Secure and Scalable QoS for Critical Applications

Marc Wyss, Giacomo Giuliani, Markus Legner, and Adrian Perrig

ETH zürich

IWQoS 2021
Objective

Communication guarantees for Critical-yet-Frugal (CyF) applications:
• Critical: requires high availability
• Frugal: low traffic volumes
Objective

Communication guarantees for **Critical-yet-Frugal (CyF) applications**:

- Critical: requires high availability
- Frugal: low traffic volumes
Objective

Communication guarantees for Critical-yet-Frugal (CyF) applications:
- Critical: requires high availability
- Frugal: low traffic volumes
Current solutions

**Leased lines**

+ Strong QoS guarantees
- High cost
- Low redundancy
- Does not scale
Current solutions

**Leased lines**
+ Strong QoS guarantees
- High cost
- Low redundancy
- Does not scale

**Bandwidth reservations over the Internet**
+ Low cost
- Does not scale (e.g., IntServ)
- No bandwidth guarantees (e.g., DiffServ)
- Centralized (e.g., SDN)
- Not secure (almost all existing protocols)
- Limited deployment
Current solutions

Leased lines
+ Strong QoS guarantees
- High cost
- Low redundancy
- Does not scale

Bandwidth reservations over the Internet
+ Low cost
- Does not scale (e.g., IntServ)
- No bandwidth guarantees (e.g., DiffServ)
- Centralized (e.g., SDN)
- Not secure (almost all existing protocols)
- Limited deployment

Our contribution: GLWP
Network model

- Internet consists of autonomous systems (ASes)
Network model

- Internet consists of autonomous systems (ASes)
- Every AS has a local secret key known by all its services and border routers
Network model

- Internet consists of autonomous systems (ASes)
- Every AS has a local secret key known by all its services and border routers
- Each AS has shared symmetric keys with every other AS (e.g., using PISKES)
Network model

- Internet consists of autonomous systems (ASes)
- Every AS has a local secret key known by all its services and border routers
- Each AS has shared symmetric keys with every other AS (e.g., using PISKES)
- Path stability (e.g., using SCION)
Calculating allocations: GMA

AS_1  AS_2  AS_3  AS_4
Calculating allocations: GMA

\[
\text{GMA}(M_1, M_2, M_3, M_4) = 5 \text{ Mbps}
\]

1) Locality
2) Bandwidth > 0
Calculating allocations: GMA

1) Locality
2) Bandwidth > 0
3) No over-allocation
GLWP

"GMA-based light-weight communication protocol"

**Discovery-phase**
- Source AS selects path
- Collect reservation information of every AS on the path
- Every AS on the path calculates bandwidth using GMA

**Transmission-phase**
- Send data traffic over the reservation
- Protect traffic from congestion and DDoS
**GLWP: Discovery phase**

**GLWP Service**
- $M_1$
- Shared symmetric keys with every other AS
- Secret key $K_1$
GLWP: Discovery phase

Border router
- Secret key $K_1$
GLWP: Discovery phase

Packet = [Path, $M_1$]
GLWP: Discovery phase

Packet = [Path, M₁, M₂]
GLWP: Discovery phase

Packet = [Path, M₁, M₂, M₃]
GLWP: Discovery phase

Packet = [Path, M_1, M_2, M_3, …, M_n]
GLWP: Discovery phase

Packet = [Path, M_1, M_2, M_3, …, M_n]

- Bandwidth: \( BW = GMA(M_1, M_2, \ldots, M_n) \)
- Hop Key of AS\(_n\): \( HK_n = MAC_{K_n}(BW, Path, TS_{exp}) \)
GLWP: Discovery phase

Packet = [Path, M\(_1\), M\(_2\), M\(_3\), ..., M\(_n\)]

- Bandwidth:
  \[BW = \text{GMA}(M\(_1\), M\(_2\), ..., M\(_n\))\]

- Hop Key of AS\(_n\):
  \[HK\(_n\) = \text{MAC}_{K\(_n\)}(BW, \text{Path}, \text{TS}_{\text{exp}})\]

Secret key of AS\(_n\)
GLWP: Discovery phase

Packet = [Path, M₁, M₂, M₃, …, Mₙ, HKₙ]

- Bandwidth: \( BW = \text{GMA}(M₁, M₂, …, Mₙ) \)
- Hop Key of ASₙ: \( HKₙ = \text{MAC}_{Kₙ}(BW, \text{Path}, TS_{\text{exp}}) \)
GLWP: Discovery phase

Packet = [Path, M₁, M₂, M₃, …, Mₙ, HKₙ, … HK₄]

- Bandwidth: \( BW = GMA(M₁, M₂, …, Mₙ) \)
- Hop Key of AS₃: \( HK₃ = MAC_{K₃}(BW, \text{Path, } TS_{exp}) \)

Secret key of AS 3
GLWP: Discovery phase

Packet = [Path, $M_1$, $M_2$, $M_3$, …, $M_n$, $HK_n$, … $HK_4$, $HK_3$]

- Bandwidth: $BW = GMA(M_1, M_2, …, M_n)$
- Hop Key of AS$_3$: $HK_3 = MAC_{K_3}(BW, Path, TS_{exp})$

Secret key of AS 3
GLWP: Discovery phase

Packet = [Path, M₁, M₂, M₃, ..., Mₙ, HKₙ, ... HK₄, HK₃]

- Bandwidth: \( BW = GMA (M₁, M₂, ..., Mₙ) \)
- Hop Key of AS₂: \( HK₂ = MAC_{K₂} (BW, Path, TS_{exp}) \)

Secret key of AS 2
GLWP: Discovery phase

Packet = [Path, M₁, M₂, M₃, ..., Mₙ, HKₙ, ... HK₄, HK₃, HK₂]

- Bandwidth: \( BW = \text{GMA}(M₁, M₂, ..., Mₙ) \)
- Hop Key of AS₂: \( HK₂ = \text{MAC}_{K₂}(BW, Path, TS_{exp}) \)

Secret key of AS 2
GLWP: Discovery phase

Packet = [Path, $M_1$, $M_2$, $M_3$, …, $M_n$, $HK_n$, … $HK_4$, $HK_3$, $HK_2$]

- Bandwidth: $BW = GMA(M_1, M_2, ..., M_n)$
- Hop Key of AS$_1$: $HK_1 = MAC_{K_1}(BW, Path, TS_{exp})$

Secret key of AS 1
GLWP: Discovery phase

Packet = [Path, M_1, M_2, M_3, ..., M_n, HK_n, ..., HK_4, HK_3, HK_2, HK_1]

- Bandwidth: \( BW = GMA(M_1, M_2, ..., M_n) \)
- Hop Key of AS_1: \( HK_1 = MAC_{K_1}(BW, Path, TS_{exp}) \)

Secret key of AS_1
GLWP: Transmission phase

Packet = [Path, BW, TS_{exp}, TS_{pkt}]
GLWP: Transmission phase

Packet = \([\text{Path}, \text{BW}, \text{TS}_{\text{exp}}, \text{TS}_{\text{pkt}}]\)

Hop authenticators:

\[\text{HA}_1 = \text{MAC}_{\text{HK}_1} (\text{AS}_1, \text{TS}_{\text{pkt}}, \text{length[ pkt]})\]
\[\text{HA}_2 = \text{MAC}_{\text{HK}_2} (\text{AS}_1, \text{TS}_{\text{pkt}}, \text{length[ pkt]})\]
\[\ldots\]
\[\text{HA}_n = \text{MAC}_{\text{HK}_n} (\text{AS}_1, \text{TS}_{\text{pkt}}, \text{length[ pkt]})\]
GLWP: Transmission phase

Packet = [Path, BW, TS_{exp}, TS_{pkt}, HA_1, HA_2, ..., HA_n, payload]

Hop authenticators:

HA_1 = MAC_{HK_1}(AS_1, TS_{pkt}, length(pkt))
HA_2 = MAC_{HK_2}(AS_1, TS_{pkt}, length(pkt))
...
HA_n = MAC_{HK_n}(AS_1, TS_{pkt}, length(pkt))
GLWP: Transmission phase

Packet = [Path, BW, TS\textsubscript{exp}, TS\textsubscript{pkt}, HA\textsubscript{1}, HA\textsubscript{2}, ..., HA\textsubscript{n}, payload]

- Recalculate hop key: \( HK_3 = \text{MAC}_{K_3}(BW, \text{Path}, TS\textsubscript{exp}) \)
- Recalculate hop authenticator: \( HA_3 = \text{MAC}_{HK_3}(AS_1, TS\textsubscript{pkt}, \text{length}[\text{pkt}]) \)
- Compare calculated hop authenticator the the one in the packet.
- Check packet using replay suppression system and bandwidth monitor.
Evaluation: GServ

![Graph showing throughput vs. number of on-path ASes for different packet sizes](image-url)
Evaluation: Border Router

![Processing time [ns] for different tasks with varying numbers of ASes.]

- Validate packet format
- Calculate hop key (1 AS, 2 ASs, 4 ASs, 8 ASs, 16 ASs)
- Calculate hop authenticator
- Others

Wyss et al.  IWQoS 2021
Security of GLWP

GLWP is secure against:

- Malicious GMA parameter announcements
- Path manipulation
- Request multiple reservations over the same path
- Reservation overuse
- Framing attacks
- Volumetric DDoS attacks
- ...
Critical-yet-Frugal applications need guaranteed communication (QoS).

Existing solutions cannot provide this.

We present **GLWP**:
- Strong QoS guarantees
- Decentralized
- Secure
- Low communication and computation overhead
- No per-path or per-connection state
- Scales to large networks
Conclusion

• Critical-yet-Frugal applications need guaranteed communication (QoS).

• Existing solutions cannot provide this.

• We present GLWP:
  • Strong QoS guarantees
  • Decentralized
  • Secure
  • Low communication and computation overhead
  • No per-path or per-connection state
  • Scales to large networks

Thank you!

Email: marc.wyss@inf.ethz.ch
## References

<table>
<thead>
<tr>
<th>Name</th>
<th>Use in GLWP</th>
<th>Reference</th>
</tr>
</thead>
</table>
| GMA    | • Bandwidth calculation  
• Locality property allows GServ to be stateless       | "GMA: A Pareto Optimal Distributed Resource-Allocation Algorithm"  
SIROCCO, 2021                                         |
| PISKES | • Efficient symmetric key distribution                                     | "PISKES: Pragmatic Internet-Scale Key-Establishment System"  
ASIA CCS, 2020                                         |
| SCION  | • Path stability  
• (Multipath)                                                        | "SCION: A Secure Internet Architecture"  
Springer, 2017                                         |