Cyber Implementation for CWIX 18

Requirements as specified in Jim Ruth email of March 28, 2018:

Category 1. EW options:
a. block a specified fraction (range 0 to 1) of messages for a specified duration
b. block a specified fraction (range 0 to 1) of messages at random intervals, off and on times both uniformly distributed, with separate on and off mean specified
c. block every nth message for a specified n

Category 2. Cyber options:
a. modify all reported locations by a specified (lat,lon) offset

Category 3. Jim's additions: (in Priority)
Add EW-d. Block all messages from specific area (lat, long, distance) ("blanket" jamming) for a specified duration (minutes).
Add Cyber-b. Modify report time by a specified (seconds, minutes) offset
Add Cyber-c. Block all messages from a specified device (IP address, CP node, etc.)

Operation

Cyber attacks may be initiated, modified, and terminated during server operation. An XML file containing cyber command language will be used to control cyber attack operation and submitted to the server using the C2SIM REST client.

A separate log file, will be created and all cyber related activity including command submission and attacks conducted will be logged. This will be a rolling logger. At the start of each day the previous days file will be renamed with the date and a new log file will be opened. The log file is located on the C2SIM Server in /home/bmluser/bmlFiles/c2simCyber. The daily log files are named: yyyy-mm-dd_cyber.log. The current daily log file is named cyber.log.

Each incoming message will be examined and one of the following will be performed:

1) The message will be processed normally,
2) The message will be modified and then processed normally
3) The message will be dropped

In all cases a positive response will be sent to the submitter.

With IBML09 reports multiple <Report> elements may be included in a single <BMLReport> document. A single report may be discarded without the entire document being discarded. In the case the parent document will be considered to be modified. In the case that all <Report> elements are discarded via a cyber attack

Obtaining Status of Cyber Attacks

The status of cyber attack operations can be obtained with a web browser by connecting to:

serverHostName:8080/BMLServer/status

A typical return from the status request is:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
     <status>OK</status>
     <serverInitialized>true</serverInitialized>
     <sessionInitialized>true</sessionInitialized>
     <cyberActive>true</cyberActive>
          <activeAttacks>EWa Cyber_b</activeAttacks>
          <messagesModified>8</messagesModified>
          <messagesDiscarded>2</messagesDiscarded>
          <messagesUnModified>2</messagesModified>
     <unitDatabaseName>default</unitDatabaseName>
     <unitDatabaseSize>7</unitDatabaseSize>
     <msgNumber>12</msgNumber>
</result>
```

Log File

In addition, a realtime view of cyber operations may be obtained by logging in to the C2SIM server and performing the following:

```
cd ~/bmlFiles/c2simCyber
tail -f cyber.log
```

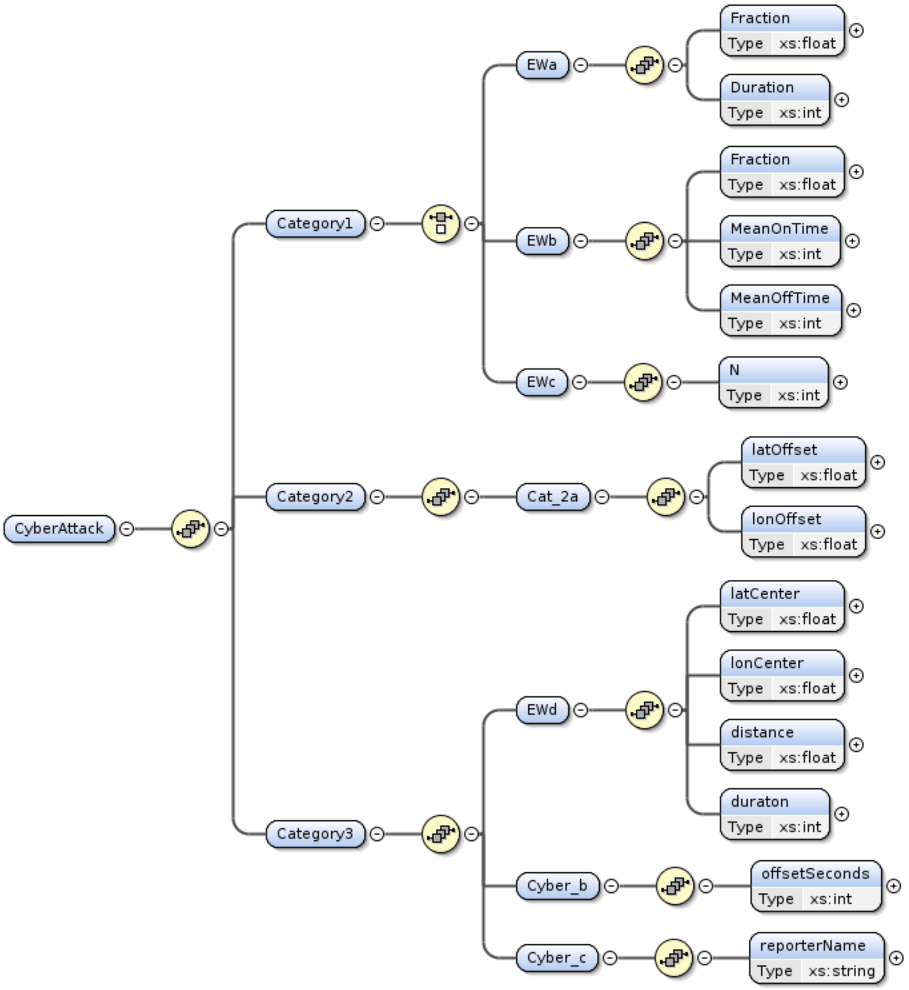
Typical output is below:

```
2018-04-16 12:22:20,524 DEBUG Cyber processCommand submitted by dsc
2018-04-16 12:22:20,525 DEBUG Cyber commands accepted - Starting cyber attacks.
Active attacks are: EWa
2018-04-16 12:22:42,549 DEBUG Cyber processCommand submitted by dsc
2018-04-16 12:23:10,125 DEBUG Cyber commands accepted - Starting cyber attacks.
Active attacks are: EWa
2018-04-16 12:25:16,657 DEBUG Starting execution
2018-04-16 12:25:16,776 DEBUG        Message 1 was not modified or discarded
2018-04-16 12:25:17,126 DEBUG        Message 2 was not modified or discarded
2018-04-16 12:25:22,841 DEBUG Cyber processCommand submitted by dsc
2018-04-16 12:25:23,957 DEBUG Cyber commands accepted - Starting cyber attacks.
Active attacks are: EWa
2018-04-16 12:26:12,393 DEBUG        Message 3 was modified
Attacks:
       EWa - Inner Report Discarded
2018-04-16 12:26:13,659 DEBUG        Message 4 was modified
Attacks:
       EWa - Inner Report Discarded
Attacks:
       EWa - Inner Report Discarded
2018-04-16 12:26:16,056 DEBUG        Message 7 was modified
```

```
Attacks:
        EWa - Inner Report Discarded
        EWa - Inner Report Discarded
        EWa - Inner Report Discarded
2018-04-16 12:26:16,933 DEBUG        Message 8 was discarded
Attacks:
        EWa - Inner Report Discarded
        EWa - Inner Report Discarded
        EWa - Inner Report Discarded
        EWa - Inner Report Discarded
        EWa - All inner reports discarded - Parent document is discarded
```

Cyber Attack Commands

The command language will be submitted by the controller of the cyber environment and will follow the XML schema shown below.



Each submission of a new cyber command language file will cancel any attacks in operation at that time and will start new attacks describes in the xml. Submission of a cyber command file containing only the root element (CyberAttack) will stop all attacks.

Submission of a cyber file is through the C2SIM REST client using cyber as the protocol. Example

```
java -jar BML_WSClient2-2.4.1_ALL.jar localhost cyber1.xml dsc cyber
```

A typical cyber command file is given below:

```
<?xml version="1.0" encoding="UTF-8"?>
<CyberAttack xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.sisostds.org/schemas/c2sim/1.0 CyberAttack.xsd"
 xmlns="http://www.sisostds.org/schemas/c2sim/1.0"
 targetNamespace="http://www.sisostds.org/schemas/c2sim/1.0"
 xmlns:vc="http://www.w3.org/2007/XMLSchema-versioning">
    <Category1>
        <EWa>
            <Fraction>0.1</Fraction>
            <Duration>300</Duration>
        </EWa>
        <EWb>
            <Fraction>.5</Fraction>
            <MeanOnTime>60</MeanOnTime>
            <MeanOffTime>15</MeanOffTime>
        </EWb>
        <EWc>
            <N>8</N>
        </EWc>
    </Category1>

    <Category2>
        <Cat_2a>
            <latOffset>5</latOffset>
            <lonOffset>8</lonOffset>
        </Cat_2a>
    </Category2>
    <Category3>
        <EWd>
            <latCenter>45</latCenter>
            <lonCenter>27.5</lonCenter>
            <distance>100</distance>
            <duraton>600</duraton>
        </EWd>
        <Cyber_b>
            <offsetSeconds>60</offsetSeconds>
        </Cyber_b>
        <Cyber_c>
            <reporterName>reporterName0</reporterName>
        </Cyber_c>
    </Category3>
</CyberAttack>
```