Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2017, 10, 167-175
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

# A Safety Relay Selection Method Based on Network Coding

**Qiang Guo, Xin Li**

College of Information and Communication Engineering, Harbin Engineer University, Harbin, China
Email: lixinxin@hrbeu.edu.cn

**How to cite this paper:** Guo, Q. and Li, X. (2017) A Safety Relay Selection Method Based on Network Coding. *Int. J. Communications, Network and System Sciences*, **10**, 167-175.
https://doi.org/10.4236/ijcns.2017.108B018

**Received:** May 28, 2017
**Accepted:** August 11, 2017
**Published:** August 14, 2017

## Abstract

A method of cooperative relay selection based on network coding security is proposed for relay selection problem of cooperative communication system security in networked multi-relay scenarios, which is different from the existing relay node selection method. The algorithm not only merged with timestamp and homomorphic signature to construct the node degree of safety to find reliable relay, at the same time to considers the received signal to noise ratio at all relay nodes value and the channel gain to the source node. The simulation results show that the proposed method can improve the achievable rate of the destination node and reduce the outage probability on the basis of guaranteeing the safety of the relay node.

## Keywords

Timestamp, Homomorphic Signature, Node Degree of Safety, Achievable Rate, Outage Probability

## 1. Introduction

The network coding technology has attracted wide attention because of the advantages of throughput and transmission delay minimization, and can balance the network load, solve the network congestion and improve the network bandwidth utilization [1]. The broadcast characteristics of wireless communication channel transmission make network coding technology more suitable for application to wireless cooperative relay communication network, which can further improve spectrum efficiency and system capacity. But at the same time it also brings a lot of security issues [2], because the principle of the network coding itself, information diffusivity is stronger, so compared with the ordinary network, in this case the attacker as long as the injection of small malicious information or a slight modification of the relevant information may affect a range or even the entire network. That is to say, the same attack means, in the mode of the network more efficient attack, more contagious, so for the secure communication relay node selection algorithm research is another focus of collaborative communication [3]. In this paper, we study the situation of selecting cooperative relay for the source node in the multi-relay scenario, analyze the security and validity of the relay selection problem in this case, combined use of fusion timestamp and homomorphic signature security detection algorithm and the optimal intermediate node selection scheme, a secure and effective multipath selection algorithm based on network coding is proposed, this method cannot only guarantee the security of data transmission, to further improve the performance of the system.

## 2. Fusion Timestamp and Homomorphic Signature Security Calculation

Due to the network coding is very vulnerable to the malicious modification of the packet by the attacker in the network, thus the obtaining-information node has the influence on the decoding of the correct packet. If the attacker repeats the malicious information which is not related to the correct data, it will cause enormous waste of network resources, this paper designs a network coding scheme that combines time-stamp and homomorphic signatures to resist pollution attacks and replay attacks on the basis of RSA homomorphic signature scheme [4]. The scheme introduces the pollution attack and replay attack as a link of safety indicators on the basis of the basic dynamic weight calculation formula. The RSA signature is used to detect the pollution attack, and the time stamp mechanism is introduced so that the scheme can detect the replay attack, Find the optimal security node of the network coding algorithm.

### 2.1. The System Model

“**Figure 1**” and “**Figure 2**” show the system model. In the system there is a source node s, A destination node d, and relay node followed by $r_1, r_2, \cdots, r_N$. The relay node uses half-duplex mode to forward the signal, Received signal using amplify-and-forward, AF approach.

### 2.2. The Specific Algorithm

There are three parts of the homomorphic signature scheme with timestamps,

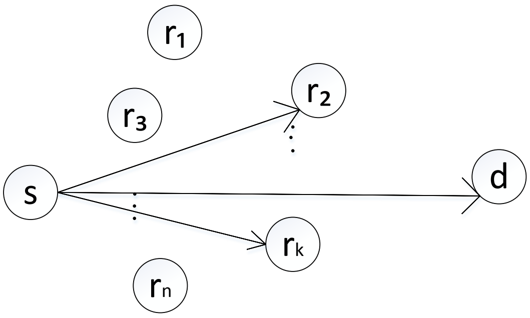

**Figure 1.** The source node sends.

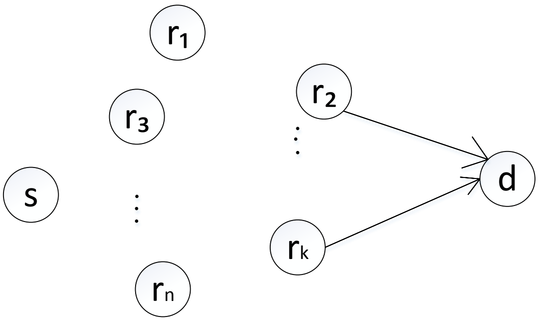

**Figure 2.** Relay nodes forward.

which are asymmetric key generation algorithm, signature generation algorithm and signature verification algorithm respectively.

Asymmetric key generation algorithm [5]:

- Randomly select two large prime numbers $p_1$, $p_2$ among them $p_2\left|\left(p_1-1\right)\right.$ Usually take $p_2$ for 256 bit, take $p_1$ for 1024 bit.
- Calculation $n=p_1p_2$, $\varphi(n)=(p_1-1)(p_2-1)$ Randomly select integers $e\le\varphi(n)$, and Satisfy:

$$\gcd\left(e,\varphi(n)\right)=1 \tag{1}$$

- Generates the RSA signature key d and the public key $(n,e)$ Where d is satisfied:

$$ed=1\bmod\left(\varphi(n)\right) \tag{2}$$

Signature generation algorithm:

- The source node generates m messages to be sent: $x_i$ ($i=1,2,\cdots,m$).
- Takes the current timestamp t as the timestamp of the message and generates a signature for the message and timestamp, The signature is denoted by $sign(x_i,T_i)$:

$$sign\left(x_i,T_i\right)=\left(\prod_{j=1}^{m}g_j^{x_i}.g_m^{T_i}\bmod p_1\right)^d \bmod r \tag{3}$$

*r* is the source private key, *d* is the source public key, and $g_j$ is the public parameter of the source.

Signature verification algorithm:

- The intermediate node receives a message $\{Y,T,sign(Y,T)\}$, To determine whether Equation (4) was established:

$$sign\left(Y,T\right)^e \bmod r=\left(\prod_{j=1}^{m}g_j^{y_i}.g_m^{T_i}\bmod p_1\right)^d \bmod r \tag{4}$$

- If Equation (4) is established, shows the message isn't subject to pollution attacks, go to the next step, if the formula 2 don't hold, indicating that the message received pollution attacks, the intermediate node should discard this message.
- By the time stamp to determine whether the replay attack, if a message timestamp within the scope of the time, it indicates that the message has not been

replayed, otherwise, this message should be discarded.

## 2.3. Security Degree Calculation

Assuming that all links can be attacked, the introduction of pollution attack and replay attack as an index to calculate the intermediate node security degree on the basis of the basic dynamic weight calculation formula, find the appropriate intermediate node for data transmission, to ensure the security of network coding.

The initial the safety degree of the intermediate node s assignment to 1, Intermediate node degree of security calculation:

$$s_i = 1 - (\alpha \frac{N_P}{N} + \beta \frac{N_r}{N}) \tag{5}$$

*N* represents the total number of messages sent by node *i*, $N_p$ indicates the number of contaminated attacks on node *i*, $N_r$ indicates the number of replay attacks by node *i*, $\alpha, \beta$ is used to measure the degree of pollution attack and replay in node *i*:

$$\alpha = \frac{N_p}{N_p + N_r} \tag{6}$$

$$\beta = \frac{N_r}{N_r + N_p} \tag{7}$$

Due to the uncertainty of the network, the dynamic threshold is introduced to calculate the security of the current intermediate nodes. The threshold chosen by this algorithm is the weighted sum of the highest security degrees of each node for a period time. As shown in Equation (8):

$$\mathrm{S}_y = \sum_{j=1}^{p} \frac{1}{p} \mathrm{S}_{j\max} \tag{8}$$

$\mathrm{S}_{j\max}$ represents the maximum value of the safety of the intermediate node *j* over a period of time, $s_y$ set of dynamic threshold, The safety of the intermediate node satisfies $S_{j\max} \geq S_y$, This node as a preselected node.

## 2.4. Security Analysis

Focuses on Pollution attacks and Replay attacks [6].

- Security Analysis of Pollution Attack: There are two kinds of attacks on pollution attacks. 1) The attacker can forge the received packet (*Y*, *T*), and intention to forge the packets to generate valid signatures, but because the attacker doesn't know the source node to the private key, so I can't to packets (*Y*, *T*) generates valid signatures, attacks a failure. 2) The attacker intends to generate the fake data $\{Y', T'\}$ with the valid signature $sign(Y,T)$ of the intercepted packet, and $\{Y', T'\} \neq (Y, T)$, the difficulty of such attack mode is equivalent to solve the problem of discrete logarithm.
- Security analysis of Replay Attack: There are two kinds of attacks on replay attacks. 1) Directly replay the intercepted message combination, assuming that the attacker intercepts the message with $\{Y, T, sign(Y,T)\}$ and the node

receives the message and sends the received timestamp with the current time $T_i$, In comparison, if it is not within the scope of limitation, it can be judged that the message is a replay message and the attack is invalid. 2) Modify the timestamp of the intercepted message and generate a signature for it. The attacker can't sign the part of the intercepted message because he does not know the private key of the source node, so the attack is invalid.

## 3. Optimal Relay Node Selection Scheme

The selection of the relay node is the key factor that affects the final transmission quality. Selecting the optimal relay node can not only reduce the network cost, but also improve the performance of the communication system. In this paper, from the point of view of system achievable rate and outage probability, combined with the intermediate nodes selected in Chapter 2, calculating the received signal-to-noise ratio of the intermediate node in the direction of the source node to the intermediate node and comparing the decision threshold with the set signal-to-noise ratio, selecting the intermediate node satisfying the condition, an intermediate node having the largest channel gain among the intermediate node and the destination node link is selected from the candidate node set.

### 3.1. Multi-Relay System Model

The channels are quasi-static Rayleigh fading channels, the channel state remains unchanged during one transmission cycle. For each "source node-relay node-destination node" link, the total power of the signal transmission is limited to p, the source node occupies half of the total power, the residual power is distributed equally by the relay node, and between the two source nodes there is no forward link [7]. $h_{\mathrm{sr}_k}$, $f_{r_i d}$ respectively represent the channel fading coefficients of the source node S to the *i*-th relay node and the *i*-th relay node to the destination node *d*, $h_{\mathrm{sr}_k}$, $f_{r_i d}$ mean is zero, Complex Gaussian Random Variables with Variance of $\delta_{si}^2$ and $\delta_{di}^2$. Each link is affected by additive white Gaussian noise $n_r$, and its mean is zero variance of 1. The whole model uses time division mode, completed in two time slots.

In the first time slot, the source node S transmits the signal *x* at the power $p_s$. The signal received by the relay node $r_i$ is represented as:

$$y_{r_i} = h_{\mathrm{sr}_i}\sqrt{p_s}\,x + n_r \tag{9}$$

In the second time slot, the relay node $r_i$ broadcasts the received signal network to the destination node d. The destination node receives the signal as:

$$y_d = Ah_{\mathrm{sr}_i} f_{r_i\mathrm{d}}\sqrt{p_r}\sqrt{p_s}\,x + Af_{r_i\mathrm{d}}\sqrt{p_r}\,n_r + n_d \tag{10}$$

The relay node $r_i$ adopts the AF protocol, then A is the amplification factor, $\mathrm{A} = \sqrt{\dfrac{p_r}{h_{\mathrm{sr}_i}{}^2 p_s + 1}}$, $p_r$ is the forwarding power of the relay node $r_i$.

So to get the destination node to accept SNR expression:

$$SNR = \frac{A^2 \left|h_{sr_r}\right|^2 \left|f_{r_i d}\right|^2 p_s}{A^2 \left|f_{r_i d}\right|^2 + 1} = \frac{p_r p_s \left|h_{sr_r}\right|^2 \left|f_{r_i d}\right|^2}{p_s \left|h_{sr_r}\right|^2 + p_r \left|f_{r_i d}\right|^2 + 1} \tag{11}$$

### 3.2. Relay Selection Method Specific Step Description

In this paper, the relay node selection scheme is used to set the SNR threshold at each intermediate node. After two selections, select the most optimal relay nodes. The specific steps are as follows:

- A reasonable threshold value $\delta_{th}$ for receiving the SNR is set in the system, In the previous section, the received SNR at the intermediate node in the source-middle node direction is given as $p_s \left|h_{sr_i}\right|^2$. we can get some preselected nodes according to Equation (12):

$$p_s \left|h_{sr_i}\right|^2 > \delta_{th} \tag{12}$$

The set of candidate nodes expressed as $C(r) = \left\{ i \mid p_s \left|h_{sr_i}\right|^2 > \delta_{th} \right\}, i = 1, 2, \cdots, n.$

- Select the relay node with the largest channel gain in the direction of the intermediate node-destination node, which satisfies the Equation (13):

$$r_m = \left\{ i \mid \max\left( f_{r_i d} \right) \right\}, i = 1, 2, \cdots, n \tag{13}$$

The optimal relay selection scheme takes into account the received SNR at the relay node and selects the maximum channel gain at the destination node.

### 3.3. Effectiveness Analysis

In order to verify the validity of the relay selection scheme used in this article, and the maximized minimum SNR relay selection scheme in [8], the maximized minimum channel gain relay selection scheme in [9] and the random relay selection scheme are carried out from the achievable rate and outage probability performance Simulation comparison. The system uses equal power allocation scheme.

"**Figure 3**" shows the simulation results of the achievable rate of each relay selection method under different total power.

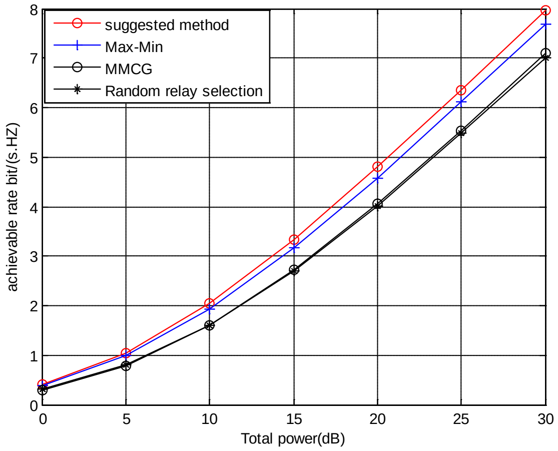

**Figure 3.** The achievable rate comparison of various relay selection schemes.

Simulation results show, Based on the method of maximizing the received SNR and channel gain, the achievable rate and performance of the cooperative system are compared with the Max-Min relay selection scheme, the channel gain harmonic mean maximum scheme, the random relay selection scheme, respectively, increased by 3.9%, 11.1%, 14.3%.

"**Figure 4**" shows the simulation results of the outage probability of each relay selection method under different total power.

Under the condition of total system power, the improved two-way relay selection scheme proposed in this paper is the smallest and the best performance in the four relay selection schemes.

## 4. Simulation Parameter Analysis

In the existing multi-relay system, the majority of the research on relay selection is based on the assumption that all relay nodes are in the middle of the two source nodes, this article will be more general circumstances to study the proposed program performance.

"**Figure 5**" shows Relay node location. The serial number 1 is the source node, the serial number 12 as the destination node, This paper assumes that the source node sends ten packets, each packet has ten components, for each intermediate node random introduction of pollution attacks and replay attacks, in a period of time, each intermediate node for three times the safety calculation results are as follows "**Table 1**":

Select the maximum security for each intermediate node Use Equation (8): $S_y = \sum_{j=1}^{p} \frac{1}{p} \mathrm{S}_{j\max}$ to calculate the dynamic threshold. Get the dynamic threshold based on this experiment:

$$\mathrm{S}_\mathrm{y} = \frac{0.600000 + 0.383333 + 0.500000 + 0.740000 + 0.666667 + 0.383333 + 0.500000 + 0.833333 + 0.575000 + 0.585714}{10}$$
$$= 0.576738$$

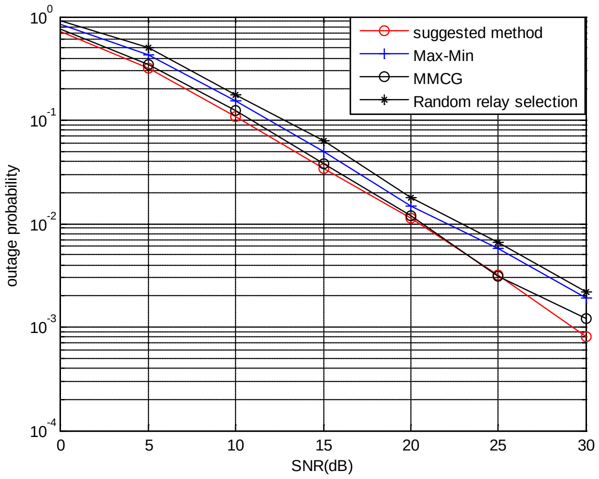

**Figure 4.** Outage probability comparison of various relay selection schemes.

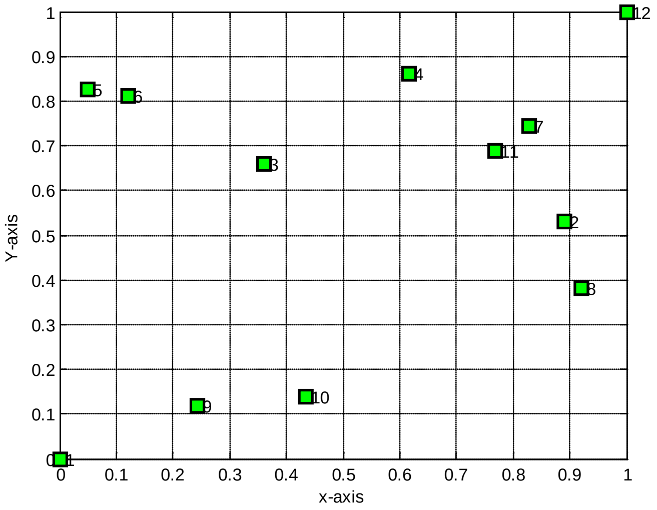

**Figure 5.** Relay node location.

**Table 1.** Relay node security calculation results.

| Intermediate node number | Node degree of security | | |
|---|---|---|---|
| | Number of experiments 1 | Number of experiments 2 | Number of experiments 3 |
| 2 | 0.600000 | 0.346154 | 0.575000 |
| 3 | 0.383333 | 0.285714 | 0.383333 |
| 4 | 0.480000 | 0.500000 | 0.336364 |
| 5 | 0.575000 | 0.285714 | 0.740000 |
| 6 | 0.420000 | 0.666667 | 0.300000 |
| 7 | 0.346154 | 0.315385 | 0.383333 |
| 8 | 0.500000 | 0.445455 | 0.346153 |
| 9 | 0.544444 | 0.285714 | 0.833333 |
| 10 | 0.383333 | 0.575000 | 0.575000 |
| 11 | 0.585714 | 0.544444 | 0.480000 |

To get the candidate nodes: 2, 5, 6, 9, 11. The above five nodes perform the optimal relay node selection algorithm.

The final selection of the relay according to Section 3.2 is the trunk of serial number 2.

## 5. Conclusion

Aiming at the characteristics of network coding application in wireless cooperative relay communication system, a relay selection method based on network coding security is proposed. The method uses the time-stamped homomorphic signature scheme to construct the node's security degree and calculate the dynamic threshold Select the trusted candidate node, the security of each node used in the past period of time the maximum value is because the threshold is a threshold, the network does not want to enter the dangerous node, so the need to set the threshold, if the current time Threshold, then it may be more dangerous nodes into the network, is not conducive to network security. Then, based on the method of maximizing the received signal-to-noise ratio and channel gain, the optimal relay node is selected from the candidate nodes. The simulation results show that the achievable rate can be improved and the outage probability can be effectively reduced on the basis of ensuring the security of the relay node.

## References

[1] Fragouli, C., Boudec, J. and Widmer, J. (2006) Network Coding: An Instant Primer. *ACM SIGCOMM Computer Communication Review*, **36**, 63-68. https://doi.org/10.1145/1111322.1111337

[2] Cao, Z.H. and Tang, Y.S. (2010) Summary of Secure Network Coding. *Computer Application*, **30**, 499-505. https://doi.org/10.3724/SP.J.1087.2010.00499

[3] Chang, X.M., Wang, J. and Wang, J.P. (2016) On the Optimal Design of Secure Network Coding against Wiretapping Attack. *Computer Networks*, **99**, 82-98. https://doi.org/10.1016/j.comnet.2015.12.012

[4] Yu, Z., Wei, Y. and Ramkumar, B. (2008) An Efficient Signature-Based Scheme for Securing Network Coding against Pollution Attacks. *Proceedings of International Conference on Computer Communications* (*INFOCOM*), Arizona, USA, 13-18 April 2008, 1409-1417. https://doi.org/10.1109/INFOCOM.2008.199

[5] Pei, H.-L., Shang, T. and Liu, J.-W. (2013) Secure Network Coding Method Merged with Timestamp and Homomorphic Signature. *Journal on Communications*.

[6] Cai, N. and Yeung, R.W. (2011) Secure Network Coding on a Wiretap Network. *IEEE Transactions on Information Theory*, **57**, 424-435. https://doi.org/10.1109/TIT.2010.2090197

[7] Dai, X.-L., Zhang, J. and Ji, X.-L. (2014) A New Method for Cooperative Relay Selection Based on Hybrid Intelligent Algorithm. *Telecommunication Engineering*.

[8] Lu, L. and Yu, H.Y. (2011) Physical Layer Network Coding Packet Opportunity Relay. *Journal of Electronics & Information Technology*, **31**, 1767-1770.

[9] Liu, S.L. and Cao, S.H. (2013) Two-Way AF Relay System Relay Selection and Power Allocation Strategy. *Computer Engineering and Applications*, **49**.