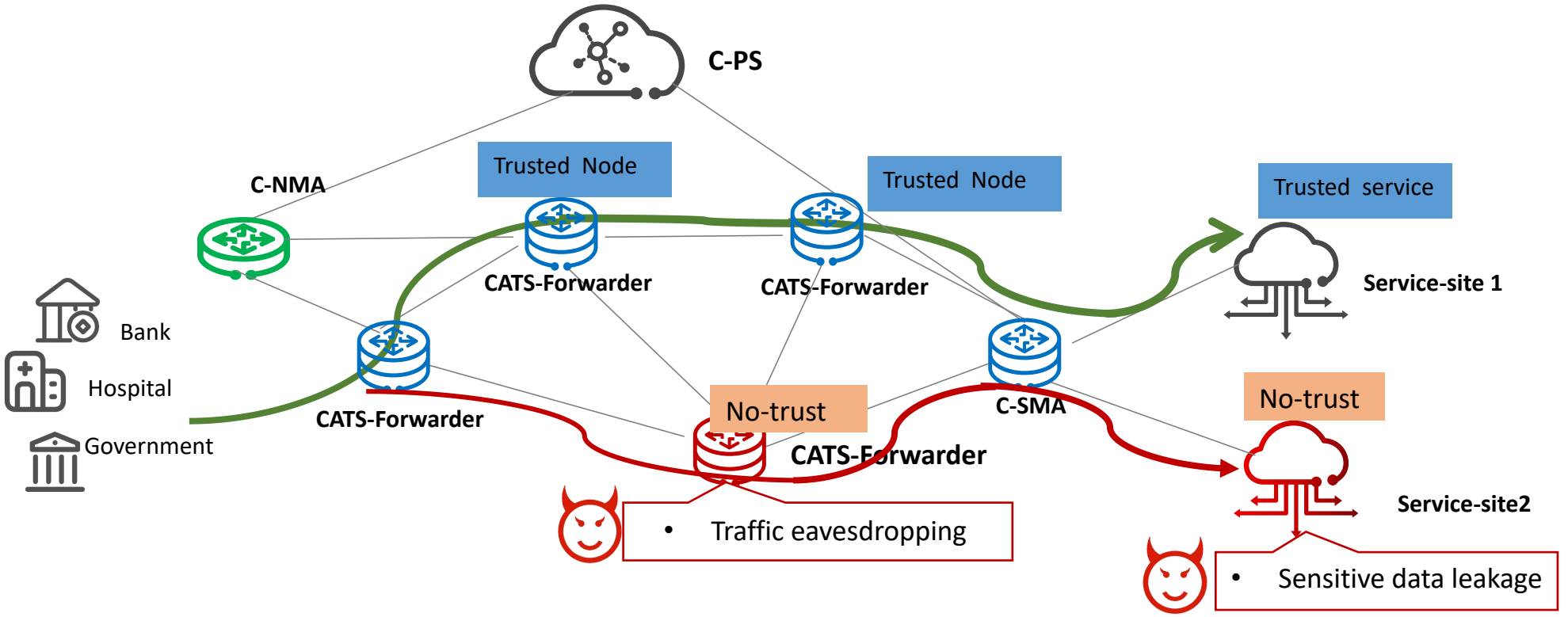
Security Considerations for Computing-Aware Traffic Steering

draft-wang-cats-security-considerations-00

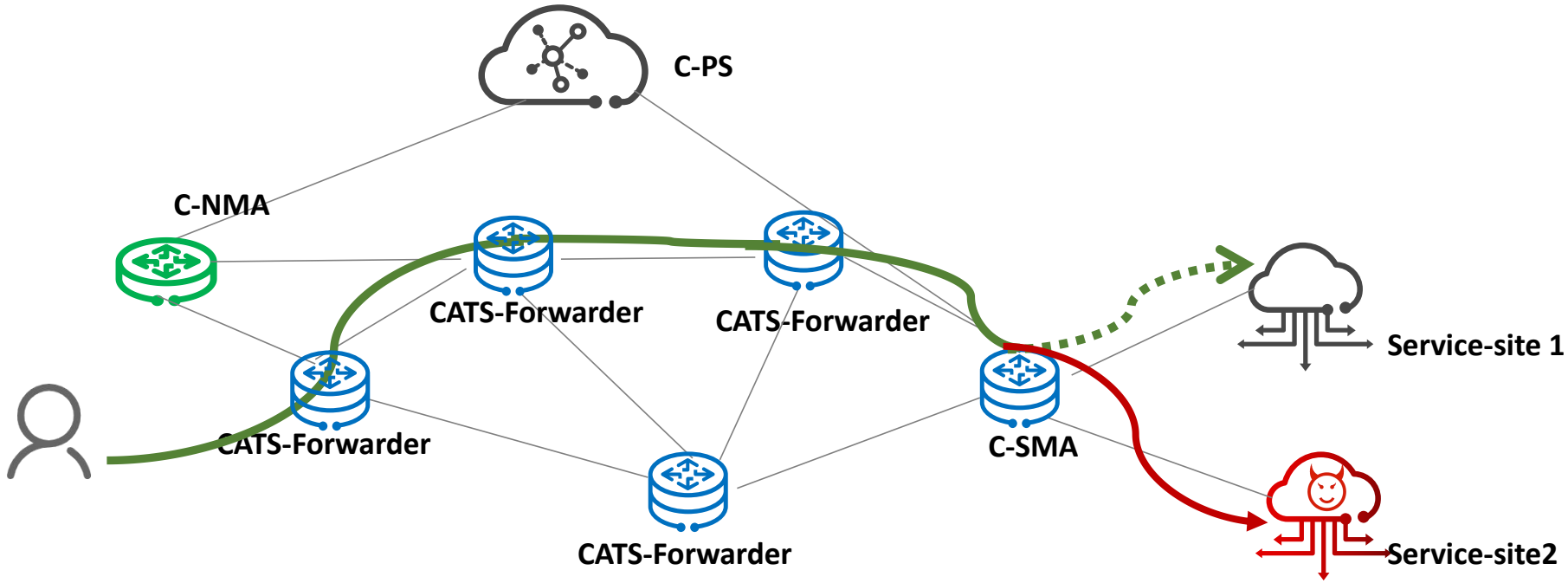
Cuicui Wang(China Unicom) Yu Fu(China Unicom)

Secure path and service requirement



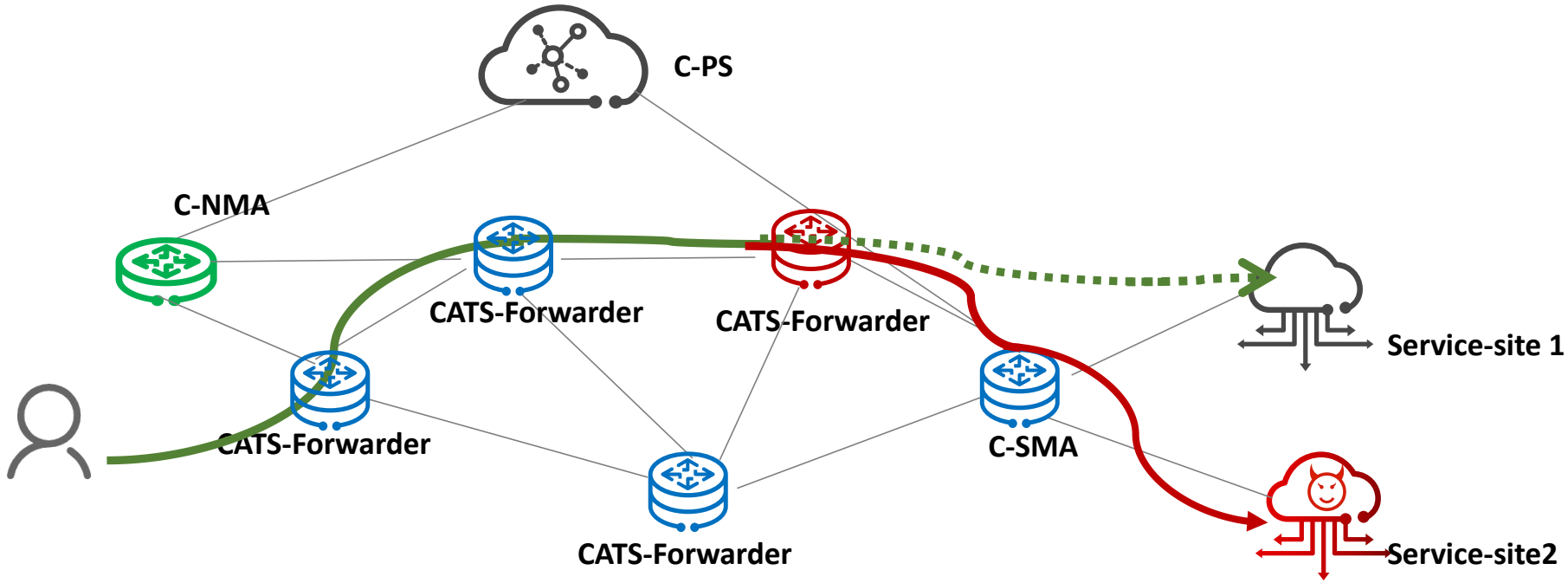
- The service and network metrics **may** include the **security-related capabilities** which could be used by the CATS Path selector to **compute paths with security guarantee**.
- Clients with high security requirements(i.e.,bank, hospital, government etc.) could choose the service with **desired security attributes** and achieve dependable forwarding on top of only **devices that satisfies certain trust requirements , which will avoid the risks of** traffic eavesdropping, sensitive data leakage etc.

Requirement for authenticity and integrity protection mechanism of service announcement



There might be mechanism that provides protection of **the integrity and sevice authenticity of messages in the service announcement**, or else it could be exploited by malicious service to **reroute traffic**, which **may** lead to DDos attacks, phishing attacks, sensitive data leakage etc.

Requirement for authentication and integrity-protection mechanisms in CATS communication



- ✓ A malicious CATS-Forwarder could tamper the messages in forwarder-forwarder or forwarder-C-SMA communication, which will have a ripple effect on routing and path-computing of C-PS.
- ✓ CATS solutions could support authentication and integrity-protection mechanisms between C-SMAs/C-NMAs and C-PSes, and between C-Pses and Ingress CATS-Forwarders.

Does CATS need to consider security issues simultaneously?

Thanks !