

**Анонимная сеть**

**«Hidden Lake»**



Коваленко Геннадий Александрович

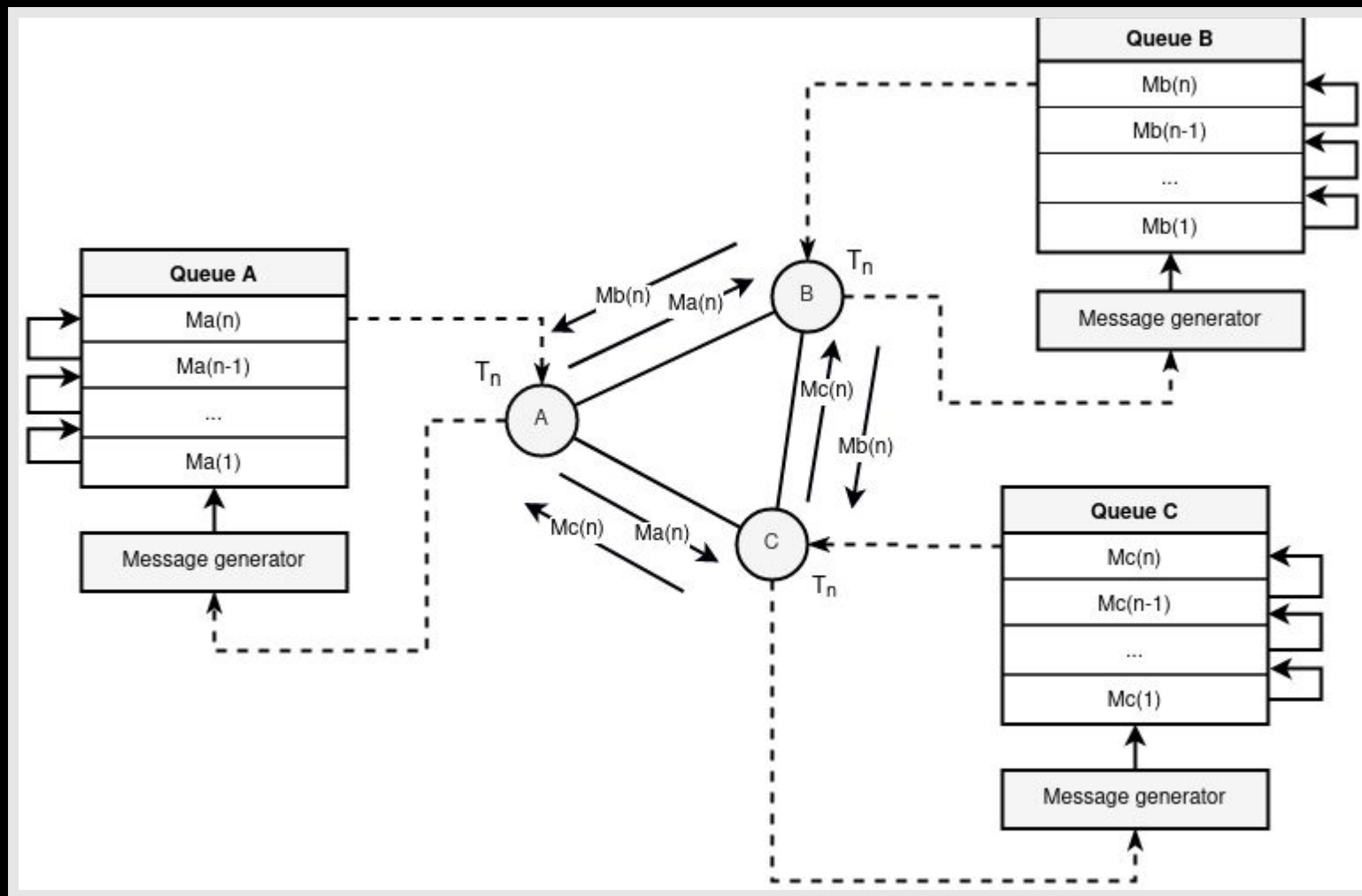
«**Hidden Lake**» (HL) — это  
одноранговая анонимная  
сеть с теоретически  
доказуемой моделью на  
базе **очередей**



# Задача на базе очередей

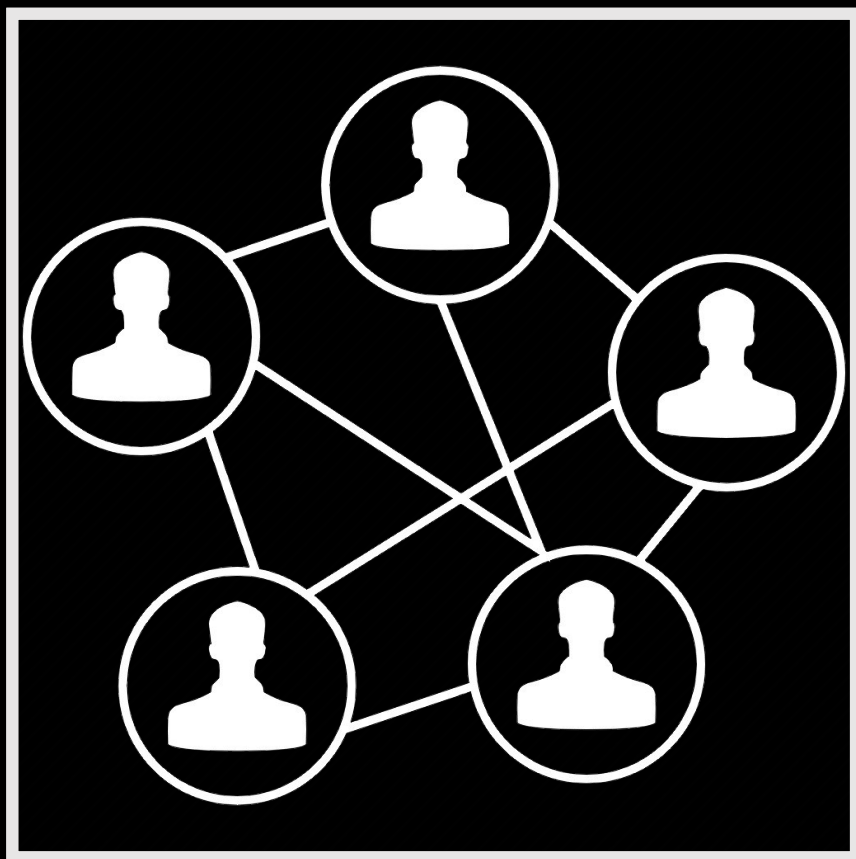
1. Каждое сообщение шифруется ключом получателя,
2. Сообщение отправляется в период  $= T$  всем участникам сети,
3. Период  $T$  одного участника независим от периодов  $T_1, T_2, \dots, T_n$  других участников,
4. Если на период  $T$  сообщения не существует, то в сеть отправляется ложное сообщение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

# Задача на базе очередей





«Hidden Lake»  
относится к  
**абстрактным**  
анонимным сетям,  
которым не важна  
замкнутость системы,  
уровень её  
централизации и  
расположение узлов



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

«Hidden Lake» является  
**Friend-to-Friend** сетью.  
Доверие к узлам  
формирует  
дополнительный уровень  
защищённости



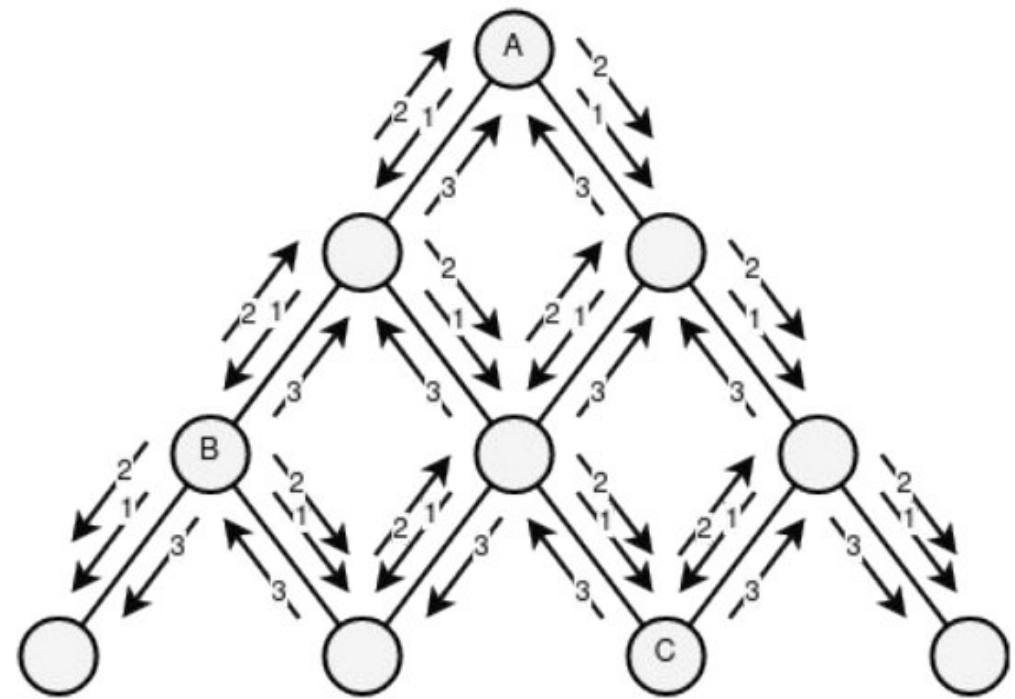
*F2F*

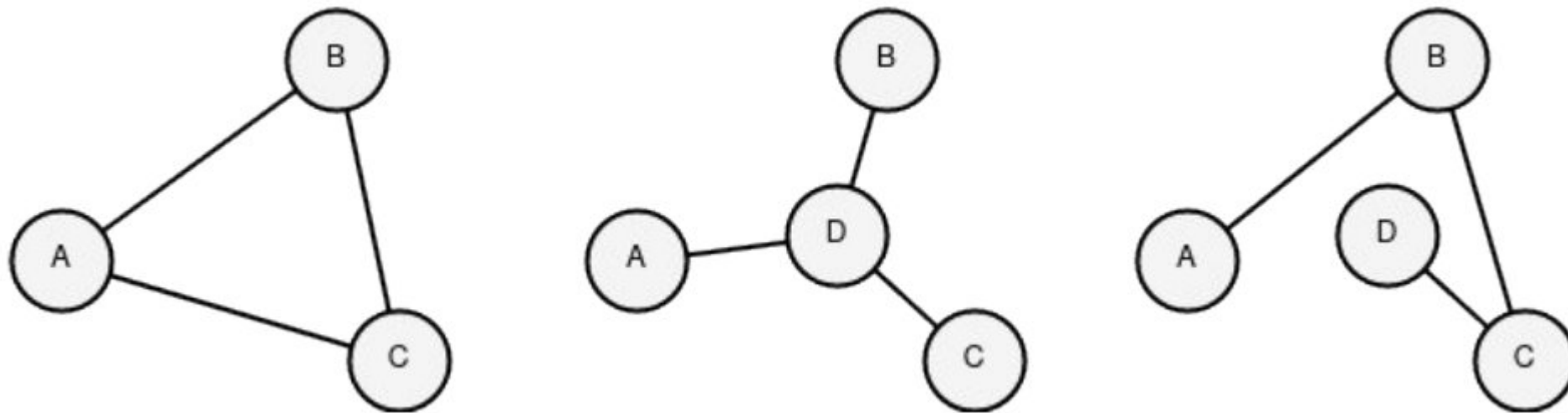
5 ^ S

Сеть относится к **пятой** ^  
**стадии анонимности**. Не  
обладает свойством  
полиморфизма, т.е.  
изменчивостью  
информации по мере своей  
маршрутизации



**Линейная нагрузка** на  
сеть является **негативным**  
качеством сети,  
зависимым от количества  
её участников



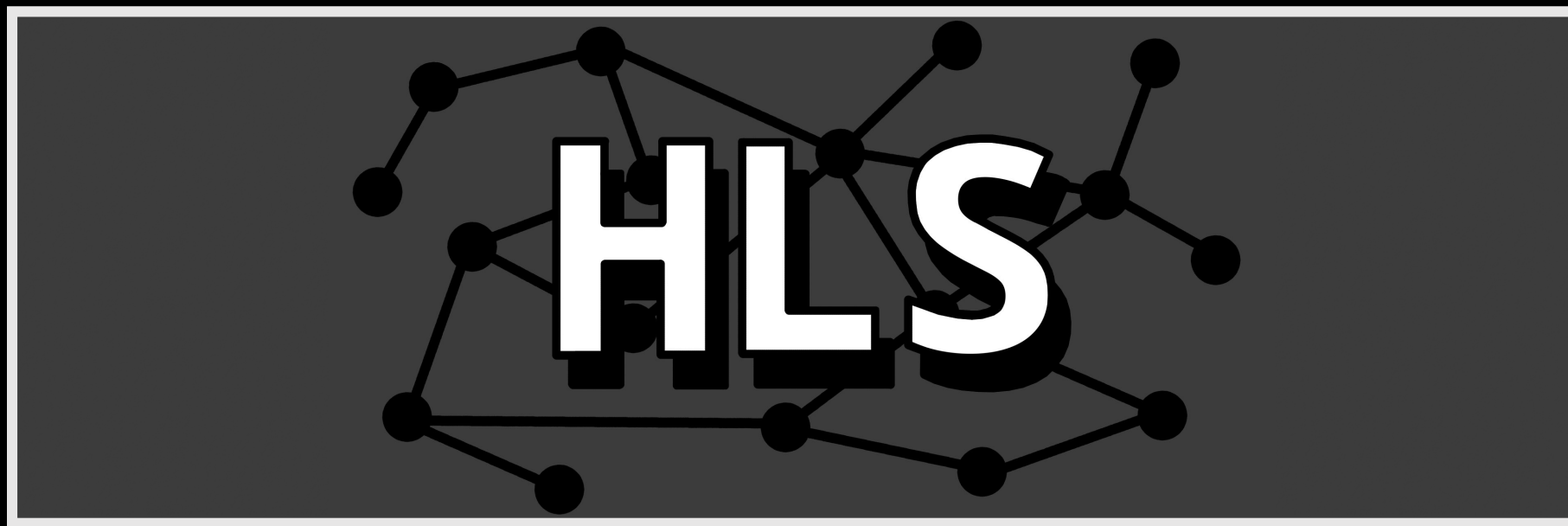


Частичным решением проблемы линейной нагрузки стало создание обособленных друг от друга **«малых озёр»** (сетей) посредством **сетевого ключа**

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

На текущий момент существует 4 сервиса: HLS, HLT, HLM, HLL

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





HLT (Hidden Lake Traffic) —  
**распределитель** трафика в  
анонимной сети. Может  
выполнять функции  
ретрансляции и сохранения  
трафика

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





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

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

The logo consists of the letters 'HLE' in a bold, white, sans-serif font, centered within a white rectangular border.

HLE





*HLA*

HLA (Hidden Lake Adapters)  
— **адаптеры** для создания  
анонимных коммуникаций в  
централизованных системах

# Сравнение с другими анонимными сетями

	Tor	I2P	Mixminion	HL	Dissent
Теоретическая доказуемость	-	-	-	+	+
Простота масштабирования	+	+	+	-	-
Простота реализации	-	-	+	+	-
Параллельность запросов	+	+	+	-	-
Закрытая внутренняя сеть	+/-	+	-	+	+
Децентрализованная архитектура	-	+	-	+	+
Сервисная API реализация	+	+	-	+	-

# Литература

1. Теория строения скрытых систем
2. Монолитный криптографический протокол
3. Абстрактные анонимные сети
4. Децентрализованный протокол обмена ключами

# Ссылки

- Проект go-peer

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

- Директория Hidden Lake

[https://github.com/number571/go-peer/tree/master/cmd/hidden\\_lake](https://github.com/number571/go-peer/tree/master/cmd/hidden_lake)