Introduction

Overview of Trust-Enhanced ALTO

Integration of Trust into ALTO

Ideas to bring Trust to ALTO
  ● Trusted IP-based Geolocation
  ● Trust as a Cost Measurement in ALTO
  ● Trust-Enhanced "Property Map"
  ● Multi-Domain and Trust as part of ALTO

Summary & Discussion
Overview of ALTO

- ALTO protocol allows internet clients to obtain information comparing network properties of paths to other endpoints.
- This information can identify the lowest-cost location to access content.
- If the overlay network knows the topology and cost of sending traffic through the underlying IP network, it can optimize decisions and routing of traffic using ALTO protocol.
Overview of a Trust-enhanced ALTO

- **Trust for Enhancing Network Decision-making in ALTO**

  - An important & complex concept for supporting decision-making in unpredictable circumstances.
  - A critical factor in many areas of technology and decision-making, including network traffic optimization.
  - Helps assess the value of information, products, and services.
  - Helps evaluate the **quality of interactions** based on reputation and trustworthiness.
Integration of Trust into ALTO

Trustworthiness Metrics

- Inclusion in ALTO: Incorporate trustworthiness metrics into ALTO’s information model.
- Factors Considered: Metrics cover reliability, security, stability, and performance.
- Objective Decision-making: Quantitative measurements for informed resource selection.

Extended Cost Metrics

- Incorporating Trust Factors: Expand ALTO’s cost metrics to include trustworthiness.
- Resource Selection: Applications can consider trust-related factors for optimal resource selection.
- Enhanced Decision-making: Trust integration improves routing decisions and resource utilization.

Real-time Trust Updates

- Continuous Monitoring: Real-time monitoring of trustworthiness metrics.
- Adaptive Decision-making: Applications can adapt decisions based on current trust levels.
- Dynamic Network Environment: Respond to changing conditions for optimized performance.
Advantages of Trust-Enhanced ALTO

Informed Decision Making

- Applications utilize trustworthiness metrics for decision-making.
- Trust-Metrics as a guide for optimized resource selection and routing.
- Reliable and secure links/resources are prioritized.

Enhanced Security

- Risk mitigation by avoiding insecure or unreliable network links/resources.
- Trust-based resource selection to prioritize trusted components.
- Identification and avoidance of network elements prone to security threats.

Improved Performance and Quality

- Mitigates security risks and promotes compliance.
- Ensures adherence to security policies and requirements.
ALTO before Trust

- **Improved network performance**: ALTO improves network performance by providing information about network properties.
- **Reduced network congestion**: ALTO reduces network congestion by helping applications choose the lowest-cost location to access content.
- **Better user experience**: ALTO provides a better user experience by improving network performance and reducing congestion.

ALTO after Trust

- **Introduce Trust as a new performance metric**: Trust can improve network performance by facilitating the exchange of detailed network information between domains.
- **Improve Network trustworthiness**: helping applications choose the most trusted location/path to access content.
- **Improve user satisfaction**: Helps assess the value of information, products, and services by reducing the risks related to lack of trust.
Ideas to bring Trust to ALTO

The initial ideas that we collected so far are:

1. Working on Trusted IP-based Geolocation of the entities in the ALTO architecture.
2. Defining Trust as a one of the possible Cost measurements to be used within ALTO.
3. Considering Trust-Enhanced “Property map”.
4. Multi-Domain settings and Trust as part of ALTO.

- These ideas contribute to enhancing trustworthiness and trust-aware decision making within the ALTO architecture.

- By prioritising such aspects, ALTO can provide applications with more reliable, secure, and trustworthy information for optimized resource selection, routing, and policy enforcement.
1- Trusted IP-based Geolocation (1/2)

Context:

• The accurate geolocation of network entities (e.g., clients, servers, resources) plays a crucial role in making informed resource selection and routing decisions in ALTO.
• However, traditional geolocation methods may suffer from inaccuracies or vulnerabilities.

Value:

• Implementing trusted IP-based geolocation mechanisms within ALTO can enhance the accuracy and reliability of geolocation information.
• It can provide a more trustworthy foundation for ALTO applications to optimize resource selection and routing based on geolocation-based criteria.

Expected Outcome:

• Trusted geolocation can improve the decision making process leading to better resource allocation and potentially improved overall user experience.
1- Trusted IP-based Geolocation (2/2)

- How to include Robust Geolocation as part of ALTO server
- Which element would benefit the most from Trusted Geolocation
- How to share trusted output with ALTO client

- How to use the inputs received from the ALTO server
- What is the expected impact on performances / user experience
- Is it possible/useful to include “Trust measurements” within ALTO client

- Focused on the “Resources”
- Focused on the PATH between the client and resource (how to access the content)

Figure 1: Basic ALTO Architecture

© 2023 Fujitsu Limited
Context:

- ALTO currently uses cost metrics to quantify the performance or quality of network paths or resources.

Value:

- Integrating trust as a cost measurement enables ALTO to factor in trust-related considerations, such as reliability, security, and stability, into its decision-making process.
- This would help extend the evaluation criteria to consider trustworthiness factors in resource selection and routing decisions.

Expected Outcome:

- Prioritize trustworthy resources would lead to enhanced security, improved reliability, and optimized resource utilization within the network.
An ALTO server would offer the “QualityOfTrust” as a cost metric.

This cost metric conveys a high-level measure for the “Quality of Trust” depending on the path between a source and a destination.

A higher value indicates a higher preference for traffic to be sent from a source to a destination.

Service providers may internally decide on the specific factors and their respective weights for computing QoT.

However, QoT is especially important for multi-domain settings, which makes standardisation efforts very crucial.

QoT should reflect/can be impacted by: sensitivity of data, type of traffic and the projected application/use case.

Simple methods of calculation can include: air miles, hop-count, and other network related metrics.
2- Trust as a Cost Measurement in ALTO (3/3)

- Defining Trust as a Cost measurement:
  - Similar to how “cost_metrics” are defined and used.
  - Consider introducing “trust-cost” (similar to “routing-cost”)

- Questions:
  - Its added value for ALTO? (ask ALTO members for feedback)
  - Consider writing an ID. about QoT to cover this.

```json
{  "meta": {  "dependent-vtags": [    {"resource-id": "my-default-network-map", "tag": "da65eca2e2b7a10ce8b059740b0b2e3f8eb1d4785" }  ],  "cost-type": {"cost-mode": "numerical", "cost-metric": "routingcost"}  },  "cost-map": {  "PID1": { "PID1": 1, "PID2": 5, "PID0": 10 },  "PID2": { "PID1": 5, "PID2": 1, "PID0": 15 },  "PID0": { "PID1": 20, "PID2": 15, "PID0": 1 }  }
```

Trust cost?

<table>
<thead>
<tr>
<th>Factor</th>
<th>Linearity</th>
<th>Linearity Examples</th>
<th>Non-linearity Example and Type</th>
<th>Dependence</th>
<th>Mathematical Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Generally linear, but exceptions may exist</td>
<td>Increasing availability increases trust in a linear manner</td>
<td>N/A</td>
<td>-</td>
<td>Trust = k1 * Availability + b1</td>
</tr>
<tr>
<td>Reliability</td>
<td>Generally linear, but exceptions may exist</td>
<td>Higher reliability leads to increased trust in a linear manner</td>
<td>N/A</td>
<td>-</td>
<td>Trust = k2 * Reliability + b2</td>
</tr>
<tr>
<td>Latency</td>
<td>Not always linear</td>
<td>Lower latency generally improves trust in a non-linear manner</td>
<td>Diminishing returns - further latency reduction may have diminishing impact on trust</td>
<td>May depend on network congestion</td>
<td>Trust = k3 * e^(-latency) + b3</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Generally linear</td>
<td>Higher packet loss rates decrease trust in a linear manner</td>
<td>N/A</td>
<td>May depend on network congestion</td>
<td>Trust = k4 * (1 - packet_loss_rate) + b4</td>
</tr>
<tr>
<td>Network Congestion</td>
<td>Not always linear</td>
<td>Increased congestion reduces trust in a non-linear manner</td>
<td>Saturation - trust decreases significantly as network becomes heavily congested</td>
<td>May impact latency, packet loss</td>
<td>Trust = k5 * (1 - congestion_level) + b5</td>
</tr>
</tbody>
</table>

Questions:

○ Its added value for ALTO? (ask ALTO members for feedback)
○ Consider writing an ID. about QoT to cover this.

```python
alto/agent/cric.py
```


© 2023 Fujitsu Limited
Context:

• The ALTO protocol utilizes property maps to provide network-related information to applications.
• Enhancing the property map with trust-related attributes can offer additional insights considering trustworthiness as a factor in the decision-making process.

Value:

• A trust-enhanced property map provides a standardized and structured way to convey trustworthiness information to ALTO clients.
• It empowers applications to leverage this information in resource selection, routing, or policy enforcement, leading to more intelligent and trust-aware decision making.

Expected Outcome:

• By incorporating trust-related properties into the property map, ALTO can facilitate the exchange of trustworthiness information between ALTO servers and clients.
• Applications can then utilize this information to optimize their resource selection, routing, or policy enforcement, resulting in improved security, enhanced reliability, and better overall network performance.
The **Network Map**

- lists all the endpoint groups that the ALTO server tracks. This map includes PIDs that uniquely identify each group.

The **Entity Property Map**

- describes the properties of each ANE in the network, including the geolocation or the connectivity type (for example, fiber or wireless) of an ANE.

The **Cost Map**

- provides the cost information (for example, hop count, latency, or bandwidth) between each pair of PIDs enclosed in the network map, where a PID identifies a group of endpoints.

The **Endpoint Cost Map**

- provides finer-grained cost information between specific endpoints.

**Trust-Enhanced Property Map**

- Provide Trust focused measurements for each ANE (Abstract Network Element) that would allow trust-based decision making.
Exposing multi-domain network information to support emerging use cases introduces issues to be considered in the current ALTO design.

One of these issues is related to security and privacy.

The information provided by the ALTO protocol is considered coarse-grained.

- Network information is exposed as abstract maps, such as Network Map and Cost Map.
- The benefits of abstract maps include protection of information privacy and improved scalability.[ref1]
- However, many ISPs dislike disclosing detailed information about their network architecture to others.
- Therefore, the ALTO protocol is designed to offer little information about an ISP’s network architecture to P2P application vendors.[ref2]

New ALTO extensions have been designed to provide fine-grained network information to the applications.

Using these ALTO extension services for multi-domain scenarios would raise new security and privacy concerns. [ref3]
Trust is important in any multi-domain system that involves the exchange of information between different parties.

In the case of the ALTO protocol in a multi-domain setting, trust between different domains can facilitate the exchange of network information.

If different domains trust that their network information will be used appropriately and not disclosed to unauthorized parties, they may be more willing to provide detailed network information to each other.

This can improve the performance of applications that use the ALTO protocol to optimize their network resource consumption across multiple domains.
The ALTO protocol can act as a facilitator for incorporating trustworthiness considerations into network-related decision-making processes.

It can provide a framework and mechanisms for applications to access trust-related information, support defining requirements for trustworthiness, and optimize their operations based on trust-related factors.

By integrating trustworthiness into the ALTO protocol, network resources can be utilized in a more informed and secure manner, aligning with the specific trust requirements of applications and users.
Questions for ALTOers

Relevance only to ALTO?

- What aspects should we prioritise?
- What are the most valued expected outcomes?
- Who needs to be involved?
- Who wants to be involved?

Relevance to other WG?

- Which WG?
- What are the Cross-sections with ALTO?
- Who are the Relevant people?
Thank you
Overview of ALTO Core and Extensions

ALTO Info Service
- Map Filtering Service
- End Property Service
- End Cost Service
- Trust-focused Service

Map Service
- Network Map
- Cost Map
- Entity Property Map
- Endpoint Cost Map

ALTO Base Protocol – RFC 7285

Extensions
- Multi-Cost RFC 8189
- Cost Calendar RFC 8896
- Path Vector RFC 9275
- Cost Mode RFC 9274
- Cost Metric
- CDNI FCI RFC 9241

Server Discovery RFC 7286
- RFC 8686
- ALTO Deployment RFC 7971
- Incremental Update RFC 8895
- ALTO OAM
- ALTO Transport

© 2023 Fujitsu Limited
With the emergence of the Metaverse and Web3, cyberspace will play a central role for conducting business activities.

- This transformation enables us to collaborate more with stakeholders across different regions and countries.
- Compliance with regulations and policies for sensitive data transfer becomes even more important.
- Trustworthy collaboration and secure data exchange can be achieved by verifying geolocation of data and its routes called Robust Localization.
The current highly virtualized and cloud-based systems obscure physical information (location of partners, data and its transfer routes) from cyberspace. This makes Robust Geolocation more challenging.
Our direction: Trust-Enhanced Networking

To enhance trustworthiness, networks connecting cyberspace and the real world should provide endorsement information about physical attributes of the communicating entities.

- Probing using multiple anchor points will enable verification of the location of data and its users in cyberspace.
- Implementing geographically-trusted routes between users and data sources avoids unintended / suspicious cross-border data transfers.