DOTS
Internet-Draft
Intended status: Proposed Standard

K. Li
H. Zhou
Z. Tu
F. Liu
W. Wang
Beijing Jiaotong University

Document: draft-li-dots-knowledge-trans-01.txt
Expires: July 2022
January 2022

Knowledge Transmission Using Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel

Status of this Memo

Copyright Notice

Abstract

The document specifies new DOTS data channel configuration parameters that customize the DDoS knowledge transmission configuration between distributed knowledge bases. These options enable assist the distributed knowledge base to share attack knowledge in different fields and actively adapt to dynamically changing DDoS attacks.

Table of Contents

1. Introduction..2
2. Terminology...3
3. DOTS Knowledge Transmission Architecture......................3
4. DOTS Knowledge Transmission YANG Module.......................5
4.1 Generic Tree Structure....................................5
4.2 YANG Module...6
5. Managing DOTS Knowledge Transmission.........................10
6. IANA Considerations..11
7. Security Considerations......................................11
8. References...11
8.1 Normative References.....................................11
8.2 Informative References...................................12
Acknowledgments...12
Author's Addresses..12

1. Introduction

To detect ~~the threat of~~ DDoS attacks, various security organizations have designed ~~a~~ series of network security datasets by ~~collecting~~ conducting various ~~complex~~ simulations or collecting data related to DDoS attacks in actual network environments. Such an effort is meant~~, aiming~~ to reflect the ~~modern~~ recent trends of DDoS attacks that are more sophisticated~~complex~~ and ~~changeable~~ dynamic ~~DDoS attack environment~~ by designing a comprehensive data set containing normal and abnormal behavior.

As a new knowledge representation method, the knowledge graph represents the relationship between entities in the form of graphs, and is essentially a semantic network that reveals the relationships between entities. Knowledge graph technology can standardize and integrate DDoS attack-related intelligence, generate DDoS attack knowledge and store it in the network security malicious behavior knowledge base to solve the problem that multi-source heterogeneous data is difficult to share and reuse.

Commenté [BMI1]: Consider adding a reference. Thanks

The DOTS data channel [RFC8783] ~~can~~ is used to exchange bulk data between DOTS agents, coordinate multiple DOTS servers and DOTS clients, and perform tasks such as creating resource aliases and managing filtering ~~strategies~~rules. ~~The DOTS data channel specification~~ [RFC8783] ~~defines the data channel hierarchical structure,~~specifies the YANG data model and the basic data channel functions ~~of the data channel~~.

~~DOTS data channel is used for reliable data interaction between DOTS client and server, but t~~The ~~existing~~ data channel as specified in [RFC8783] lacks a knowledge transmission structure ~~and corresponding YANG data model~~, and cannot realize the transmission of DDoS attack knowledge stored in a knowledge graph structure. Therefore, it is difficult to meet the dynamically changing form of DDoS attacks.

This document defines new DOTS data channel attributes. It mainly builds a new YANG data model for distributed scenarios that need to constantly update and synchronize the content of the knowledge base, including a general tree structure and YANG data modules, aiming to customize the DDoS knowledge transmission configuration between distributed knowledge bases.

Commenté [BMI2]: Should be defined first + include a discussion how this is useful

Commenté [BMI3]: This can be deleted as this is redundant with the first part of the sentence.

Commenté [BMI4]: The causality effect is not trivial as there is no discussion to demonstrate the claim. Please consider elaborating this further. Thanks.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Readers should be familiar with the terms and concepts defined in [RFC8612], [RFC8783], and [RFC8811].

3. DOTS Knowledge Transmission Architecture

The basic DOTS knowledge transmission architecture is illustrated in Figure 1:

```
               +-------------+  +---------------+     +--------------+
               |             |  |    DOTSG      |     |              |
               | +---------+ |  +---------------+     | +----------+ |
               | |DDoS     | |  |  Knowledge    |     | |knowledge| |
               | |Target-1| |  |  Collection   | +--> |base-1    | |
               | +---------+ |  +-------+-------+  |  | +----------+ |
               |             |  |       |       |  |  |              |
         DDoS  | +---------+ |  +-------v-------+  |  | +----------+ |
         Attack | |DDoS    | |  | Knowledge     |  |  | |knowledge| |
         ------>| |Target-2| |  | Transmission  | +--> |base-2    | |
               | +---------+ |  +------+-+------+  |  | +----------+ |
               |   ......    |  |      | |      |  |  |   ......     |
               | +---------+ |  |      | |      |  |  | +----------+ |
               | |DDoS     | |  |      | |      |  |  | |knowledge| |
               | |Target-n| |  |      | |      | +--> |base-n    | |
               | +---------+ |  | Data Channel |  |  | +----------+ |
```

Commenté [BMI5]: DOTS gateway ?

Please note this is an optional functional entity in DOTS.

```
        |        C    <--+--------------+--+-->  S          |
        +------------+  +---------------+     +-------------+
```

* C is for DOTS client ~~functionality~~
* S is for DOTS server ~~functionality~~

Figure 1: Basic DOTS Knowledge Transmission Architecture

A simple example of the DOTS knowledge transmission architecture may be a DDoS attack-oriented network security knowledge base deployed on a large scale in the form of distributed nodes as the server, and the attacked target as the client. The host suspects that it has been attacked by a DDoS, and obtains information about the DDoS attack based on the DOTS client and forwards it via the DOTS gateway. The DOTS gateway matches DDoS attack traffic and converts it into attack knowledge and stores it in a nearby network security knowledge base. After a certain period of time, distributed nodes transmit new knowledge through data channels to achieve knowledge synchronization. Therefore, they aim to share attack knowledge in different domains and actively adapt to dynamically changing DDoS attacks.

In some cases, part of the domain is always in a state of being unattended, and another part of the domain may be frequently subjected to DDoS attacks, so new knowledge of DDoS attacks will be continuously introduced. The administrator needs to configure a reasonable update cycle according to the attack situation in the control domain. For domains with few attack records, the update period should be appropriately extended to reduce bandwidth consumption. For domains with high security requirements, the number of requests should be increased and DOTS data channel~~s~~ should be established with more domains to obtain more comprehensive knowledge of DDoS attacks.

This document augments the "ietf-dots-data-channel" (dots-data) DOTS data YANG module defined in [RFC8783] with ~~these~~ the following additional attributes that can be negotiated between DOTS servers to realize the secure and periodic transmission of DDoS attack knowledge:

related-time: This attribute contains the creation-time and merge-time of DDoS attack knowledge. The default value of this attribute is 'now-date' obtained from the system.

This is an optional attribute.

label: This attribute represents the type of network security knowledge graph currently transmitted. The default value of this attribute is '0'.

This is an optional attribute.

Commenté [BMI6]: I don't parse this well

Commenté [BMI7]: Do you really need to use a co-located model as a "simple example"?

Commenté [BMI8]: Or is under attack ?

Commenté [BMI9]: How ?

Commenté [BMI10]: To be further characterized (how to determine where such a base is located)

Mis en forme : Surlignage

Commenté [BMI11]: Do you mean during the time where it suspects an attack is ongoing?

If so, there is a chance that the data channel will ne broken.

Commenté [BMI12]: That is ?

Commenté [BMI13]: How this is set ?

Commenté [BMI14]: I guess you meant « DOTS client domain"

Mis en forme : Surlignage

Commenté [BMI15]: Which domains ?

Commenté [BMI16]: There is no « concept » of negotiation in RESTCONF, in general.

Commenté [BMI17]: How this type is defined ?

knowledge-base-name: This attribute represents the name of the currently transmitted network security knowledge graph. The default value of this attribute is 'none'.

Commenté [BMI18]: Who sets the name ? Does it have a local significance?

This is an optional attribute.

entities: This attribute contains all node information in the knowledge graph. Optional under this attribute include 'type', 'id', 'labels', and 'properties'.

This is an optional attribute.

relationship: This attribute contains all the node relationships in the knowledge graph. Optional under this attribute include 'id', 'type', 'label', 'properties', 'start', and 'end'.

This is an optional attribute.

4. DOTS Knowledge Transmission YANG Module

4.1 Generic Tree Structure

This document defines the YANG module "li-dots-knowledge-trans" (Section 3), which has the following tree structure:

```
module: li-dots-knowledge-trans
  +--rw dots-data
     +--rw dots-client* [cuid]
     |  ...
     +--ro capabilities
     |  ...
     +--rw knowledge-trans
        +--rw related-time
        |  +--rw creation-time       string
        |  +--rw merge-time          string
        +--rw label
        +--rw knowledge-base-name     string
        +--rw model-param     string
        +--rw ~~eneities~~ entities
        |  +--rw type                string
        |  +--rw id                  uint32
        |  +--rw labels              string
        |  +--rw properties
        |     +-- rw name            string
        |     +-- rw establish-date      uint8
        +--rw relationship
           +--rw id                  uint32
           +--rw type                string
           +--rw label               string
```

Commenté [BMI19]: Shouldn't this be a list?

Commenté [BMI20]: Why isn't this a date-and-time?

Commenté [BMI21]: Shouldn't this be defined as a list?

```
           +--rw properties         string
           +--rw start
           |  +--rw id              uint32
           |  +--rw labels          string
           +--rw end
              +--rw id              uint32
              +--rw labels1         string
```

Figure 2: DOTS Knowledge Transmission Subtree

Based on the above-mentioned yang module structure, a method is provided for the distributed network security knowledge base to periodically update and synchronize the new DDoS attack knowledge in each domain, so as to more effectively deal with the ever-changing DDoS attack types.

4.2 YANG Module

This module uses the common YANG types defined in [RFC6991] and types defined in [RFC8519].

```
<CODE BEGINS> file "li-dots-knowledge-trans@2021-08-06.yang"
module li-dots-knowledge-trans {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:li-dots-knowledge-trans";
  prefix dots-knowledge;

  import ietf-dots-data-channel {
    prefix dots-data;
    reference
      "RFC 8783: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) Data Channel Specification";
  }

  organization
     "IETF DDoS Open Threat Signaling (DOTS) Working Group";
  contact
       "WG Web:   <https://datatracker.ietf.org/wg/dots/>
        WG List:  <mailto:dots@ietf.org>

        Author:  Kun Li
                 <mailto:19111021@bjtu.edu.cn>;

        Author:  Huachun Zhou
                 <mailto:hchzhou@bjtu.edu.cn>";

        Author:  Zhe Tu
                 <mailto:19111038@bjtu.edu.cn>;
```

```
          Author:  Feiyang Liu
                   <mailto:19120077@bjtu.edu.cn>;

          Author:  Weilin Wang
                   <mailto:19111021@bjtu.edu.cn>;

    description
      "This module contains YANG definitions for the configuration
       of parameters that can be negotiated between DOTS servers to
       realize the secure and periodic transmission of DDoS
       attack knowledge.

       Copyright (c) 2021 IETF Trust and the persons identified as
       authors of the code.  All rights reserved.

       Redistribution and use in source and binary forms, with or
       without modification, is permitted pursuant to, and subject
       to the license terms contained in, the Simplified BSD License
       set forth in Section 4.c of the IETF Trust's Legal Provisions
       Relating to IETF Documents
       (http://trustee.ietf.org/license-info).

       This version of this YANG module is part of RFC 8783; see
       the RFC itself for full legal notices.";

    revision 2021-08-06 {
      description
        "Initial revision.";
      reference
        "RFC 8783: Knowledge Transmission Using Distributed
                   Denial-of-Service Open Threat Signaling
                   (DOTS) Data Channel";
    }

    grouping knowledge-trans {
       description
         "Top-level grouping for knowledge transmission.";
       container related-time {
         description
           "Relevant time for knowledge transmission.";
         leaf creation-time {
           type string
           description
             "Knowledge graph establishment time.";
        }
        leaf merge-time {
          type string
           description
             "Knowledge synchronization initiation time.";
        }
       }
       leaf label {
         type string
         description
           "Type of network security knowledge graph currently
            transmitted.";
       }
       leaf knowledge-base-name {
         type string
         description
           "Name of network security knowledge graph currently
            transmitted.";
       }
       leaf model-param {
         type string
         description
           "Attached machine learning h5 model parameters.";
       }
       list eneities {
         key id;
         description
           "Entity contains all node information in the knowledge
            graph.";
         leaf id {
           type uint32
           description
             "Id of the new node.";
         }
         leaf type {
           type string
           description
             "Type of the new node.";
         }
         leaf labels {
           type string
           description
             "Label of the new node.";
         }
         container properties {
           description
             "Properties of the new node.";
           leaf name {
             type string
             description
               "Property name of the new node.";
           }
           leaf establishdate {
             type uint8
             description
               "Node creation time.";
           }
         }
       }
```

```
      list relationship {
        key id;
        description
        "Relationship contains all the node relationships in the
          knowledge graph.";
       leaf id {
         type uint32
         description
           "Id of the new relationship.";
       }
       leaf type {
         type string
         description
           "Type of the new relationship.";
       }
       leaf labels {
         type string
         description
           "Label of the new relationship.";
       }
       leaf properties {
         type string
         description
           "Properties of the new relationship.";
       }
        container start {
          description
            "Starting node of the new relationship.";
          leaf id {
            type uint32
            description
              "Id of starting node.";
          }
          leaf labels {
            type string
            description
              "Label of starting node.";
          }
        }
        container end {
          description
            "Ending node of the new relationship.";
          leaf id {
            type uint32
            description
              "Id of ending node.";
          }
          leaf labels {
            type string
            description
              "Label of ending node.";
          }
        }
      }
   }
   <CODE ENDS>
```

5. Managing DOTS Knowledge Transmission

A POST request is used by a DOTS client to periodically synchronize knowledge about DDoS attacks. This knowledge can be used to guide subsequent mitigation measures to more effectively deal with multiple types of DDoS attacks. An example of a request for periodic transmission of DDoS attack knowledge is shown in Figure 3.

```
POST /restconf/data/ietf-dots-data-channel:dots-data\
     /dots-client=cuid HTTP/1.1
Host: {host}: {port}
Content-Type: application/yang-data+json

{
  "ietf-dots-data-channel:knowledge-trans": {
    [
      {
        "type": "node",
        "id": 0,
        "labels": ["Slow-DDoS"],
        "properties": {
          "name": "Shrew",
          "establishdate": 20210806094618
        },
      {
        "type": "node",
        "id": 1,
        "labels": ["Application-layer-DDoS"],
        "properties": {
          "name": "Http-get",
          "establishdate": 20210806100512
        },
      },
      {
        "id": 0,
        "type": "relationship",
        "label": "Related-to",
        "properties": {}
        "start": {
          "id": 0,
          "labels": "Slow-DDoS"
        }
        "end": {
          "id": 1,
          "labels": "Application-layer-DDoS"
        }
      }
    ]
  }
}
```

Figure 3: An Example of DOTS Request Knowledge Update Process

A DOTS client MUST use the POST request to request to update the knowledge, otherwise the server MUST respond with a "404 Not Found" status-line.

6. IANA Considerations

This document has no IANA actions.

7. Security Considerations

The security considerations for the DOTS data channel protocol are discussed in Section 10 of [RFC8783].

This document defines YANG data structures that are meant to be used as an abstract representation in DOTS data channel messages. As such, the "li-dots-knowledge-trans" module does not introduce any new vulnerabilities beyond those specified above.

8. References

8.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8783] Boucadair, M., Ed. and T. Reddy.K, Ed., "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", RFC 8783, DOI 10.17487/RFC8783, May 2020, <https://www.rfc-editor.org/info/rfc8783>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC8519] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair, "YANG Data Model for Network Access Control Lists (ACLs)", RFC 8519, DOI 10.17487/RFC8519, March 2019, <https://www.rfc-editor.org/info/rfc8519>.

8.2 Informative References

[RFC8612] Mortensen, A., Reddy, T., and R. Moskowitz, "DDoS Open Threat Signaling (DOTS) Requirements", RFC 8612, DOI 10.17487/RFC8612, May 2019, <https://www.rfc-editor.org/info/rfc8612>.

[RFC8811] Mortensen, A., Ed., Reddy.K, T., Ed., Andreasen, F., Teague, N., and R. Compton, "DDoS Open Threat Signaling (DOTS) Architecture", RFC 8811, DOI 10.17487/RFC8811, August 2020, <https://www.rfc-editor.org/info/rfc8811>.

Acknowledgments

TBC

Author's Addresses

Kun Li
Beijing Jiaotong University
Beijing
Phone: <86-15652992293>
Email: 19111021@bjtu.edu.cn

Huachun Zhou
Beijing Jiaotong University
Beijing
Phone: <86-13718168186>
Email: hchzhou@bjtu.edu.cn

Zhe Tu
Beijing Jiaotong University
Beijing
Phone: <86-13146050755>
Email: 19111038@bjtu.edu.cn

Feiyang Liu
Beijing Jiaotong University

Beijing
Phone: <86-18813006511>
Email: 19120077@bjtu.edu.cn

Weilin Wang
Beijing Jiaotong University
Beijing
Phone: <86-15910887582>
Email: 20120122@bjtu.edu.cn