计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(4):253−259 [doi: 10.15888/j.cnki.csa.007822]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

认知协作网络中安全传输策略①

梅世纪, 朱　峰, 李　磊, 鲁兴河, 李泽宇, 宋　恺

(中电莱斯信息系统有限公司, 南京 210007)
通讯作者: 梅世纪, E-mail: m811064565@126.com

摘　要: 认知协作网络是一种基于协作通信技术的认知无线电网络, 不仅解决了不同网络在特定的时间与空间中频谱资源分配不均的问题, 而且可以通过主次用户间的协作提高网络性能. 但随着各种无线技术和移动应用日益丰富, 由于无线信道的固有特性, 服务质量会因安全问题造成性能损失与波动. 针对认知协作网络中, 因受到恶意用户攻击, 引起的网络传输性能下降的问题, 提出基于区块链的安全协作传输策略. 首先, 采用区块链进行身份认证, 避免数据污染而导致传输性能的损失与波动; 然后采用 RS (Reed-Solomon) 码编码来提升纠错能力, 进一步提高网络性能的稳定性. 仿真结果进一步证明了所提出的方案优于现有的认知协作网络传输方式, 具有较高的安全稳定性.

关键词: 认知协作网络; 身份认证; 区块链; RS 码

引用格式: 梅世纪,朱峰,李磊,鲁兴河,李泽宇,宋恺.认知协作网络中安全传输策略.计算机系统应用,2021,30(4):253–259. http://www.c-s-a.org.cn/1003-3254/7822.html

Safe Transmission Strategy in Cognitive Cooperative Network

MEI Shi-Ji, ZHU Feng, LI Lei, LU Xing-He, LI Ze-Yu, SONG Kai

(China Electronics Technology Group LES Information System Group Co. Ltd., Nanjing 210007, China)

Abstract: As a kind of cognitive radio network based on cooperative communication technology, cognitive cooperative network not only solves the problem of uneven distribution of spectrum resources in different networks in specific time and space, but also improves network performance through cooperation between primary and secondary users. However, with the increasing variety of wireless technologies and mobile applications, due to the inherent characteristics of wireless channels can lead to the loss of and fluctuation in performance of service quality, due to safety problems. To deal with the descending transmission of the cognitive cooperative network attacked by malicious users, we put forward a Blockchain-based safe transmission strategy. First, Blockchain is used for authentication, avoiding the loss of and fluctuation in transmission performance caused by data corruption. Second, Reed-Solomon (RS) codes are adopted for better error correction, further enhancing the stability. Eventually, the simulation result shows that the proposed strategy is more stable than existing transmission modes of the cognitive cooperative network.

Key words: cognitive cooperative networks; authentication; Blockchain; RS codes

随着物联网的发展, 对网络的传输效率与能耗要求越来越严格. 只有满足物联网设备对传输速率、容量和延迟等要求, 才能实现物联网的普及[1,2]. 同时, 针对各种各样的物联网设备部署, 未来需要面临高度密集的异构无线网络问题[3], 以及频谱资源有限、利用率低的现状, 需要采用多种技术建立认知协作网络. 从而通过有效利用空闲频谱资源, 使更多的无线设备可以接入网络. 以及通过不同设备之间的协作, 结合线性或非线性编码方案的网络编码, 也是实现增加吞吐量和满足高弹性的关键因素[4].

① 收稿时间: 2020-07-08; 修改时间: 2020-08-11, 2020-08-17; 采用时间: 2020-08-21; csa 在线出版时间: 2021-03-30

未来网络环境还将需要通过受信任或不受信任的物联网设备构成的网络进行信息传输. 因此, 移动运营商和用户越来越关注无线网络的安全性问题. 网络犯罪已成为互联网发展中所面临的严重阻碍, 国家主管部门和电信利益相关者已大力投资研究预防措施. 因此, 为了在认知协作网络中, 开发出高效的安全网络编码解决方案, 从而促进物联网的发展.

基于网络编码的体系结构特别容易受到污染攻击, 因为网络编码需要将数据经过继节点重新编码, 再分发给其他节点. 在这个过程中, 如果存在一个或多个恶意节点通过在网络中注入虚假数据, 就可以破坏数据传输. 为了保证数据传输的有效性, 必须具有足够的安全措施以防止污染攻击.

目前已有不少关于网络编码安全解决方案, 文献 [5] 提出了将任何线性网络编码转换为监视网络链接数量有限的窃听者无法获得有关所传输消息的任何信息的形式. 文献 [6] 中提出了可以抵抗拜占庭对手的分布式多项式时间率最优网络编码. 此外, 微软还启动了一个名为“Microsoft Secure Content Downloader”的网络编码文件打包应用程序[6]. 如先前在文献 [7] 中提出的, 网络编码还可用于通过减少网络传输中的丢失和故障来提高系统整体健壮性, 保护传输数据免受恶意用户攻击. 但由于新技术的引入, 使得物联网不仅面临较高的漏洞威胁, 还面临认知无线电数据篡改与网络编码的污染攻击等安全问题. 因此, 如何保护物联网免受各种威胁是一项艰巨的任务.

针对上述认知协作网络的安全问题, 本文提出一种基于区块链的安全网络编码方案 (BRNC) 来防止污染攻击. 主要贡献如下:

(1) 本文提出一种基于区块链的认知协作网络身份认证, 构建安全网络编码机制, 使网络避免污染攻击, 进而提高频谱资源有效利用率与网络传输效率, 实现信息安全稳定的传输.

(2) 采用 RS 编码, 对数据中的传输错误进行纠错, 进一步提高数据传输的有效性与网络传输效率.

(3) 通过仿真实验, 与现有工作比较, 验证所提出的认知协作网络中的安全网络编码方案的性能.

1 认知协作网络中安全传输模型

如图 1 所示, 针对的是一个具有多个主、次用户的认知协作中继网络. 该网络由一对主用户对和n对次级用户对组成. 其中, 主用户对分别为发送端T_p和接收端R_p, 次级用户对分别为发送端$T_s=\{T_{s1},T_{s2},T_{s3},\cdots,T_{sn}\}$和接收端$R_s=\{R_{s1},R_{s2},R_{s3},\cdots,R_{sn}\}$. 假设次级用户由于发射功率较小, 其接收端与发送端因信道衰落与间隔距离等因素, 无法直接实现次级用户间通信, 需要通过主用户进行中继协作通信, 并且主用户可以实现同时收发信息. 即在第 1 阶段中, 当主用户对之间进行数据交流时, 也可以接收来自次级用户所发送的信息. 第 2 阶段中, 当主用户传输结束, 存在空闲频谱时, 中继节点将接收到的次级用户信息进行处理, 以及重新编码发送给次级用户接收端.

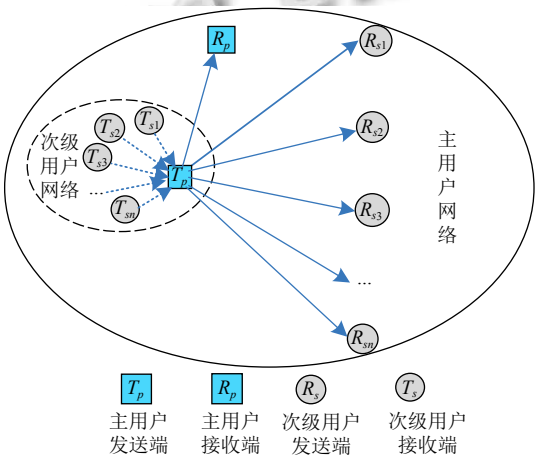

图 1 认知协作中继网络图

在认知协作网络中, 假设中继节点或者目的节点, 即主用户或者次级用户接收端可能接收到污染数据. 如图 2 所示, 次级用户会遵循认知无线电的工作原理, 不会对主用户通信造成干扰, 但可能会存在恶意节点污染网络编码数据, 造成次级用户接收端接收到无效数据. 甚至无法获取有效数据, 从而导致服务质量与频谱资源利用率下降. 因此, 为了实现数据的安全传输, 需要满足相应的安全需求, 即中继节点进行编码的数据包是有效安全的.

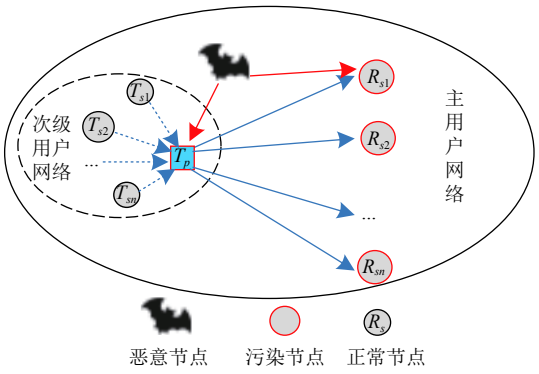

图 2 存在恶意节点的认知协作中继网络

2 安全网络编码策略设计

2.1 安全方案概述

尽管随机线性网络编码在带宽, 能耗以及丢包率方面具有巨大优势, 但在实际运用中, 使用网络编码, 需要解决其可能面临的各种安全问题. 尤其在基于网络编码实现的密集物联网应用中, 需要解决污染攻击, 否则会因污染攻击导致严重的网络性能下降和能量浪费. 为此, 需要采取合适的安全方案, 以抵抗污染攻击. 现有研究提出了使用身份认证技术来防止污染攻击的不同机制, 比如: 同态消息认证码和签名被认为是防止污染攻击的合适解决方案. 这样的方案虽然在防止数据污染攻击方面具有较高的安全性, 但没有考虑提高网络传输性能. 本文提出的基于区块链的安全网络编码方案, 通过引入区块链, 使用较少的密钥数和简单得多的密钥分发系统来实现, 实现加密与验证每个数据包; 同时, RS 纠错码可以提高网络传输性能. 如图 3 和算法 1 所示, 将介绍基于区块链的安全网络编码方案, 可以分为以下 3 个阶段: 源节点生成基于区块链验证的带转发信息; 中继节点验证信息标签, 生成基于网络编码与 RS 编码的信息; 目的节点验证、纠错与解码信息.

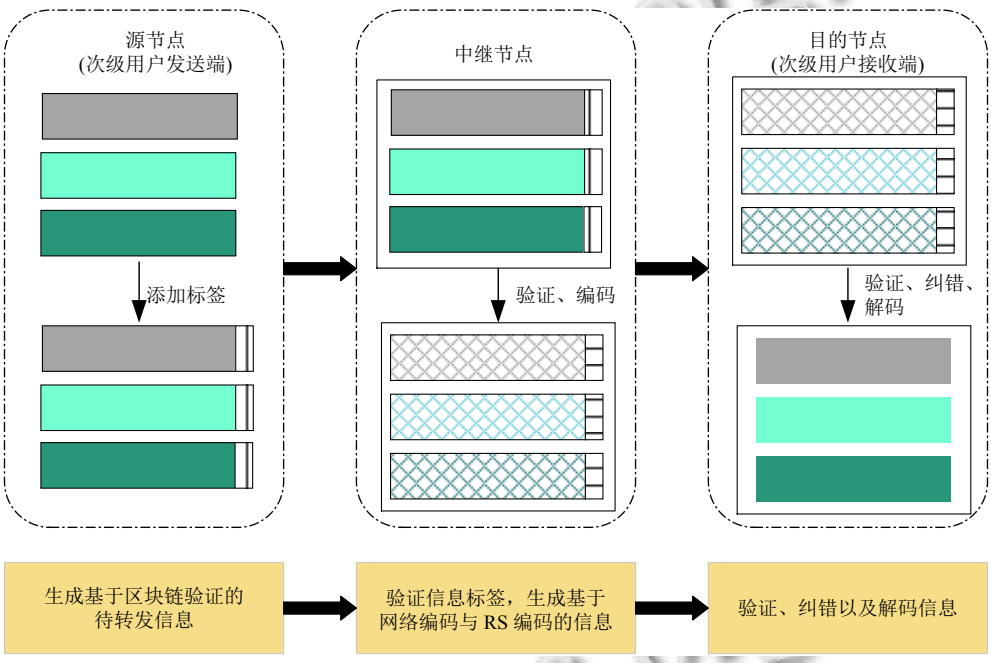

图 3 基于区块链和 RS 的安全网络编码方案

(1) 源节点添加标签

由于发送数据的节点中可能存在恶意节点, 所以对用户通信范围内的每个可信源节点分配密钥. 当这些节点需要发送信息时, 利用密钥生成标签并附加到发送的信息上, 然后将信息发送给中继节点.

1) 系统初始化

密钥分发中心将一组U个密钥的集合分发给网络中的所有节点. 这些密钥用于在源节点创建标签, 并在中继节点和目标节点处验证标签. 因此, 每个节点都必须保存此密钥集$K=[K_1,K_2,K_3,\cdots,K_U]$, $K_i\in F_q^{L+1}$, 即每个密钥K_i将在具有$L+1$个符号的字段大小q的有限字段上定义. 此外, 每个源节点将具有其自己的私钥, 以对在源节点创建的标签进行签名. 相应的公钥可用于网络中的所有其他节点, 所有密钥分发都可以在预处理阶段脱机完成的. 即密钥分发中心发送信息为:

$$SP=K \tag{1}$$

2) 标签生成

系统中有m个需要发送数据的源节点, 即存在m个数据包$P=\{P_1,P_2,P_3,\cdots,P_m\}$, 对于每个数据包$P_i$, 源节点使用$MAC(P_i,K)$算法生成$S$个标签将数据, 然后, 将标签添加到区块链中. 每个标签是由以下公式创建:

$$Tag_i=\frac{\sum_j^L P_{i,j}\times K_{i,j}}{K_{i,j+1}} \tag{2}$$

3) 数据添加标签

每个次级用户的发送端将生成的标签Tag_i添加到

带转发的信息P_i, 生成数据c_i发送至中继节点, 其中c_i可以表示为:

$$c_i = (P_i, Tag_i) \tag{3}$$

(2) 中继节点验证、编码

1) 身份认证

当中继节点接收到源节点的信息后, 提取c_i^*中的标签, 利用接收到的密钥集$SP = K$对标签进行验证, 判断是否为可信源节点发送的信息, 以避免恶意节点的干扰, 确保消息的真实性, 获取信息P_i.

算法 1. 基于区块链的 BRNC 算法

```
步骤 1. 从接收到的c_i*中检索系数矩阵;
步骤 2. 将从区块链中获取的标签乘以相应的系数;
步骤 3. 将标记与接收到的数据Tag_i'比较;
if 标签没有匹配成功 then
  c_i*是污染信息;
else
  提取信息;
  if 当前节点是中继节点 then
    将信息存放在缓存区;
    if 中继节点接收到 m 个数据包 then
      进行编码;
      将编码好的数据发送给目的节点;
    end
  else if 当前节点是目的节点 then
    if 当前数据存在错误 then
      通过 RS 修复解码;
    else
      直接解码;
    end
    将信息存放在缓存区;
    if 接收到足够的数据包 then
      解码;
    else
      继续等待接收数据;
    end
  end
end
```

2) 数据编码

将所接收到的可信源节点的信息$P = \{P_1, P_2, P_3, \cdots, P_m\}$, 采用随机线性网络编码对信息进行叠加. 首先, 生成网络编码矢量为:

$$V = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1m} \\ v_{21} & v_{22} & \cdots & v_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mm} \end{pmatrix} \tag{4}$$

编码数据分别可以表示为:

$$C = V \cdot P^{\mathrm{T}} = (C_1, C_2, C_3, \cdots, C_m) \tag{5}$$

之后将编码好的数据, 通过公式生成的标签Tag_i'. 把输入数据视为向量$C_i = (D_1, D_2, D_3, \cdots, D_L)$, B 为 RS 的编码矩阵, 编码后的数据为$C_i' = (D_1, D_2, D_3, \cdots, D_L, D_1', D_2', D_3', \cdots, D_L')$, 其关系符合$C_i' = B * C_i$. 将$Tag_i'$添加到带转发的信息, 生成数据$c_i'$发送至目的节点.

$$c_i' = \left(C_i', Tag_i'\right) \tag{6}$$

(3) 目的节点验证、纠错与解码

1) 信息验证、纠错

当目的节点接收到数据c_i^*后, 利用标签进行身份认证, 若为可信信息, 则将提取信息. 若信息中存在误码, 则通过 RS 对信息进行纠错, 删除错误的数据块, 以及对应位置的编码矩阵B, 得到保留的数据W和编码矩阵B', 利用B'的可逆性, 得到原始数据为C_i为:

$$C_i = B' * W \tag{7}$$

将C_i存放在缓存区, 目的节点继续接收中继节点发送的信息.

2) 信息解码

由于 BRNC 采用了网络编码, 提高网络的组播性能, 从而实现传输效率的提升. 只要当目的节点获取足够的数据后, 即可通过高斯消元进行解码, 得到所需数据P.

2.2 安全与性能分析

(1) 安全分析

本文中的安全分析是描述如何实现针对数据污染攻击的安全性. 网络中的易受攻击点是中继节点, 其具有密钥集K, 接收到的数据包P_i, 并且还能够查看本节点消息的原始标签. 在数据污染攻击中, 恶意节点将尝试破坏并传递消息. 在本文的方案中, 中继节点进行网络编码之前, 需要将接收数据包中标签与区块链中的标签匹配, 这样就可以对数据包进行验证, 避免数据污染. 通过区块链进行多方协作安全身份认证机制可以满足以下要求:

1) 数据访问控制

只有可信无线设备才能进入区块链, 查看相关信息, 如果设备要进行申请授权的操作, 则对操作进行数字签名, 最大限度的保护身份数据的安全.

2) 数据隐私保护

为了防止攻击者查看、篡改或伪造身份数据、账

户数据或者授权信息, 对数据和信息进行加密操作, 将可用设备特征数据加密, 在密码学层面上保证了区块链的高度隐私.

3) 匿名化

为了避免恶意用户通过统计分析等方式将身份信息和账户一一对应, 对设备特征数据进行匿名化处理, 使恶意用户在无用户私钥时不可查. 从而达到消除或混淆账户与用户真实身份、授权信息和认证信息之间的实际联系的目的.

(2) 性能分析

本文采用差分相移键控 (DPSK) 调制方案, 利用调制信号前后码元之间载波相对相位的变化来传递信息, 它不需要在接收端有相干参考信号, 使接收机复杂度降低的优点. 该方案下的误码率为:

$$p = \frac{1}{2}\mathrm{e}^{-\frac{E_b}{N_0}} \tag{8}$$

其中, E_b为每比特能量, N_0为噪声功率谱密度, L为数据的长度. 而集合间进行广播是在主用户信道被使用期间进行的, 所以不需要考虑其传输时间, 信道损失可以忽略.

在消息传输中, 接收节点无法确定数据包错误位置时, RS 编码设置L'个校正符号, 可以纠正数据包内$L'/2$个错误. 即成功传输的概率为:

$$p' = \sum_{i=0}^{i=\frac{L'}{2}} C_0^i (1-p)^{L+\frac{L'}{2}-i} p^i \tag{9}$$

3 仿真实验及分析

3.1 实验设计

在本节中, 将评估本文所提出的模型与算法. 该方案考虑的是在一个存在恶意用户的认知协作网络, 并且主、次用户接收端与发送端存在信道干扰和传输距离等问题. 在该网络中, 次级用户间需要通过中继进行传输数据, 主用户作为中继节点协作传输. 假设在次级用户通信范围内, 存在一个主用户, 其中多个次级用户发送端通过中继, 将信息传输到更远范围的次级用户接收端. 在仿真实验中, 原始数据包长度L_0 = 1200 bit, 不同数据间空隙长度L_s = 50 bit, 因网络编码增加的数据包长度L_h = 44 bit, 带宽 B=15 kHz, 次级用户发送端数目m = 4, 次级用户数目接收端n = 8, 一定时间内接入信道的主用户数目λ=2.

3.2 结果分析

(1) 不同编码率下, SNR 对 BRNC 传输性能的影响

如图 4 所示, 随着无线传输信噪比的增加, 认知无线电的虚警概率与无线传输误码率降低, 使无线传输的成功到达率上升. 与此同时, 成功到达率在一定的范围内随着信噪比的增加迅速上升, 而且 BRNC 编码率越低, 成功到达率迅速上升的时期越早. 但当信噪比增大到一定程度, 对无线传输的成功到达率性能的影响逐渐减小, 不同编码率之间成功到达率差别越来越小, 逐渐趋于一致. 当网络传输处于信噪比较低的通信环境中, 若没有 BRNC 编码进行纠错, 无线传输成功到达率较低, 几乎无法完成通信; 而采用 BRNC 方案编码, 仍然可以具有较高的成功到达率.

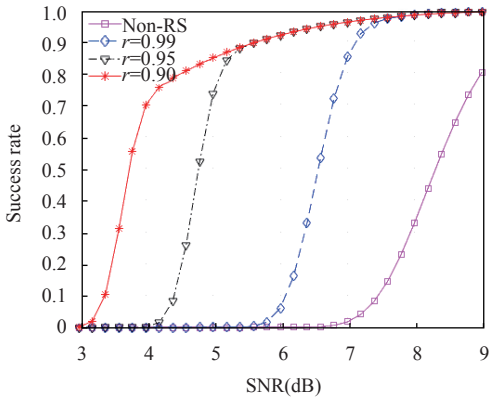

图 4 不同编码率下, SNR 对纠错性能的影响

(2) 不同 SNR 下, 编码率对 BRNC 传输性能的影响

如图 5 所示, 在相同编码率情况下, SNR 越高网络吞吐量越大. 因为 SNR 越大, 其传输速率越高, 成功到达率越高, 从而传输性能越好. 从该图还可以发现 SNR 一定的情况下, 随着编码率的增加, 传输性能先缓慢上升后逐渐下降. 因为在编码率较低的情况下, 增加校验信息对传输成功到达率的增益小于校验信息所造成的冗余代价. 当编码率超过一定的范围, 校验信息对传输成功到达率的增益大于校验信息所造成的冗余代价. 因此, 针对不同的通信环境选择合适编码率才能发挥网络传输性能.

(3) 不同攻击程度下, SNR 对传输性能的影响

如图 6, 图 7 所示, 本文采用基于区块链的安全网络编码方案 (BRNC) 与没有安全措施的受攻击概率 (Attack Probability, AP) 分别为 0.3, 0.5 的网络传输方案进行对比. 在图 6 中, 可以发现随着 SNR 的增加, 每个方案的

传输吞吐量都呈现出增长趋势. 与此同时, BRNC 始终优于没有采用安全措施的方案, 而且 BRNC 随着 SNR 的增长, 性能会平稳的增加. 因为其他方案由于受到恶意用户攻击, 所以吞吐量网络容量损失与性能波动. 在图 7 中, 可以发现传统方案在每个时隙传输性能波动性大, 且受到的攻击程度越大传输性能稳定性越差. 而 BRNC 可以避免恶意用户的污染攻击, 从而保证数据的稳定传输.

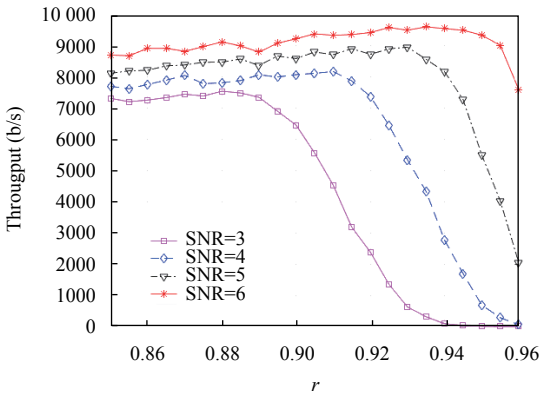

图 5 不同 SNR 下, 编码率对传输性能的影响

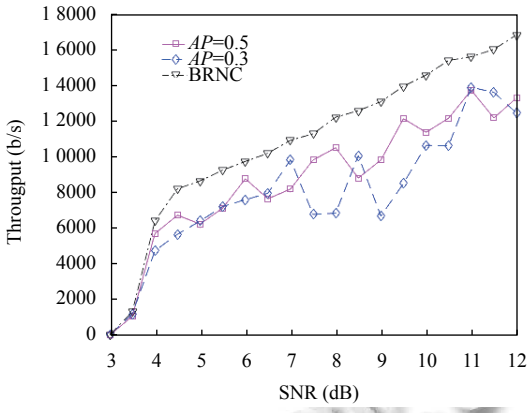

图 6 不同攻击程度下, SNR 对传输性能的影响

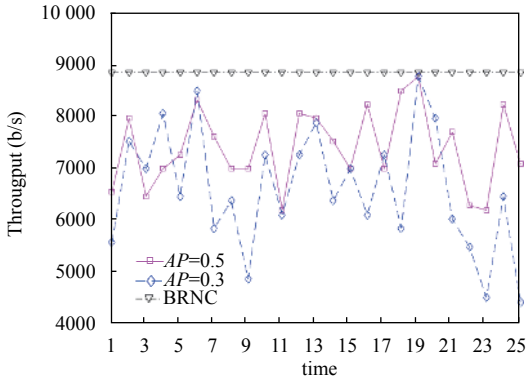

图 7 不同攻击程度下, 网络性能稳定情况

(4) 不同方案下, SNR 对传输性能的影响

如图 8 所示, 本文采用基于区块链的安全网络编码方案,分别与基于 RS 的网络编码方案 (RNC)[8]、基于区块链的安全传输方案 (BNC)[9] 和协作网络编码 (HNC-II)[10] 进行对比. 可以发现随着 SNR 的增加, 传输速率与成功到达率也会逐渐增长, 从而每个方案的吞吐量都会出现不同程度的增长. 该图还显示了在 SNR 较低的情况下, HNC-II 与 BNC 网络吞吐量极低, BRNC 与 RNC 仍具有良好的传输性能. 因为 BRNC 与 RNC 采用 RS 码进行编码纠错, 所以接收端即使存在一定的误码仍可以进行纠错完成传输. 与此同时, BRNC 与 BNC 随着 SNR 的增加, 网络传输性能平滑的上升, 而 HNC-II 与 RNC 波动性比较大, 因为前者通过身份认证的安全措施, 阻止了恶意用户的攻击, 避免了传输性能的损失. 此外, 当 SNR 低于 10.5 dB 时, BRNC 的传输性能最优. 因为 BRNC 不仅可以避免恶意用户攻击造成的性能损失, 还可以通过 RS 进行数据纠错以减少数据重传次数, 达到提升传输性能的目的. 而 SNR 高于 10.5 dB 时, BNC 的传输性能优于 BRNC. 因为该情况下数据传输的误码率较低, 这样 RS 造成的冗余信息传输代价大于编码所获取的增益, 所以 BRNC 传输性能劣于 BNC. 因此, 本文的 BRNC 方案可以满足低 SNR 条件下的通信, 可以有效阻止污染攻击, 保证数据安全稳定传输.

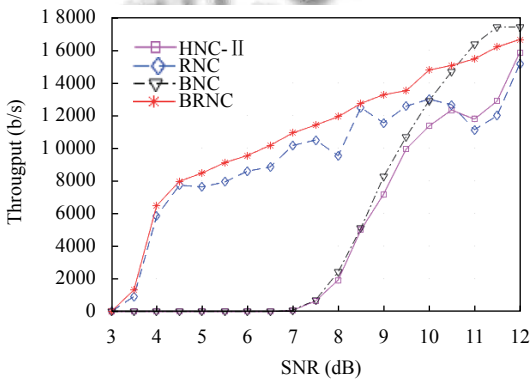

图 8 不同方案下, SNR 对传输性能的影响

4 总结

针对认知协作网络, 提出了一种基于区块链的安全网络编码方案. 首先, 该方案通过区块链分发密钥, 与对应次级用户需要发送的信息生成身份认证标签, 在中继节点和目的节点验证相应标签, 避免污染攻击.

其次, 在中继节点采用 RS 编码, 对接收到的次级用户信息进行编码发送. 并且在次级用户接收端对接收的信息进行验证、纠错, 降低传输差错引起的重传次数, 进而提高传输性能. 经过仿真实验表明, 与传统的传输方案相比, 本方案不仅具有较好的抗污染能力, 而且具有较好的传输性能, 从而能够充分发挥频谱资源的性能, 保证数据安全稳定传输. 而物联网设备随机移动性和无线链路的不确定性, 安全防护技术难应用; 设备加入或退出网络时, 身份认证和密钥更新困难; 有限的资源决定了复杂的算法难以应用. 在本文的安全传输策略中, 结合区块链安全、便捷的特点, 进行身份认证, 使无线设备可以识别恶意用户的信息, 避免数据污染, 使物联网设备可以快速、便捷、高效地安全部署.

参考文献

1 Tselios C, Tsolis G. On QoE-awareness through virtualized probes in 5G networks. 2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD). Toronto, ON, Canada. 2016. 159–164.

2 Politis I, Tselios C, Lykourgiotis A, *et al*. On optimizing scalable video delivery over media aware mobile clouds. 2017 IEEE International Conference on Communications (ICC). Paris, France. 2017. 1–6.

3 Rodriguez J, Radwan A, Barbosa C, *et al*. SECRET—secure network coding for reduced energy next generation mobile small cells: A European training network in wireless communications and networking for 5G. 2017 Internet Technologies and Applications (ITA). Wrexham, UK. 2017. 329–333.

4 Cai N, Yeung RW. Secure network coding. Proceedings IEEE International Symposium on Information Theory. Lausanne, Switzerland. 2002. 323.

5 Jaggi S, Langberg M, Katti S, *et al*. Resilient network coding in the presence of byzantine adversaries. IEEE Transactions on Information Theory, 2008, 54(6): 2596–2603. [doi: 10.1109/TIT.2008.921711]

6 Gkantsidis C, Rodriguez PR. Network coding for large scale content distribution. Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Miami, FL, USA. 2005. 2235–2245.

7 Lima L, Gheorghiu S, Barros J, *et al*. Secure network coding for multi-resolution wireless video streaming. IEEE Journal on Selected Areas in Communications, 2010, 28(3): 377–388. [doi: 10.1109/JSAC.2010.100409]

8 Yin YZ, Pyndiah R, Amis K. Performance of random linear network codes concatenated with reed-Solomon codes using turbo decoding. 2010 6th International Symposium on Turbo Codes & Iterative Information Processing. Brest, France. 2010. 132–136.

9 Adat V, Politis I, Kotsopoulos S. On blockchain based secure network coding for mobile small cells. 2019 IEEE 2nd 5G World Forum (5GWF). Dresden, Germany. 2019. 274–279.

10 Mei SJ, Chen B, Hu F, *et al*. Hybrid network coding scheme in cognitive radio networks with multiple secondary users. IEEE Access, 2018, 6: 63948–63957. [doi: 10.1109/ACCESS.2018.2877219]