Network Working Group   Z. Du
Internet-Draft   P. Liu
Intended status: Informational   China Mobile
Expires: July 4, 2022   December 31, 2021

~~Gateway~~ Gateway-~~Based~~ based Trust Relationship Between ~~the~~ Endpoints and ~~the~~ Intermediate Nodes

draft-du-panrg-gateway-based-trust-relationship-01

Abstract

This document describes a mechanism about establishing trust relationship between ~~the~~ an endpoint and ~~the~~ an intermediate node along the path and which involves ~~based on~~ ~~the~~ a gateway that services ~~of~~ the endpoint.

Commenté [BMI1]: An endpoint may interact with more than one intermediate node.

Commenté [BMI2]: There might be many “gateways” (e.g., multihoming with distinct gateways)

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft will expire on July 4, 2022.

Copyright Notice

Table of Contents

1. Introduction

~~In future, m~~Many new services ~~would emerge in the network,~~are considered such as the 5G URLLC (Ultra Reliable Low Latency Communication) service~~,~~ and the holographic type communications. Many of these new services need ~~a higher~~ strict traffic performance guarantees (including QoS (Quality of Service)). Such guarantees are usually captured in specific ~~level than the current Internet services, and some of them have a critical~~ SLAs (Service-Level Agreements) ~~requirement~~. The SLA differences between the new services and traditional services would become larger and lager. However, current networks can only provide the Best Effort bearing, in which all the traffic ~~are~~ is treated as the same kind. ~~In summary, c~~Current networks are short of negotiation abilities between the network and the applications. PANRG in the IRTF has proposed a research direction to enable the path aware networking. A lot of analyses have been done in the [RFC9049], which explains reasons why various Path Aware techniques have seen limited or no deployment.

One of the reasons is that it is hard to establish a trust relationship between ~~the~~ an ~~Endpoint~~ endpoint and an i~~I~~ntermediate ~~Node~~node. ~~In the current network structure,~~When establishing a communication, ~~the~~ ~~E~~endpoints only needs to be aware of ~~the~~ each other, and assume that the network can ~~provide a good connection service for them~~deliver packets between them. On the other hand, traditionally, ~~Intermediate~~ intermediate ~~Nodes~~ nodes only need to support IP forwarding and do not need to be aware of up-layer information. In addition, the network nodes work in a per-packet model, not a per-flow model. Also in the [RFC9049], it is said that "per-connection state in intermediate nodes has been an impediment to adoption and deployment".

However, we can find that the gateway of the Endpoint is able to maintain a per-connection state and a trust-relationship for each

Commenté [BMI3]: Not sure to parse this. The clauses in the SLA are likely to be the same, what differs are the committed values that may be more constraining.

Commenté [BMI4]: I'm afraid this is not true as many classes of service are already in use in many networks.

Commenté [BMI5]: I think I see the intent here (expose capabilities, capture application, requirement, negotiate and commit). However, I suggest you elaborate further and explicit the intent.

Also, how this is addressed in the draft?

Commenté [BMI6]: Not only. Please refer to the definition of node in draft-irtf-panrg-path-properties

Mis en forme : Surlignage

Commenté [BMI7]: To be defined.

user. For example, the users in the fixed network need to be authorized by the BNG (Broadband Network Gateway), and the BNG also needs to do the accounting for each user. It is hard and unnecessary to make every intermediate node along the path has the same ability as the BNG; however, if they can have some communication with the BNG, perhaps they can make a better path choice for the user. Following this direction, this document proposes a mechanism about how to enable the communication between the BNG and ~~the~~ a Head-End node in the network, because the Head-End node is the main node to select the path for a flow in the network. If any future work on the trust relationship between the Endpoint and the Intermediate Node is considered, the mechanism in this document can be a reference.

Mis en forme : Surlignage

Commenté [BMI8]: To be defined.

Commenté [BMI9]: Not sure I would maintain this text.

2. Proposed Mechanism for the Trust Problem

As shown in the Figure 1, in the fixed network, the BNG works as the gateway for the Client, and provides the ~~Internet connection~~ connectivity service for the Applications. The Client and Server are the EndPoints, and the BNG, Head-End, Mid-Node, End-Node are the nodes along the path from the Client to the Server. There are three paths, i.e., A, B, C, with different properties such as high bandwidth or low latency, between the Head-End and the End-Node in the network.

By default, all the traffic from the APPs are forwarded from the Head-End to the End-Node with the same treatment in the network. In the Head-end, perhaps a load balance mechanism can be enabled, but normally without any per-flow mechanism, because the Head-End does not know the requirements of each flow. If the Applications need different treatments in the network, and the Head-End can schedule the traffic to a proper path, the user can have a better experience and the network resource can be used more efficiently.

Commenté [BMI10]: Is this similar to bearer establishment and qci handling in mobile networks?

```
   Client                                                        Server
   +-----+                                                       +-----+
   |App x|-\                                                  /->|App x|
   +-----+ |   +-----+ +---------+   +--------+   +---------+ |  +-----+
            \->|     | |         |-A-|        |-A-|         |-/
   User side   | BNG |-|Head-End |-B-|Mid-Node|-B-|End-Node |
            /->|     | |         |-C-|        |-C-|         |-\
   +-----+ |   +-----+ +---------+   +--------+   +---------+ |  +-----+
   |App y|-/                                                  \->|App y|
   +-----+           ---------  Uplink   ---------->             +-----+
```

Figure 1: Path-aware Mechanism in the Fixed Network (Simplified)

Commenté [BMI11]: You may indicate that, for simplification, both control and user planes are covered here. Otherwise, configurations such as those in draft-wadhwa-rtgwg-bng-cups are more accurate.

The following paragraphs are about the trust problems and the potential solutions for them.

The first problem is the path information collection for the Endpoints. The Endpoints should be able to trust the path information that the Intermediate Nodes signal. As a first step, we only consider the situation that information is limited and does not need to be updated frequently. In this case, if the Head-End needs to inform the Endpoints something, it can send the information with its signature generated by using a private key. The Endpoints can check the information using the corresponding public key. For example, the public key can be obtained by the Endpoint in the authentication procedure.

Commenté [BMI12]: How this is achieved?

Mis en forme : Surlignage

The second problem is the Head-End should trust the Endpoints if it receives some path selection suggestions from the Endpoints. In this case, we think that the BNG has authenticated the Endpoints, so that the BNG can send some information to the Head-End indicating that the Endpoint is not a fake one. For example, the BNG and the Head-End can ~~using~~ use an ~~IPSec~~ IPsec tunnel to transfer the traffic that needs specific treatment. Another option is that the BNG can forward the traffic that needs specific treatment with its signature generated by using a private key. The Head-End can check the information using the corresponding public key of the BNG.

Commenté [BMI13]: Why ipsec is mentioned here and for which usage?

Commenté [BMI14]: If advanced service functions are needed to meet the requested connectivity service, the traffic may be steered using specific service chains. In order to avoid misbehaving nodes, service chain instruction sets by an ingress node can be protected using RFC9145.

The reason that we do not suggest that the Endpoints make the signature is because their number is much larger than the number of BNGs. We do not think the Head-End can handle a large number of keys. Meanwhile, in this mechanism, the Intermediate Node does not need to maintain per-connection state.

3. IANA Considerations

TBD.

4. Security Considerations

TBD.

5. Acknowledgements

TBD.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

6.2. Informative References

[RFC9049] Dawkins, S., Ed., "Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)", RFC 9049, DOI 10.17487/RFC9049, June 2021, <https://www.rfc-editor.org/info/rfc9049>.

Authors' Addresses

Zongpeng Du
China Mobile
No.32 XuanWuMen West Street
Beijing 100053
China

Email: duzongpeng@foxmail.com

Peng Liu
China Mobile
No.32 XuanWuMen West Street
Beijing 100053
China

Email: liupengyjy@chinamobile.com