Threat Modelling & Security Analysis for Robot and Service

Shabnaz Khanam
Matriculation ID :11143655

Content Overview

1 Introduction

A Robot is a modern technology and its industrial demand is growing day by day

1 Introduction

Likewise, it becomes a threat due to its vulnerabilities and produces trash instead of accurate services. This has a negative impact on maintenance costs of the industry.

2 Object

Define the security mechanism of the system where the implemented protocol claims that the stable communication is established between application and system with balance their privacy to control the device

3 Implementation

System Overview

node

node

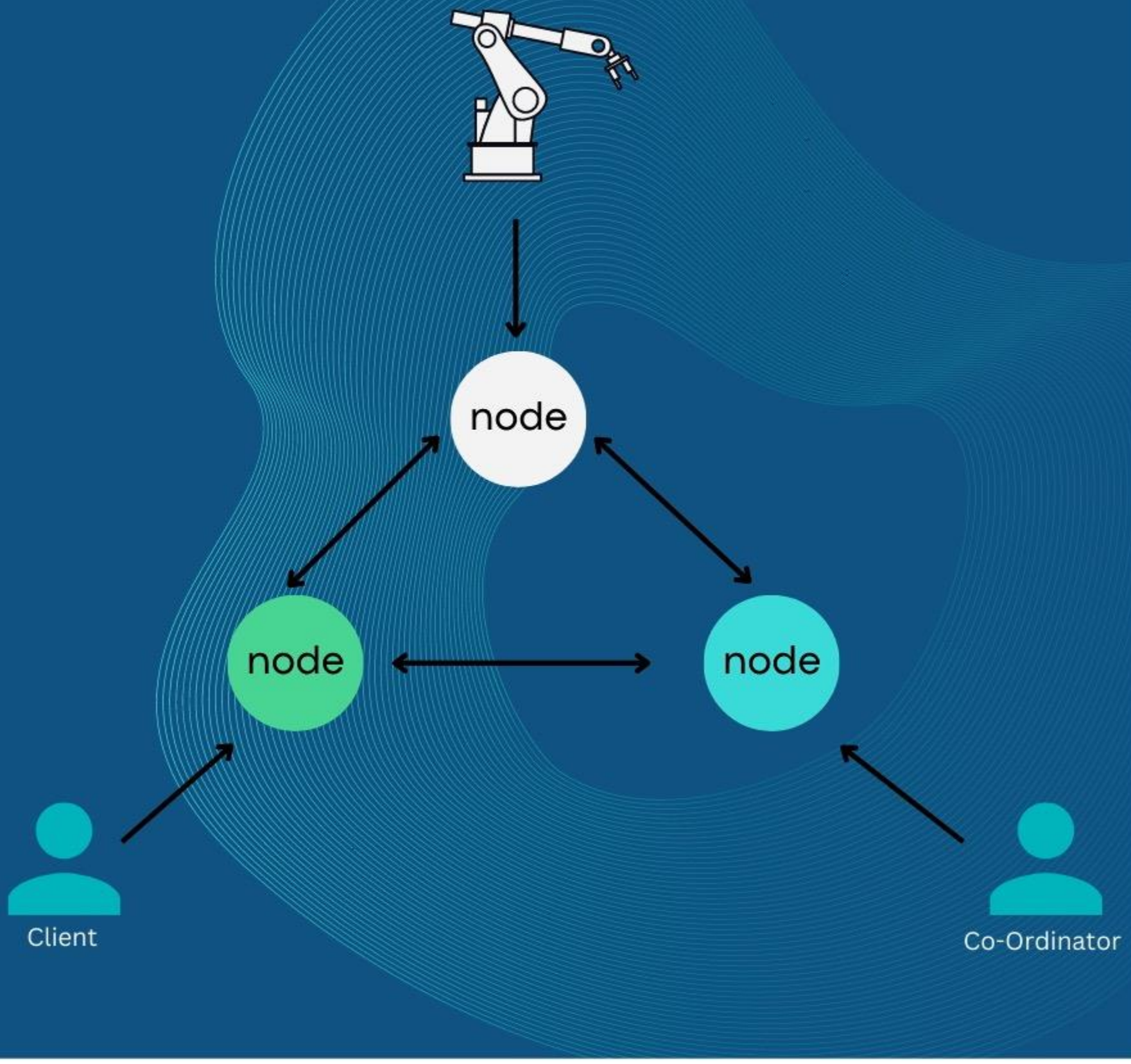
node

Client

Co-Ordinator

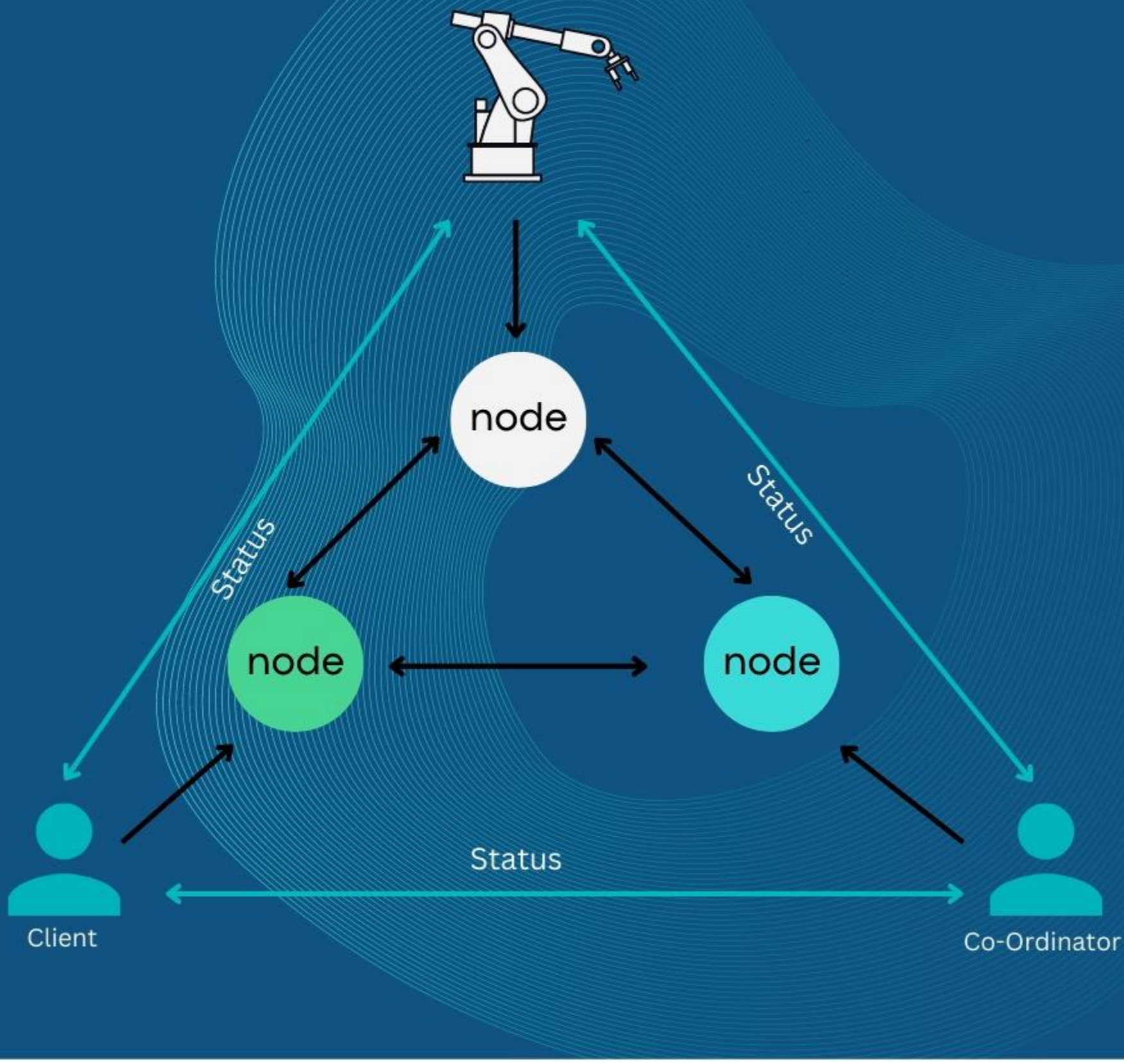
3 Implementation

System Overview



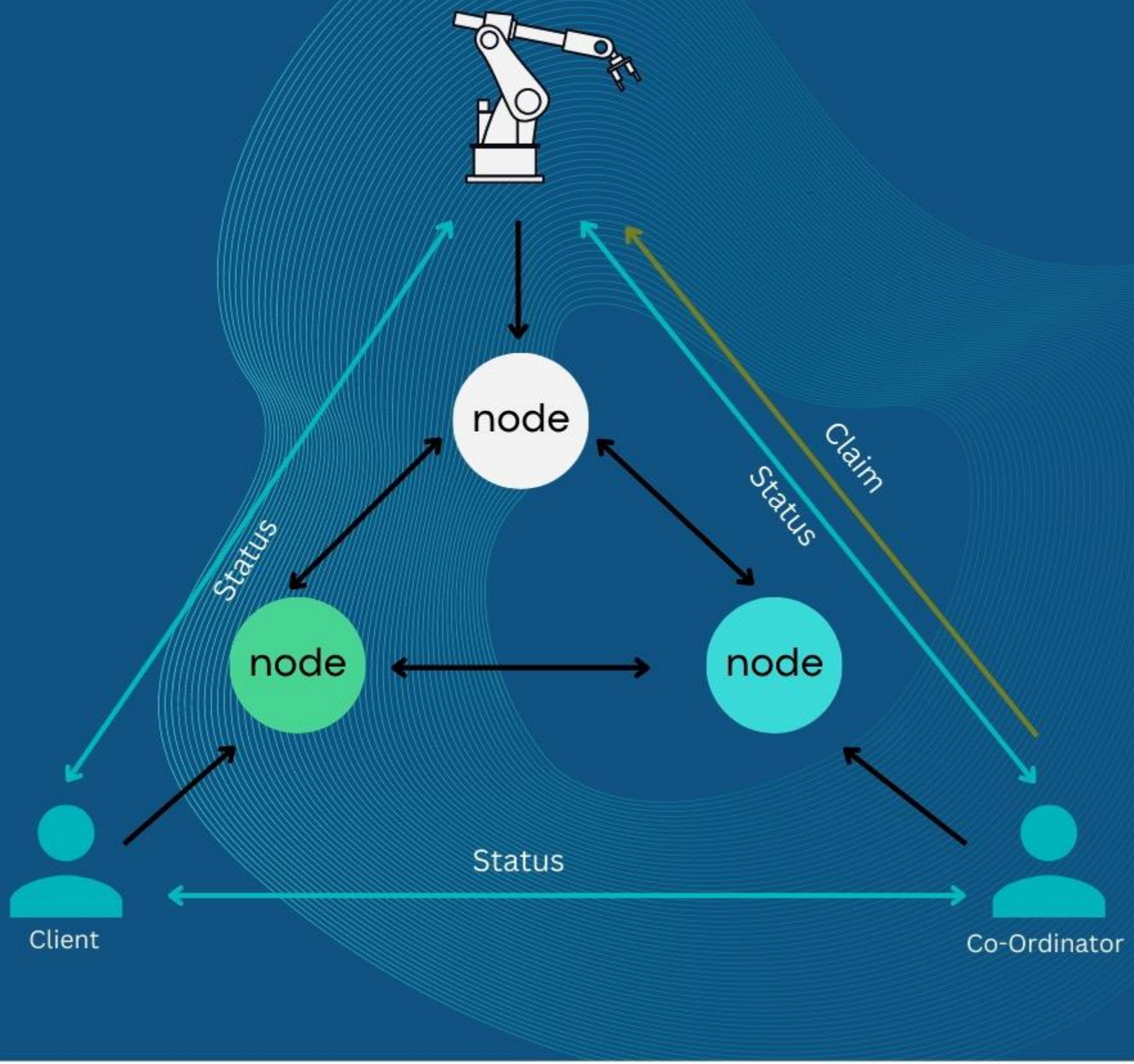
3 Implementation

System Overview



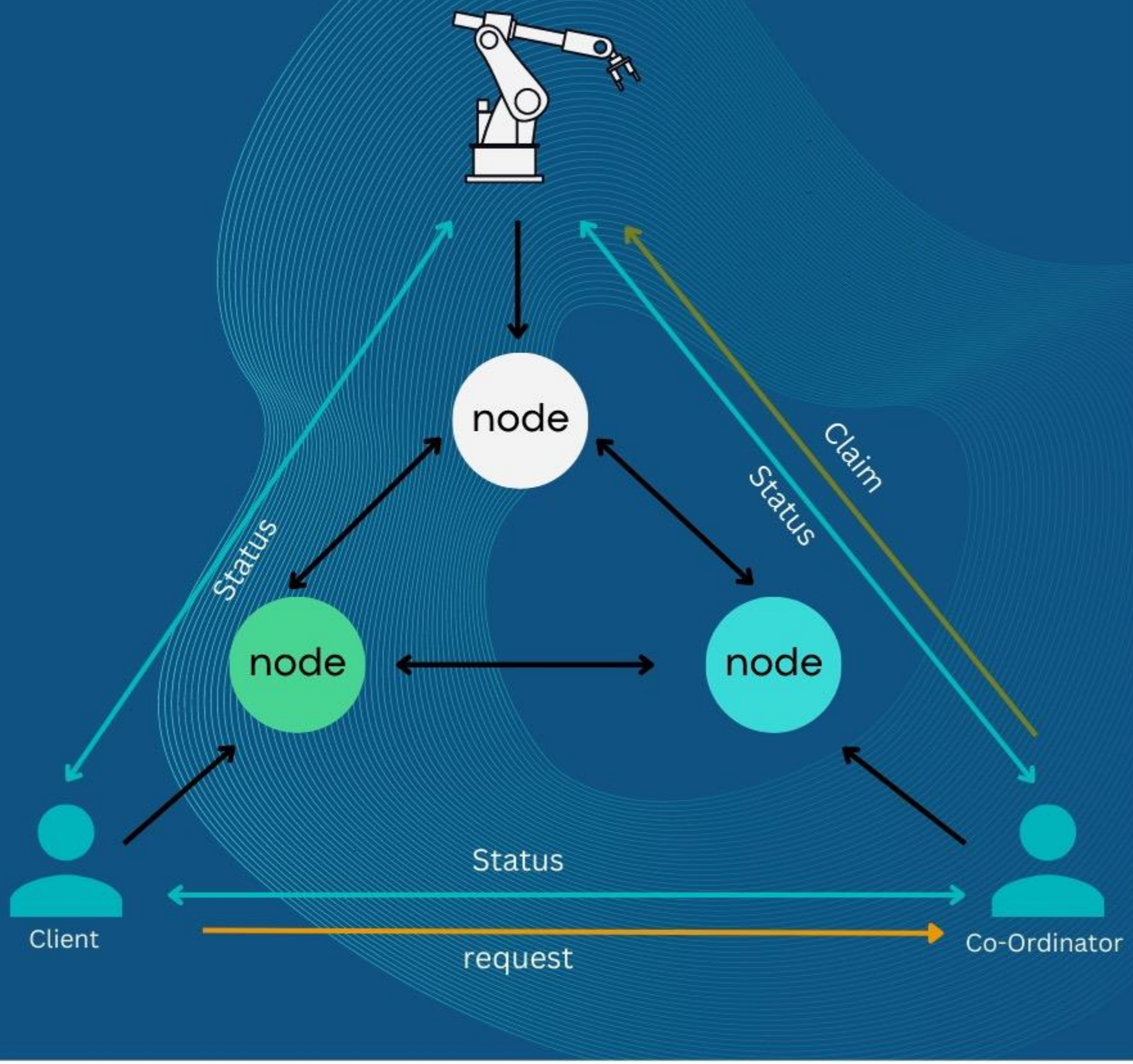
3 Implementation

System Overview



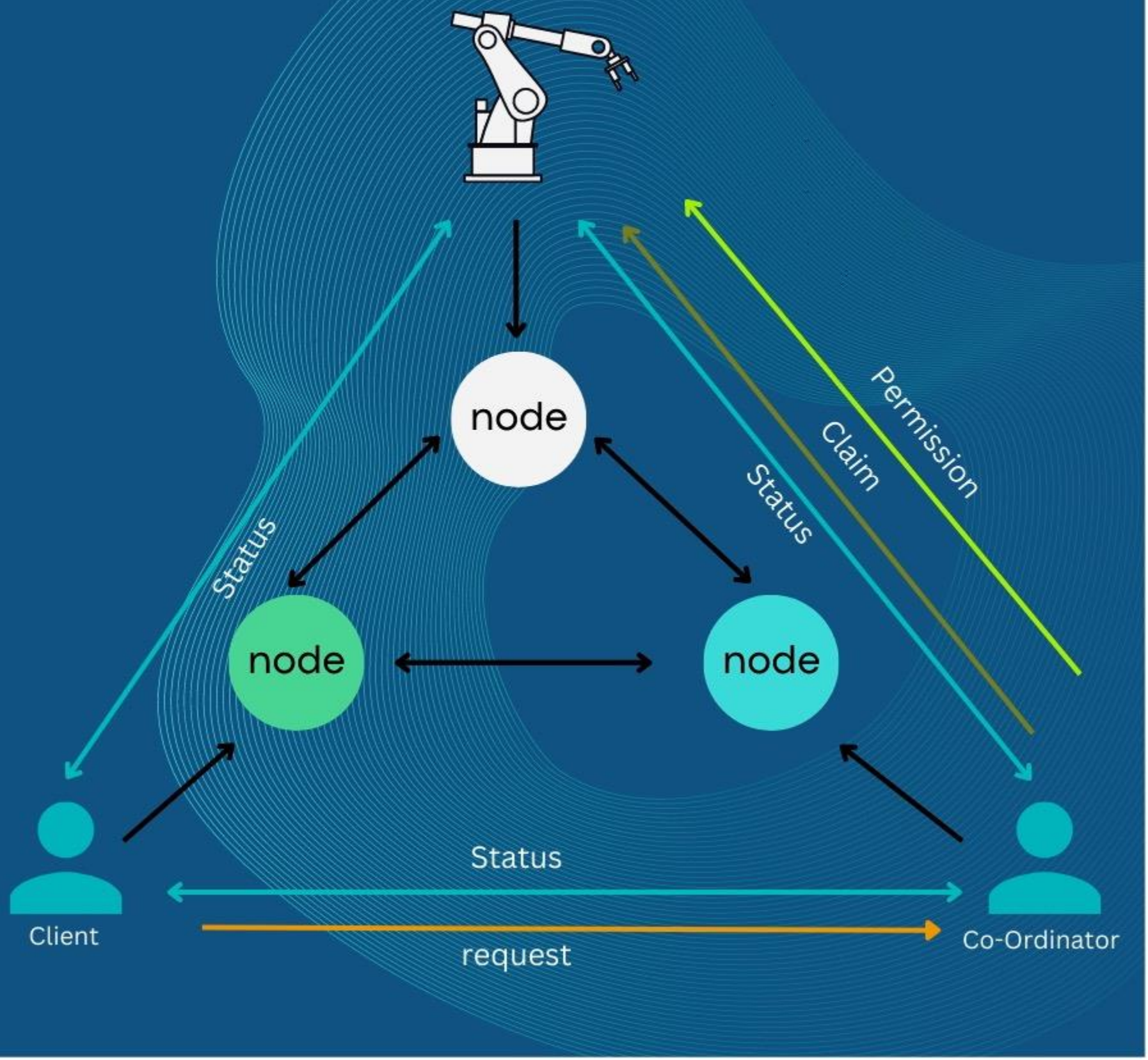
3 Implementation

System Overview



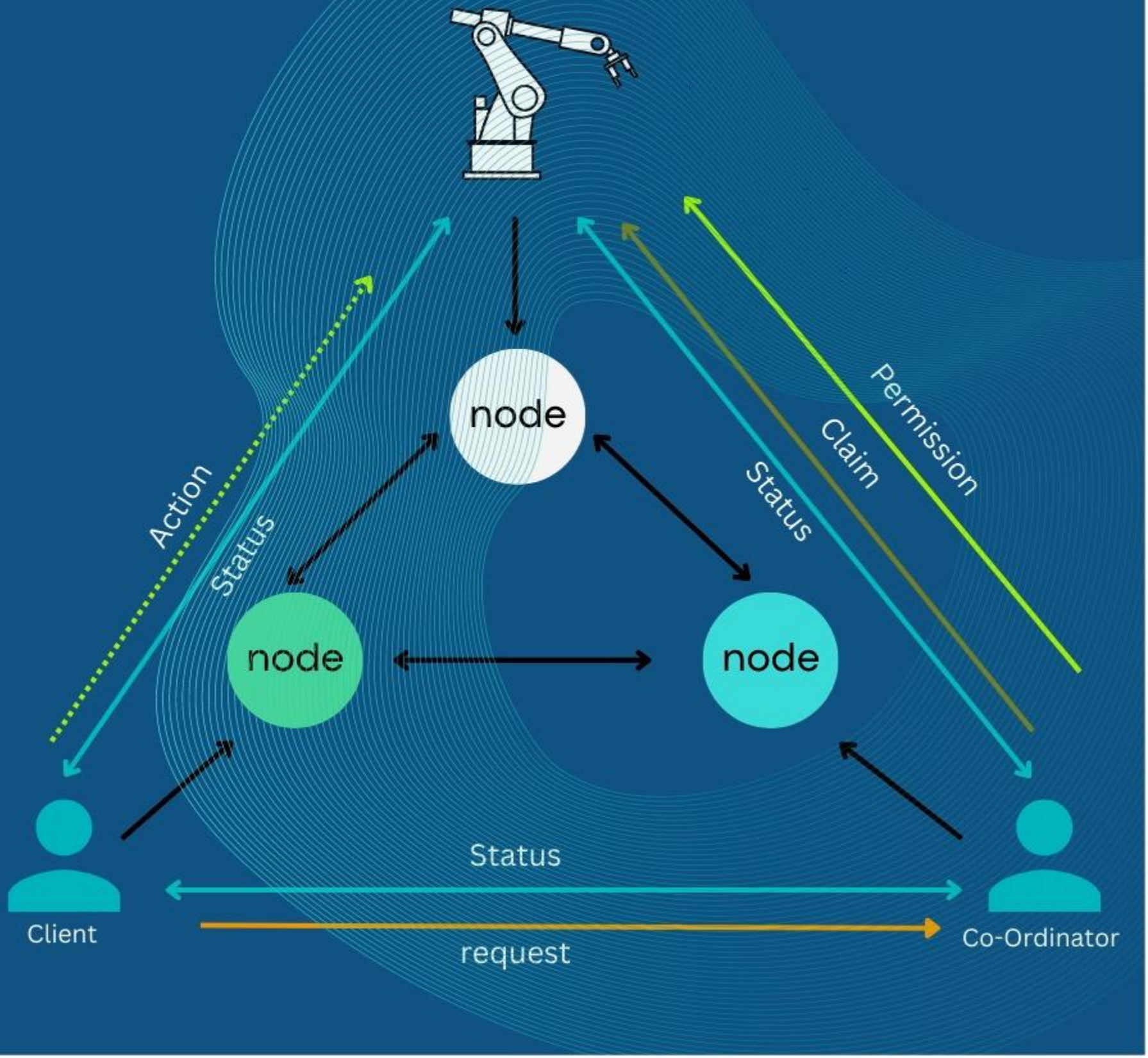
3 Implementation

System Overview



3 Implementation

System Overview



4 Neuropil : Real-Life Implementation

Now we come to a short overview of the function of Neuropil by using the robot

5 Identify threat

Confidentiality	*Decryption key is disclosed*
Integrity	*Modified by attacker, losing the Control of Robot,Maintenance cost is increased*
Authentication/ Authorization	*Lacing of identity, can't make difference real user/client and third party*

6 Neuropil protocol

Based on a Public key Infrastructure (PKI) with a distributed Hash Table (DHT)

6 Neuropil protocol

E2E encrypted

Token

Handshake Message (Signature)

Subject based

Data Network (data channel)

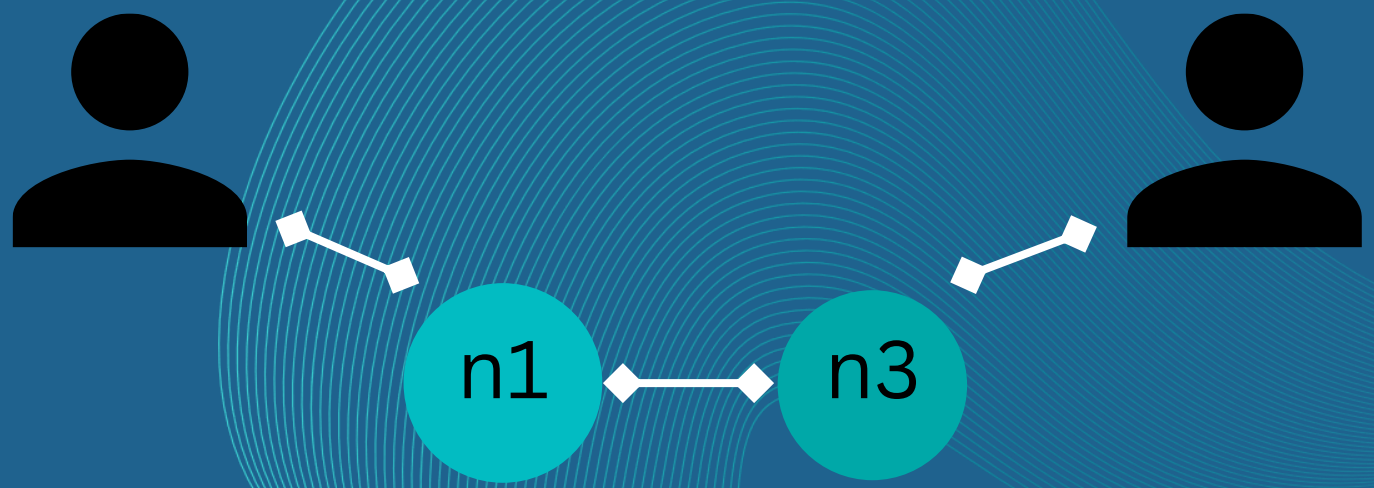
Self -Sovereign Identity (Digital Identities)

Zero Architecture (Verification)

Attribute based access control

7 Security structure

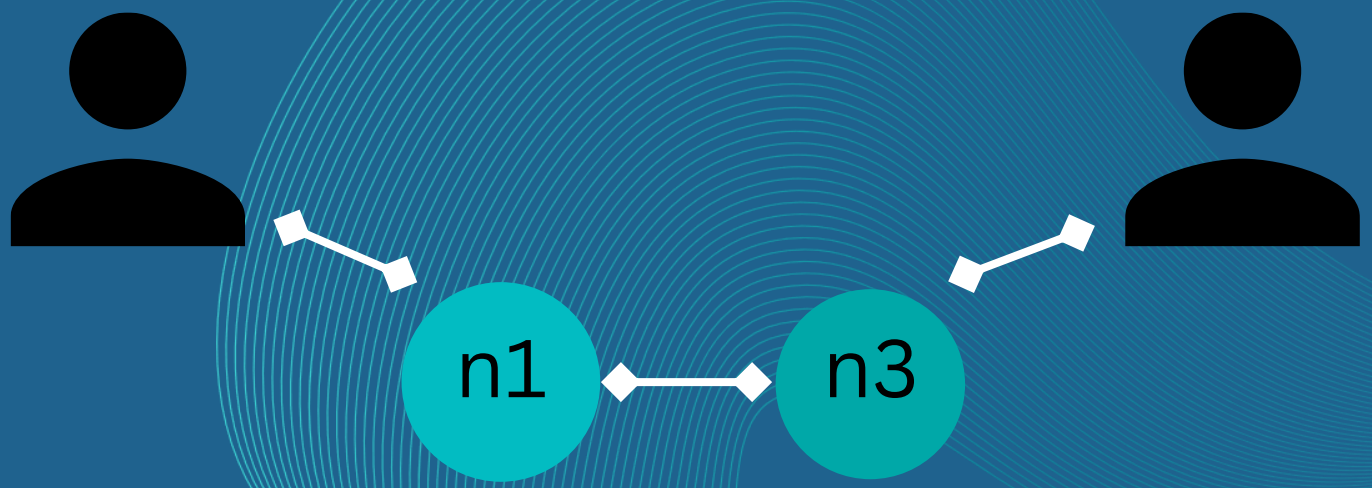
Handshake Message



Exchanging Handshake message

7 Security structure

Handshake Message

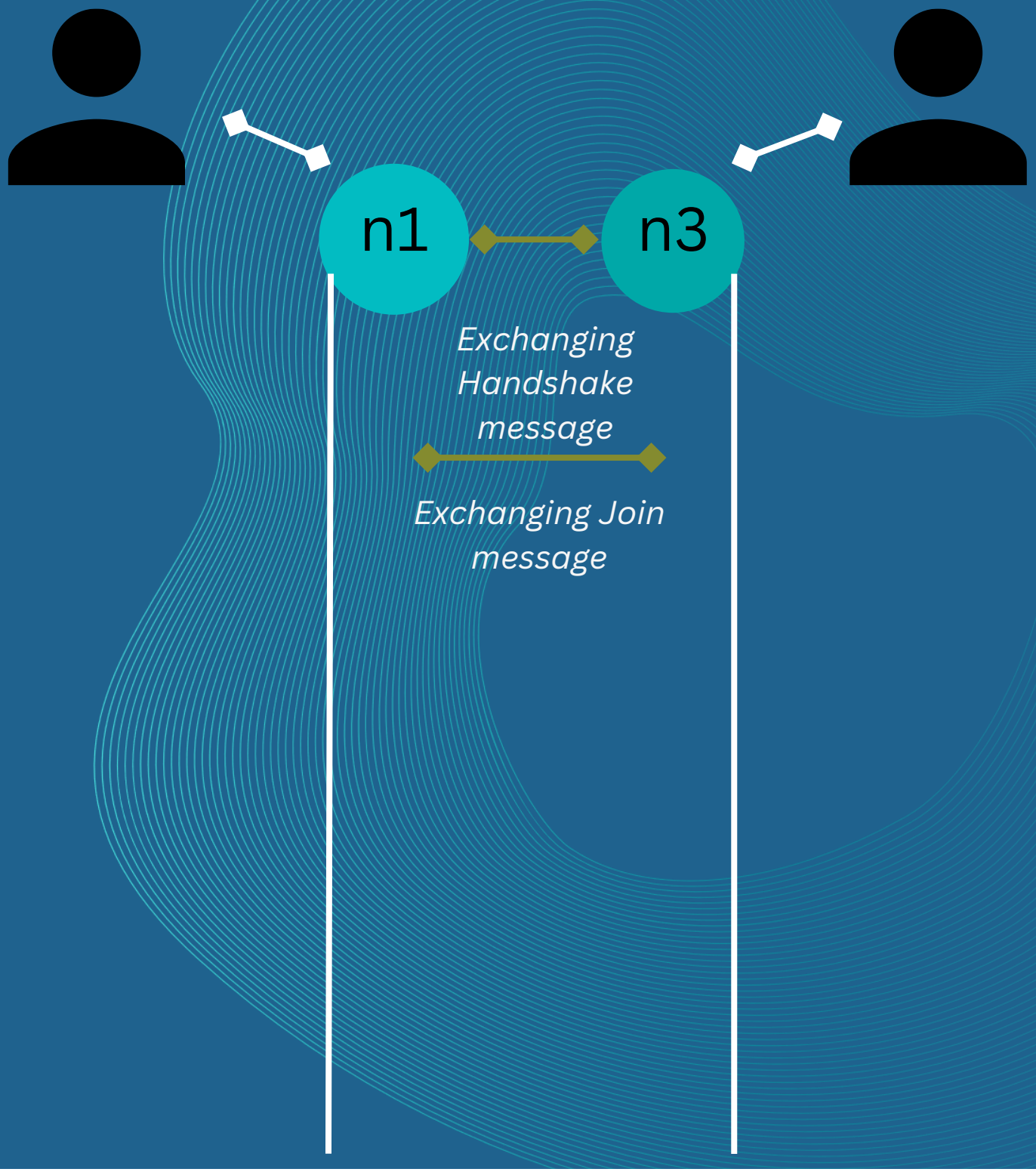


Exchanging Handshake message

Realm:	empty
Issuer:	fingerprint(n)
Subject:	hostname & port number
Audience:	empty
Attribute:	empty
Pk:	public key(n)
Signature :	sig without attributes
Signature :	sig with attributes

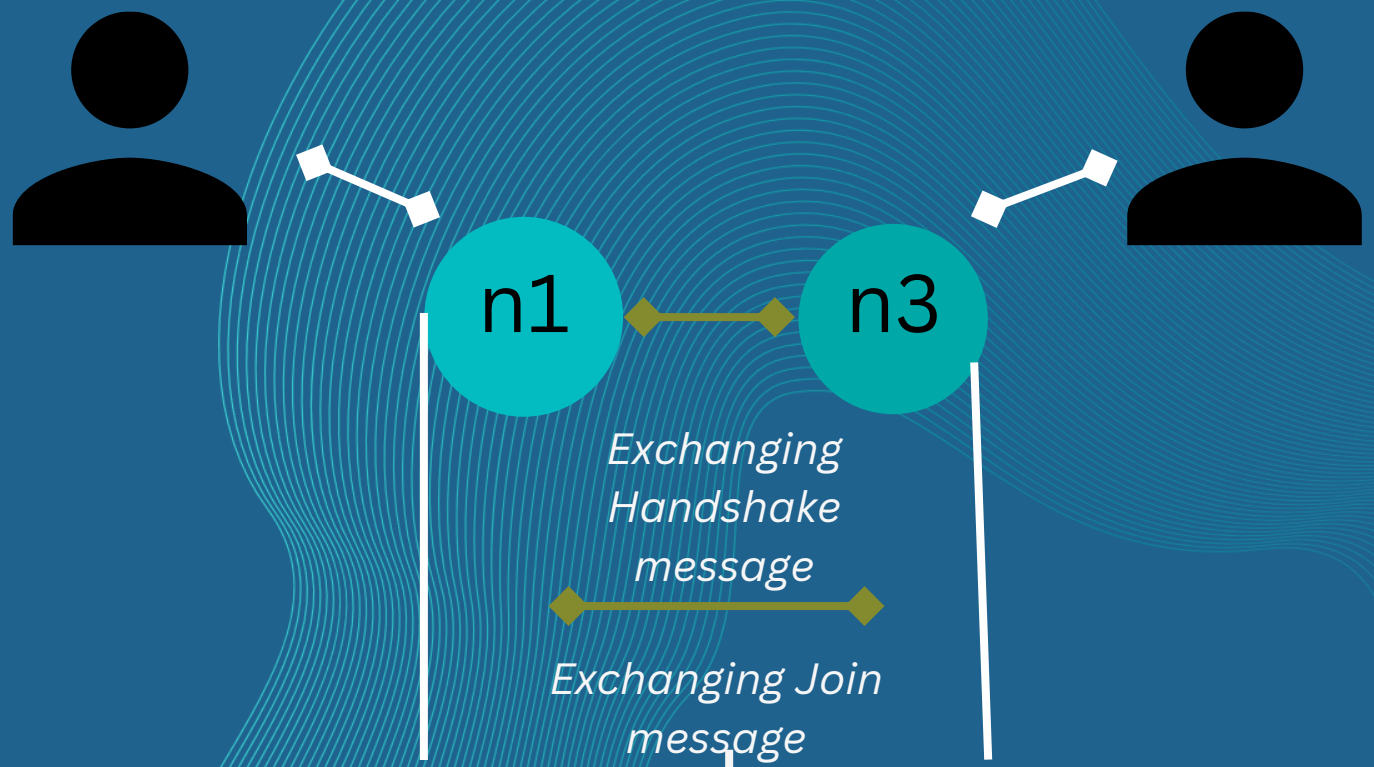
7 Security structure

Data flow



7 Security structure

Data flow



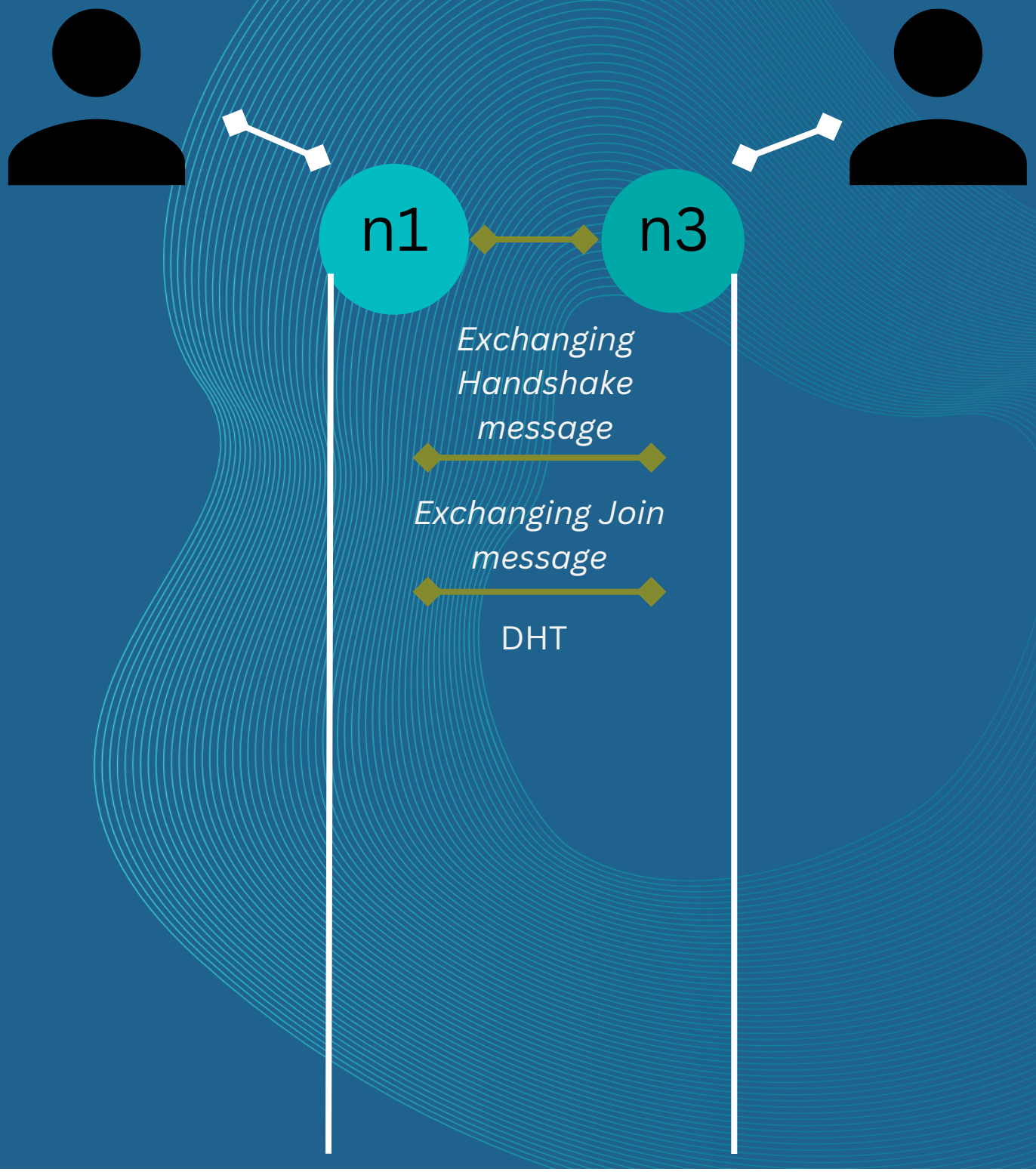
nfp = Hash(node token,signature)
ifp =Hash (identity token,signature)

Realm:	empty
Issuer:	empty
Subject:	hash(user data)
Audience:	empty
Attribute:	nfp
Pk:	public key(n)
Signature :	sig without attributes
Signature :	sig with attributes

Realm:	empty
Issuer:	fingerprint(n)
Subject:	hostname & port number
Audience:	empty
Attribute:	ifp
Pk:	public key(n)
Signature :	sig without attributes
Signature :	sig with attributes

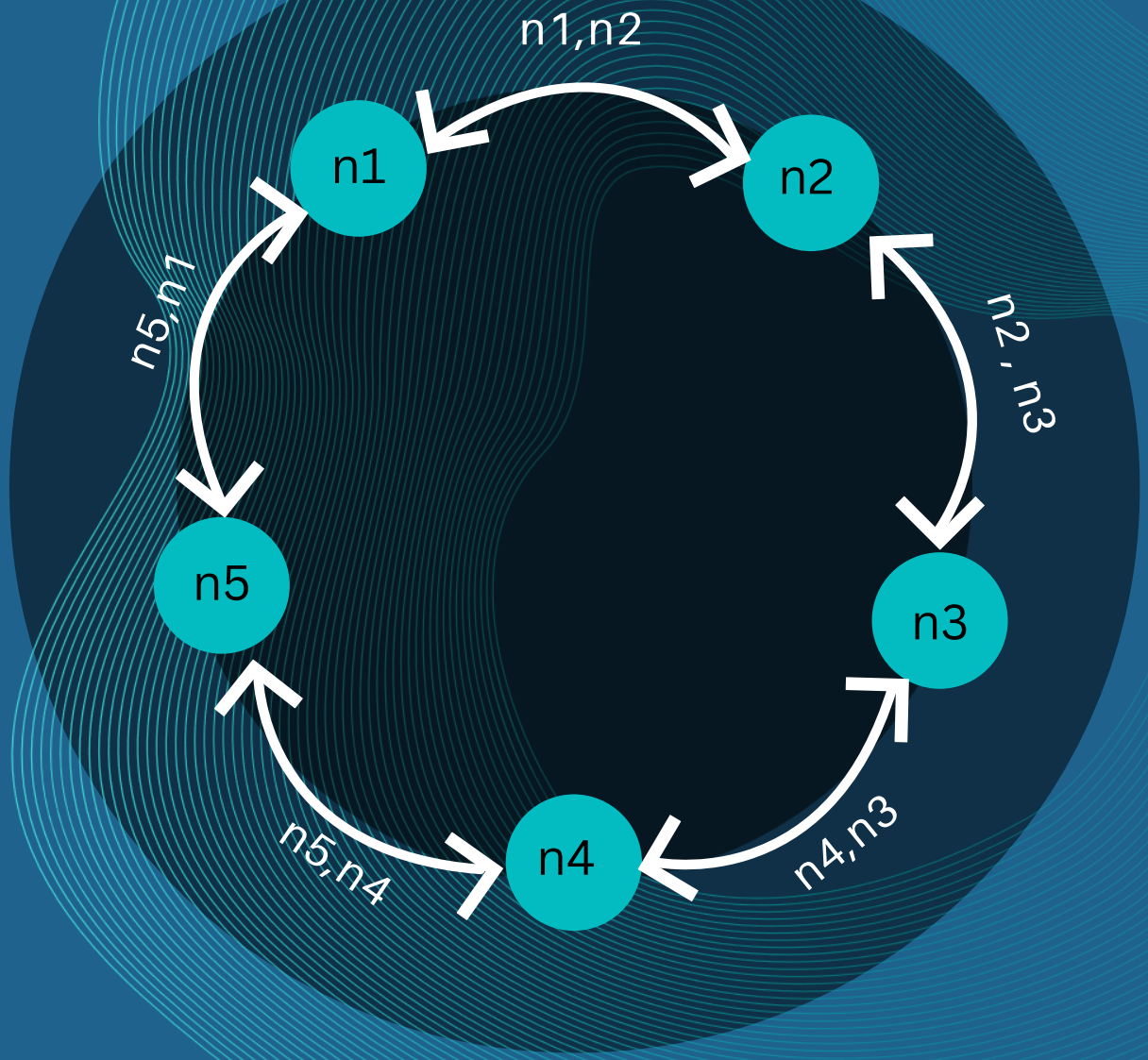
7 Security structure

Data flow



7 Security structure

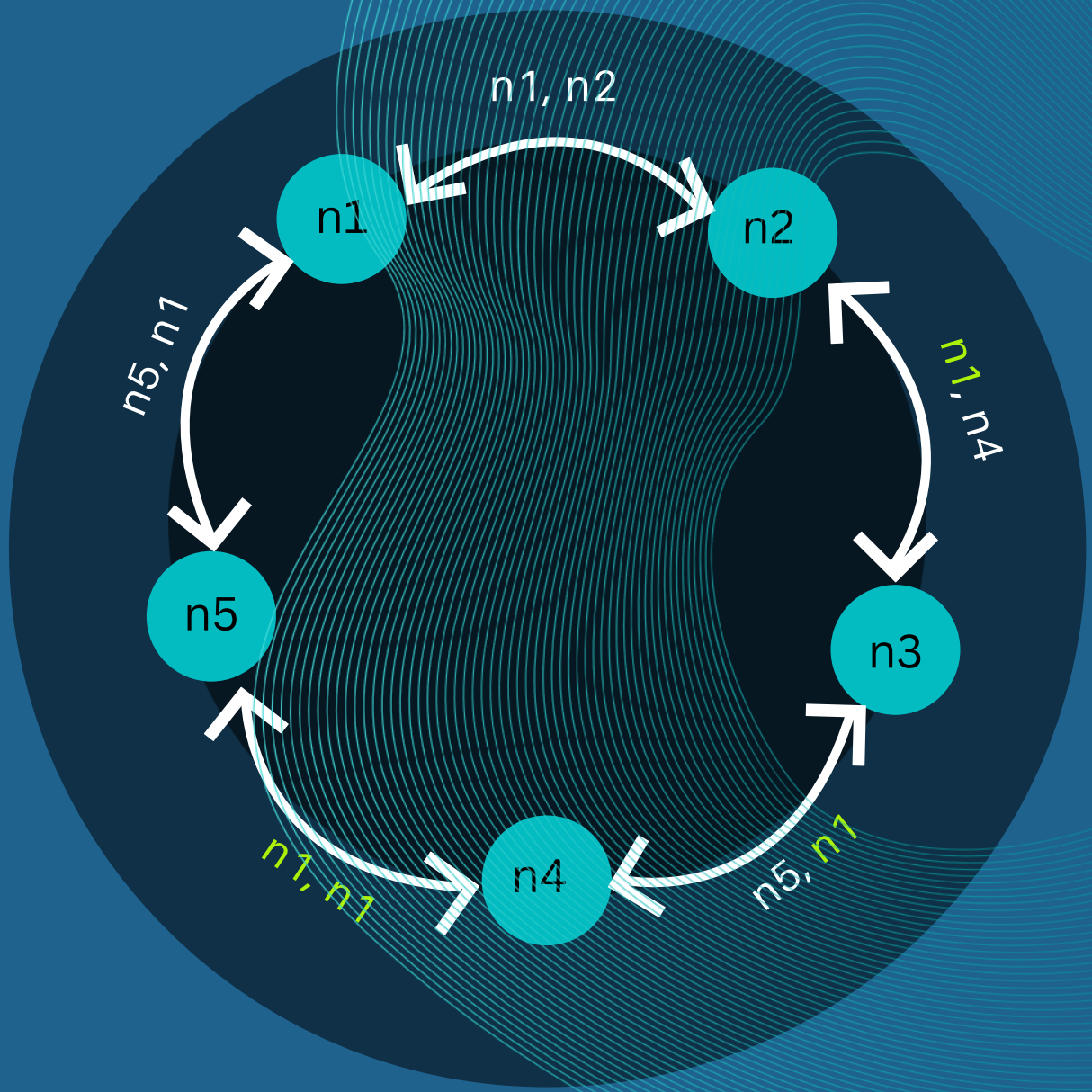
Distributed Hash Table



Nodes are connected

7 Security structure

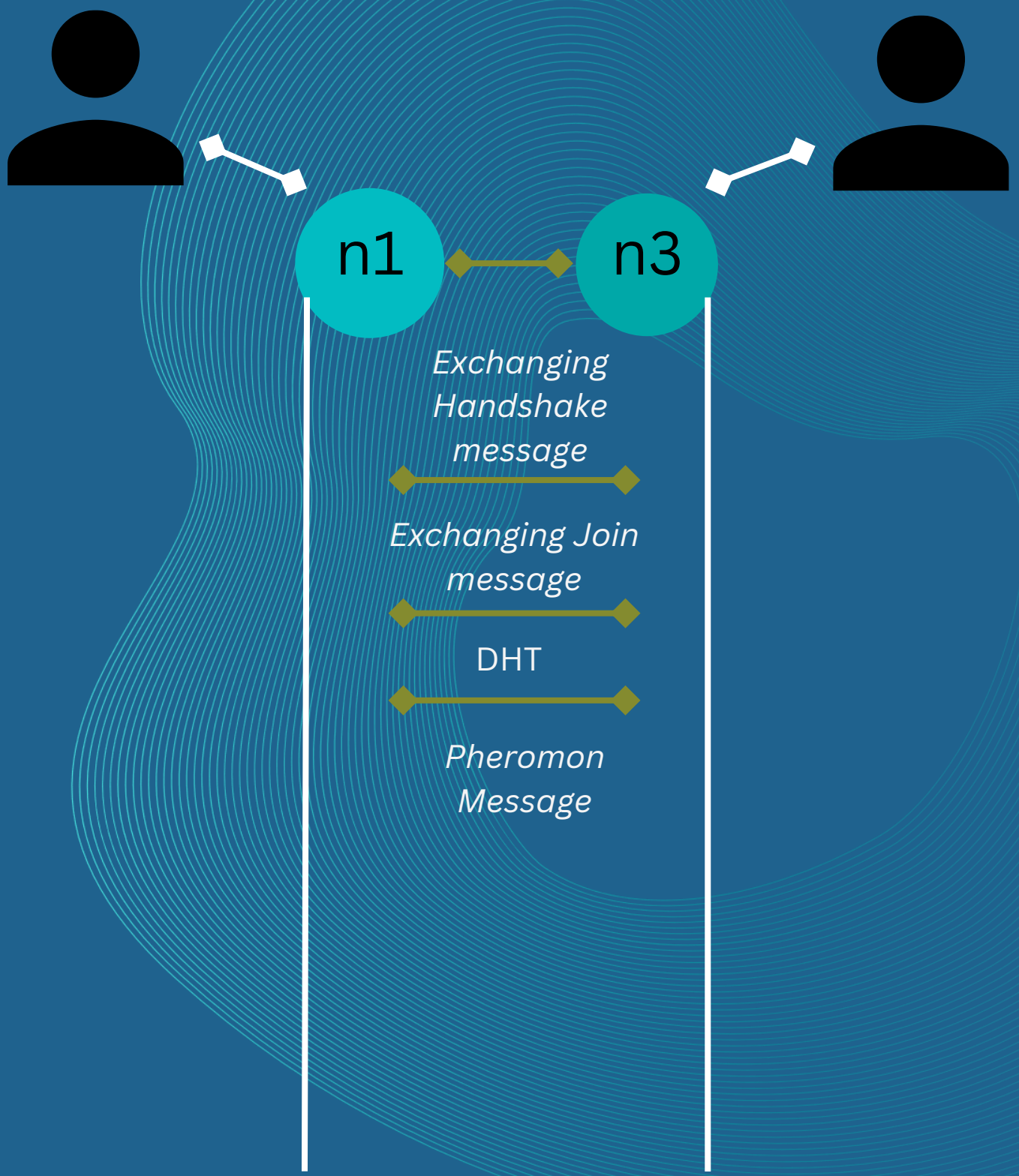
Distributed Hash Table



Through The update message other nodes are informed about new node

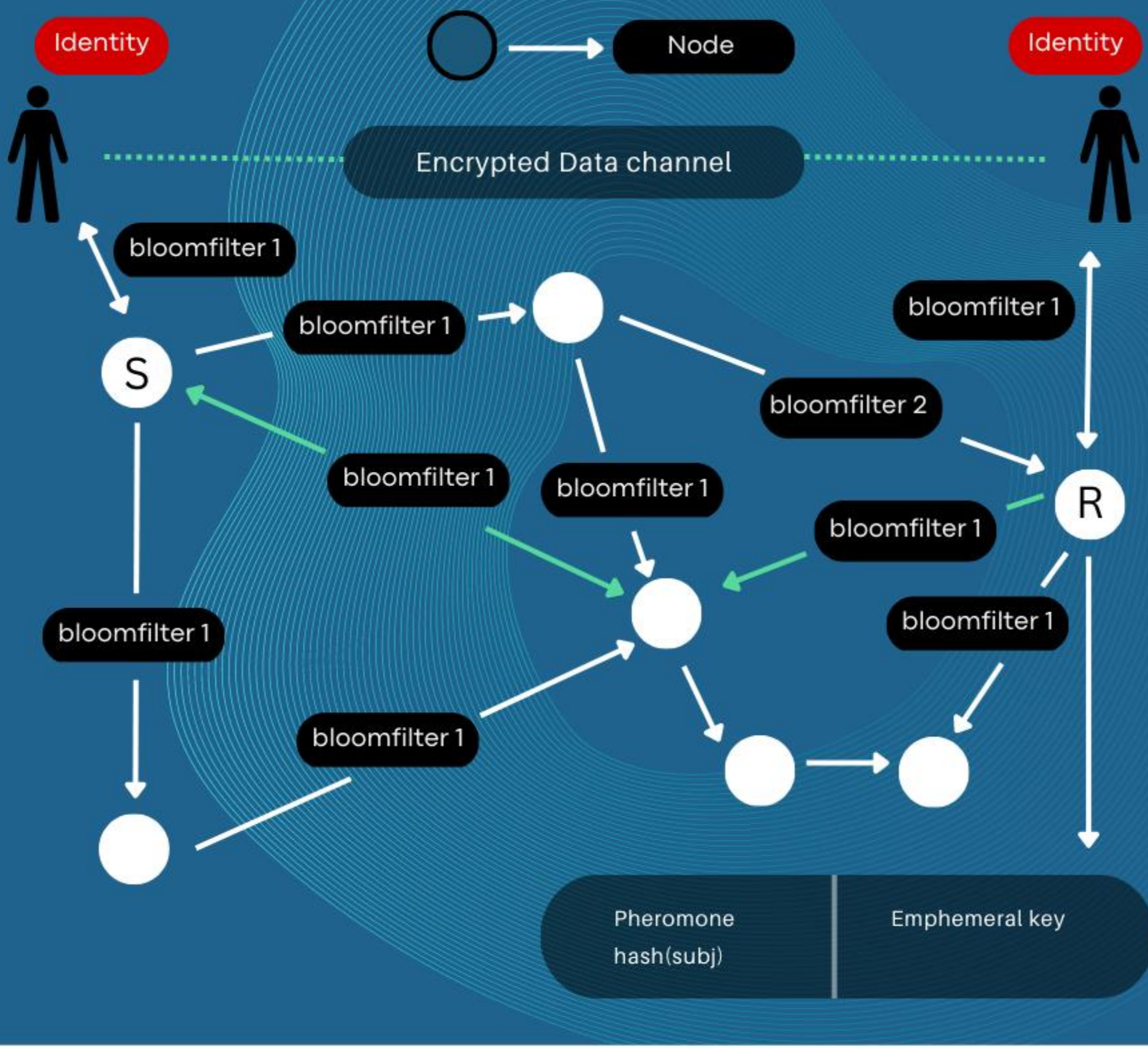
7 Security structure

Data flow



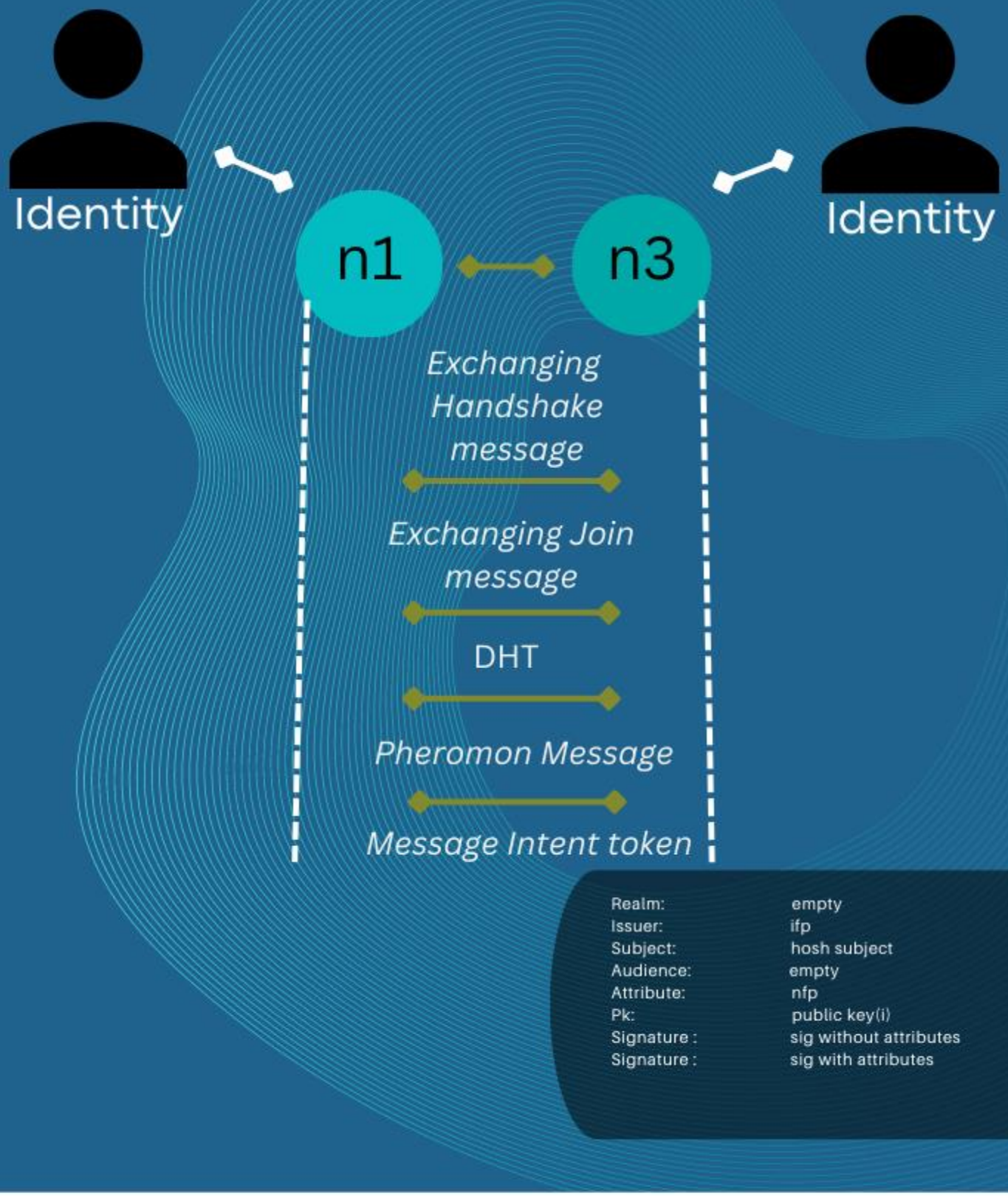
7 Security structure

Pheromone Message



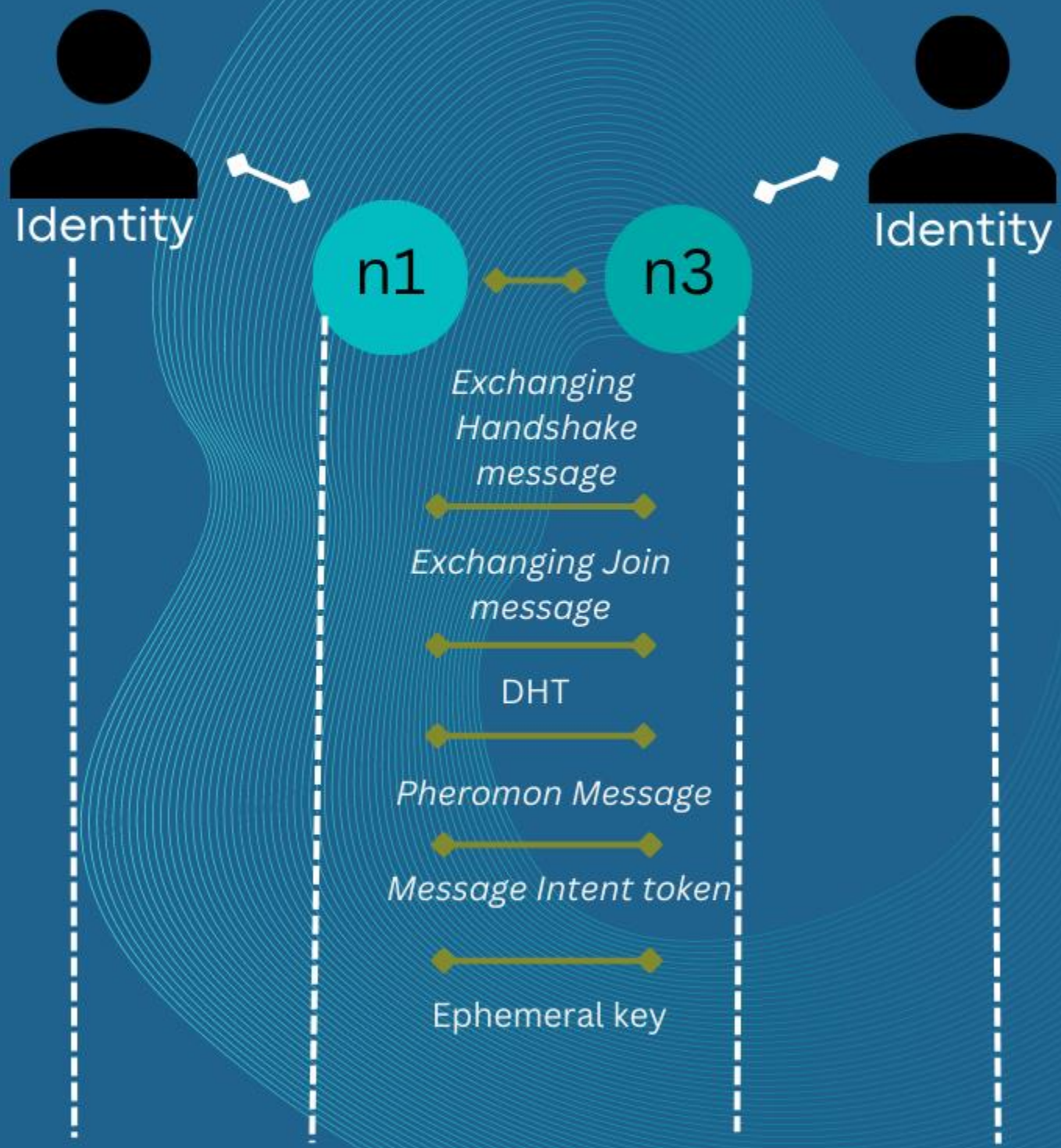
7 Security structure

Data flow



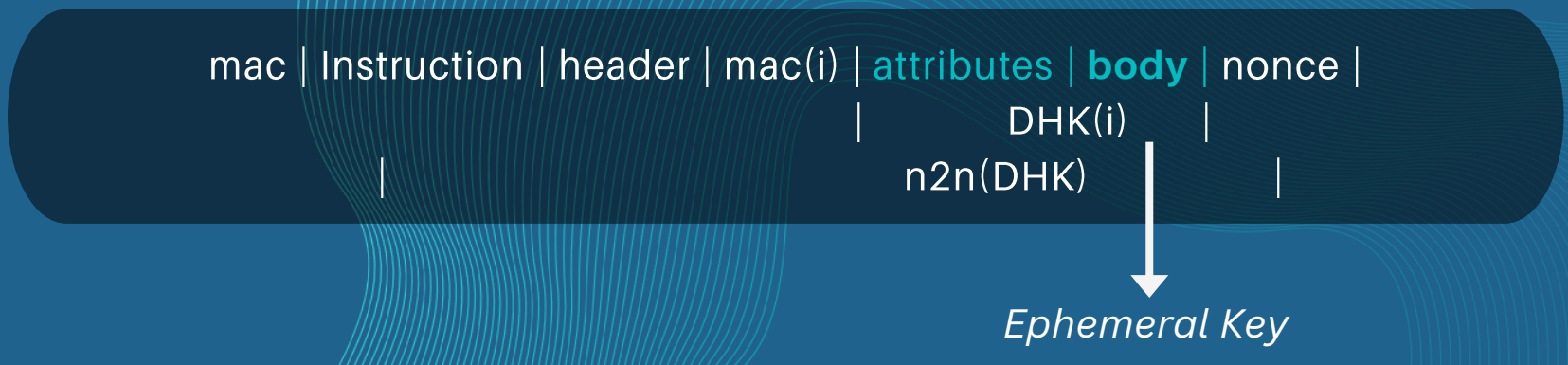
7 Security structure

Ephemeral Key



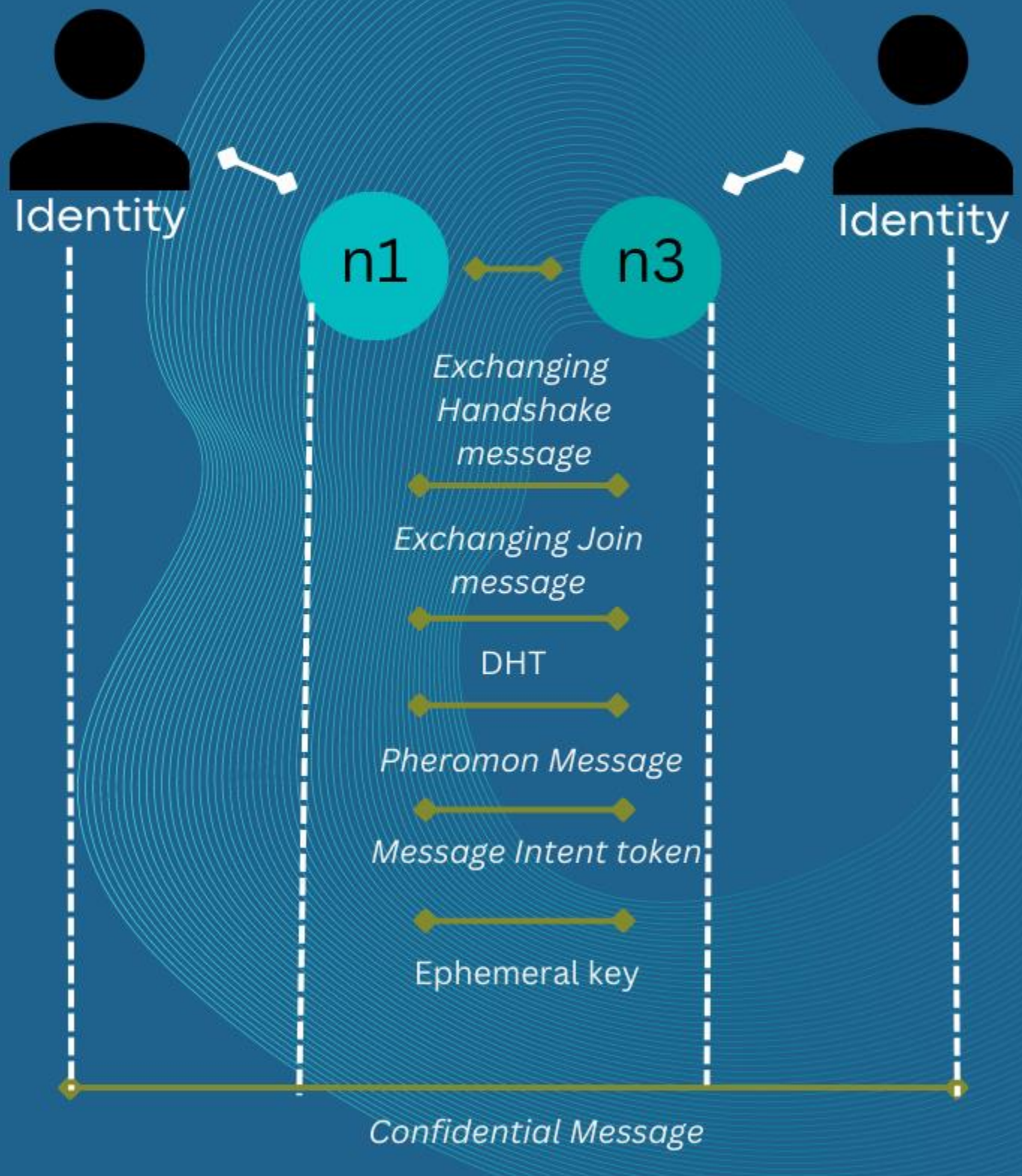
7 Security structure

Data flow



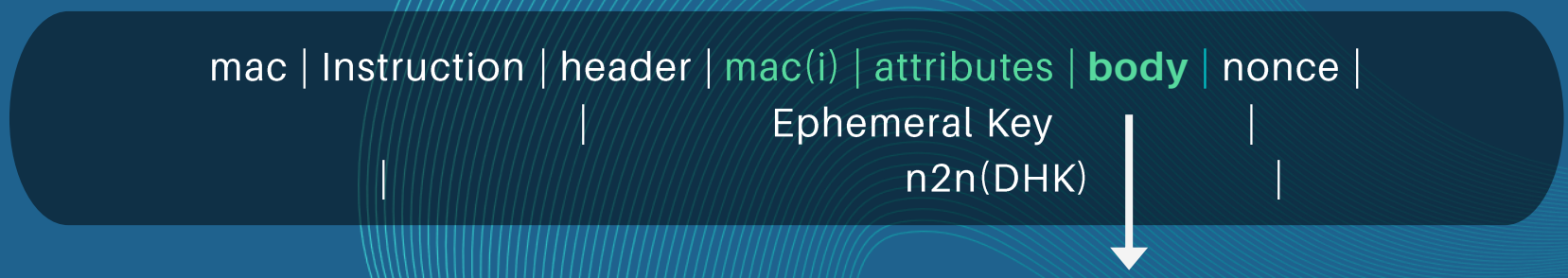
7 Security structure

Data flow



7 Security structure

End-to-End Encryption



7 Security structure

End-to-End Encryption

Action Message

mac | Instruction | header | mac(i) | attributes | **body** | nonce |
| Ephemeral Key |
| n2n(DHK)

Confidential Message

MAC = Message(mac(n)+Instruction,header,nonce,mac(i))+ DHK(n)
Instructions = Sequence Number of node
Header =

From : Fingerprint
To : Fingerprint
UUID : Universal Unique Identifier
TTL : Time to live
Subject : Hash (subject)
Timestamp : Record with time

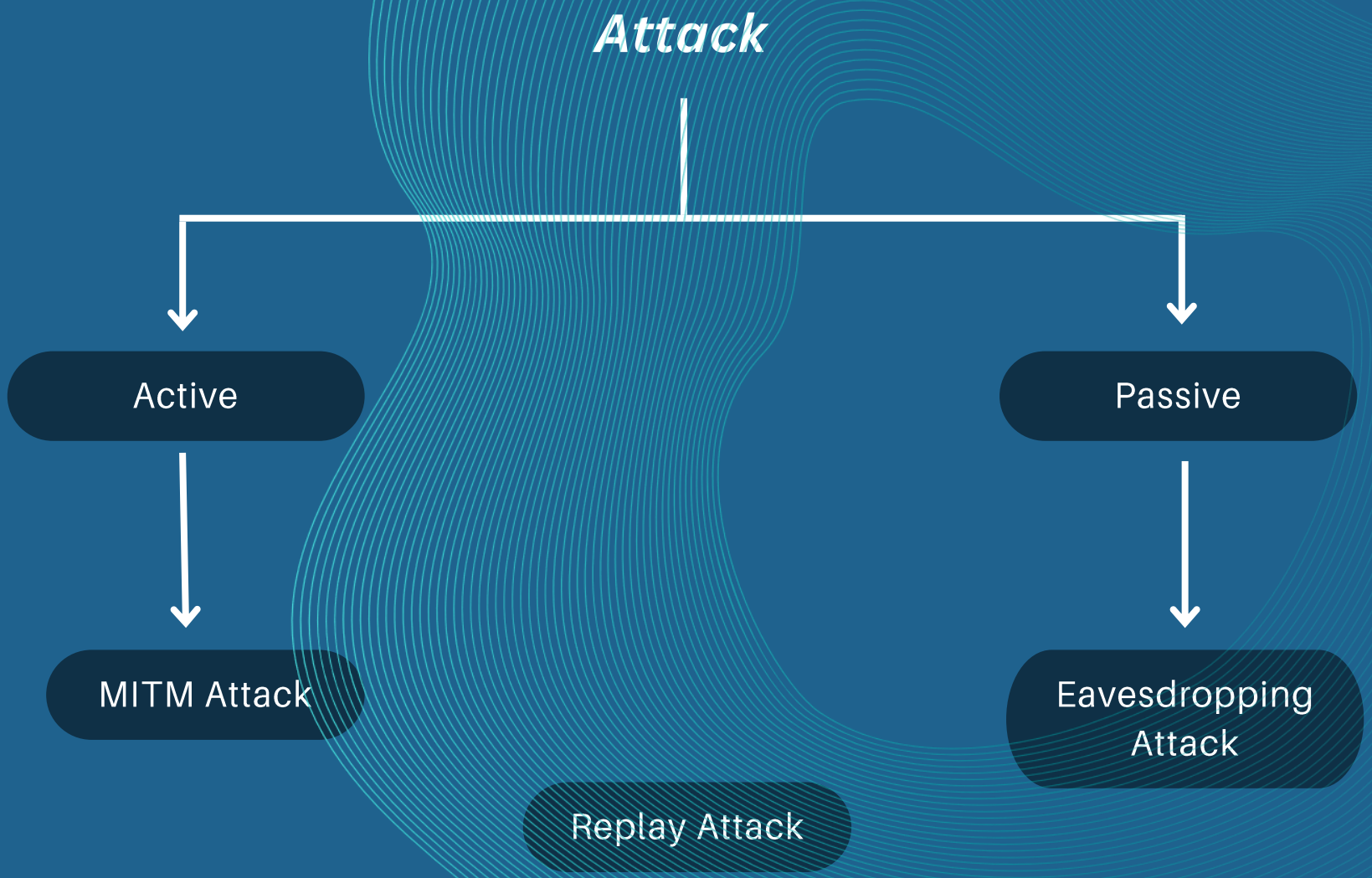
MAC(i) = Message(mac(i),Attribute, body) + Ephemeral key
Attributes = Extra attributes of a message (similar to http header fields)
Body = Payload
nonce = Random value

8 Attack

In order to define performance and security, let's analyze with some attacks

8 Attack

In order to define performance and security, let's analyze with some attacks



8 Attack

Eavesdropping Attack

8 Attack

Eavesdropping Attack

The attacker is able to read the message

8 **Attack**

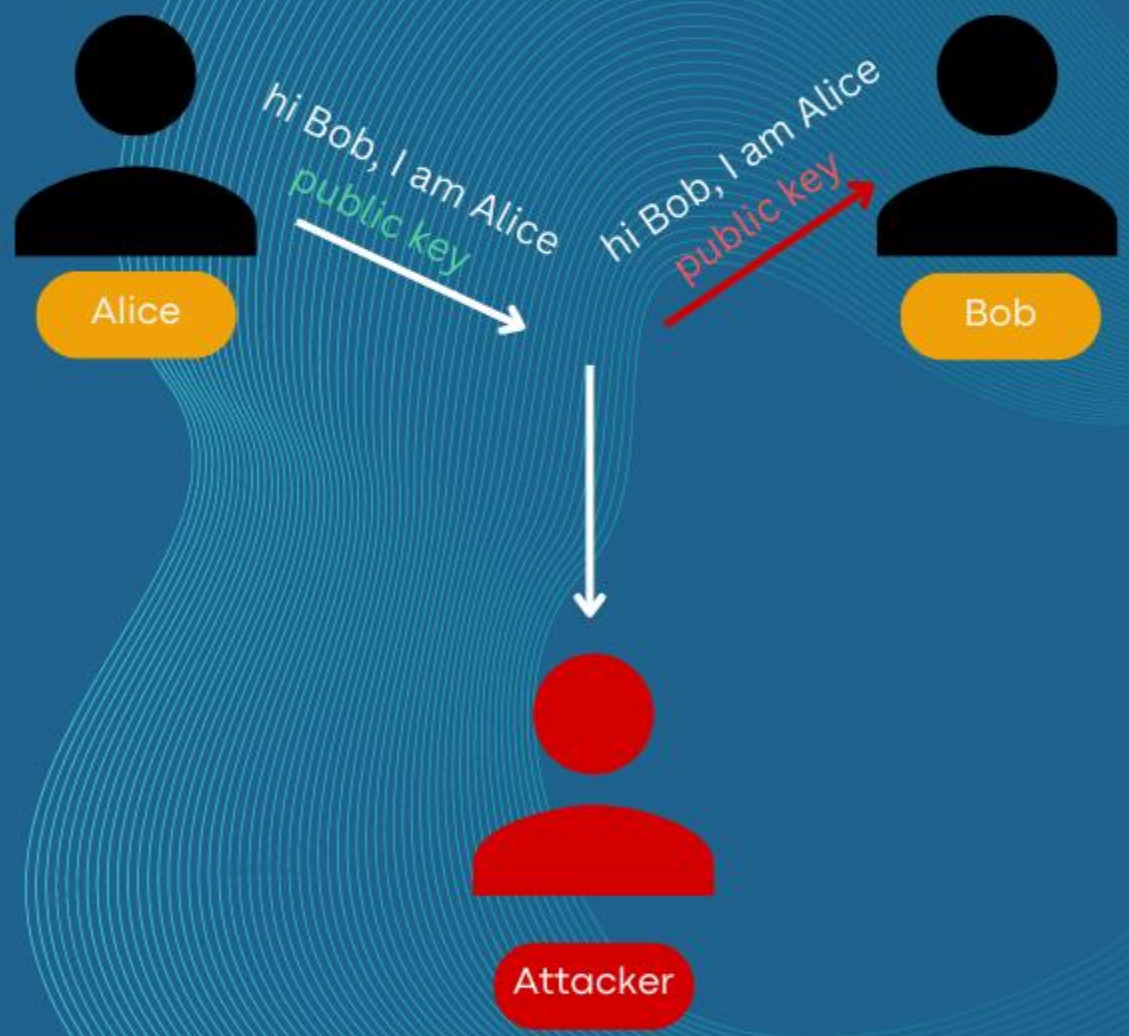
Eavesdropping Attack

In the Neuropil Protocol messages are encrypted except the handshake message

During an encryption, the message maintain a transport layer security and a handshake message contains core of information of node

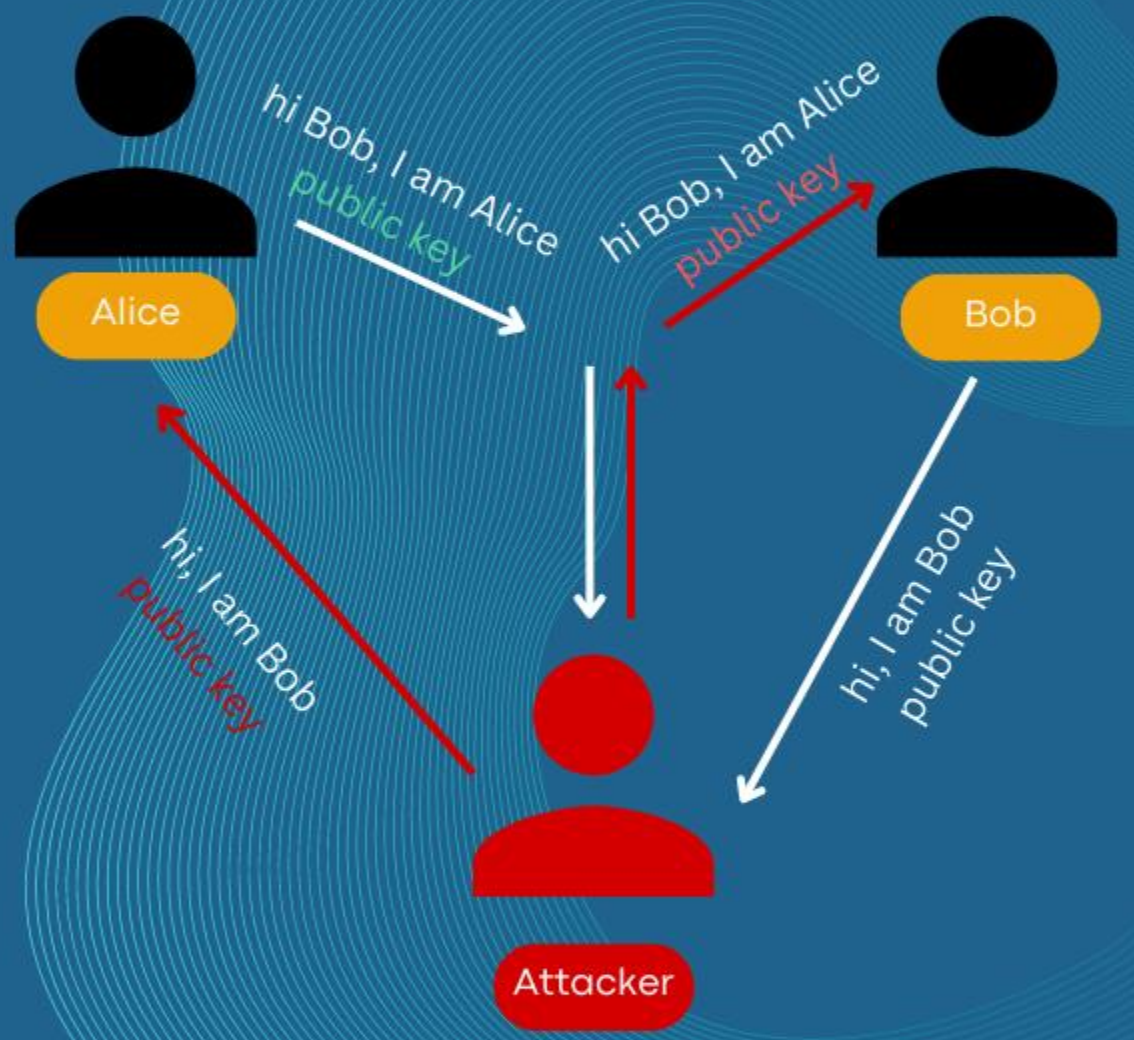
8 Attack

Man-in-the-middle (MITM) Attack



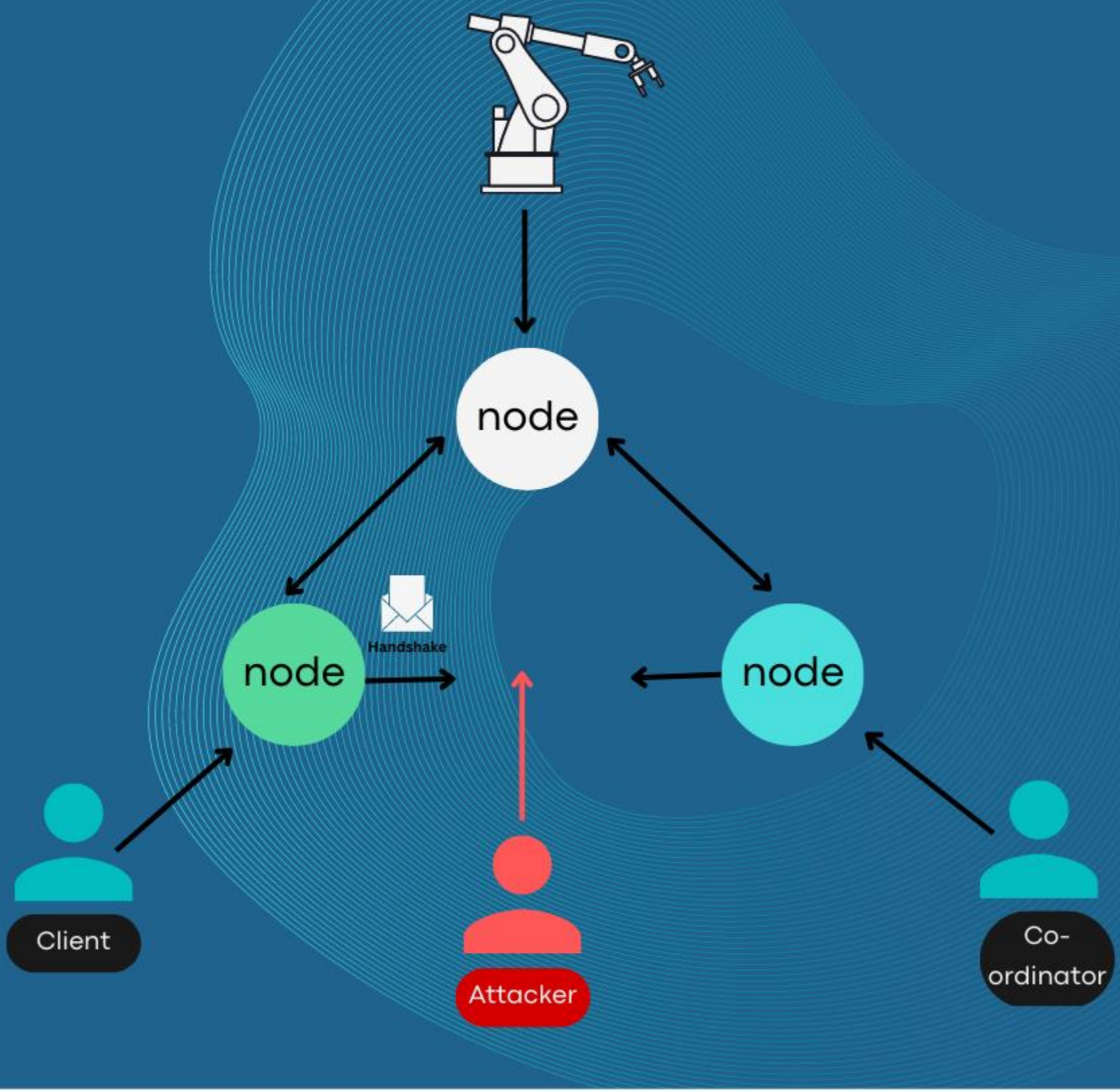
8 Attack

Man-in-the-middle (MITM) Attack



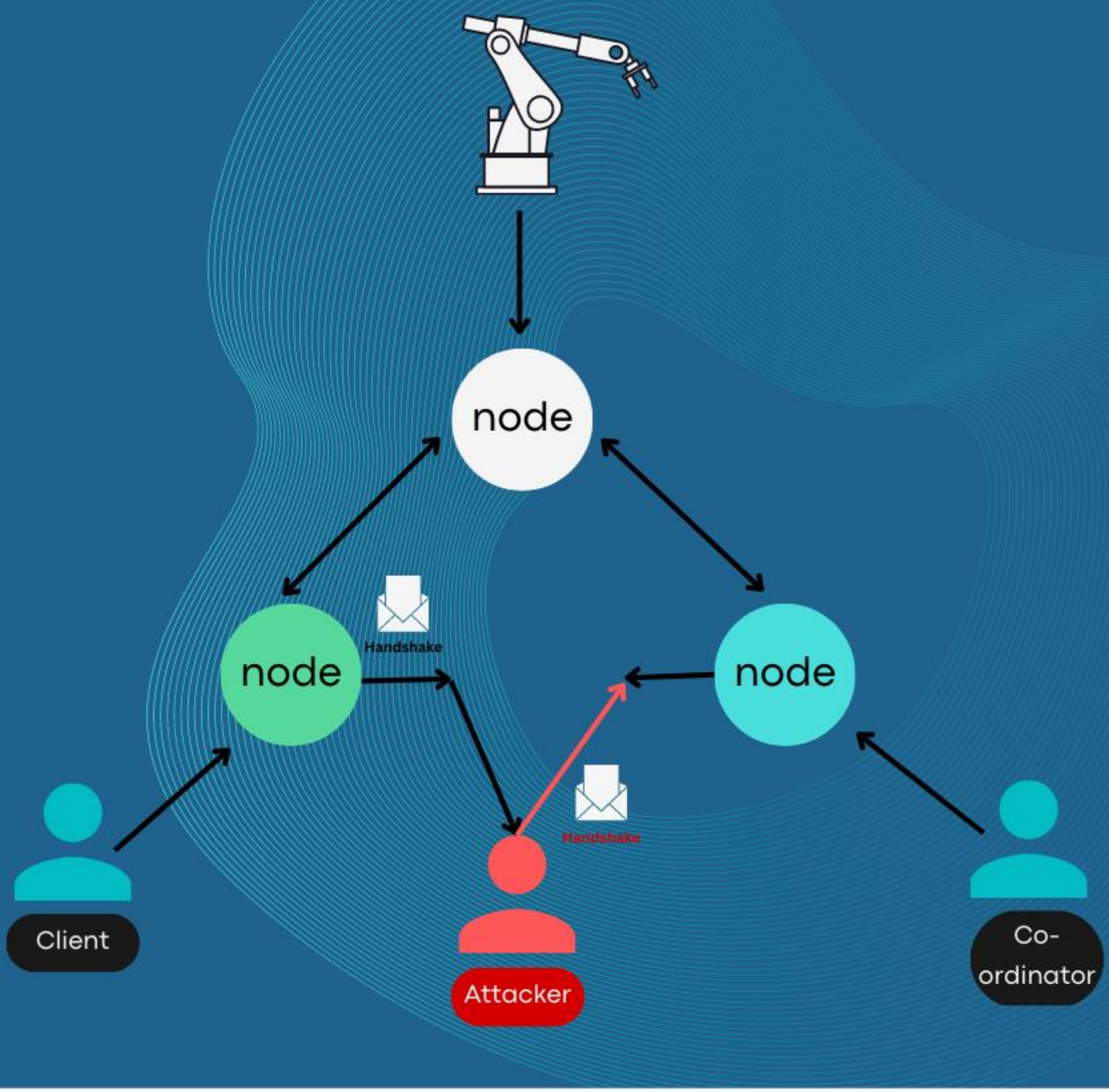
8 Attack

Man-in-the-middle (MITM) Attack



8 Attack

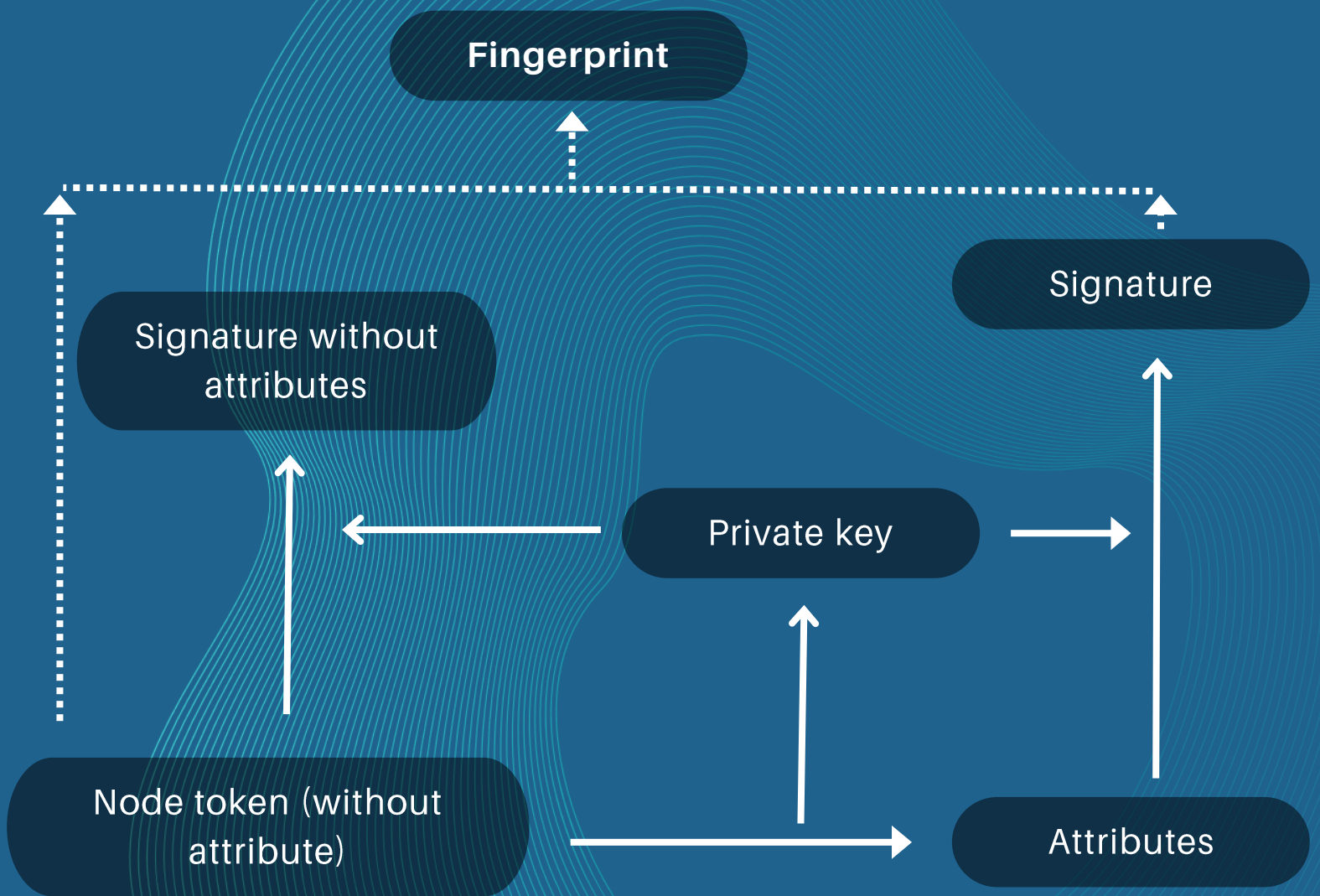
Man-in-the-middle (MITM) Attack



8 Attack

Man-in-the-middle (MITM) Attack

Handshake Message



So the signature will be broken if any field of handshake is modified by a MITM Attacker

8 Attack

Man-in-the-middle (MITM) Attack

Otherwise, to ensure the node token, the join message carries the node fingerprint in the identity token

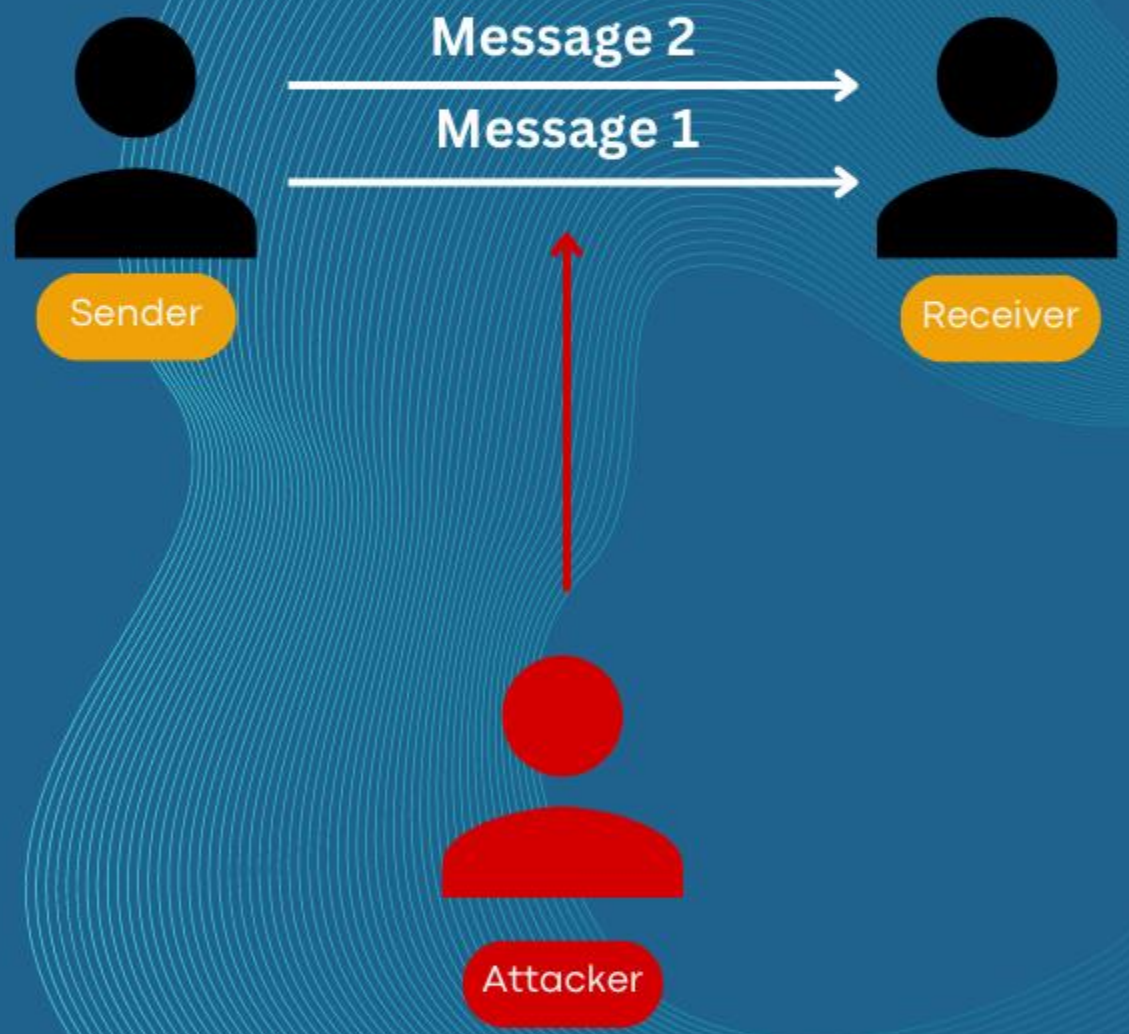
realm:	empty
issuer:	empty
subject:	Hash (userdata)
attribute:	nfp
pk:	public key(i)
signature :	sig without attributes
Signature :	sig with attributes

+

realm:	empty
issuer:	fingerprint(n)
subject:	hostname & port number
attribute:	ifp
pk:	public key(n)
signature:	sig without attributes
Signature:	sig with attributes

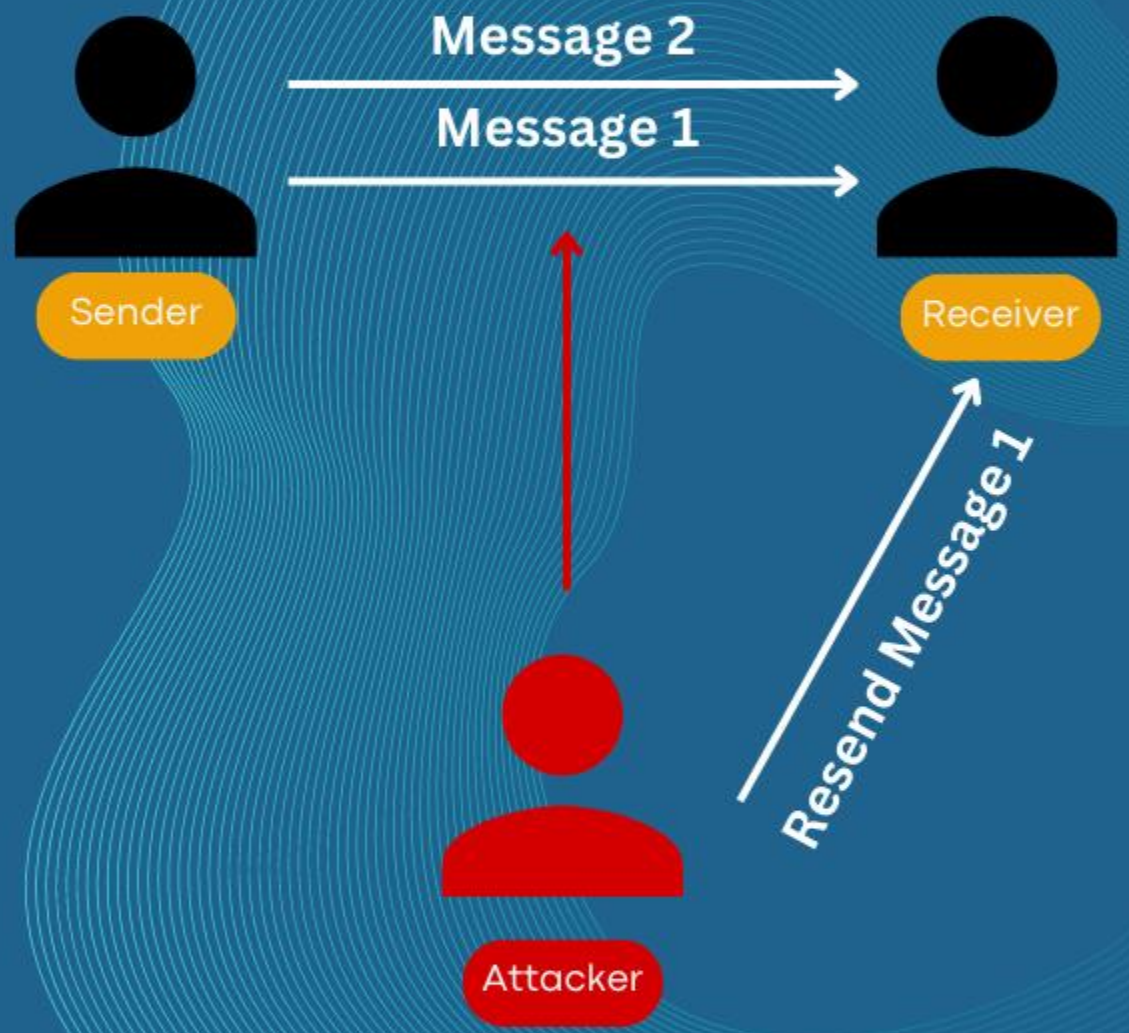
8 Attack

Replay Attack



8 Attack

Replay Attack



8 Attack

Replay Attack

mac | Instruction | header | mac(i) | attributes | **body** | nonce |

Ephemeral Key

n2n(DHK)

Every message is created with a new nonce

UUID which is unique and different for every message - Time stamp is exit

8 Attack

MITM Attack

Modify one's message – lacking of own identity (non-visible in the network)

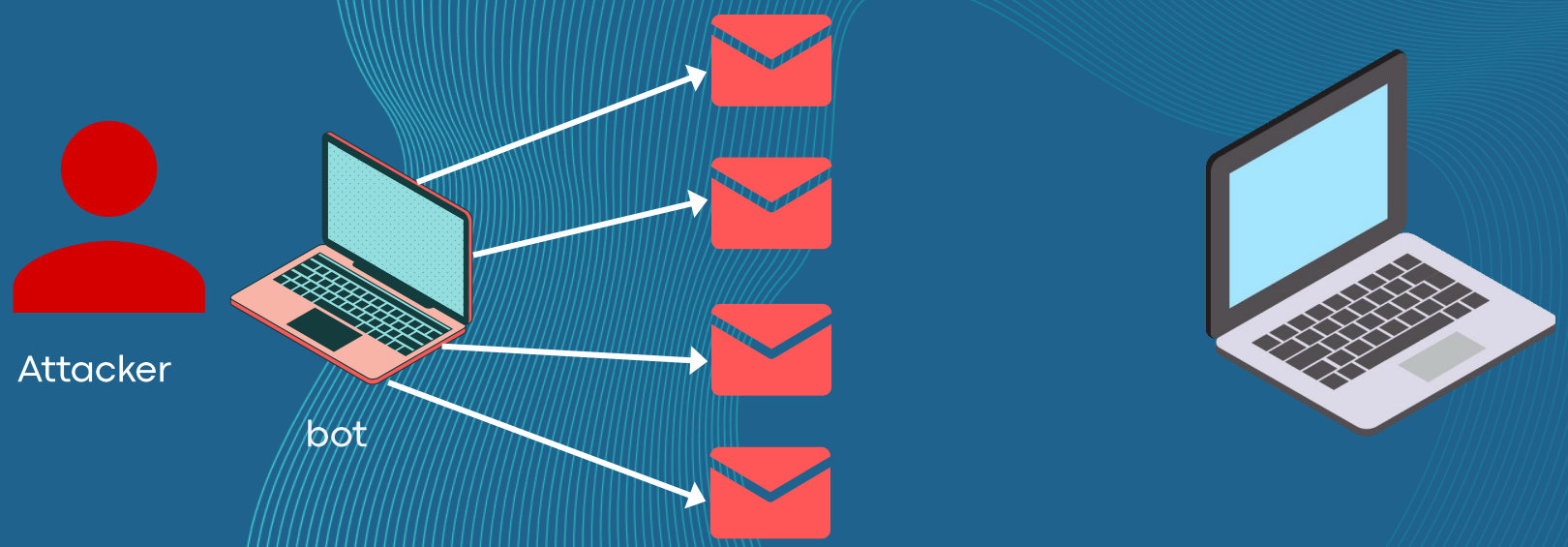
Replay Attack

Sending one transmitted message - lacking of identity (non-visible in the network)

8 Attack

Denial of Service

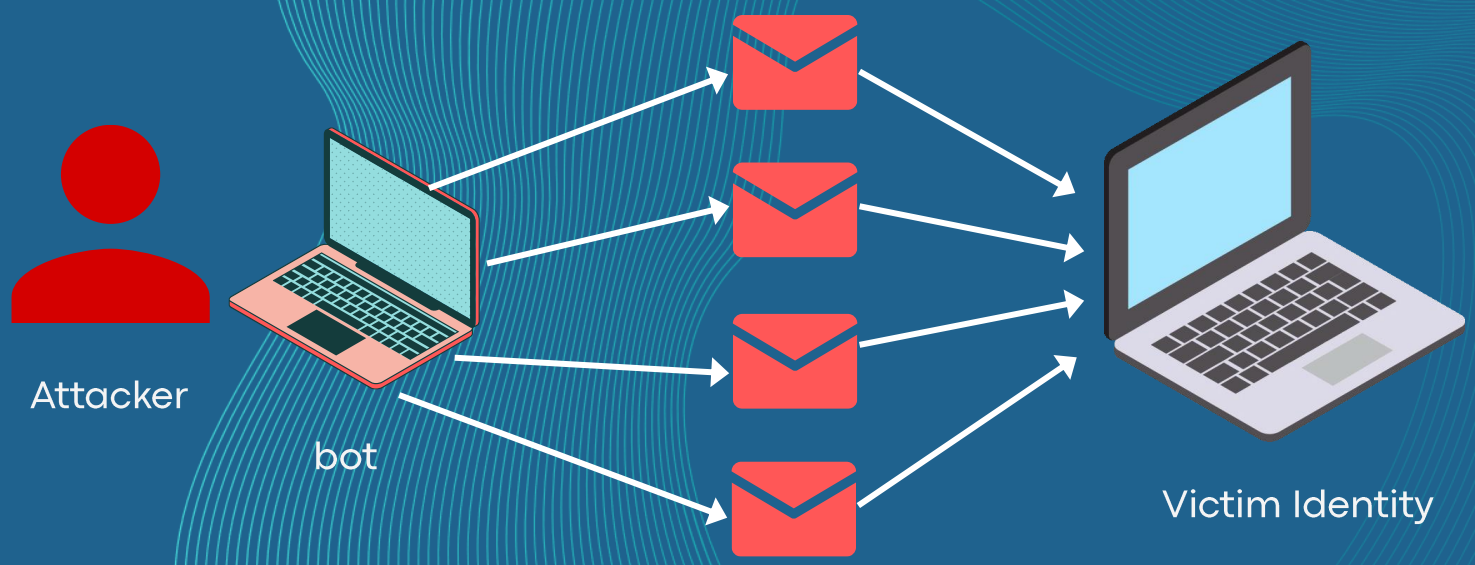
Attack the network with own identity



8 Attack

Denial of Service

Attack the network with own identity



8 Attack

Denial of Service

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS 1 JUPYTER

```
INFO 2023-01-03 15:30:19,902 - attack
INFO 2023-01-03 15:30:19,902 - attack
INFO 2023-01-03 15:30:19,902 - attack
INFO 2023-01-03 15:30:19,902 - attack
INFO 2023-01-03 15:30:19,903 - attack
INFO 2023-01-03 15:30:19,903 - attack
INFO 2023-01-03 15:30:19,903 - attack
INFO 2023-01-03 15:30:19,903 - attack
INFO 2023-01-03 15:30:19,904 - attack
INFO 2023-01-03 15:30:19,904 - attack
INFO 2023-01-03 15:30:19,904 - attack
INFO 2023-01-03 15:30:19,904 - attack
INFO 2023-01-03 15:30:19,905 - attack
INFO 2023-01-03 15:30:19,905 - attack
INFO 2023-01-03 15:30:19,905 - attack
INFO 2023-01-03 15:30:19,905 - attack
INFO 2023-01-03 15:30:19,906 - attack
INFO 2023-01-03 15:30:19,906 - attack
INFO 2023-01-03 15:30:19,906 - attack
INFO 2023-01-03 15:30:19,906 - attack
Abort ERROR in _np_decaying_bloom_add:
shabnaz-dev%
```

The attacker sending request

8 Attack

Denial of Service

```
4:03,372 - Rejoining *:udp4:localhost:9999
4:03,473 - Rejoining *:udp4:localhost:9999
4:03,573 - Rejoining *:udp4:localhost:9999
4:03,674 - Rejoining *:udp4:localhost:9999
4:03,774 - Rejoining *:udp4:localhost:9999
4:03,875 - Rejoining *:udp4:localhost:9999
4:03,975 - Rejoining *:udp4:localhost:9999
4:04,076 - Rejoining *:udp4:localhost:9999
4:04,176 - Rejoining *:udp4:localhost:9999
4:04,277 - Rejoining *:udp4:localhost:9999
4:04,377 - Rejoining *:udp4:localhost:9999
4:04,478 - Rejoining *:udp4:localhost:9999
4:04,579 - Rejoining *:udp4:localhost:9999
4:04,681 - Rejoining *:udp4:localhost:9999
4:04,781 - Rejoining *:udp4:localhost:9999
4:04,882 - Rejoining *:udp4:localhost:9999
4:04,982 - Rejoining *:udp4:localhost:9999
4:05,083 - Rejoining *:udp4:localhost:9999
4:05,183 - Rejoining *:udp4:localhost:9999
4:05,284 - Rejoining *:udp4:localhost:9999
4:05,384 - Rejoining *:udp4:localhost:9999
```

After getting the request from an attacker, the Robot disconnect the communication

9 Implementation & Overcome strategy

Decay Bloom Filter

The mechanism is used to prevent sending a message

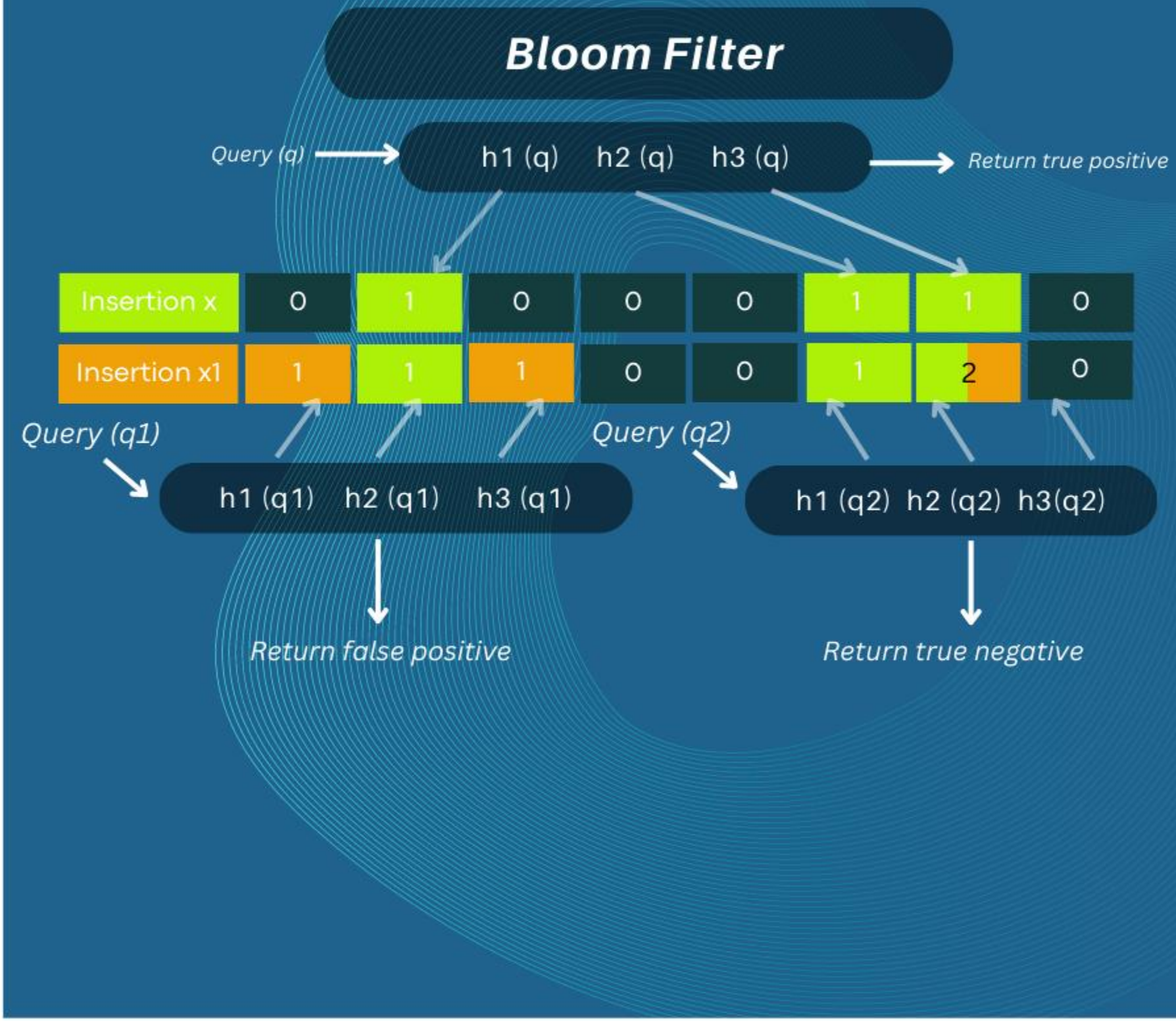
9

Implementation & Overcome strategy

Bloom Filter

9

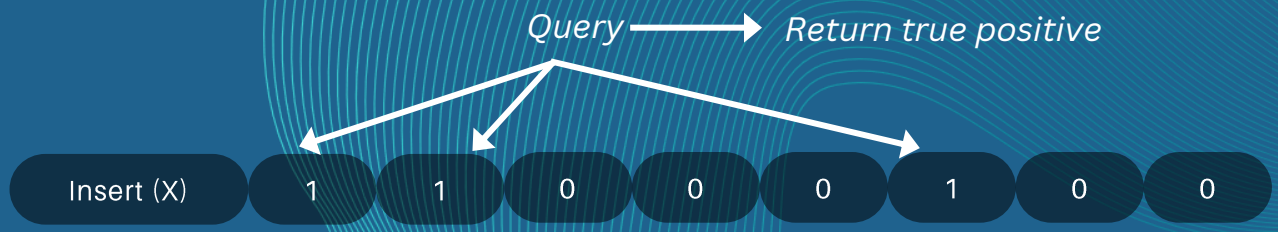
Implementation & Overcome strategy



9

Implementation & Overcome strategy

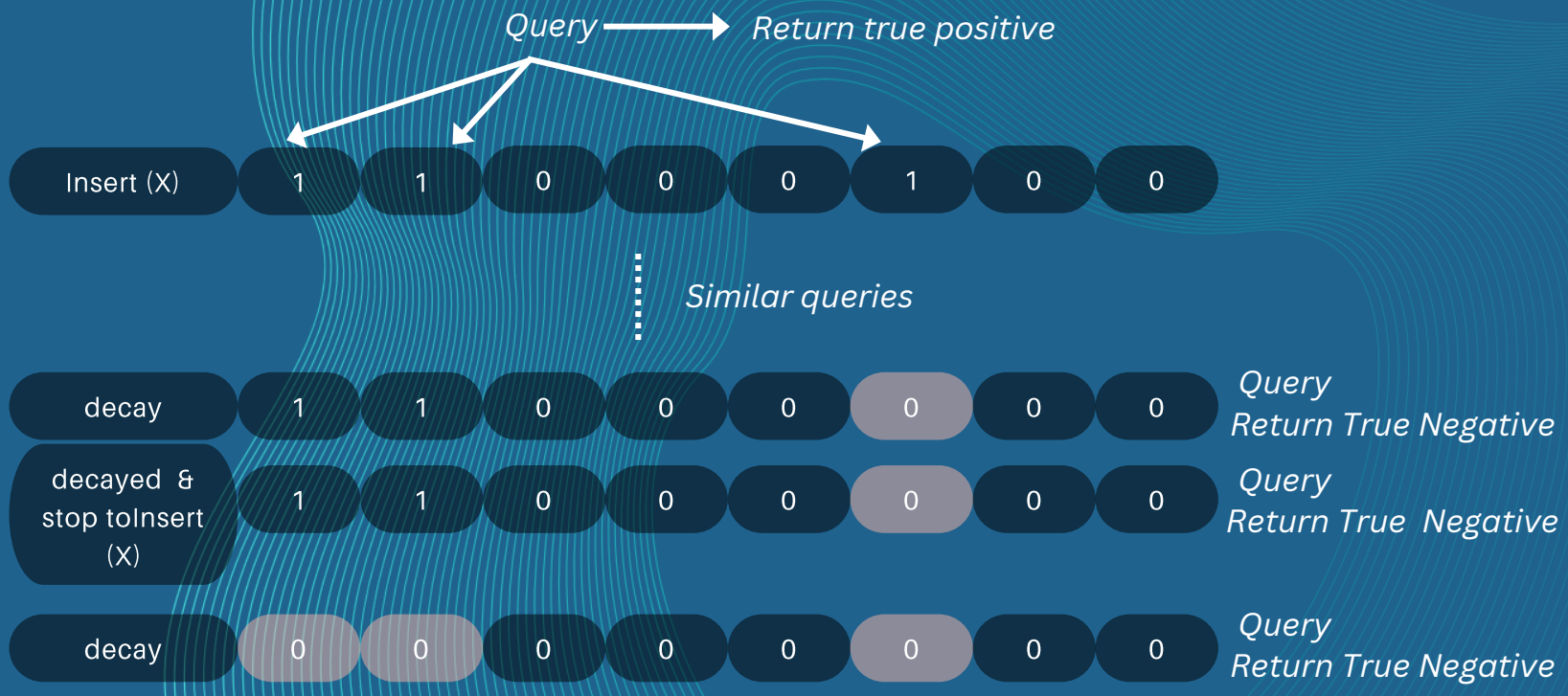
Decay Bloom Filter



9

Implementation & Overcome strategy

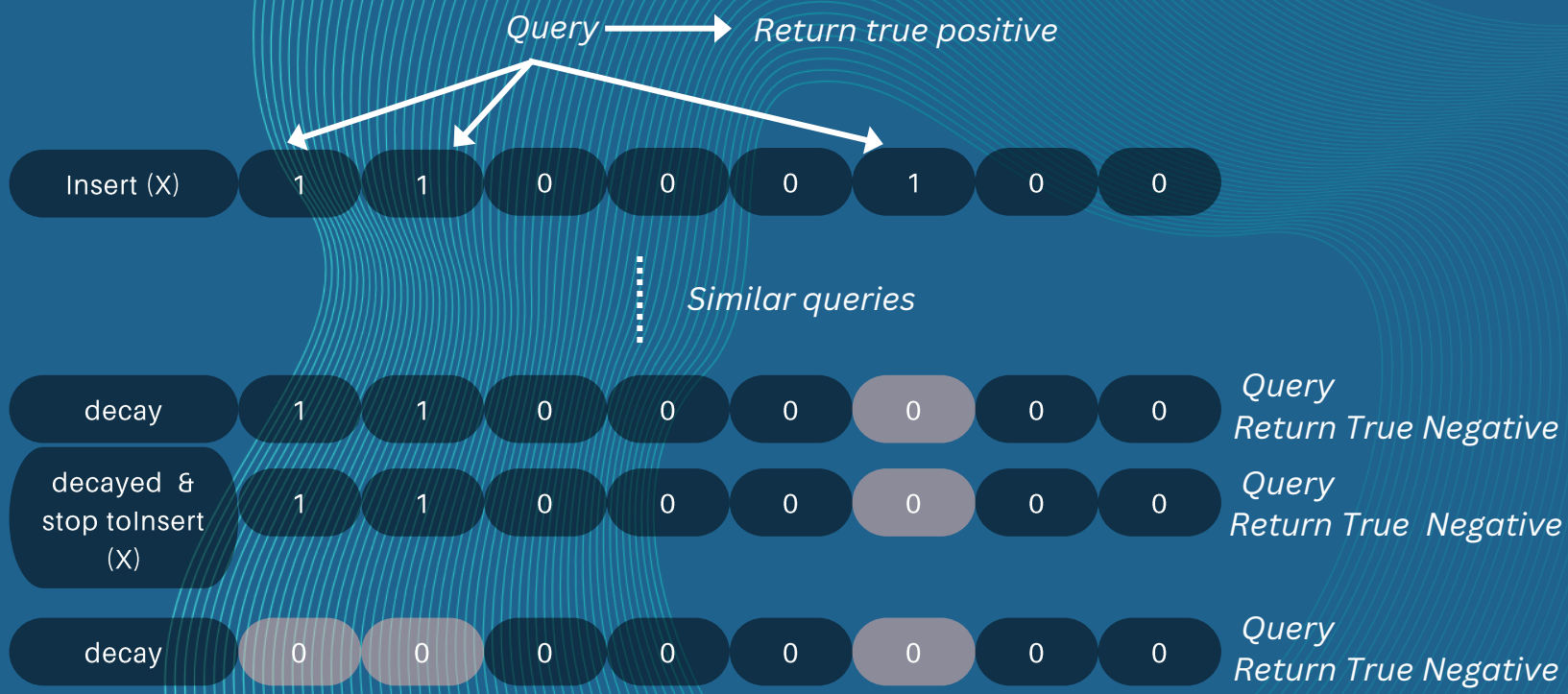
Decay Bloom Filter



9

Implementation & Overcome strategy

Decay Bloom Filter



Query returns in true negative, that means message is not transmitted

10 Conclusion & future work

Criteria	Neuropil	Mechanism
Verifying Identification	Yes	Token
Verifying Authentication	Yes	Fingerprint = black2b (signature)
Verifying Authorization	Yes	End-to- end encryption
Verifying confidentiality of data	Yes	Symmetric & Asymmetric Key
Verifying data's accuracy	Yes	MAC
Verifying data's freshness	Yes	Subject, UUID,Nonce
Verifying User's Password	Not Available	Secret key of Identity

10 Conclusion & future work

- *Neuropil is mainly focused on the authentication and verification within the cyber security mesh*
- *Business perspective: Robot control & maintenance are time consuming*
- *Additionally if it's affected by adverse & loose its authenticity, it would be more costly in financial and spreads its effect on the parts of the system*
- *To minimize the threat > Neuropil cyber security mesh*
- *Result: Communication of networks and device will be secured*
- *Future: The authentication will need an analyzation whether an attacker can break or not*

Question

Thank you for your attention!