information

MDPI

Article

BGP Neighbor Trust Establishment Mechanism Based on the Bargaining Game

Peipei Li [1,2], Bin Lu [1,2] and Daofeng Li [1,2,*]

[1] School of Computer Electrical and Information, Guangxi University, Nanning 530004, China; 1813301016@st.gxu.edu.cn (P.L.); 1813393009@st.gxu.edu.cn (B.L.)
[2] Guangxi Colleges and Universities Key Laboratory of Multimedia Communications and Information Processing, Guangxi University, Nanning 530004, China
* Correspondence: ldf-0123@gxu.edu.cn; Tel.: +86-1362-771-3816

Abstract: The Border Gateway Protocol (BGP) is the standard inter-domain route protocol on the Internet. Autonomous System (AS) traffic is forwarded by the BGP neighbors. In the route selection, if there are malicious or inactive neighbors, it will affect the network's performance or even cause the network to crash. Therefore, choosing trusted and safe neighbors is an essential part of BGP security research. In response to such a problem, in this paper we propose a BGP Neighbor Trust Establishment Mechanism based on the Bargaining Game (BNTE-BG). By combining service quality attributes such as bandwidth, packet loss rate, jitter, delay, and price with bargaining game theory, it allows the AS to select trusted neighbors which satisfy the Quality of Service independently. When the trusted neighbors are forwarding data, we draw on the gray correlation algorithm to calculate neighbors' behavioral trust and detect malicious or inactive BGP neighbors.

Keywords: Border Gateway Protocol; bargaining game; neighbor; trust; gray correlation algorithm

Citation: Li, P.; Lu, B.; Li, D. BGP Neighbor Trust Establishment Mechanism Based on the Bargaining Game. *Information* **2021**, *12*, 110. https://doi.org/10.3390/info12030110

Academic Editor: Georgios Kambourakis

Received: 7 December 2020
Accepted: 27 February 2021
Published: 4 March 2021

1. Introduction

Currently, the Border Gateway Protocol (BGP) [1] is the only inter-domain route protocol used on the Internet and is the key component of the Internet route infrastructure. However, the designers of the BGP did not initially consider security issues, which led to the BGP's security vulnerability [2]. Existing research [3–7] mostly protects Autonomous System (AS) traffic data by verifying the authenticity and integrity of routing information. However, how to confirm trusted neighbors is also an important issue. Neighbors play an important role in the BGP protocol. Due to the large scale and dynamic nature of the Internet, AS data must rely on neighbors to reach the destination network. If an AS establishes a neighbor relationship with a malicious/inactive AS, the AS data will not be forwarded efficiently. Malicious/inactive neighbors will restrict AS network traffic by setting routing policies [8]. For example, some inactive neighbors will adopt the "hot potato" [9] routing strategy to reduce the overhead caused by traffic passing through the domain and choose the fastest exit from the domain, regardless of its path length through other networks. Even malicious/inactive neighbors will launch malicious attacks, causing the AS network to paralyze. For example, in May 2004, DataOne, an internet service provider in Malaysia, announced to its neighbors the prefix of Yahoo's data center in Santa Clara, California, which caused the network of neighbors to go down. Therefore, establishing a safe and trusted neighbor relationship is a key issue in BGP security research.

In researching about the BGP neighbor trust establishment mechanism, we must first realize that deploying any security mechanism on the BGP will have a certain impact on it. Therefore, it should be easy to deploy and achieve security protection. Easy to deploy means that the security mechanism added to the BGP should minimize the impact on it, such as increased storage and resource overhead, the impact of convergence time, and scalability. Security protection means that it should allow the arbitrary AS to establish

neighbor relationships with trusted ASes. The two ASes involved in neighbor establishment belong to different Internet Service Providers (ISPs). Thus, ASes are profit-seeking and selfish. It must consider the practical factors and encourage ASes to establish a trusted neighbor relationship. For the BGP trusted neighbor, there are some relevant studies. For example, some researchers have introduced trust technology [10–14] to inter-domain security research. Its basic idea is to construct a reputation system by evaluating the target AS's behaviors. However, the evaluation result has uncertainty. It is not easy to guarantee safety. Yi et al. [15] proposed a Neighbor-specific BGP (NS-BGP) mechanism based on specific neighbors. By remodeling the route export and import strategy, the BGP routers can customize routes for each neighbor flexibly. However it does not take into account the AS's selfishness. Besides, the above solutions did not discuss the pros and cons of neighbors' service performance during the operation of the BGP protocol, such as bandwidth, packet loss rate, jitter, and delay. Thus, studying the BGP neighbor trust establishment mechanism, which is easy to deploy and can provide security protection, has important theoretical value and practical significance.

Since the AS is a rational entity driven by customer needs, we can describe the BGP neighbor trust established as a cooperation between the AS and the adjacent AS on network service quality. This cooperation has the following characteristics: (1) In the process of cooperation, both the AS and the adjacent AS will pursue the maximization of interests, and there is a game of interests between them. (2) As the BGP neighbor establishment process is based on the Transmission Control Protocol (TCP), the AS and the adjacent AS can interact dynamically through a three-way handshake protocol. Based on these two characteristics, we propose a BGP Neighbor Trust Establishment Mechanism based on the Bargaining Game (BNTE-BG). The bargaining game [16–19] is a game process in which participants with common interests try to reach a consensus when facing conflict. During the game, the AS and the adjacent AS can flexibly negotiate bandwidth, packet loss rate, jitter, delay, and payment price according to their own preferences. When the negotiation is successful, the AS judges the adjacent AS as a trusted neighbor, and they establish a neighbor relationship. When the negotiation fails, the AS judges the adjacent AS as an untrusted neighbor, and they do not establish a neighbor relationship. When trusted neighbors start work, we draw on the gray correlation algorithm [20] to design a detection algorithm for evaluating its behavioral trust, that is, to detect whether the bandwidth, packet loss rate, jitter, and delay of the data traffic meet the negotiated agreement. Through the detection algorithm, we can detect malicious/inactive neighbors.

The main contributions of this paper are as follows: (1) We propose a BGP neighbor trust establishment mechanism based on the bargaining game, which allows an AS to select trusted neighbors that meet the network service quality. (2) We draw on the gray correlation algorithm to detect malicious/inactive BGP neighbors. The advantages of the above work are as follows: Using bargaining game theory, an AS can independently choose trusted neighbors according to its own security strategy; the services quality is guaranteed by negotiating service quality attributes such as bandwidth, packet loss rate, jitter, and delay; by detecting malicious/inactive neighbors, the loss of AS is effectively reduced.

The rest of the paper is organized as follows. In Section 2, we discuss research related to BGP security protection. Section 3 introduces the bargaining game model and proposes the BGP neighbor trust mechanism based on the bargaining game. Section 4 describes the detection mechanism of BGP malicious/inactive neighbors. In Section 5, we provide details of the simulated experiment and efficiency analysis. Finally, conclusions are drawn in Section 6.

2. Related Work

To date, there have been many studies on BGP security, which are mainly divided into BGP security extension and abnormal route detection. The main research results in BGP security extension are Secure BGP (S-BGP) [3], secure origin BGP (soBGP) [4], and pretty security (psBGP) [5]. The most complete and representative work is S-BGP. S-BGP

protocol uses digital certificates and digital signatures to verify the credibility of routing information. Although these solutions can effectively guarantee BGP security, they have not been implemented on the Internet due to difficulties in deployment.

Anomaly detection is one of the methods to protect BGP route security. The core work of anomaly detection is to diagnose and analyze the characteristics of abnormal behavior on the network, and then identify the abnormal behavior and information and send an alarm to the victim. The main research results in this field are Prefix Hijack Alert System (PHAS) [21] and iSPY [22]. Although anomaly detection can detect incorrect routes from route information, it cannot prevent malicious ASes from declaring untrusted routes again. The detection result also depends on the attack feature extraction algorithm and route data set, and there will be certain errors.

Simultaneously, more and more researchers have proposed methods to solve BGP security problems from the perspective of identifying trusted ASes. It is a feasible method besides security extension and anomaly detection. One study [10] shows that the reputation mechanism has an incentive effect, effectively reducing the propagation speed of false information and inhibiting deceptive behavior. The inter-domain routing system has the conditions to establish a reputation mechanism. Yu et al. [11] proposed a distributed reputation protocol for cooperation between ASes. The key idea is to simulate the trust relationship in the real world, where an AS can selectively receive information collected from neighbors. Konte et al. [12] proposed the AS reputation system, ASwatch, which can identify a malicious AS by monitoring the credibility of its behavior. Experimental results show that ASwatch can detect 93% of malicious ASes, and the false alarm rate is only 5%. Siganos [13] proposed a neighbor watch method, where ASes form a trusted group and monitor abnormal ASes by exchanging information and querying abnormal results. Literature [14] proposed the AS-TRUST mechanism. This analyzes the collected update messages and forms different types of feedback, and then uses the Bayes algorithm to calculate the reputation of a global AS.

Inter-domain trust technology is a lightweight solution with good implementation capability. At the same time, it can incentivize legitimate ASes to punish malicious ASes and improve overall inter-domain security. In recent years, it has received increasing attention from researchers

3. The BGP Neighbor Trust Mechanism Based on the Bargaining Game

3.1. Related Definitions

To facilitate the introduction of our mechanism, this section provides the relevant concepts and definitions.

Definition 1. *The service quality attribute vector is the attribute index used to describe the Quality of Service (QoS) and price. It comprises bandwidth, packet loss rate, jitter, delay, and price. We mark it as* $X = \{x_1, x_2, x_3, x_4, x_5\}$ *={bandwidth, packet loss rate, jitter, delay, price}. For attributes such as bandwidth, the larger they are, the better the QoS. We call them benefit attributes* x_i*. For attributes such as packet loss rate, jitter, and delay, the smaller they are, the better the QoS. We call them cost attributes* x_j*. To facilitate implementation, we classify the "price" attribute as the cost attribute.*

Definition 2. *The BGP trusted neighbor refers to neighbor routers that provide QoS, which is within the acceptable range.*

3.2. Bargaining Game Model

This section draws on the bargaining game model. The bargaining model is made of seven tuples of the form <*seller*, *buyer*, X^{acc}, X^{pro}, U_n, δ_n, T_n>. Here, *seller* represents the owner of the resource; *buyer* represents the requester of good QoS; X^{acc} represents the range of acceptable service quality attribute vector for the *buyer*; X^{pro} represents the range of service quality attribute vector that the *seller* can provide; U_n represents *buyer*'s or *seller*'s payoffs; δ_n represents *buyer* or *seller*'s negotiation ability; and T_n represents *buyer*'s

or *seller*'s number of quotations. A bargaining game consists of three steps—setup system parameter, quote, and dicker judgment—as follows:

1. Setup System Parameter. *buyer* sets the service quality attribute vector range X^{acc}. *seller* sets the service quality attribute vector range X^{pro}. X^{acc} and X^{pro} are private information and will not be disclosed to the public.
2. Quote. Within the number of quotations T_n, given X^{acc}/X^{pro}, δ_n and the current quotation number $t_n(t_n \leq T_n)$, *buyer*/*seller* generates the t_nth service quality attribute quotation vector $X^{(t_n)}$, $n \in \{seller,\ buyer\}$.
3. Dicker Judgment. Within the number of quotations T_n, given the service quality attribute quotation vector $X^{(t_n)}$, *buyer*/*seller* calculates the payoff U_n. When U_n is greater than or equal to the expected payoff, it outputs "True". The negotiation is successful and the game ends. When U_n is less than the expected payoff, it outputs "False". The negotiation continues.
4. If the *buyer* and *seller* fail to reach an agreement within the deadline, the negotiation ends.

3.3. BNTE-BG Mechanism

In the BGP neighbor establishment process, first, ASes with different AS numbers complete the TCP connection at the transport layer and then exchange the parameters through the Finite State Machine (FSM). We will combine the bargaining game model with the first stage of BGP neighbor establishment, proposing BNTE-BG. The mechanism process is as follows:

1. System Initialization. The BGP router sets the service quality attribute vector range X^{acc} and X^{pro} independently. $X^{acc} = \left[X^{acc}_{min},\ X^{acc}_{max}\right]$ represents the range of service quality attributes that the BGP router can accept. $X^{acc}_{min} = \left\{x^{acc}_{1min}, x^{acc}_{2min}, x^{acc}_{3min}, x^{acc}_{4min}, x^{acc}_{5min}\right\}$ represents the minimum value of each service quality attribute that can be accepted. $X^{acc}_{max} = \left\{x^{acc}_{1max}, x^{acc}_{2max}, x^{acc}_{3max}, x^{acc}_{4max}, x^{acc}_{5max}\right\}$ represents the maximum value of each service quality attribute that can be accepted. $X^{pro} = \left[X^{pro}_{min},\ X^{pro}_{max}\right]$ represents the range of service quality attributes that the BGP router can provide [23]. $X^{pro}_{min} = \left\{x^{pro}_{1min}, x^{pro}_{2min}, x^{pro}_{3min}, x^{pro}_{4min}, x^{pro}_{5min}\right\}$ represents the minimum value of each service quality attribute that can be provided. $X^{pro}_{max} = \left\{x^{pro}_{1max}, x^{pro}_{2max}, x^{pro}_{3max}, x^{pro}_{4max}, x^{pro}_{5max}\right\}$ represents the maximum value of each service quality attribute that can be provided. The specific settings are as follows:

$$\begin{cases} x^{acc}_{1min} \leq x_1 \leq x^{acc}_{1max} \\ x^{acc}_{2min} \leq x_2 \leq x^{acc}_{2max} \\ x^{acc}_{3min} \leq x_3 \leq x^{acc}_{3max} \\ x^{acc}_{4min} \leq x_4 \leq x^{acc}_{4max} \\ x^{acc}_{5min} \leq x_5 \leq x^{acc}_{5max} \end{cases} \qquad \begin{cases} x^{pro}_{1min} \leq x_1 \leq x^{pro}_{1max} \\ x^{pro}_{2min} \leq x_2 \leq x^{pro}_{2max} \\ x^{pro}_{3min} \leq x_3 \leq x^{pro}_{3max} \\ x^{pro}_{4min} \leq x_4 \leq x^{pro}_{4max} \\ x^{pro}_{5min} \leq x_5 \leq x^{pro}_{5max} \end{cases}$$

where x_1, x_2, x_3, x_4, and x_5 are defined as in Section 3.1.

Simultaneously, the BGP router sets u^{req} and u^{agr}. u^{req} is the neighbor trust establishment requester's expected payoff. u^{agr} is the neighbor trust establishment agreer's expected payoff.

2. The BGP Neighbor Trust Establishment Process. We suppose that AS_1 wants to establish a trusted neighbor relationship with its adjacent AS_2. AS_1 is the neighbor trust establishment requester, with the service quality attribute vector range $X^{acc}_{AS_1}$, the negotiation ability δ_{AS_1} and the expected payoff $u^{req}_{AS_1}$. AS_2 is the neighbor trust establishment agreer, with the service quality attribute vector range $X^{pro}_{AS_2}$, the negotiation ability δ_{AS_2}, and the expected payoff $u^{agr}_{AS_2}$. The number of quotations for AS_1/AS_2 is T_{AS_1}/T_{AS_2}. In order to better describe the process, we

take $T_{AS_1} = T_{AS_2} = 1$. The implementation of BNTE-BG is shown in Figure 1 and Algorithm 1:

Step 1: First, AS_1 initiates a neighbor trust establishment request to AS_2. It uses the service quality attribute vector range $X^{acc}_{AS_1}$, the current quotation number t_{AS_1} and the negotiation ability δ_{AS_1} to generate the service quality attribute quotation vector $X^{(1)}$ through the quote strategy function $Quote\_{req}$. Then AS_1 adds it to the TCP message and sends it to AS_2.

Step 2: When AS_2 receives the new TCP message from AS_1, it extracts the service quality attribute quotation vector $X^{(1)}$. It calculates the payoff, then judges whether AS_1's $X^{(1)}$ satisfy the expected payoff $u^{agr}_{AS_2}$. If it does, AS_2 outputs "Establish neighbor". If not, it uses the service quality attribute vector range $X^{pro}_{AS_2}$, the current quotation number t_{AS_2}, and the negotiation ability δ_{AS_2} to generate the service quality attribute quotation vector $X^{(1)}$ through the quote strategy function $Quote\_{agr}$. Then AS_2 adds it to the TCP message and sends to AS_1.

Step 3: When AS_1 receives the new TCP message from AS_2, it extracts the service quality attribute quotation vector $X^{(1)}$. It calculates the payoff, then judges whether AS_2's $X^{(1)}$ satisfy the expected payoff $u^{req}_{AS_1}$. If it does, AS_1 outputs "Establish neighbor". If not, it outputs "Establish neighbor failed".

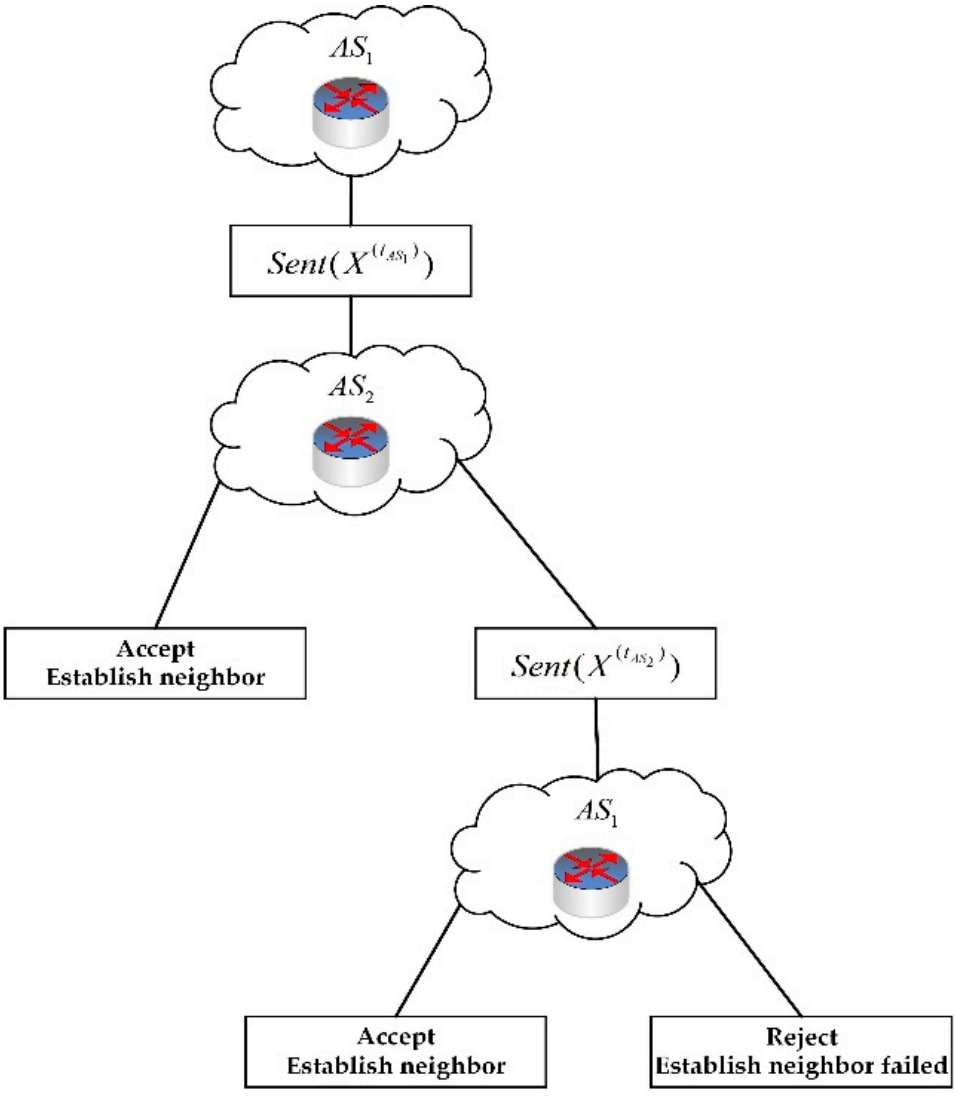

Figure 1. BNTE-BG flowchart.

The functions involved in Algorithm 1 are described as follows:

- *Send* indicates that the BGP router sends its service quality attribute quotation vector to the adjacent BGP router.
- $Quote\_req\left(X_{AS_1}^{acc}, t_{AS_1}, \delta_{AS_1}\right)$ indicates that AS_1 performs t_{AS_1}th quotation to generate the service quality attribute quotation vector $X^{(t_{AS_1})}$.
- $Quote\_agr\left(X_{AS_2}^{pro}, t_{AS_2}, \delta_{AS_2}\right)$ indicates that AS_2 performs t_{AS_2}th quotation to generate the service quality attribute quotation vector $X^{(t_{AS_2})}$.
- $U\_req\left(X^{(t_{AS_2})}, X_{AS_1}^{acc}\right)$ indicates that AS_1 obtains the payoff accepting the service quality attribute quotation vector $X^{(t_{AS_2})}$.
- $U\_agr\left(X^{(t_{AS_1})}, X_{AS_2}^{pro}\right)$ indicates that AS_2 obtains the payoff accepting the service quality attribute quotation vector $X^{(t_{AS_1})}$.
- $Dick(U, u)$ indicates that AS_1/AS_2 determines whether to establish a neighbor relationship.

Algorithm 1: BNTE-BG establishment

Input: AS_1, AS_2, T_{AS_1}, T_{AS_2}, $X_{AS_1}^{acc}$, $X_{AS_2}^{pro}$, δ_{AS_1}, δ_{AS_2}, $u_{AS_1}^{req}$, $u_{AS_2}^{agr}$
Output: Establish neighbor, Establish neighbor failed

1: $t_{AS_1} = 1, t_{AS_2} = 1$;
2: if $(t_{AS_1} \leq T_{AS_1})$
3: {
4: $X^{(t_{AS_1})} \leftarrow Quote\_req\left(X_{AS_1}^{acc},\ t_{AS_1}, \delta_{AS_1}\right)$;
5: $t_{AS_1} = t_{AS_1} + 1$;
6: AS_1 send $(X^{(t_{AS_1})})$ to AS_2;
7: go 17;
8: }
9: else
10: output Establish neighbor failed;
11: $AS_1\ U_{req} \leftarrow U\_req\left(X^{(t_{AS_2})}, X_{AS_1}^{acc}\right)$;
12: $a \leftarrow Dick\left(U_{req}, u_{AS_1}^{req}\right)$;
13: if $(a = true)$
14: output Establish neighbor
15: else
16: go 2;
17: $AS_2\ U_{agr} \leftarrow U\_agr\left(X^{(t_{AS_1})}, X_{AS_2}^{pro}\right)$;
18: $a \leftarrow Dick\left(U_{agr}, u_{AS_2}^{agr}\right)$;
19: if $(a = true)$
20: output Establish neighbor;
21: else if $(t_{AS_2} \leq T_{AS_2})$
22: {
23: $X^{(t_{AS_2})} \leftarrow Quote\_agr\left(X_{AS_2}^{pro},\ t_{AS_2}, \delta_{AS_2}\right)$;
24: $t_{AS_2} = t_{AS_2} + 1$;
25: AS_2 send $(X^{(t_{AS_1})})$ to AS_1;
26: go 11;
27: }
28: else
29: output Establish neighbor failed

3.4. Implementation of BNTE-BG Mechanism

This section explains the implementation of the functions in the BNTE-BG. AS_1 and AS_2 call $Quote\_req\left(X_{AS_1}^{acc}, t_{AS_1}, \delta_{AS_1}\right)$, $Quote\_agr\left(X_{AS_2}^{pro}, t_{AS_2}, \delta_{AS_2}\right)$, $U\_req\left(X^{(t_{AS_2})}, X_{AS_1}^{acc}\right)$, $U\_agr\left(X^{(t_{AS_1})}, X_{AS_2}^{pro}\right)$, and $Dick(U, u)$. The implementation of the functions is as follows:

- The quote strategy function $Quote\_req\left(X_{AS_1}^{acc}, t_{AS_1}, \delta_{AS_1}\right)$ is implemented as follows:

When AS_1 wants to send the t_{AS_1}th quotation to AS_2, it calls $Quote\_req\left(X_{AS_1}^{acc}, t_{AS_1}, \delta_{AS_1}\right)$ to generate the t_{AS_1}th service quality attribute quotation vector $X^{(t_{AS_1})} = \left\{x_1^{(t_{AS_1})}, x_2^{(t_{AS_1})}, x_3^{(t_{AS_1})}, x_4^{(t_{AS_1})}, x_5^{(t_{AS_1})}\right\}$.

Calculate the benefit attribute quotation $x_i^{(t_{AS_1})}$ as Formula (1)

$$x_i^{(t_{AS_1})} = x_{imax_{AS_1}}^{\text{acc}} - \left[k + (1-k) * \left(\frac{t_{AS_1}}{T_{AS_1}}\right)^{\delta_{AS_1}}\right] * \left(x_{imax_{AS_1}}^{\text{acc}} - x_{imin_{AS_1}}^{\text{acc}}\right) \tag{1}$$

Calculate the cost attribute quotation $x_j^{(t_{AS_1})}$ as Formula (2)

$$x_j^{(t_{AS_1})} = x_{jmin_{AS_1}}^{acc} + \left[k + (1-k) * \left(\frac{t_{AS_1}}{T_{AS_1}}\right)^{\delta_{AS_1}}\right] * \left(x_{jmax_{AS_1}}^{acc} - x_{jmin_{AS_1}}^{acc}\right) \tag{2}$$

where $i + j = 5$, $0 < \delta_{AS_1} < 1$, $0 < k < 1$, concession factor k, and δ_{AS_1} are set by AS_1.

- The quote strategy function $Quote\_agr\left(X_{AS_2}^{pro}, t_{AS_2}, \delta_{AS_2}\right)$ is implemented as follows:

When AS_2 wants to send the t_{AS_2}th quotation to AS_1, it calls $Quote\_agr\left(X_{AS_2}^{pro}, t_{AS_2}, \delta_{AS_2}\right)$ to generate the t_{AS_2}th service quality attribute quotation vector $X^{(t_{AS_2})} = \left\{x_1^{(t_{AS_2})}, x_2^{(t_{AS_2})}, x_3^{(t_{AS_2})}, x_4^{(t_{AS_2})}, x_5^{(t_{AS_2})}\right\}$.

Calculate the benefit attribute quotation $x_i^{(t_{AS_2})}$ as Formula (3)

$$x_i^{(t_{AS_2})} = x_{imin_{AS_2}}^{pro} + \left[k + (1-k) * \left(\frac{t_{AS_2}}{T_{AS_2}}\right)^{\delta_{AS_2}}\right] * \left(x_{imax_{AS_2}}^{pro} - x_{imin_{AS_2}}^{pro}\right) \tag{3}$$

Calculate the cost attribute quotation $x_j^{(t_{AS_2})}$ as Formula (4)

$$x_j^{(t_{AS_2})} = x_{jmax_{AS_2}}^{pro} - \left[k + (1-k) * \left(\frac{t_{AS_2}}{T_{AS_2}}\right)^{\delta_{AS_2}}\right] * \left(x_{jmax_{AS_2}}^{pro} - x_{jmin_{AS_2}}^{pro}\right) \tag{4}$$

where $i + j = 5$, $0 < \delta_{AS_2} < 1$, $0 < k < 1$, concession factor k, and δ_{AS_2} are set by AS_2.

- The payoff function $U\_agr\left(X^{(t_{AS_1})}, X_{AS_2}^{pro}\right)$ and dicker judgment function $Dick(U, u)$ are implemented as follows:

When AS_2 receives the service quality attribute quote vector $X^{(t_{AS_1})}$, it calls $Dick(U, u)$ to judge whether to establish a neighbor relationship.

Step 1: Call $U\_agr\left(X^{(t_{AS_1})}, X_{AS_2}^{pro}\right)$ function to generate the total payoff U_{agr}.

For the benefit attribute x_i, the payoff of AS_2 is calculated as Formula (5)

$$\Delta x_{i_{AS_2}} = x_i^{t_{AS_1}} - x_{imin_{AS_2}}^{pro} \tag{5}$$

For the cost attribute x_j, the payoff of AS_2 is calculated as Formula (6)

$$\Delta x_{j_{AS_2}} = x_{jmax_{AS_2}}^{pro} - x_j^{t_{AS_1}} \tag{6}$$

Standardized processing: $\Delta v_{i_{AS_2}} = \frac{\Delta x_{i_{AS_2}}}{x_{imax_{AS_2}}^{pro} - x_{imin_{AS_2}}^{pro}}$; $\Delta v_{j_{AS_2}} = \frac{\Delta x_{j_{AS_2}}}{x_{jmax_{AS_2}}^{pro} - x_{jmin_{AS_2}}^{pro}}$

Calculate the total payoff of AS_2 as Formula (7)

$$U_{arg} = \sum_{e=1}^{5} \Delta v_{e_{AS_2}} * w''_e \tag{7}$$

where $W'' = \{w''_1, w''_2, w''_3, w''_4, w''_5\}$ represents AS_2's private preference for service quality attributes. It is set by AS_2.

Step 2: Call $Dick\left(U_{agr}, u^{agr}_{AS_2}\right)$ to determine whether to establish a neighbor relationship.

$$Dick\left(U_{agr}, u^{agr}_{AS_2}\right) = \begin{cases} U_{agr} - u^{agr}_{AS_2} \geq 0\,; & \text{output ``Establish neighbor''} \\ U_{agr} - u^{agr}_{AS_2} < 0,\ t_{AS_2} \leq T_{AS_2}; & \text{Continue negotiation} \\ U_{agr} - u^{agr}_{AS_2} < 0\,; & \text{output'' Establish neighbor failed''} \end{cases}$$

- The payoff function $U\_{req}\left(X^{(t_{AS_2})}, X^{acc}_{AS_1}\right)$ and dicker judgment function $Dick(U, u)$ are implemented as follows:

When AS_1 receives the service quality attribute quote vector $X^{(t_{AS_2})}$, it calls $Dick(U, u)$ to judge whether to establish a neighbor relationship.

Step 1: Call $U\_{req}\left(X^{(t_{AS_2})}, X^{pro}_{AS_2}\right)$ function to generate the total payoff U_{req}.

For benefit attribute x_i, the payoff of AS_1 is calculated as Formula (8)

$$\Delta x_{i_{AS_1}} = x^{\text{acc}}_{imax_{AS_1}} - x_i^{t_{AS_2}} \tag{8}$$

For cost attribute x_j, the payoff of AS_1 is calculated as Formula (9)

$$\Delta x_{j_{AS_1}} = x_j^{t_{AS_2}} - x^{acc}_{jmin_{AS_1}} \tag{9}$$

Standardized processing: $\Delta v_{i_{AS_1}} = \frac{\Delta x_{i_{AS_1}}}{x^{\text{acc}}_{imax_{AS_1}} - x^{\text{acc}}_{imin_{AS_1}}}$; $\Delta v_{j_{AS_1}} = \frac{\Delta x_{j_{AS_1}}}{x^{\text{acc}}_{jmax_{AS_1}} - x^{\text{acc}}_{jmin_{AS_1}}}$

Calculate the total payoff of AS_1 as Formula (10)

$$U_{req} = \sum_{e=1}^{5} \Delta v_{e_{AS_1}} * w'_e \tag{10}$$

where $W' = \{w'_1, w'_2, w'_3, w'_4, w'_5\}$ represents AS_1's private preference for service quality attributes, It is set by AS_1.

Step 2: Call $Dick\left(U_{req}, u^{req}_{AS_1}\right)$ to determine whether to establish a neighbor relationship.

$$Dick\left(U_{req}, u^{req}_{AS_1}\right) = \begin{cases} U_{req} - u^{req}_{AS_1} \geq 0\,; & \text{output ``Establish neighbor''} \\ U_{req} - u^{req}_{AS_1} < 0,\ t_{AS_1} \leq T_{AS_1}; & \text{Continue negotiation} \\ U_{req} - u^{req}_{AS_1} < 0\,; & \text{output'' Establish neighbor failed''} \end{cases}$$

Therefore, as long as AS follows the BNTE-BG mechanism during the neighbor establishment process, it can be guaranteed to establish a neighbor relationship with the trusted AS. The quote strategy function is based on the premise that AS is rational and willing to cooperate.

4. The Detection Mechanism of the BGP Malicious/Inactive Neighbors

This section mainly presents the detection algorithm of AS and the BGP malicious/inactive neighbors' detection process.

Definition 3. *Behavioral trust is the credibility of BGP neighbors' behavior when trusted neighbors forward data every time, denoted by* γ $(0 < \gamma \leq 1)$.

Detection Process

Let us assume AS_1 and AS_2 have established a trusted neighbor relationship through the process described in Section 3. $X^{succ} = \{x_1^{succ}, x_2^{succ}, x_3^{succ}, x_4^{succ}, x_5^{succ}\}$ represents their agreement on bandwidth, packet loss rate, jitter, delay, and price. At this time, AS_1 needs to calculate AS_2's behavioral trusts and checks whether it is a malicious/inactive neighbor. The specific process is as follows:

Step 1: AS_1 collects the data set of bandwidth, packet loss rate, jitter, and delay when AS_2 forwards AS_1 traffic T times. The data set is marked as $[X]_{\mathrm{T}} = \{X^1, X^2 \ldots X^T\}$.

Step 2: AS_1 draw on the gray correlation algorithm to calculate the AS_2's behavioral trust γ_T. Since x_2, x_3, and x_4 are the cost attributes, to facilitate calculation, we use the worst packet loss rate R, the largest jitter J, and the longest delay D in the actual network to process data with the same attributes in the data set $[X]_{\mathrm{T}}$. The detection algorithm is Algorithm 2.

Step 3: If behavioral trusts are all within the normal range, AS_1 and AS_2 continue to maintain the trusted neighbor relationship. If the behavioral trust γ_T appears abnormal, go to Step4.

Step 4: AS_1 sends a warning to AS_2 and sets the number of forwarding Δ T . AS_1 continues to calculate the AS_2's behavioral trusts when it forwards ΔT times.

Step 5: If behavioral trusts are all within the normal range, AS_1 and AS_2 continue to maintain the trusted neighbor relationship. If $\gamma_{\Delta \mathrm{T}}$ still appears abnormal, AS_1 judges AS_2 as the malicious/inactive neighbor. Then, AS_1 stops paying AS_2 and filters the routing information announced/forwarded by AS_2.

Algorithm 2: Detection algorithm

Input: X^{succ}, $[X]_T$, R, J, D
Output: γ_{AS_2}

x_1^{succ1}=x_1^{succ}; x_2^{succ1}=R-x_2^{succ}; x_3^{succ1}=J-x_3^{succ}; x_4^{succ1}=D-x_4^{succ};
for (i =1; i<=T; i++)
{
if ($x_1^i \geq x_1^{succ}$&& $x_2^i \leq x_2^{succ}$ && $x_3^i \leq x_3^{succ}$&& $x_4^i \leq x_4^{succ}$)
output $\gamma_{AS_2}^i$= 1;
else
{
x_2^i= R-x_2^i; x_3^i=J-x_3^i; x_4^i=D-x_4^i;
for (j=1; j<=4; j++)
{

$$\gamma_{AS_2}^{ij} = \frac{\min\limits_i \min\limits_j \left|x_j^{succ1} - x_j^i\right| + \theta \max\limits_i \max\limits_j \left|x_j^{succ1} - x_j^i\right|}{\left|x_j^{succ1} - x_j^i\right| + \theta \max\limits_i \max\limits_j \left|x_j^{succ1} - x_j^i\right|}$$

}
output $\gamma_{AS_2}^i = \frac{1}{4} \sum \gamma_{AS_2}^{ij}$;
}
}

5. Simulation and Efficiency Analysis

This section mainly discusses the efficiency of the BNTE-BG mechanism and the detection algorithm's correctness. In terms of correctness, we mainly investigate whether the detection algorithm can correctly describe neighbors' behavior. In terms of efficiency, we consider storage increment and average convergence time. Storage increment includes the message increment and storage overhead. In terms of route average convergence time, we mainly consider the number of neighbor establishments, the number of quotations and the time spent, and the number of dicker judgments and the time spent.

5.1. Correctness

Correctness means that the detection algorithm can effectively describe whether the trusted neighbor's behaviors meet the negotiation agreement. The AS can judge malicious/inactive neighbors by the detection result. The experimental scene settings are as follows: the neighbor trust establishment requester AS_1 and the neighbor trust establishment agreer AS_2 have successfully established a trusted neighbor relationship through the BNTE-BG mechanism, and AS_2 has forwarded data $T = 7$ times. Negotiation agreement is $X^{succ} = \{x_1^{succ}, x_2^{succ}, x_3^{succ}, x_4^{succ}, x_5^{succ}\}$ = {50, 0.1, 15, 60, 300}. R = 1, J = 200 ms, D = 500 ms, $\theta = 0.3$. Table 1 shows the data set collected by AS_1.

Table 1. Data set collected by AS_1.

Serial Number	Bandwidth/G	Packet Loss Rate	Jitter/ms	Delay/ms
1	50	0	10	40
2	52	0.05	13	45
3	53	0.2	25	70
4	40	0.1	16	50
5	45	0.5	113	172
6	7	0.7	148	230
7	5	0.9	156	389

Figure 2 shows the changes in AS_2's behavioral trusts, which are (1, 1, 0.8331, 0.8729, 0.4998, 0.3126, 0.2557). In the first and second forwardings, AS_2's service fully meets the negotiation agreement, and the behavioral trusts are 1. In the third, fourth, and fifth forwardings, the service provided by AS_2 could not fully meet the negotiation agreement. Among them, in the third and fourth forwardings, the service provided by AS_2 is not much different from the negotiation agreement, and AS_2's behavioral trusts are greater than 0.8. In the fifth forwarding, the AS_2's service is too far away from the negotiation agreement, and the behavioral trust is less than 0.5. In the sixth and seventh forwardings, the AS_2's service completely deviates from the negotiation agreement, and the behavioral trusts are only about 0.3. During the entire period, the quality of services provided by AS_2 gradually declined, and AS_2's behavioral trusts also gradually decreased. The results show that our detection algorithm can effectively characterize the behavior of AS_2. When AS_1 detects that the sixth and seventh time's behavior trusts are too low, it could issue a warning to AS_2 to further verify whether it is a malicious neighbor. The AS_1 can also analyze the bandwidth and packet loss rate of the sixth and seventh forwarding to determine whether the AS_2 is a malicious/inactive neighbor. Due to the limited length of this paper, no more experiments will be carried out.

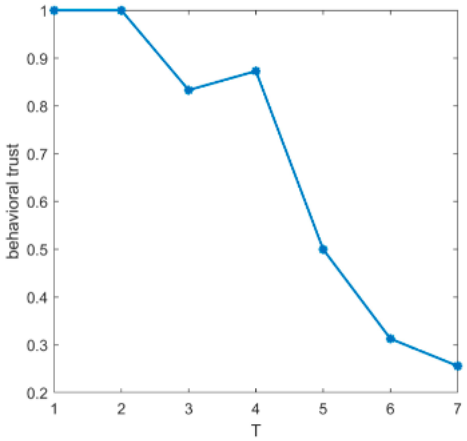

Figure 2. The behavioral trust of AS_2.

5.2. Storage Increment

First, we consider the increase in the TCP message's length after adding the BNTE-BG mechanism. Because the BNTE-BG mechanism adds service quality attribute negotiation to the first stage of neighbor establishment, it is necessary to add a service quality attribute quotation vector to the TCP message, which will cause message expansion. The service quality attributes contain the bandwidth, packet loss rate, delay, jitter, and price. Each attribute occupies one byte. Therefore, the TCP message's length in the BNTE-BG mechanism is 5 bytes longer than that of the BGP.

Secondly, in storage overhead, the AS guarantees data service quality by negotiating with the adjacent AS in BNTE-BG. Therefore, each BGP router only needs 20 bytes to store the service quality attribute vector range (X^{acc} and X^{pro}). Table 2 shows us the storage increment of the BNTE-BG mechanism.

Table 2. Storage increment of BNTE-BG.

	Storage Overhead Per Router/Byte	**Packet Length Increment/Byte**
BNTE-BG	20	5

From Table 2, we can see that the storage increment of the BNTE-BG mechanism is very small, so the burden on BGP routers will not be great.

5.3. Average Convergence Time

In the BNTE-BG mechanism, we add the service quality attribute quotations and payoffs calculations during the TCP three-way handshake, which will cause a time delay. Therefore, adding the BNTE-BG mechanism to the BGP will have an impact on the convergence time. The average convergence time is related to the number of neighbor establishment instances #*sum*, the number of quotations #*quote*, the time spent in quotation calculation t_{quote}, the number of dicker judgments #*dick*, and the time spent in dicker judgment t_{dick}, etc. Assuming that the number of ASes in the network topology is N, the maximum number of neighbor establishment times are $\#sum = \frac{N*(N-1)}{2}$, $N \geq 2$. In the BGP protocol neighbor establishment process, after the TCP connection is completed at the transport layer, it needs to exchange parameters through FSM. If exchanging parameters fails, the neighbor establishment will fail. Thus, a successful neighbor establishment has a probably. Assuming that the probability of a successful FSM is p, then the convergence time increment model is as follows:

$$\Delta\text{Time} = \text{p}*\#\text{sum}*\left(\#\text{quote} * \text{t}_{\text{quote}} + \#\text{dick} * \text{t}_{\text{dick}}\right),$$

where $\Delta Time$ represents the increase in convergence time after adding the BNTE-BG mechanism to the BGP.

Before the average convergence time experiment, we analyze the influence of concession factor k, the negotiation ability δ and, the number of quotations T on $k + (1-k) * (t/T)^{\delta}$ representing the concession of AS.

By setting δ = 0.8, we respectively examined the changes of $k + (1-k) * (t/T)^{\delta}$ under k = 0.1, k = 0.5, and k = 0.9.

The experimental results are shown in Figure 3; the greater the value of k, the greater the concession that AS will make, but the lower the concession rate.

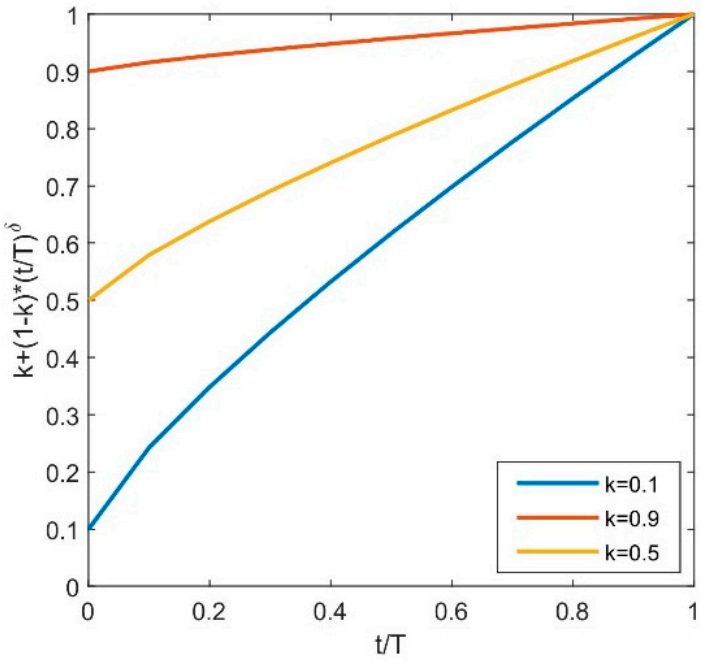

Figure 3. The influence of concession factor k on $k + (1 - k) * (t/T)^{\delta}$.

By setting k = 0.4, we respectively examined the changes of $k + (1 - k) * (t/T)^{\delta}$ under $T = 3$, $T = 5$ and $T = 7$.

The experimental results are shown in Figure 4; the fewer the number of quotations, the greater the concession and concession rate of AS.

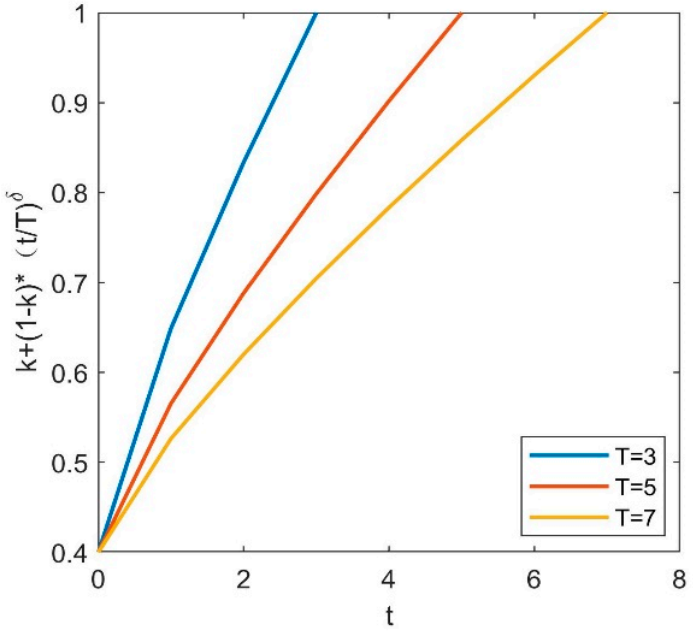

Figure 4. The influence of the number of quotations T on $k + (1 - k) * (t/T)^{\delta}$.

We set $k = 0.4$ and examined the changes of $k + (1 - k) * (t/T)^{\delta}$ under $\delta = 0.1$, $\delta = 0.5$, and $\delta = 0.9$.

The experimental results are shown in Figure 5; the greater the value of δ, the greater the concession that AS will make. When $\delta = 0.1$, $k + (1 - k) * (t/T)^{\delta}$ initially increases rapidly and then tends to level off. When $\delta = 0.9$, $k + (1 - k) * (t/T)^{\delta}$ increases at a steady speed. Therefore, AS can be divided into two types. When $0 < \delta < 0.5$, the AS is eager to

establish neighbor relations. When $0.5 \leq \delta < 1$, the AS is calm and has enough patience to negotiate.

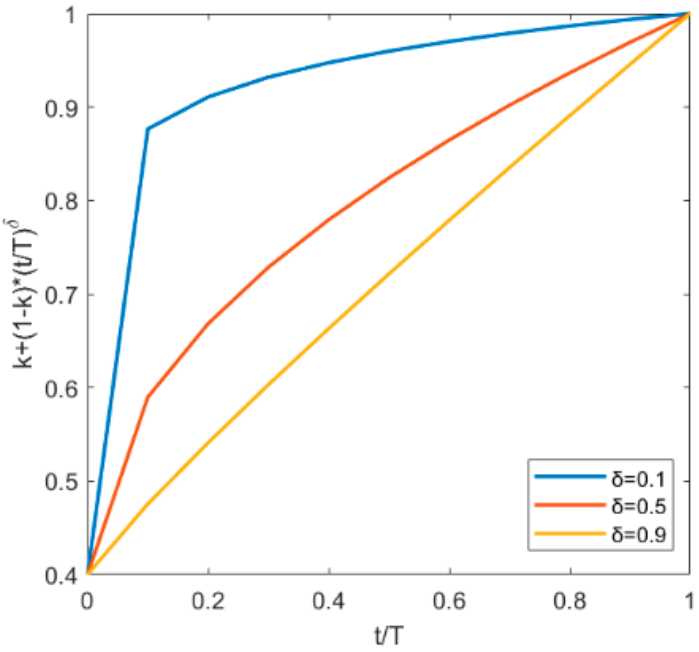

Figure 5. The influence of negotiation ability δ on $k + (1 - k) * (t/T)^{\delta}$.

In the average convergence time experiment, we use the CAIDA IPv4 Routed/24 Topology Dataset [24] and extract some subgraphs from it for experiments. The specific parameters were set as follows: the link delay was 0.6 s, $p = 0.9$, $\delta = 0.7$, $k = 0.5$, and $T = 3$. The purpose of the experiment is to investigate the changes in the average convergence time of BNTE-BG, BGP, and NS-BGP mechanisms as the size of the AS topology changes. The experimental results are shown in Figure 6.

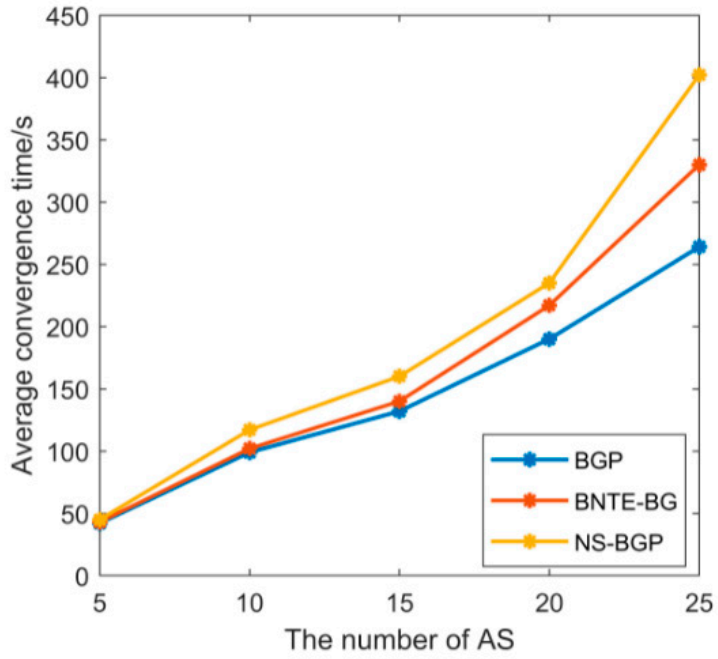

Figure 6. Average convergence time.

As the topology's scale expands and the number of neighbor establishments increases, the average convergence time of the BNTE-BG mechanism, BGP, and NS-BGP mechanism gradually increases. At the same time, the convergence speed of the BNTE-BG mechanism and the NS-BGP mechanism decreases. Because the BNTE-BG mechanism adds quotations and payoffs calculations during the neighbor establishment phase, the average convergence time is longer than that of the BGP. NS-BGP needs a special route for each neighbor, and the average convergence time will be longer than that of the BGP. Unlike NS-BGP, which requires special calculations for the needs of each neighbor, the BNTE-BG mechanism only needs to negotiate at a fixed time, so the average convergence time of the BNTE-BG mechanism is less than that of NS-BGP. Experimental results show that the BNTE-BG mechanism has better convergence than the NS-BGP mechanism.

6. Conclusions

The secure establishment of neighbors in the BGP is an important issue of BGP security. Research resources are scarce, and an easily deployed neighbor trust establishment mechanism is still an important research direction. Therefore, this paper proposes a BGP neighbor trust establishment mechanism based on the bargaining game, BNTE-BG, which combines the bargaining game model with bandwidth, delay, jitter, packet loss rate, and price. It allows ASes to choose trusted neighbors that meet route security requirements flexibly and ultimately achieves network security. When the trusted neighbor is working, we use the gray correlation algorithm to calculate the behavioral trust of the trusted neighbor, and effectively detect malicious/inactive neighbors. The BNTE-BG mechanism has the advantages of less storage increment, less modification of the BGP protocol content, and easier implementation in networks with complex business relationships. Based on analysis of correctness experiments, the detection algorithm can effectively detect malicious/inactive neighbors. Our future research will further expand the service quality attributes, such as adding the attribute "geographic location", so that ASes can select trusted neighbors in more detail.

Author Contributions: Conceptualization, P.L. and D.L.; methodology, P.L.; software, P.L. and D.L.; validation, D.L. and B.L.; formal analysis, P.L. and B.L.; investigation, P.L.; data curation, P.L. and B.L.; writing—original draft preparation, P.L.; writing—review and editing, P.L. and D.L.; project administration, D.L.; funding acquisition, D.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No.61662004).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rekhter, Y.; Li, T.; Hares, S. A Border Gateway Protocol 4 (BGP-4). Network Working Group. 2006. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc4271.txt.pdf (accessed on 10 May 2020).
2. Murphy, S. BGP Security Vulnerabilities Analysis. Network Working Group. 2006. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc4227.txt.pdf (accessed on 15 May 2020).
3. White, R. Securing BGP through secure origin BGP (soBGP). *Bus. Commun. Rev.* **2003**, *6*, 15–22.
4. Kent, S.; Lynn, C.; Seo, K. Secure border gateway protocol (S-BGP). *IEEE J. Sel. Areas Commun.* **2000**, *18*, 582–592. [CrossRef]
5. Oorschot, P.C.; Wan, T.; Kranakis, E. On interdomain routing security and pretty secure BGP (psBGP). *ACM TOPS* **2007**, *10*. [CrossRef]
6. Liu, Y.; Deng, W.; Liu, Z.; Huang, F. 3S: Three-signature path authentication for BGP security. *Secur. Commun. Netw.* **2015**, *18*, 3002–3014. [CrossRef]
7. Xing, Q.; Wang, B.; Wang, X. Blockchain-based internet number resource authority and bgp security solution. *Symmetry* **2018**, *10*, 408. [CrossRef]
8. Gao, L.; Rexford, J. Stable Internet routing without global coordination. *IEEE-ACM Trans. Netw.* **2001**, *9*, 681–692.
9. Teixeira, R.; Shaikh, A.; Griffin, T.G.; Rexford, J. Impact of hot-potato routing changes in IP networks. *IEEE-ACM Trans. Netw.* **2008**, *16*, 1295–1307. [CrossRef]
10. Resnick, P.; Zeckhauser, R.; Friedman, E.; Kuwabara, K. Reputation systems: Facilitating trust in Internet interactions. *Commun. ACM* **2000**, *43*, 45–48. [CrossRef]

11. Yu, H.; Rexford, J.; Felten, E.W. A distributed reputation approach to cooperative internet routing protection. In Proceedings of the 1st IEEE ICNP Workshop on Secure Network Protocols, 2005. (NPSec), Boston, MA, USA, 6 November 2005; pp. 73–78.
12. Konte, M.; Perdisci, R.; Feamster, N. Aswatch: An as reputation system to expose bulletproof hosting ases. In Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, London, UK, 17–21 August 2015; Association for Computing Machinery: New York, NY, USA, 2015.
13. Siganos, G.; Faloutsos, M. Neighborhood watch for internet routing: Can we improve the robustness of internet routing today? In Proceedings of the IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, Barcelona, Spain, 6–12 May 2007.
14. Chang, J.; Venkatasubramanian, K.K.; West, A.G.; Kannan, S.; Loo, B.T.; Sokolsky, O.; Lee, I. *AS-TRUST: A Trust Quantification Scheme for Autonomous Systems in BGP. International Conference on Trust and Trustworthy Computing*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 262–276.
15. Wang, Y.; Schapira, M.; Rexford, J. Neighbor-specific BGP: More flexible routing policies while improving global stability. In Proceedings of the Eleventh International Joint Conference on Measurement and Modeling of Computer Systems, Seattle, WA, USA, 15–19 June 2009; Association for Computing Machinery: New York, NY, USA, 2009; pp. 217–228.
16. Rubinstein, A. Perfect equilibrium in a bargaining model. *Econometrica* **1982**, *50*, 97–109. [CrossRef]
17. Njilla, L.Y.; Pissinou, N. Dynamics of data delivery in mobile ad-hoc networks: A bargaining game approach. In Proceedings of the 2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), Verona, NY, USA, 26–28 May 2015; pp. 1–6.
18. Liu, C.; Li, K.; Tang, Z. Bargaining game-based scheduling for performance guarantees in cloud computing. *ACM TOMPECS* **2018**, *3*, 1–25. [CrossRef]
19. Li, P.; Han, B.; Li, H.; Hou, D.; Liu, D.; Wang, G. The Research of Dynamic Spectrum Allocation Based on Nash Bargaining Game. In Proceedings of the 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 26–28 May 2018; pp. 70–74.
20. Sun, G.; Guan, X.; Yi, X.; Zhou, Z. Gray relational analysis between hesitant fuzzy sets with applications to pattern recognition. *Expert Syst. Appl.* **2018**, *92*, 521–532. [CrossRef]
21. Lad, M.; Massey, D.; Pei, D.; Wu, Y.; Zhang, B.; Zhang, L. PHAS: A Prefix Hijack Alert System. In Proceedings of the USENIX Security Symposium, Vancouver, BC, Canada, 31 July–4 August 2006.
22. Zhang, Z.; Zhang, Y.; Hu, Y.C. iSPY: Detecting IP prefix hijacking on my own. *IEEE-ACM Trans. Netw.* **2010**, *18*, 1815–1828. [CrossRef]
23. Li, J.; Luo, H.; Zhang, S.; Li, H.; Yan, F. Design and implementation of efficient control for incoming inter-domain traffic with information-centric networking. *J. Netw. Comput. Appl.* **2019**, *133*, 109–125. [CrossRef]
24. The CAIDA Internet Topology Data Kit. 2019.01. Available online: https://www.caida.org/data/internet-topology-data-kit (accessed on 3 March 2021).