1-p_e)^S\\ &= 1-\sum_{S=0}^{K}\underbrace{\sum_{t=0}^{K-(K-S)} C_{K-(K-S)}^{K-(K-S)-t} p_f^{K-(K-S)-t}(1-p_f)^t}_{=1}(1-p_f)^{K-S}\\ &\quad C_K^S P_e^{K-S}(1-P_e)^S\end{aligned}$$

$$=1-\sum_{S=0}^{K} C_K^S P_e^{K-S}(1-P_e)^S(1-p_f)^{K-S}$$

$$=1-\underbrace{\sum_{S=0}^{K} C_K^S[P_e(1-p_f)]^{K-S}(1-P_e)^S}_{\sum_{i=0}^{m} C_m^i a^i b^{m-i}=(a+b)^m}$$

$$=1-(1-p_f P_e)^K \tag{6}$$

其中公式(6)中(Ⅰ)与(Ⅱ)相等是因为

$$\frac{C_K^{S'} C_{S'}^{K-S}}{C_K^{K-S}}=\frac{\dfrac{K!}{S'!\ (K-S')!}\cdot\dfrac{S'!}{(K-S)!\ (S'-(K-S))!}}{\dfrac{K!}{(K-S)!\ (K-(K-S))!}}$$

$$=\frac{(K-(K-S))!}{(K-S')!\ (S'-(K-S))!}$$

$$=C_{K-(K-S)}^{K-S'} \tag{7}$$

4.3　加密方案

加密方案是指节点 A 与节点 B 相互发送消息时,先对消息进行加密操作。若节点 A 与节点 B 接收到的消息若没有被污染,则节点 A 与节点 B 正确译码;若节点 A 与节点 B 接收到的消息被污染,节点 A 与节点 B 不能正确解码。因此在加密方案中,解码差错概率为:

$$P_E=1-P(T)$$

$$=1-\sum_{S=0}^{K}\sum_{S'=K-S}^{K} P(T\mid y_a=S,y_A=S')P(y_a=S)P(y_A=S') \tag{8}$$

其中 $P(T\mid y_a=S,y_A=S')=1$ 或 $P(T\mid y_a=S,y_A=S')=0$。

5　仿真

如图 2,当污染概率 p_f 确定时,三种方案的节点解码差错概率 P_E 与两节点之间的信道交叉概率 p_s 的关系。其中 $q=32$,$N=31$,$K=3$,$p_f=0.3$。从图中可知当 $0.15\leqslant p_s\leqslant 0.25$ 时,CRC-NC 方案与加密方案相比,解码差错概率相差不大。这是因为在这种情况下 $W_H(-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i})$ 比 $W_H(f_r-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i})$ 要小。在此概率下,污染的数据可以很好的从没被污染的数据包中区分出来。随着 p_s 的增加,CRC-NC 方案与随机选取方案相差不大。因为所有消息的组合消息的汉明重量 $W_H(f_r-\sum_{i=1}^{K}\beta_{i,r}e_{sb_i})$ 都相差不大。当 $p_s\leqslant 0.2$ 时,由对方节点发送的消息大多可以正确译码。所以在此概率下 CRC-NC 方案与随机选取方案和加密方案相比,效果更明显。

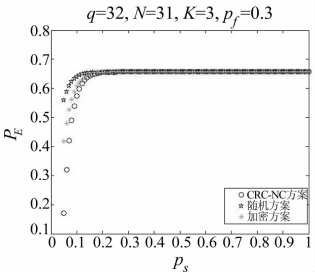

图 2　当污染概率 $p_f=0.3$ 时,节点解码差错概率 P_E 与交叉概率 p_s 的关系

Fig. 2　The probability of decoding error P_E versus cross-over probability p_s; $q=32$, $N=31$, $K=3$, $p_f=0.3$

如图 3,当交叉概率 p_s 确定时,三种方案的节点解码差错概率 P_E 与污染概率 p_f 的关系。其中 $q=32$,$N=31$,$K=3$,$p_s=0.1$。从图中可知,随着 p_f 的增加,三种方案的节点解码差错概率 P_E 也增加。但是,CRC-NC 方案与随机选取方案和加密方案相比,效果更明显。

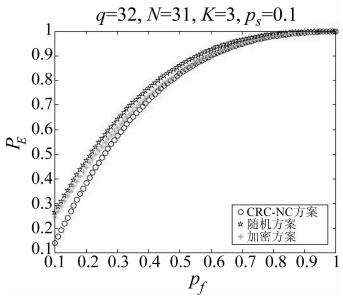

图 3　当交叉概率 $p_s=0.1$ 时,节点解码差错概率 P_E 与污染概率 p_f 的关系

Fig. 3　The probability of decoding error P_E versus the probability of false injection p_f; $q=32$, $N=31$, $K=3$, $p_s=0.1$

由图 4 可知,与图 3 相比,污染概率 p_f 越大,三种方案的节点解码差错概率总体增加。因为,在交叉概率相同的情况下,来自中继节点发送的消息被污染的概率越大,节点解码越困难,因此解码差错概率也随之变大。

由图 5 可知,交叉概率 $p_s=0.2$ 时,随着污染概率 p_f 的增加,三种方案的节点的解码差错概率相近。因为,由图 3 可知,当交叉概率 $p_s=0.2$ 时三种方案的效果相近,而 $p_s=0.1$,CRC-NC 方案的节点解码差错概率比其它两种方案都要低。

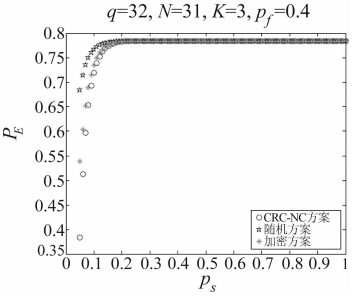

图 4　当污染概率 $p_f=0.4$ 时,节点解码差错概率 P_E 与交叉概率 p_s 的关系

Fig. 4　The probability of decoding error P_E versus cross-over probability p_s; $q=32$, $N=31$, $K=3$, $p_f=0.4$

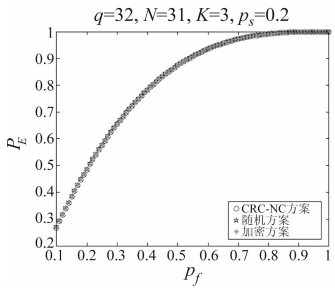

图5 当交叉概率 $p_s=0.2$ 时，节点解码差错概率 P_E 与污染概率 p_f 的关系

Fig. 5 The probability of decoding error P_E versus the probability of false injection p_f; $q=32$, $N=31$, $K=3$, $p_s=0.2$

6 结论

本文提出一种 CRC-NC 方案，即在无线双向通信网络中利用网络编码和循环冗余校验编码相结合的方法检测消息的可信度，抵抗污染攻击。在中继节点的辅助下双方相互发送消息，节点在接收到中继节点和对方节点发送来的消息后，计算组合消息差的汉明重量，若直接接收到对方消息中有 S 个消息是正确的，则剩下的 $K-S$ 个消息从组合消息中选择 $K-S$ 个汉明重量最小所对应的中继节点发送的消息 $y_{A,r}$ 进行解码。通过仿真结果可知，CRC-NC 方案与随机选取方案和加密方案相比，解码差错概率更低。

参考文献

[1] Ahlswede R, Ning Cai, Li S-Y R. Network information flow[J]. IEEE Transactions on Information Theory, 2000, 46(4): 1204-1216.

[2] Sidharth J, Michael L, Sachin K. Resilient network coding in the presence of Byzantine adversaries[J]. IEEE Transactions on Information Theory, 2008, 54(6): 616-624.

[3] Tracey H, Ben L, Ralf K. Byzantine Modification Detection in Multicast Networks With Random Network Coding. IEEE Information Theory Society, 2008, 54(6): 2596-2603.

[4] Zhen Y, Yawen W, Bhuvaneswari R. An Efficient Signature-Based Scheme for Securing Network Coding against Pollution Attack[C]//INFOCOM 2008, the 27th Conference on Computer Communications: IEEE, 2008: 1409-1417.

[5] Oggier F, Fathi H. An Authentication Code Against Pollution Attacks in Network Coding[J]. IEEE/ACM Transactions on Networking, 2011, 19(6): 1587-1596.

[6] Lu Lu, Taotao Wang, Soung Chang Liew. Implementation of physical-layer network coding[C]// Communications (ICC), 2012 IEEE International Conference on 2012: IEEE, 2012: 4734 - 4740.

[7] S C Liew, Shengli Zhang, Lu Lu. Physical-Layer Network Coding: Tutorial, Survey, and Beyond[J]. Network Coding and its Applications to Wireless Communications, 2012, vol. 6.

[8] D H Yoon, S W Kim. Trustworthy Decoding of Random Network Coded Packets Under Pollution Attack: Physical-Layer Approach[C]//Network Coding (NetCod): IEEE, 2013: 1-6.

[9] S Kim, S W Kim. Recycling Polluted Packet at the Physical Layer in Wireless network Coding[J]. IEEE Communications Letters, 2013, 17(5): 856-859.

[10] T Ho, M Médard, P Koetter, M Effros. A Random Linear Network Coding Approach to Multicast[J]. IEEE Trans. Information Theory, 2006, 52(10): 4413-4430.

[11] Jasper Goseling, Michael Gastpar, J H Weber. Random Access with Physical-layer Network Coding[C]//Information Theory and Applications Workshop: IEEE, 2013: 1-7.

[12] Aaram Y, Jung H Cheon, Yongdae Kim. Brief Contributions On Homomorphic Signatures for Network Coding[J]. IEEE Transactions on Computers, 2010, 59(9): 1295-1296.

[13] Zhen Y, Yawen W, Bhuvaneswari R. An Efficient Scheme for Securing XOR Network Coding against Pollution Attacks[C]//IEEE INFOCOM: IEEE, 2009: 406-414.

[14] Xiaohu Wu, Yinlong Xu, Chau Yuen. A Tag Encoding Scheme against Pollution Attack to Linear Network Coding [J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 33-42.

[15] Shimizu T, Iwai H, Sasaoka H. Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 650-660.

[16] G R Grimmett, D R Stirzaker. Probability and Random Processes[M]. Oxford, U. K: Oxford Univ. Press, 2006.

作者简介

罗晓晴 女，1990 年生，湖南衡阳人，福建师范大学数学与计算机科学学院硕士研究生。主要研究方向为网络安全、网络编码。

E-mail: xqLuo0318@gmail.com

李世唐 男，1973 年生，福建明溪人，福建师范大学讲师。主要研究方向为网络编码、信息论。

E-mail: tangshili@fjnu.edu.cn

许 力(通讯作者) 男，1970 年生，福建福州人，福建师范大学数学与计算机科学学院教授，博士生导师。主要研究方向为无线网络与移动通信、网络与信息安全、复杂网络和系统。

E-mail: xuli@fjnu.edu.cn