Distributed Ledger based Online Trading System for DDoS Mitigation Services

Section 1 Summary

Use Case Summary			
Use Case ID:	ICT-005	**Use Case Type:**	Vertical
Use Case Title:	Distributed Ledger based Online Trading System for DDoS Mitigation Services	**Is Use Case supporting SDGs**	Yes
		Domain:	Industries
Status of Case	Proof-of-Concept	**Sub-Domain**	IT and telco
Contact information of person submitting/ managing the use-case	*Xinpeng Wei* *Bingyang Liu*	*wexinpeng@huawei.com* *liubingyang@huawei.com*	
Proposing Organization	*Huawei*		
Short Description	This use case is a proposal for utilizing DLT-based online trading system for DDoS mitigation services, which enables a victim network to on-demand purchase DDoS mitigation services close to the attack sources.		
Long description	This use case describes how DLT is used in DDoS mitigation service. Distributed Denial of Service (DDoS) attacks combine multiple distributed attack sources to attack a single victim, thereby amplify the attack power and downgrade the services of the victim network. DDoS mitigation service aims at mitigating DDoS attacks for the victim network. By using DLT, it's much easier to mitigate attack at the point of attack sources, and prevents the attack traffic from consuming bandwidth resources of the intermediate networks.		
SDG in Focus (when applicable)	Goal 9: Industry, Innovation and Infrastructure 9.3 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.		
Value Transfer:	Tokens which is used to pay for DDoS Mitigation service	**Number of Users:**	thousands
Types of Users:	Network operators, OTT (Over The Top), Internet users, enterprise, residential customer network		

Stakeholders	Network operators, OTT, Internet users, enterprise, residential customer network
Data:	Token balance to each account. Service smart contract: Each DDoS mitigation service provider has a service smart contract to accept service requests from DDoS victim. Service smart contract include information about the service and price that DDoS mitigation service provider can provide. IP prefix-related information: The DLT records information about IP prefix and AS (Autonomous System) numbers, so given an IP prefix the corresponding AS number can be retrieved. By using these information, the DDoS victim can find the DDoS mitigation service provider when the IP address of attack source is identified.
Identification:	Full identification of each entity is required.
Predicted Outcomes:	1. Minimize time to negotiate DDoS mitigation service. 2. Eliminate the need of pre-sign SLAs between customer and service providers.

Overview of the Business Problem or Opportunity

Distributed Denial of Service (DDoS) attacks combine multiple distributed attack sources to attack a single victim, thereby amplify the attack power and downgrade the services of the victim network. DDoS can exhaust not only the resources of victim networks but also of the uplinks. Mitigation near attack sources is better than near attack targets, because it prevents the attack traffic from consuming bandwidth resources of the intermediate networks. Besides, the burden of DDoS mitigation is shared, so the required service capacity of single provider will not be so challenging.

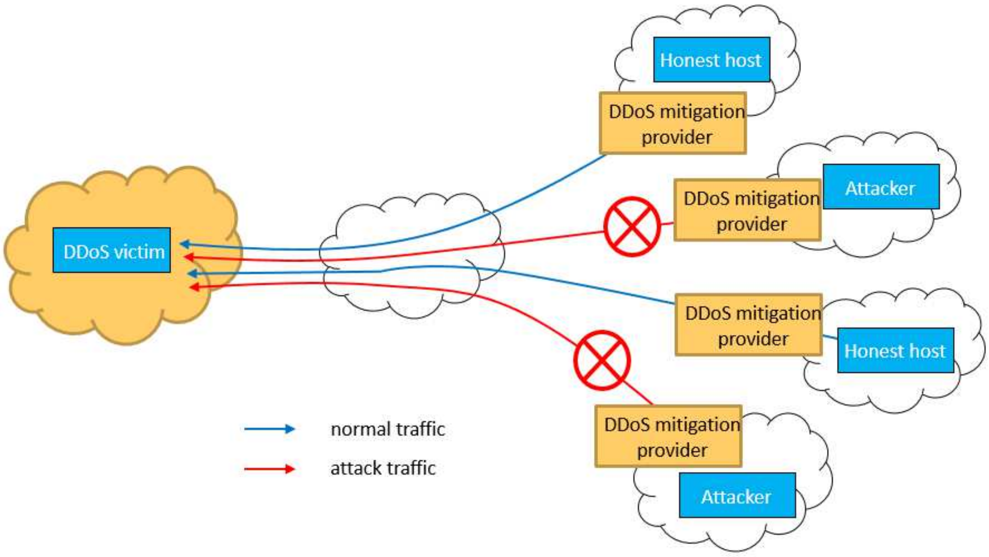


Figure 1: Overview of DDoS Protection System

However, near-source DDoS mitigation requires a business model that the victim network to purchase mitigation services from multiple providers close to the multiple source networks, which can be any of the tens of thousands of autonomous systems (ASes). There are two challenges:

First, the victim network has to set up business relationship with the remote providers, who may be unknown to the victim;

Second, different attacks have different sources, and thus require setting up business relationship with different providers. Due to the challenges, existing mitigation services are typically provided closed to the victim networks.

Why Distributed Ledger Technology?

DLT is to build a trust infrastructure, which helps the victim network to set up trust relationship with the remote providers, and enables fast on-line trading between them to start DDoS mitigation as soon as possible.

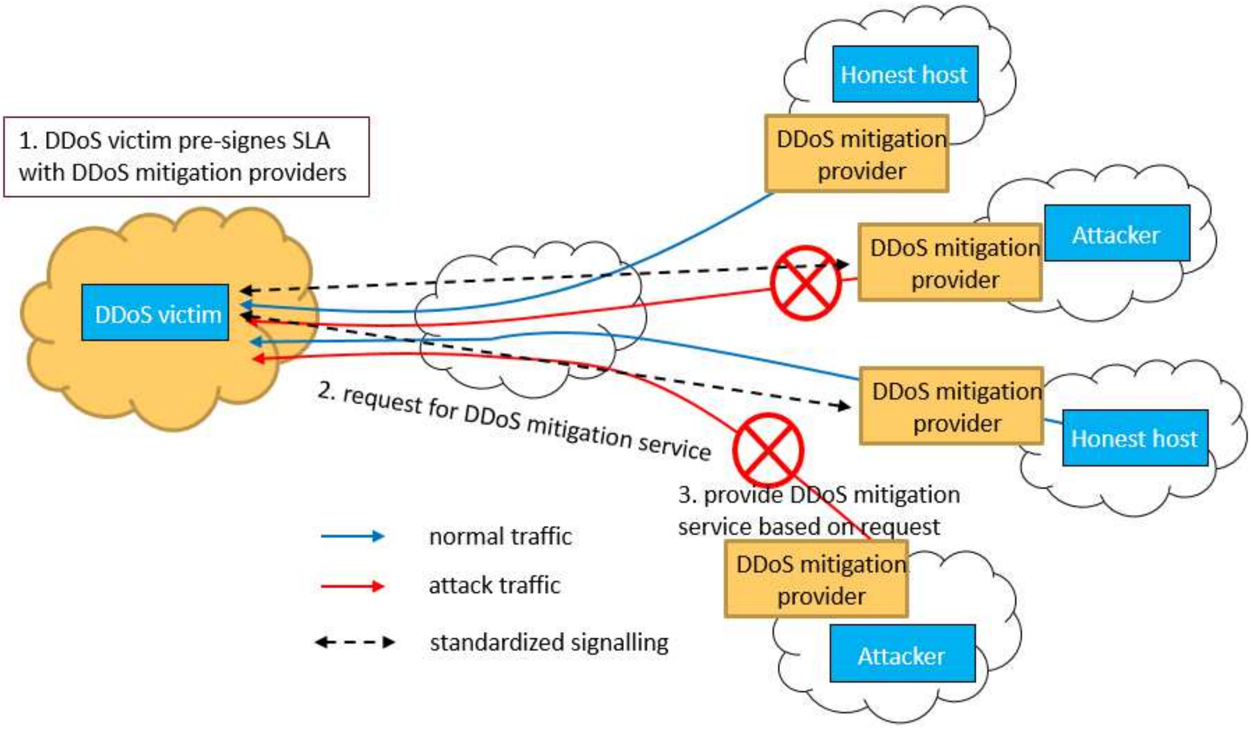
Section 2 Current process

Current Solutions

In the current solution, victim network has to set up business relationship with the DDoS mitigation service providers, and when the DDoS attack happens, the victim network sends request to the specific DDoS mitigation service provider.

Existing Flow (as-is)

Step	User Actions	System Actions
1.	DDoS victim pre-signes SLA with DDoS mitigation providers	N/A
2.	Request for DDoS mitigation service	N/A
3	Provide DDoS mitigation service based on request	N/A

Process scheme (as-is)
 1. DDoS victim pre-signes SLA with DDoS mitigation providers DDoS victim Honest host DDoS mitigation provider Attacker DDoS mitigation provider DDoS mitigation provider Honest host 2. request for DDoS mitigation service 3. provide DDoS mitigation service based on request DDoS mitigation provider Attacker normal traffic attack traffic standardized signalling Figure 2: The Existing Distributed DDoS Mitigation Solution

Data and information (as-is)		
Data	**Type**	**Description**
1	DDoS mitigation service request	The victim send this request to service provider for DDoS mitigation service.

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	DDoS victim	The entity who suffers from DDoS attack. Any entities connected to Internet could be a DDoS victim. E.g. ISP, enterprise, residential customer network, OTT etc.
2	DDoS mitigation provider	The entity who provide DDoS mitigation service. Usually, it is a network provider.

Other Notes
N/A

Section 3 Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	DDoS victim initiates a transaction to DDoS mitigation provider's smart contract to request for DDoS mitigation service.	DLT checks the DDoS victim is authorized to send out the transaction, and the target DDoS mitigation provider's smart contract exist. If true, DLT record the transaction.
2.	DDoS mitigation provider evaluates DDoS victim's credibility verifying that the DDoS victim has the ownership of the attacked IP address.	N/A
3	DDoS mitigation provider initiates a transaction with the DDoS victim to agree to provide DDoS mitigation server.	DLT checks the transaction sent by DDoS mitigation provider is valid, and then record the transaction. After that the DDoS mitigation provider's smart contract will be executed, and token will be transferred from DDoS victim's account to DDoS mitigation provider's account.

Process scheme (to-be)

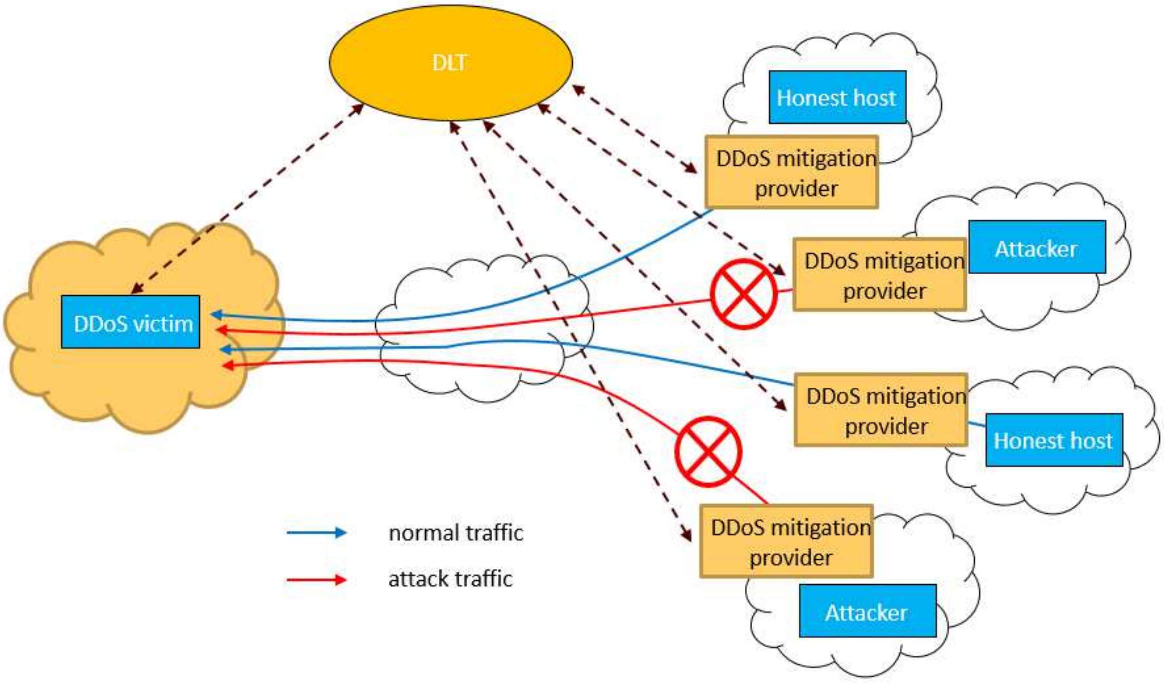


Figure 3: Overview of DLT and DDoS Mitigation System

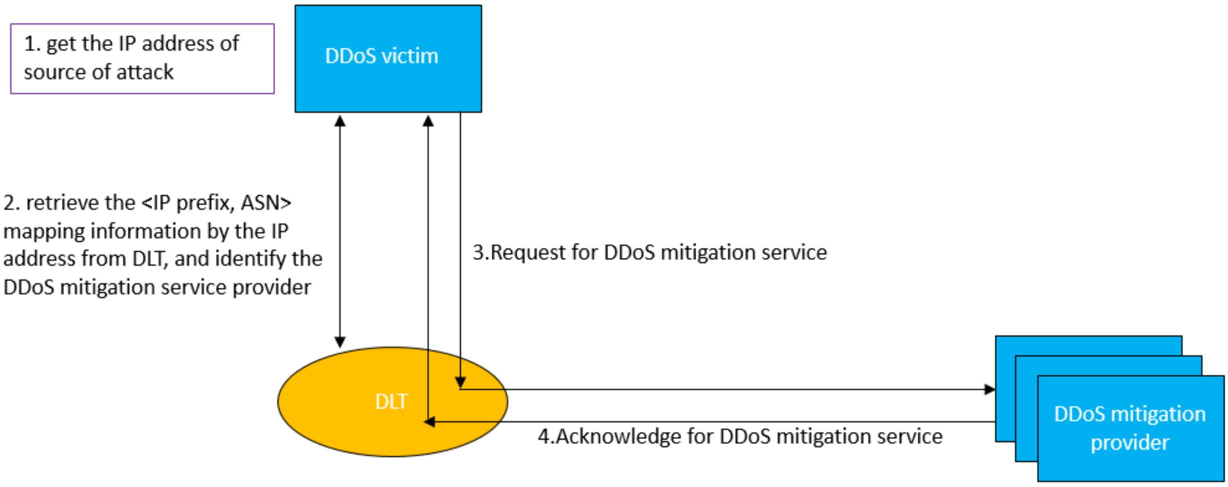

1. get the IP address of source of attack
DDoS victim
2. retrieve the <IP prefix, ASN> mapping information by the IP address from DLT, and identify the DDoS mitigation service provider
3.Request for DDoS mitigation service
DLT
4.Acknowledge for DDoS mitigation service
DDoS mitigation provider

Figure 4: Procedures of DDoS Mitigation Service

Participants and their roles		
Actor	**Type/Role**	**Description**
1	DDoS victim	The entity who suffers from DDoS attack. Any entities connected to Internet could be a DDoS victim. E.g. ISP, enterprise, residential customer network, OTT etc.

Participants and their roles		
Actor	**Type/Role**	**Description**
2	DDoS mitigation provider	The entity who provide DDoS mitigation service. Usually, it is a network provider.

Data and information		
Data	**Type**	**Description**
1	token	Token representing money value. It is used to transfer value between DDoS victims and DDoS mitigation providers.
2	Service request transactions	The DDoS victim use service request transaction to ask for DDoS mitigation service from DDoS mitigation service provider, and payment for the service will also be included.
3	Service acknowledge transactions	The DDoS mitigation service provider use service acknowledge transaction to agree for DDoS mitigation service to DDoS victim.
4	Service smart contract	Each DDoS mitigation service provider has a service smart contract to accept service requests from DDoS victim. Service smart contract include information about the service and price that DDoS mitigation service provider can provide.
5	IP prefix-related information	The DLT records information about IP prefix and AS numbers, so given an IP prefix the corresponding AS number can be retrieved. By using these information, the DDoS victim can find the DDoS mitigation service provider when the IP address of attack source is identified.

Security and privacy
1. The DDoS mitigation provider's service ability recorded in DLT system DDoS mitigation provider should be trustable. 2. The IP prefix-related information recorded in DLT system should be trustable.

Main Success Scenario
1. All information exchange and payments occur in Distributed Ledger in automatic mode. 2. Payment and service are exchanged without human intervention.

Conditions (pre- or post-)
1. The token must be created in some way. 2. All parties are connected to DLT system. 3. All parties should have a recognizable identity.

Performance needs
1. Transactions processing near real time; 2. 24/7/365 availability; 3. Volume of transactions > 1000 TPS.

Legal considerations
N/A

Risks
1. DLT-related security risk.

Special Requirements
N/A

External References and Miscellaneous
N/A

Other Notes
N/A

____

Appendix 1

Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity Management
2. Security Management
    a. Public Key Infrastructure

3. Internet of Things
4. Data processing, storage and management
    a. Data Validation (includes provenance)