Анонимная сеть «Hidden Lake»

Коваленко Геннадий Александрович

«Hidden Lake» (HL) — это децентрализованная анонимная F2F (Friend-to-Friend) сеть с теоретической доказуемостью на базе очередей (QB-задача)

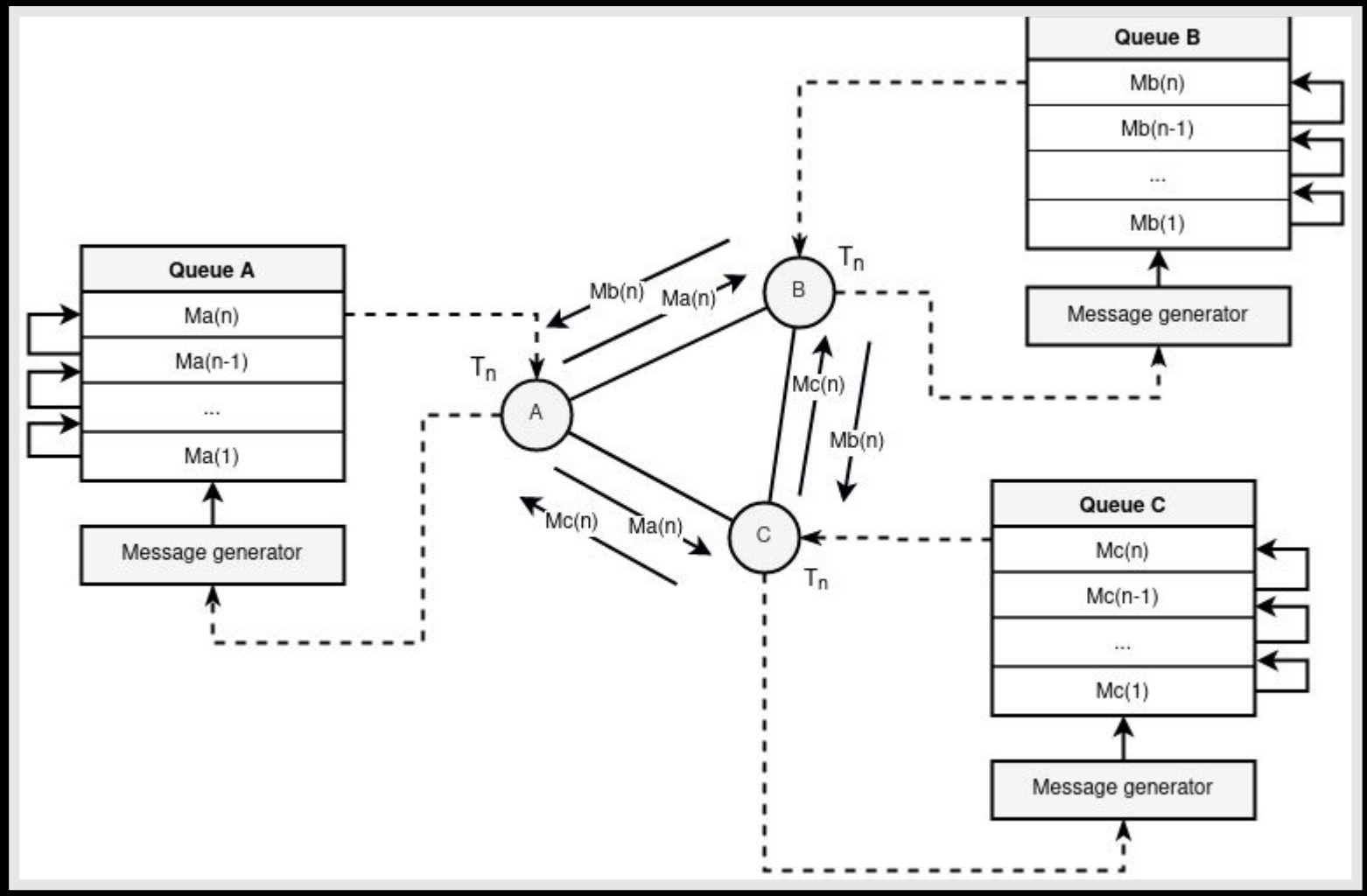
«Hidden Lake» является **Friend-to-Friend** сетью. Данное свойство определяет специфичный вид соединения участников в системе посредством ручной установки списка друзей

Задача на базе очередей (QB-задача)

простыми словами

1. Каждое сообщение шифруется ключом получателя,
2. Сообщение отправляется в период = **T** всем участникам сети,
3. Период **T** одного участника независим от периодов $\mathbf{T_1}$, $\mathbf{T_2}$, ..., $\mathbf{T_n}$ других участников,
4. Если на период **T** сообщения не существует, то в сеть отправляется ложное сообщение без получателя,
5. Каждый участник пытается расшифровать принятое им сообщение из сети.

Задача на базе очередей (QB-задача)



Задача на базе очередей (QB-задача)

формальным языком

Система:

$QB\text{-}net = \Sigma^{n}_{i=1}(T = \{t_i\}, K = \{k_i\}, C = \{(c \in \{E_{kj}(m), E_r(v)\}) \leftarrow^{ti} Qi\})$

Состояния:

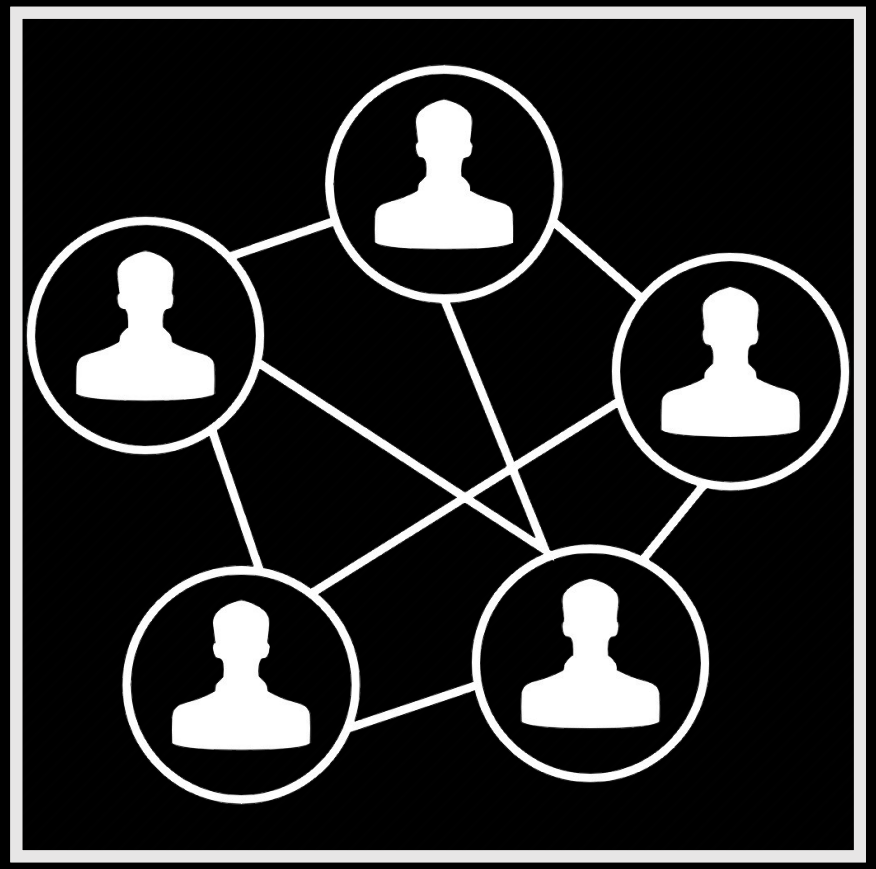
1. $Q \leftarrow (c = E_{ki}(m))$, где $k_i \in K$, $c \in C$,
2. $(c = E_{ki}(m)) \leftarrow^{t} Q$, если $Q \neq \emptyset$, где $t \in T$, $k_i \in K$, $c \in C$,
3. $(c = E_r(v)) \leftarrow^{t} Q$, если $Q = \emptyset$, где $t \in T$, $r \notin K$, $c \in C$,
4. $m' = D_k^{-1}(c)$, где $c \in C$

Сравнение с другими задачами анонимизации

	QB	EI	DC	Onion	Proxy
Теоретическая доказуемость	+	+	+	-	-
Накопительный эффект анонимности	-	+	-	-	-
Полиморфизм информации	-	+	+	+	-
Вероятностная маршрутизация	-	+	-	+/-	+/-
Периодичность генерации сообщений	+/-	-	+	-	-
Независимость анонимности от связей	+	-	-	-	-
Простота масштабирования	-	-	-	+	+
Простота программной реализации	+	-	-	+	+
Стадия анонимности	5^	6	1^	4 или 6	3
Сеть-представитель	Hidden Lake	-	Herbivore	Tor	Crowds

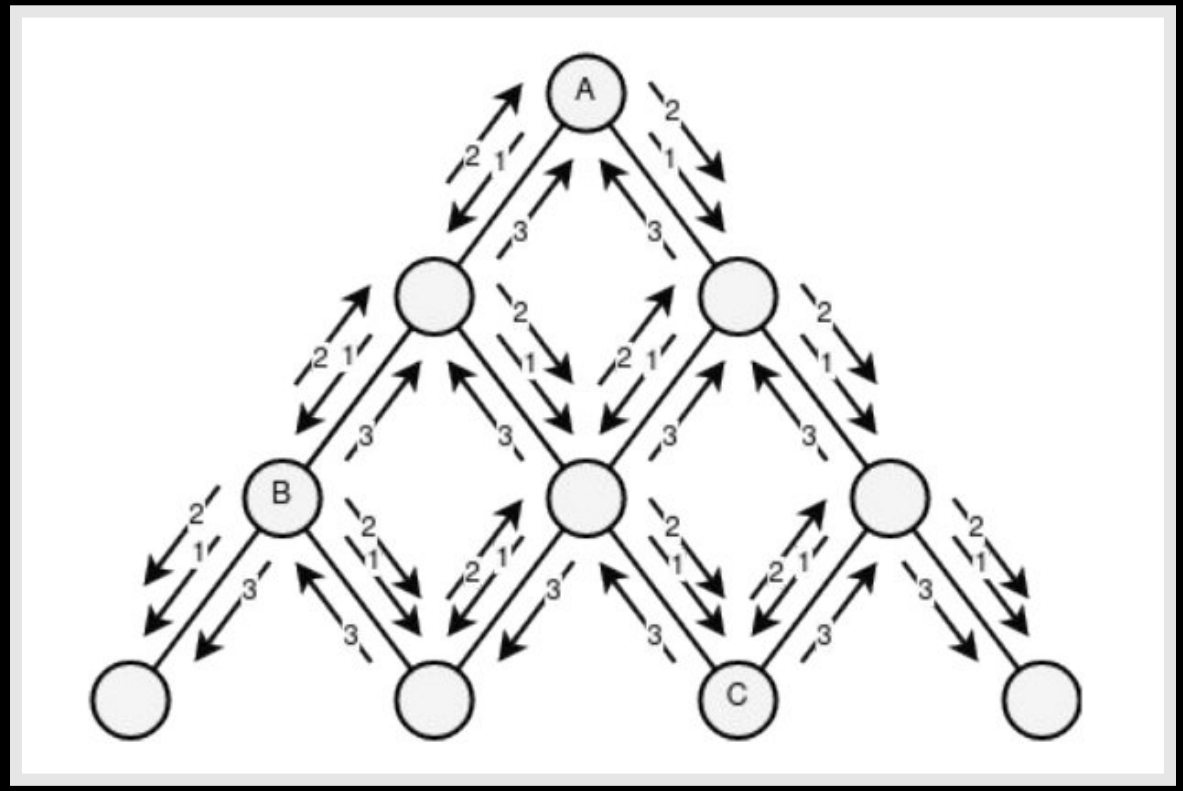
«Hidden Lake» относится к **абстрактным** анонимным сетям, которым не важны такие критерии, как:

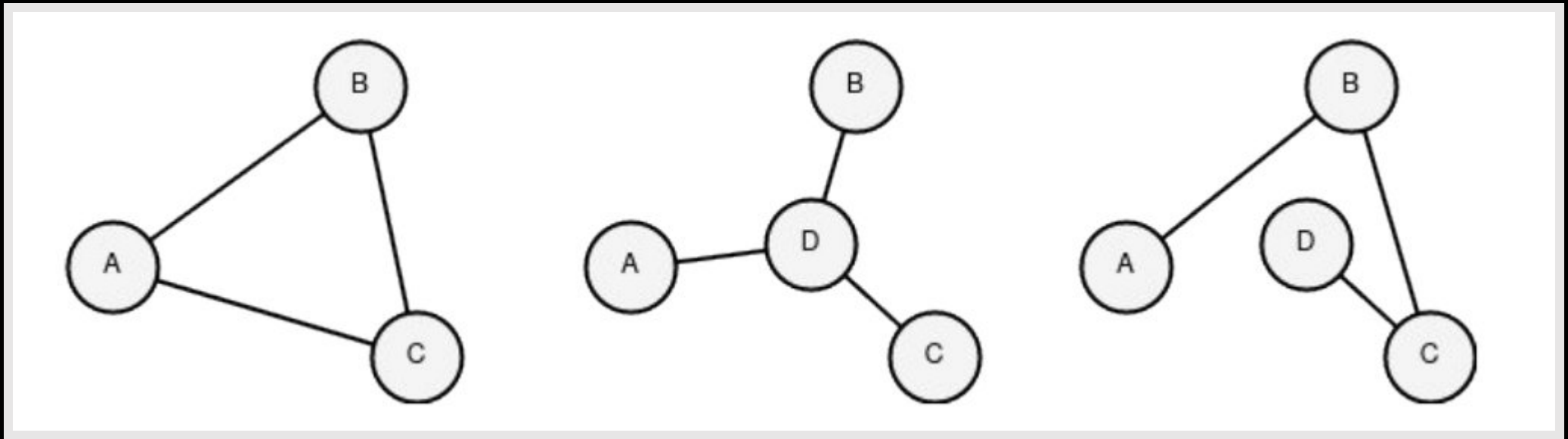
1. уровень централизации
2. количество узлов
3. расположение узлов
4. связь между узлами



За счёт своей абстрактности сеть «Hidden Lake» способна формировать **тайные каналы связи** с анонимизирующим свойством даже внутри централизованных сервисов

Главным недостатком сети является **линейная нагрузка** на систему, зависимая от количества участников



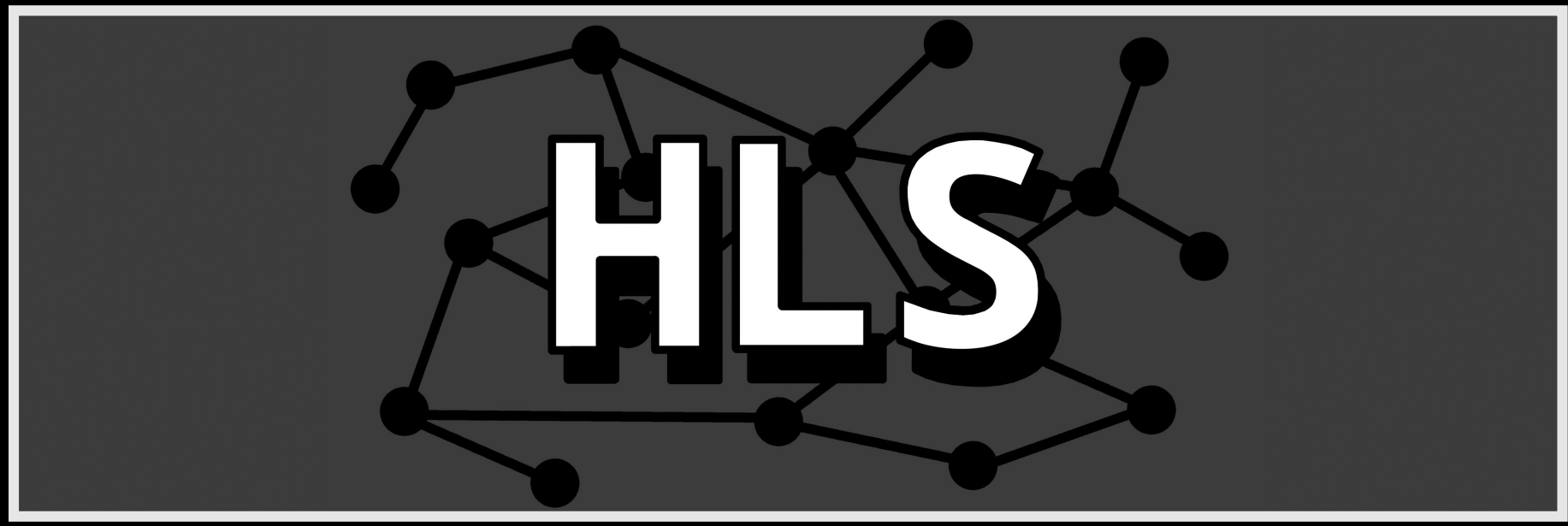


Частичным решением проблемы линейной нагрузки стало создание обособленных друг от друга **«малых озёр»** (сетей) посредством применения **сетевого ключа**

Философия разработки сети «Hidden Lake» основывается на **микросервисной** архитектуре

- На текущий момент существует 6 сервисов, где один **основной** сервис — HLS, два **прикладных** сервиса — HLM, HLF, три **вспомогательных** сервиса — HLT, HLE, HLL
- В описании сети «Hidden Lake» могут существовать также специфичные сервисы — **адаптеры**, именуемые как HLA. Они исполняют роль «вживления» анонимизированного трафика в инородную систему

HLS (Hidden Lake Service) — **ядро** анонимной сети.
Представляет **API** для отправления / получения
сообщений поверх анонимизирующего трафика

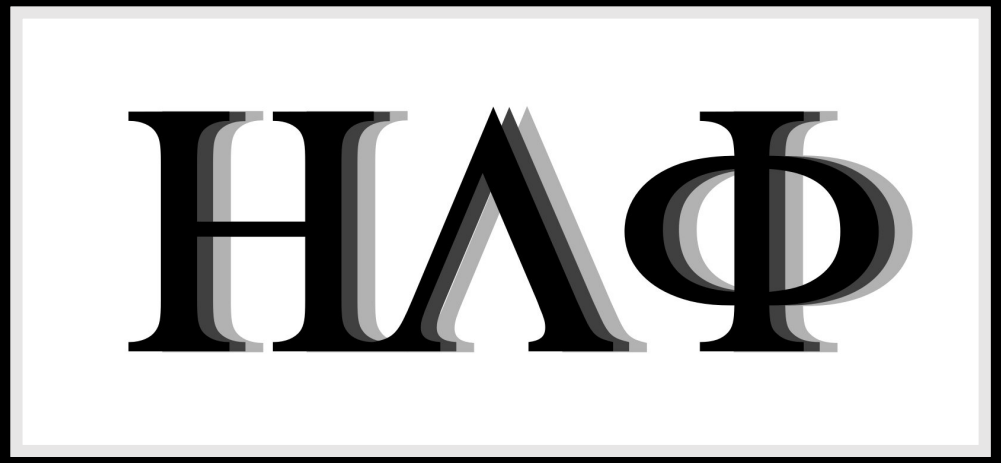


Генерация анонимизированного трафика в HLS приложении

```
[INFO] 2024/05/23 08:54:13 service=HLS type=BRDCS hash=B3305C11...5AA39CB8 addr=2651BBEC...776FD02F proof=0000012410 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:13 service=HLS type=BRDCS hash=B3305C11...5AA39CB8 addr=00000000...00000000 proof=0000012410 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:13 service=HLS type=UNDEC hash=B3305C11...5AA39CB8 addr=00000000...00000000 proof=0000012410 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:18 service=HLS type=BRDCS hash=C5C4F678...F2C76932 addr=5D4CD87B...936A4961 proof=0003749177 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:18 service=HLS type=BRDCS hash=C5C4F678...F2C76932 addr=00000000...00000000 proof=0003749177 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:18 service=HLS type=UNDEC hash=C5C4F678...F2C76932 addr=00000000...00000000 proof=0003749177 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:23 service=HLS type=BRDCS hash=5B11A80F...3B474F7E addr=2651BBEC...776FD02F proof=0000791686 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:23 service=HLS type=BRDCS hash=5B11A80F...3B474F7E addr=00000000...00000000 proof=0000791686 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:23 service=HLS type=UNDEC hash=5B11A80F...3B474F7E addr=00000000...00000000 proof=0000791686 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:27 service=HLS type=BRDCS hash=377A241E...DE62A796 addr=5D4CD87B...936A4961 proof=0009487840 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:27 service=HLS type=BRDCS hash=377A241E...DE62A796 addr=00000000...00000000 proof=0009487840 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:27 service=HLS type=UNDEC hash=377A241E...DE62A796 addr=00000000...00000000 proof=0009487840 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:32 service=HLS type=BRDCS hash=2106ACE8...7E6B7FC1 addr=2651BBEC...776FD02F proof=0008226170 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:32 service=HLS type=BRDCS hash=2106ACE8...7E6B7FC1 addr=00000000...00000000 proof=0008226170 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:32 service=HLS type=UNDEC hash=2106ACE8...7E6B7FC1 addr=00000000...00000000 proof=0008226170 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:34 service=HLS type=BRDCS hash=D920F8AA...CA891EE5 addr=5D4CD87B...936A4961 proof=0001232878 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:34 service=HLS type=BRDCS hash=D920F8AA...CA891EE5 addr=00000000...00000000 proof=0001232878 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:34 service=HLS type=UNDEC hash=D920F8AA...CA891EE5 addr=00000000...00000000 proof=0001232878 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:39 service=HLS type=BRDCS hash=6664487F...2173349A addr=2651BBEC...776FD02F proof=0000573139 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:39 service=HLS type=BRDCS hash=6664487F...2173349A addr=00000000...00000000 proof=0000573139 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:39 service=HLS type=UNDEC hash=6664487F...2173349A addr=00000000...00000000 proof=0000573139 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:44 service=HLS type=BRDCS hash=3CECCF91...A4D8FE17 addr=5D4CD87B...936A4961 proof=0000573419 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:44 service=HLS type=BRDCS hash=3CECCF91...A4D8FE17 addr=00000000...00000000 proof=0000573419 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:44 service=HLS type=UNDEC hash=3CECCF91...A4D8FE17 addr=00000000...00000000 proof=0000573419 size=8192B conn=172.22.0.3:59998
[INFO] 2024/05/23 08:54:45 service=HLS type=BRDCS hash=B493C5DE...77C5E5B7 addr=2651BBEC...776FD02F proof=0004410364 size=8192B conn=127.0.0.1:
[INFO] 2024/05/23 08:54:45 service=HLS type=BRDCS hash=B493C5DE...77C5E5B7 addr=00000000...00000000 proof=0004410364 size=8192B conn=172.22.0.2:7571
[INFO] 2024/05/23 08:54:45 service=HLS type=UNDEC hash=B493C5DE...77C5E5B7 addr=00000000...00000000 proof=0004410364 size=8192B conn=172.22.0.2:7571
```

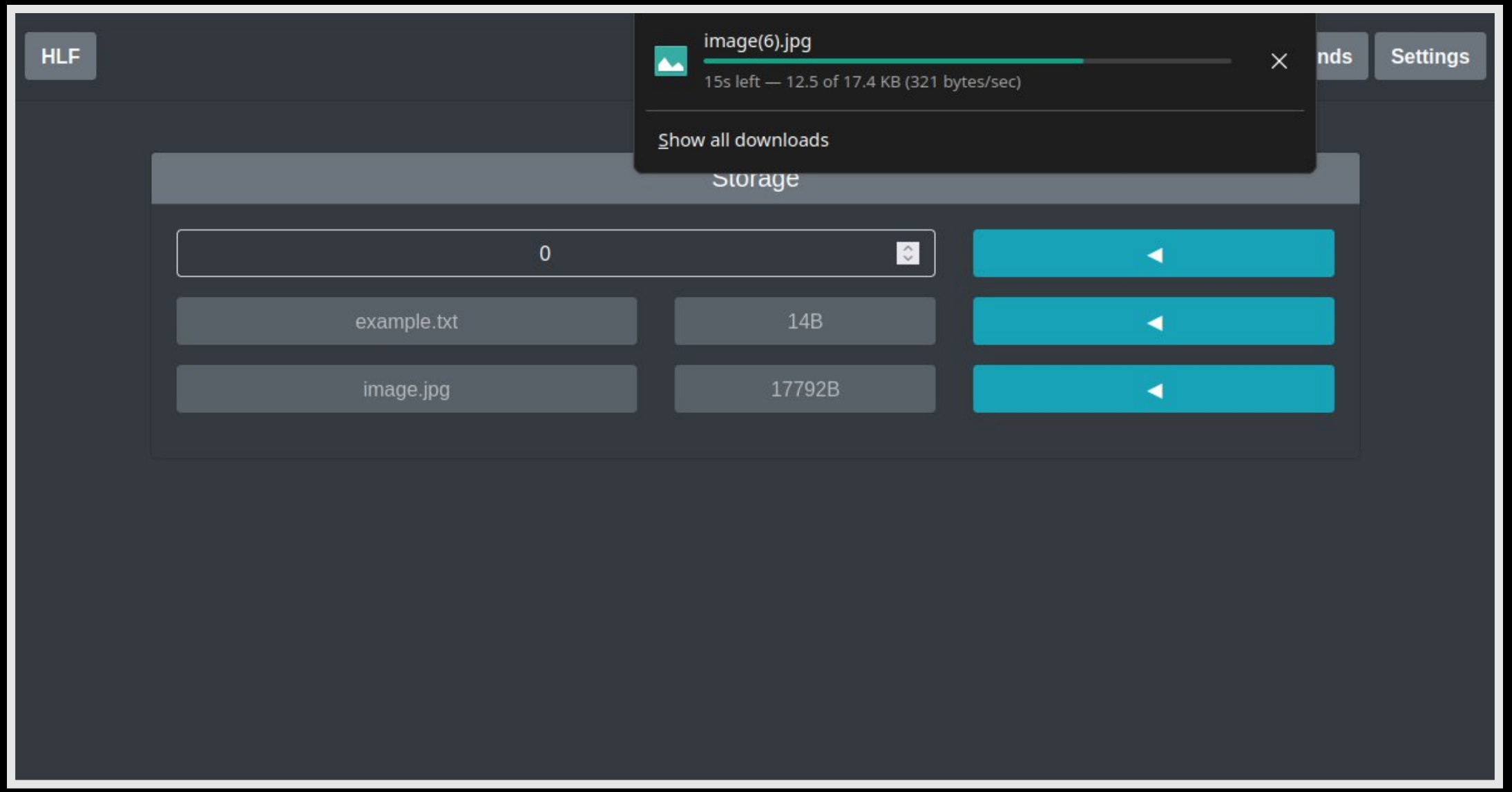
HLM (Hidden Lake Messenger)
— анонимный **мессенджер**,
вызывающий функции HLS

Интерфейс чата в HLM приложении



HLF (Hidden Lake Filesharer) — анонимный **файлообменник**, вызывающий функции HLS

Скачивание файла в HLF приложении



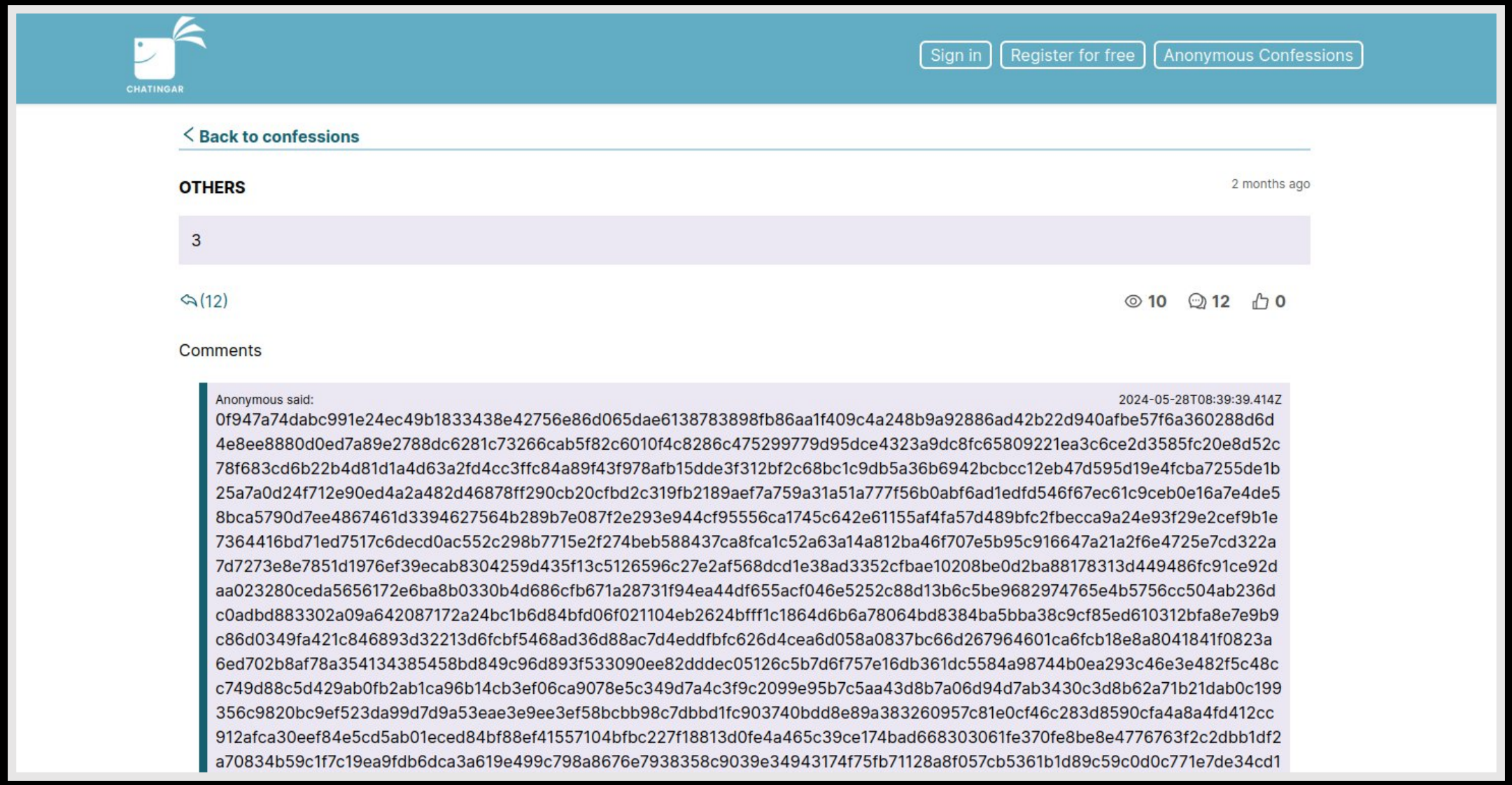
HLT (Hidden Lake Traffic) — **распределитель** трафика в анонимной сети. Может исполнять роль ретрансляции и хранения трафика

HLE (Hidden Lake Encryptor) — сервис **шифрования** и расшифрования сообщений формата **go-peer**

HLL (Hidden Lake Loader) — **скачиватель** и ручной распределитель трафика между несколькими HLT сервисами

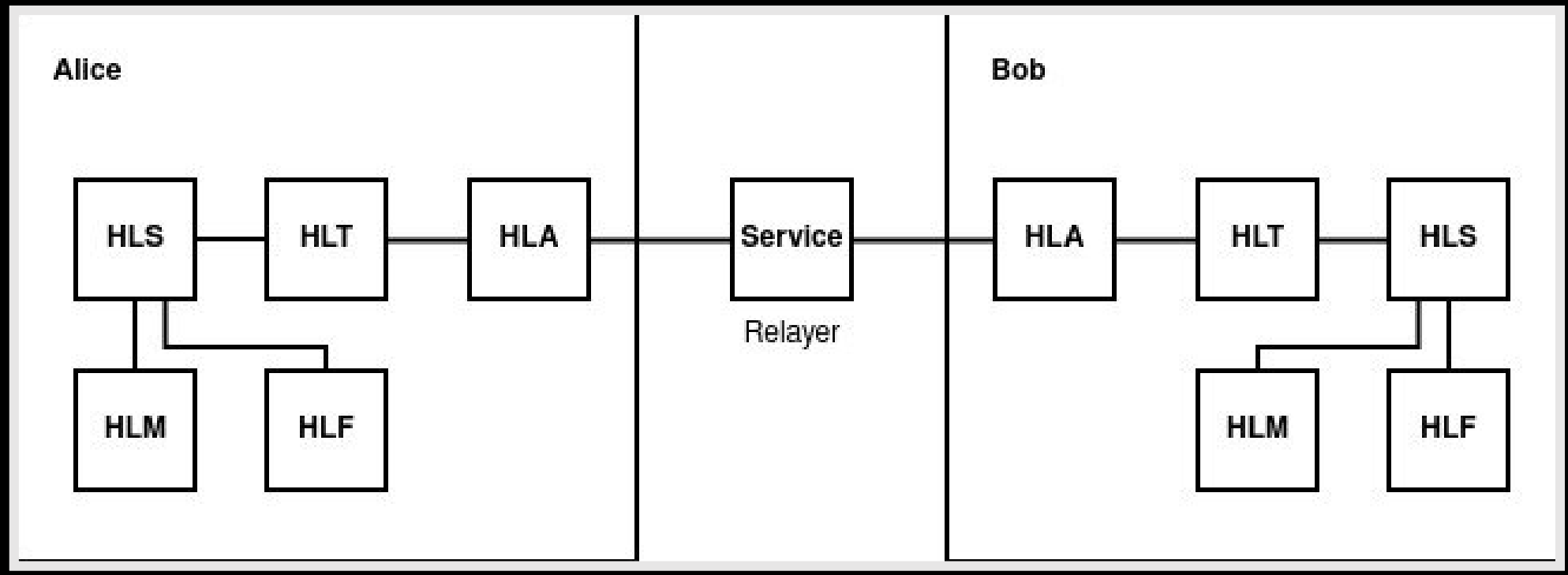
HLA (Hidden Lake Adapters) — **адаптеры** для создания анонимных коммуникаций в инородных системах, включая централизованные

Использование централизованного сервиса «chatingar»



Формальное описание композиции сервисов

$$Hidden\text{-}Lake = \Sigma^{n}_{i=1} APP_i \times HLS \times (HLT \times \Sigma^{m}_{j=1} HLA_j)^t$$



Сравнение с другими анонимными сетями

	Hidden Lake	Herbivore	I2P	Tor	Mixminion	Crowds
Децентрализованная архитектура	+	+	+	-	-	+
Сервисная API реализация	+	-	+	+	-	-
Задержка в передаче данных	+	+	-	-	+	-
Замкнутая архитектура сети	+	-	+	+/-	-	-
Сокрытие факта генерации данных	+	-	-	-	-	-
Сокрытие получателя от отправителя	+/-	-	+	+/-	-	-
Сокрытие отправителя от получателя	+/-	+	+	+	+	+
Задача анонимизации	QB	DC	Onion	Onion	Onion	Proxy

Возможные способы применения анонимной сети «Hidden Lake»

1. Защита локальных / корпоративных сетей от прослушивания
2. Защита военных коммуникационных узлов от прослушивания
3. Усиление безопасности уже готовых / сформированных систем
4. Использование существующей платформы для создания собственных приложений

Ссылки

- Проект go-peer

https://github.com/number571/go-peer

- Документация

https://github.com/number571/go-peer/tree/master/docs

- Директория Hidden Lake

https://github.com/number571/go-peer/tree/master/cmd/hidden_lake