DOTS
First Interoperability Test

IETF 100 Hackathon Report

Kaname Nishizuka/NTT Communications
Jon Shallow/NCC Group
Liang Xia/Huawei

DOTS is now working!

- DOTS WG is aiming to make it standardized in this year
- Now we have several individual implementations
    - go-dots (open-sourced project) from NTT
    - NCC Group's proprietary implementation
- This first interoperability test at the hackathon is a giant step for proving it works.

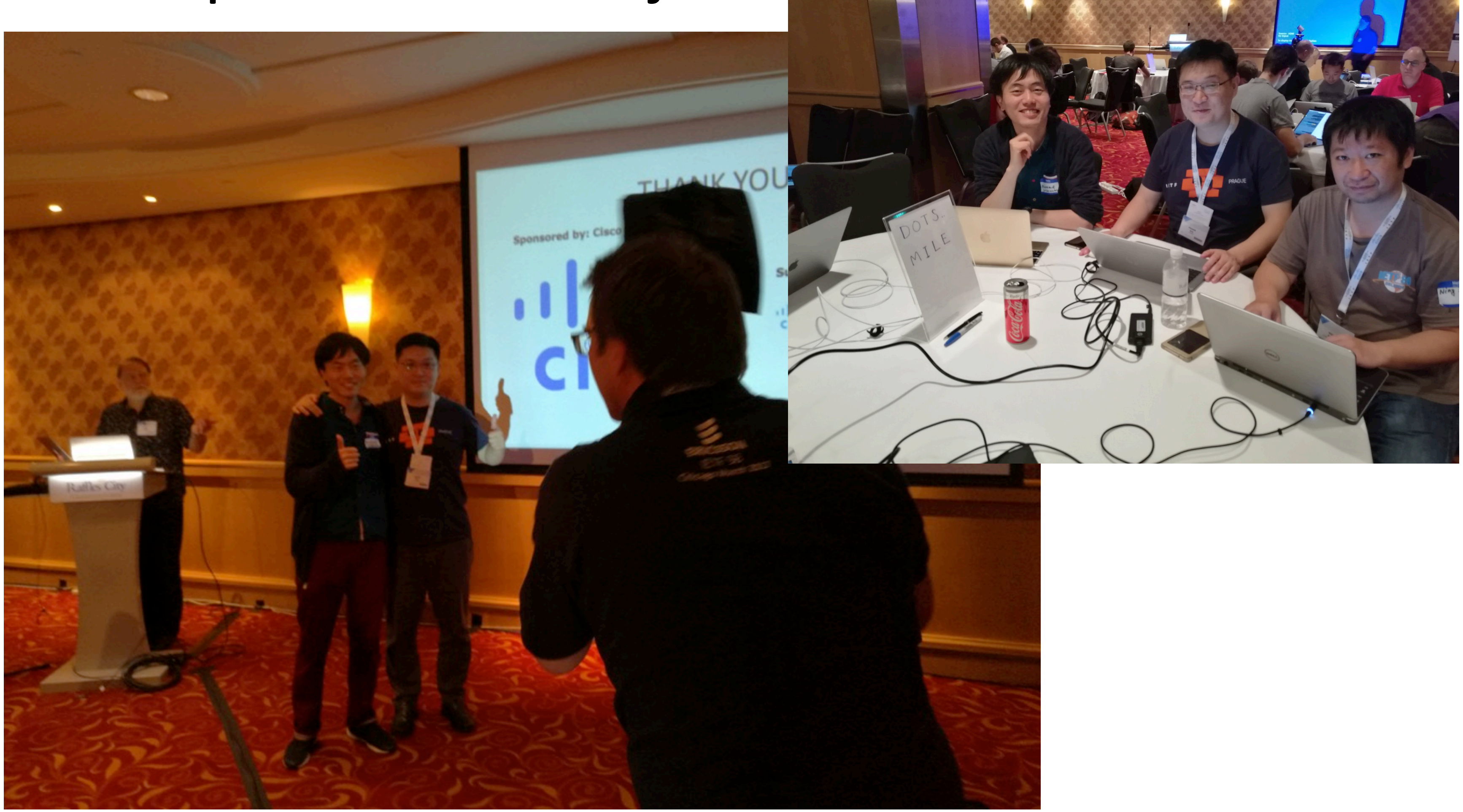
What happened in the Hackathon

- 3 active projects with 7 participants
  - include 3 remotely from Tokyo, London, Nanjing
- 3 Projects are:

1. First Interoperability test of 2 individual implementations
2. Adding new features and extensions to the open-sourced implementation
3. (Integration with a detection system of Mirai botnet)

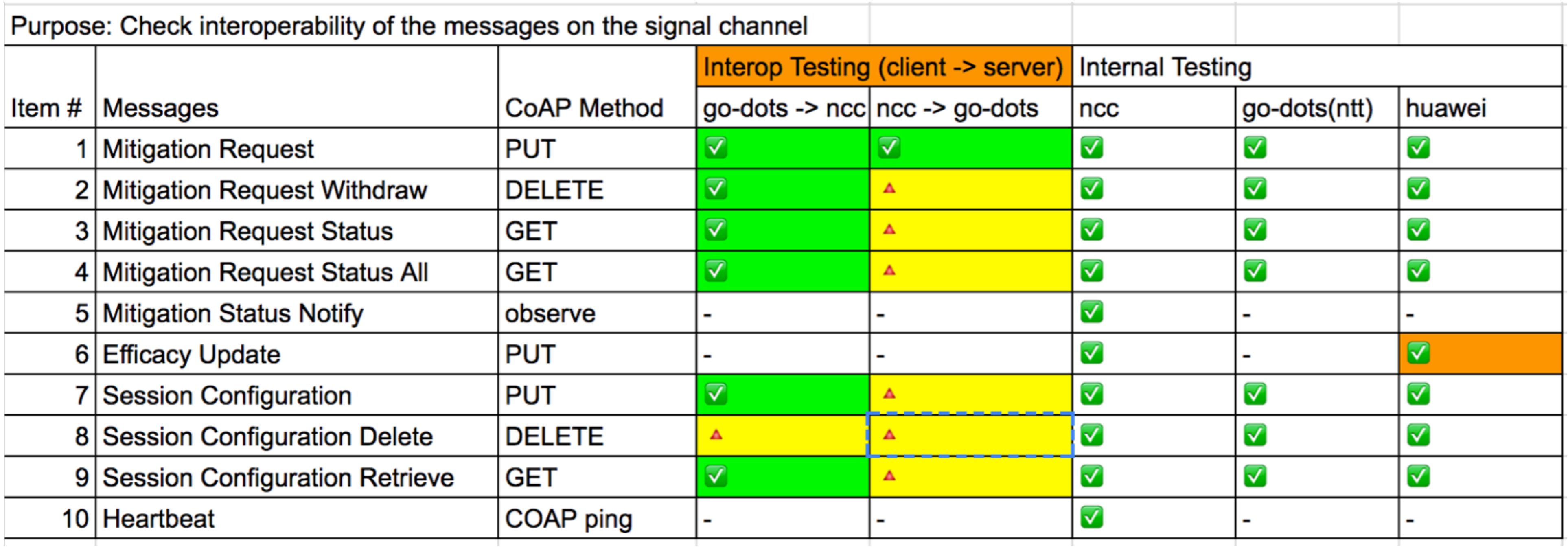
We won an award!

- Best Open Source Project



1. First Interoperability test of 2 individual implementations
   - go-dots (open-sourced project) from NTT
     - Kaname Nishizuka, Takahiko Nagata(Remote)
   - NCC Group’s proprietary implementation
     - Jon Shallow(Remote)

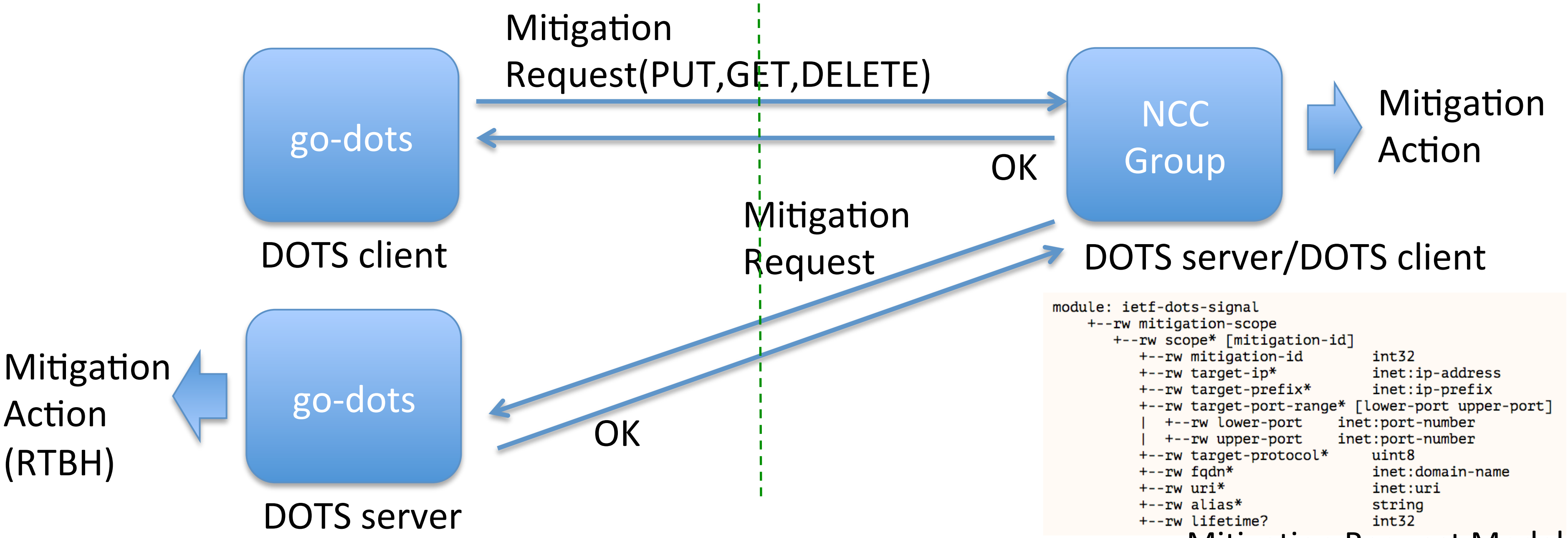
Result of the Interop Test



Purpose: Check interoperability of the messages on the signal channel

			Interop Testing (client -> server)		Internal Testing		
Item #	Messages	CoAP Method	go-dots -> ncc	ncc -> go-dots	ncc	go-dots(ntt)	huawei
1	Mitigation Request	PUT	✅	✅	✅	✅	✅
2	Mitigation Request Withdraw	DELETE	✅	🔺	✅	✅	✅
3	Mitigation Request Status	GET	✅	🔺	✅	✅	✅
4	Mitigation Request Status All	GET	✅	🔺	✅	✅	✅
5	Mitigation Status Notify	observe	-	-	✅	-	-
6	Efficacy Update	PUT	-	-	✅	-	✅
7	Session Configuration	PUT	✅	🔺	✅	✅	✅
8	Session Configuration Delete	DELETE	🔺	🔺	✅	✅	✅
9	Session Configuration Retrieve	GET	✅	🔺	✅	✅	✅
10	Heartbeat	COAP ping	-	-	✅	-	-

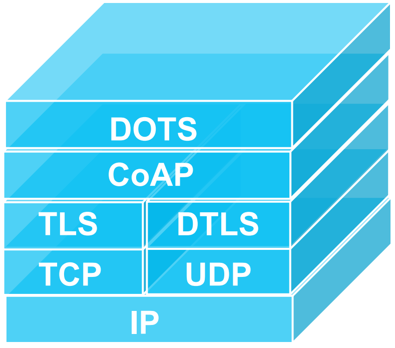
What we proved in the Interop



```
module: ietf-dots-signal
   +--rw mitigation-scope
      +--rw scope* [mitigation-id]
         +--rw mitigation-id          int32
         +--rw target-ip*             inet:ip-address
         +--rw target-prefix*         inet:ip-prefix
         +--rw target-port-range* [lower-port upper-port]
         |  +--rw lower-port    inet:port-number
         |  +--rw upper-port    inet:port-number
         +--rw target-protocol*       uint8
         +--rw fqdn*                  inet:domain-name
         +--rw uri*                   inet:uri
         +--rw alias*                 string
         +--rw lifetime?              int32
```

Mitigation Request Model

- We can start and handle a mitigation from each client over DOTS signal–channel (CoAP over DTLS)
- Plus, NCC Group’s implementation can act as a DOTS relay (gateway), so we proved that relayed mitigation requests can work over multiple organizations.



DOTS Signal Channel Layers

General Feedback to DOTS WG

- Implementation Experiences
  - For example most of the code modification was related to encode/decode of CoAP mapping
  - there were many implicit specifications we need to figure out and agree on
- Need more description of the content and code
- approx. 60% of the signal-channel spec has been proved to work
  - The rest will be done at/by the next IETF

go-dots Feedback to DOTS WG

- Preparation for the interop test
  - Agree on port number(-06) and URI path(-07)
  - Fixed CBOR mapping
  - Updated data models
- Code Updates during Hackathon
  - Omit empty(NULL) entries in requests
  - Fixed response body
- Test scenarios should be listed and shared
  - to get every patterns of request/response type and see normal/error behavior
  - unintended behavior can be found only by interop

NCC Group Feedback to DOTS WG (Pt 1)

- Code Updates during Hackathon
  - CBOR <-> JSON mapping fixes for NULL entries
  - Remove NULL entries confusion and deleted NULL entries in any response
  - Added support for multiple mitigation requests within a single PUT
- NCC DOTS Client crashing go-dots DOTS server
  - Disabled Signal Configuration requests
  - Disabled Heartbeats
  - Still go-dots server issues handling NCC client requests - to be worked on

NCC Group Feedback to DOTS WG (Pt 2)

- Outstanding NCC Group to be fixed
  - DOTS Client handling bad CoAP Ping responses
  - Support of GET empty requests that are not CBOR encoded
- Questions
  - Should NULL entries be allowed ?
  - Should a NULL entry of type Object be allowed when definition is Array ?
  - What should happen when lifetime = 0 is requested ?
  - Should there be support for multiple mitigation requests within a single PUT ?

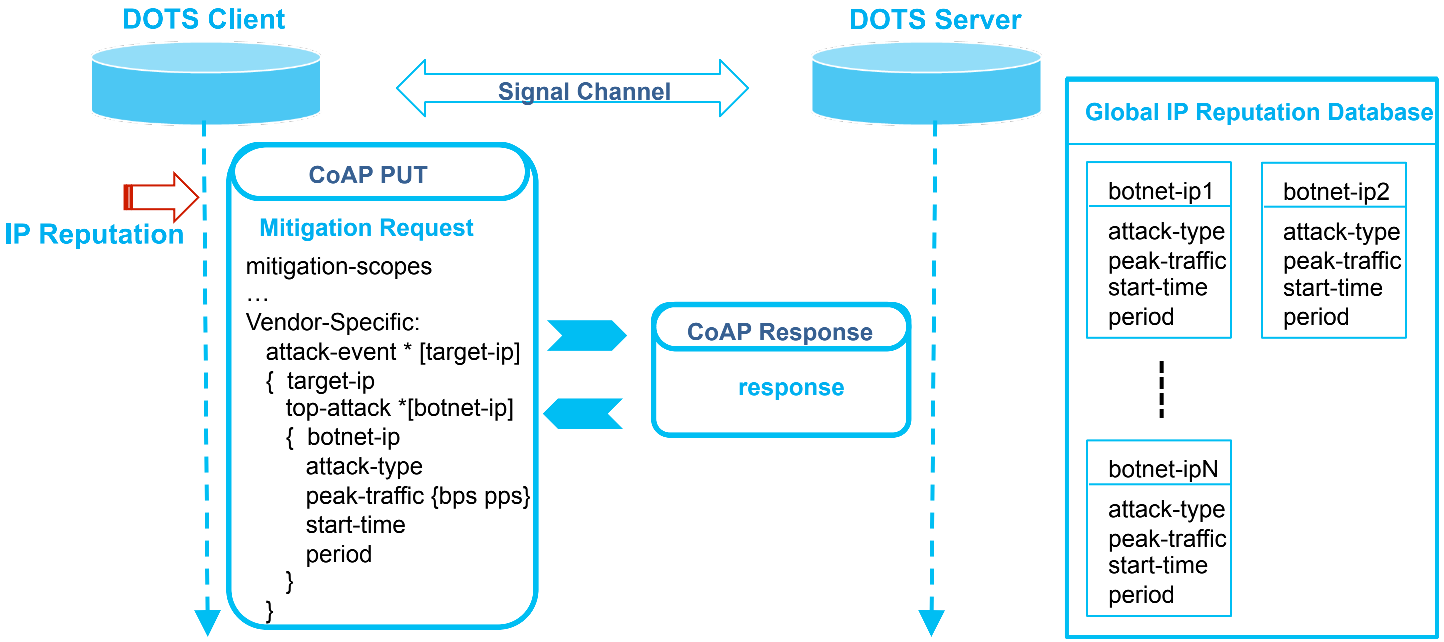
Questions

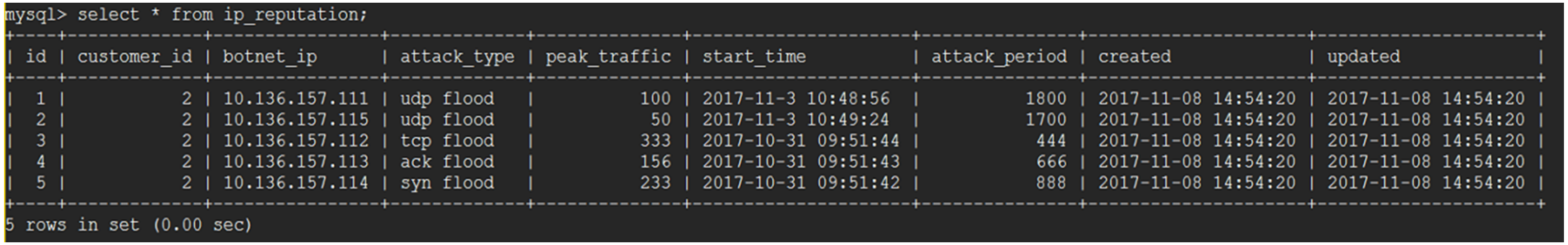
Or

Comments?

2. Adding new features and extensions to the open-sourced implementation

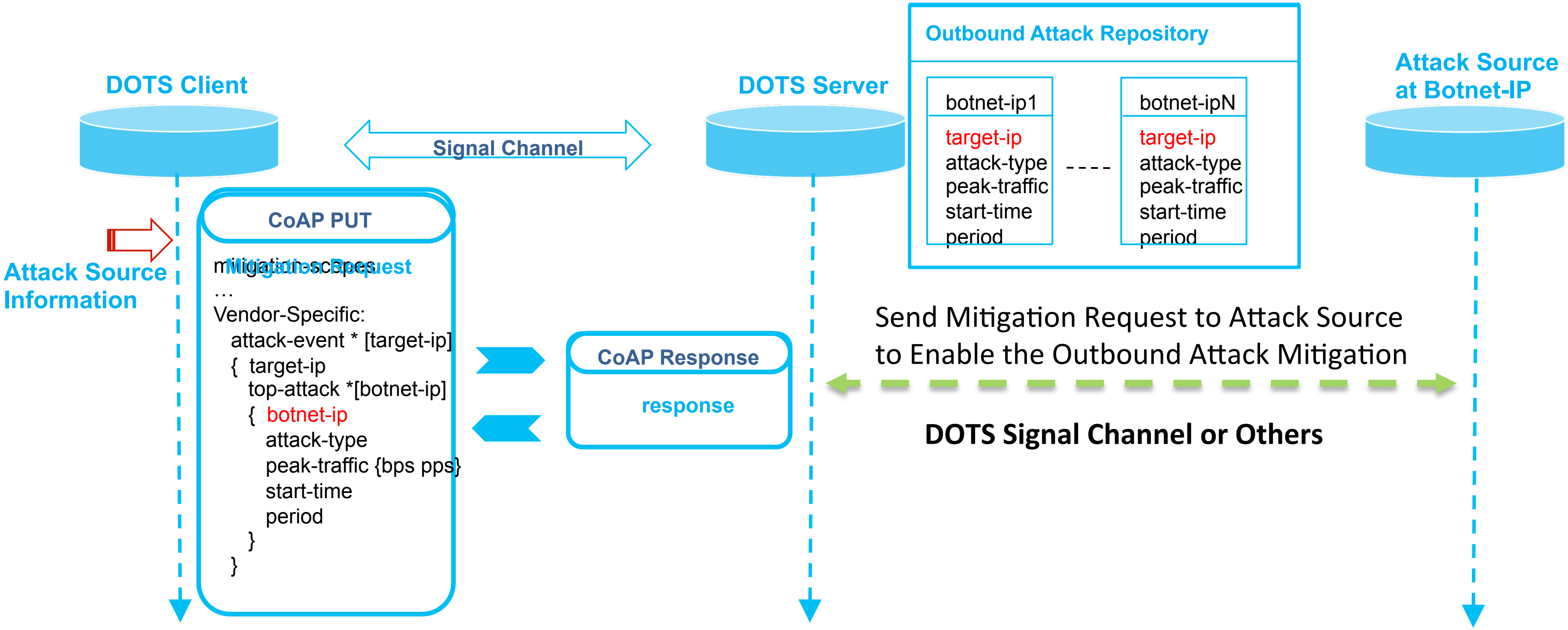
Using DOTS Vendor-Specific Attributes for Global IP Reputation Sharing





```
mysql> select * from ip_reputation;
+----+-------------+----------------+-------------+--------------+---------------------+---------------+---------------------+---------------------+
| id | customer_id | botnet_ip      | attack_type | peak_traffic | start_time          | attack_period | created             | updated             |
+----+-------------+----------------+-------------+--------------+---------------------+---------------+---------------------+---------------------+
|  1 |           2 | 10.136.157.111 | udp flood   |          100 | 2017-11-3 10:48:56  |          1800 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  2 |           2 | 10.136.157.115 | udp flood   |           50 | 2017-11-3 10:49:24  |          1700 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  3 |           2 | 10.136.157.112 | tcp flood   |          333 | 2017-10-31 09:51:44 |           444 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  4 |           2 | 10.136.157.113 | ack flood   |          156 | 2017-10-31 09:51:43 |           666 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  5 |           2 | 10.136.157.114 | syn flood   |          233 | 2017-10-31 09:51:42 |           888 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
+----+-------------+----------------+-------------+--------------+---------------------+---------------+---------------------+---------------------+
5 rows in set (0.00 sec)
```

Using DOTS Vendor-Specific Attributes for Outbound Attack Mitigation



DOTS Client

Signal Channel

DOTS Server

Outbound Attack Repository

botnet-ip1		botnet-ipN
target-ip attack-type peak-traffic start-time period	----	target-ip attack-type peak-traffic start-time period

Attack Source at Botnet-IP

Attack Source Information

CoAP PUT

Mitigation Request

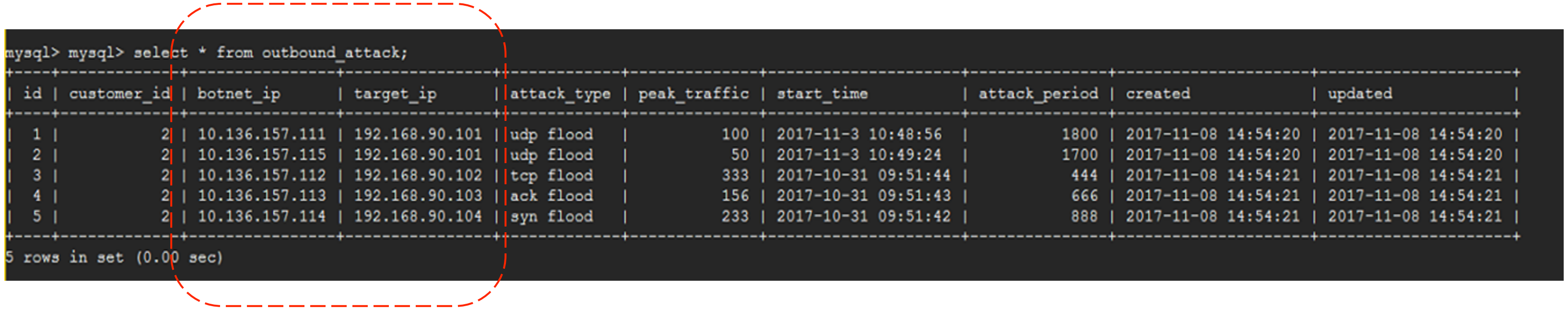
```
mitigation-scopes
…
Vendor-Specific:
  attack-event * [target-ip]
  { target-ip
    top-attack *[botnet-ip]
    { botnet-ip
      attack-type
      peak-traffic {bps pps}
      start-time
      period
    }
  }
```

CoAP Response

response

Send Mitigation Request to Attack Source to Enable the Outbound Attack Mitigation

DOTS Signal Channel or Others



```
mysql> mysql> select * from outbound_attack;
+----+-------------+----------------+----------------+-------------+--------------+--------------------+---------------+---------------------+---------------------+
| id | customer_id | botnet_ip      | target_ip      |attack_type | peak_traffic | start_time         | attack_period | created             | updated             |
+----+-------------+----------------+----------------+-------------+--------------+--------------------+---------------+---------------------+---------------------+
|  1 |           2 | 10.136.157.111 | 192.168.90.101 |udp flood   |          100 | 2017-11-3 10:48:56  |          1800 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  2 |           2 | 10.136.157.115 | 192.168.90.101 |udp flood   |           50 | 2017-11-3 10:49:24  |          1700 | 2017-11-08 14:54:20 | 2017-11-08 14:54:20 |
|  3 |           2 | 10.136.157.112 | 192.168.90.102 |tcp flood   |          333 | 2017-10-31 09:51:44 |           444 | 2017-11-08 14:54:21 | 2017-11-08 14:54:21 |
|  4 |           2 | 10.136.157.113 | 192.168.90.103 |ack flood   |          156 | 2017-10-31 09:51:43 |           666 | 2017-11-08 14:54:21 | 2017-11-08 14:54:21 |
|  5 |           2 | 10.136.157.114 | 192.168.90.104 |syn flood   |          233 | 2017-10-31 09:51:42 |           888 | 2017-11-08 14:54:21 | 2017-11-08 14:54:21 |
+----+-------------+----------------+----------------+-------------+--------------+--------------------+---------------+---------------------+---------------------+
5 rows in set (0.00 sec)
```

Thank You