**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ**

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

**«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ ВЫДЕЛЕНИЯ ЛОГИЧЕСКИ СВЯЗАННЫХ ПОТОКОВ В ВЫСОКОСКОРОСТНОМ СЕТЕВОМ ТРАФИКЕ**  **Руководство оператора**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.05.03-01 01-1-ЛУ** | | |
|  |  | |
| Исполнитель:  студент группы БПИ197  \_\_\_\_\_\_\_\_\_\_\_\_ / Глущенко З. С./  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2022 г. | |
|  | | |
| **Москва 2022** | |  |

|  |  |
| --- | --- |
| ***Подп. и дата*** |  |
| ***Инв. № дубл.*** |  |
| ***Взам. инв. №*** |  |
| ***Подп. и дата*** |  |
| ***Инв. № подл*** |  |

Департамент программной инженерии

|  |  |  |
| --- | --- | --- |
| СОГЛАСОВАНО  Преподаватель факультета компьютерных наук, доцент базовой кафедры «Системное программирование» ИСП ран, канд. техн. наук  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. И. Гетьман  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г.  СОГЛАСОВАНО  Руководитель департамента программной инженерии, доцент факультета компьютерных наук, канд. экон. наук  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С. А. Лебедев  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2022 г. |  | УТВЕРЖДАЮ  Академический руководитель образовательной программы «Программная инженерия»,  канд. техн .наук  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В. В. Шилов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г. |

|  |  |  |  |
| --- | --- | --- | --- |
| УТВЕРЖДЕНО  RU.17701729.05.03-01 81 01-1-ЛУ | |  |  |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл*** |  | | **ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ ВЫДЕЛЕНИЯ ЛОГИЧЕСКИ СВЯЗАННЫХ ПОТОКОВ В ВЫСОКОСКОРОСТНОМ СЕТЕВОМ ТРАФИКЕ**  **Руководство оператора**  **RU.17701729.05.03-01 81 01-1**  **Листов 15** | | | | |
|  |  | | | |
|  | | | |
| **Москва 2022** | | | | |
|  |  | | | | |

|  |  |
| --- | --- |
|  |  |
|  |  |

СОДЕРЖАНИЕ

[**1.** **Назначение программы** 4](#_Toc100921542)

[**1.1.** **Назначение программы** 4](#_Toc100921543)

[**1.1.1.** **Функциональное назначение** 4](#_Toc100921544)

[**1.1.2.** **Эксплуатационное назначение** 4](#_Toc100921545)

[**1.2.** **Состав функций программы** 4](#_Toc100921546)

[**2.** **Условие выполнения программы** 5](#_Toc100921547)

[**2.1.** **Состав технических средств** 5](#_Toc100921548)

[**2.2.** **Состав технических средств** 5](#_Toc100921549)

[**3.** **Выполнение программы** 6](#_Toc100921550)

[**3.1.** **Конфигурационный файл для модуля IPC** 6](#_Toc100921551)

[**3.2.** **Конфигурационный файл для модуля Producer** 7](#_Toc100921552)

[**3.3.** **Конфигурационный файл для модуля StreamSelector** 8](#_Toc100921553)

[**3.4.** **Конфигурационный файл для модуля PacketFilter** 9](#_Toc100921554)

[**3.5.** **Конфигурационный файл для модуля FTP\_Extractor** 9](#_Toc100921555)

[**3.6.** **Конфигурационный файл для модуля SignalConverter** 10](#_Toc100921556)

[**3.7.** **Конфигурационный файл для модуля StreamSaver** 10](#_Toc100921557)

[**3.8.** **Конфигурационный файл для модуля StreamMerger** 11](#_Toc100921558)

[**3.9.** **Запуск программы** 11](#_Toc100921559)

[**4.** **Сообщение оператору** 12](#_Toc100921560)

[**5.** **Приложение 1. Список используемой литературы** 13](#_Toc100921561)

[**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ** 14](#_Toc100921562)

1. **Назначение программы**
   1. **Назначение программы**
      1. **Функциональное назначение**

Программный модуль позволяет выделять логически связанные потоки в сетевом трафике. Получая на вход группу потоков и предоставляя на выходе поток, состоящий из связанных потоков, пакеты которых упорядочены по временным меткам.

* + 1. **Эксплуатационное назначение**

Данный программный модуль может быть использован в составе системы анализа трафика, разрабатываемой в ИСП РАН и применяться, когда нужно найти и объединить логически связанные потоки.

* 1. **Состав функций программы**

Программа должна обеспечивать возможность выполнения следующих функций:

1. Выделять логически связанные потоки на основе сигнатур;
2. Объединять связанные логические потоки в один поток;
3. Выдавать логически связанные потоки как один поток и группу других потоков, которые не связаны логически;
4. **Условие выполнения программы**
   1. **Состав технических средств**

Для надежной и бесперебойной работы программы требуется следующий состав технических средств:

1. Процессор Intel Core i7 с тактовой частотой не менее 3,5 Ггц;;
2. Не менее 8 ГБ оперативной памяти;
3. Не менее 20 ГБ свободного места на жестком диске;
4. Клавиатура и мышь;
   1. **Состав технических средств**

Для нормального функционирования программы требуется компьютер, оснащенный следующими программными компонентами:

1. Система автоматизации сборки программного обеспечения из исходного кода CMake 3.5.1;
2. Установленный компилятор g++ 9.3.0;
3. Python версии 3.5 или выше;
4. **Выполнение программы**
   1. **Конфигурационный файл для модуля IPC**

{

"buffers": [

{

"name": "fragBuffer"

},

{

"name": "inputBuffer"

}

],

"queues": [

{

"name": "fragQueue",

"type": "PacketMessage"

},

{

"name": "inputQueue",

"type": "PacketMessage"

},

{

"size": 214000,

"name": "selectedFTPPackets",

"type": "StreamPacket"

},

{

"size": 214000,

"name": "streamPackets",

"type": "StreamPacket"

},

{

"size": 214000,

"name": "pairSignals\_converter",

"type": "PairStreamsSignalV4"

},

{

"size": 214000,

"name": "packetMessage",

"type": "PacketMessage"

},

{

"size": 214000,

"name": "streamPackets2",

"type": "StreamPacket"

},

{

"size": 214000,

"name": "signals\_selector",

"type": "SelectSignalV4"

},

{

"size": 214000,

"name": "selectSignals\_merger",

"type": "SelectSignalV4"

},

{

"size": 214000,

"name": "pairSignals\_merger",

"type": "PairStreamsSignalV4"

}

],

"tract\_prefix": "",

"name": "FTP\_module\_debug"

}

* 1. **Конфигурационный файл для модуля Producer**

{

"core": " AutomataTest",

"name": "Producer",

"networkCardId": 1,

"packetQueueName": "inputQueue",

"packetBufferName": "inputBuffer",

"fragmentQueueName": "fragQueue",

"fragmentBufferName": "fragBuffer",

"saveFullPackets": "true",

"reader": {

"isCycled": false,

"useTimeStamps": false,

"pcap file": "/home/zakhar/Desktop/smeshariki\_localnetwork.pcap",

"path": "./libprocess\_reader\_pcap\_file.so"

},

"defaultParser": "ETHER",

"parsers": [

{

"name": "CISCO\_HDLC",

"path": "./libprocess\_parser\_cisco\_hdlc.so"

},

{

"name": "ETHER",

"path": "./libprocess\_parser\_ether.so"

},

{

"name": "IP",

"path": "./libprocess\_parser\_ip.so"

},

{

"name": "MPLS\_UNICAST",

"path": "./libprocess\_parser\_mpls.so"

},

{

"name": "PPP",

"path": "./libprocess\_parser\_ppp.so"

},

{

"name": "FR",

"path": "./libprocess\_parser\_fr.so"

}

]

}

Параметрами, на которые стоит обратить внимание являются “pcap file”, в котором указывается путь до файла, из которого будет производиться чтение, и выходные очереди, и буферы.

* 1. **Конфигурационный файл для модуля StreamSelector**

{

"packetQueueName": "inputQueue",

"isSendSignals": false,

"signalQueueName": "signals\_selector",

"name": "StreamSelector",

"outputs": [

{

"queueName": "selectedFTPPackets",

"lifetime": 1000000,

"reasonNum": 1,

"isSendStreamPackets": true

}

],

"markersCount": 2000000,

"streamsCount": 200000,

"getInversed": true,

"packetBufferName": "inputBuffer",

"streamPacketQueueName": "streamPackets",

"streamSelectorsCount": 1,

"core": " AutomataTest"

}

Параметры, на которые стоит обратить внимание:

* + streamPacketQueueName – выходная очередь, в которую пересылаются поступившие пакеты с идентификатором потока
  + signalQueueName – входная очередь, из которой читаются сигналы на отбор
  + queueName – имя выходной очереди, куда попадают соответствующие отобранные пакеты
  1. **Конфигурационный файл для модуля PacketFilter**

{

"core": "AutomataTest",

"name": "Filter",

"packetFilterCount": 1,

"packetQueueName": "streamPackets2",

"packetBufferName": "inputBuffer",

"addressAuto": "",

"contextAuto": "accept\_context",

"useDoubleJumps": false,

"streamsCount": 10000,

"automataPath": "Automata/example/",

"outputs": [

{

"queueType": "PacketMessage",

"queueName": "packetMessage",

"reasonNum": 1,

"criterionName": "FTP\_PASV\_PORT"

}

]

}

* 1. **Конфигурационный файл для модуля FTP\_Extractor**

{

"core": "AutomataTest",

"name": "ftp\_extractor",

"packetQueue": "packetMessage",

"packetBuffer": "inputBuffer",

"pairSignals\_merger": "pairSignals\_merger",

"SelectSignals\_selector": "signals\_selector",

"pairSignals\_converter": "pairSignals\_converter"

}

Параметры, на которые стоит обратить внимание:

* + pairSignals\_merger – очередь сигналов с информацией о связанности потоков
  + SelectSignals\_selector – очередь сигналов на отбор
  + pairSignals\_converter - очередь с сигналов с частичными признаками
  1. **Конфигурационный файл для модуля SignalConverter**

{

"core": "AutomataTest",

"name": "SignalConverter",

"maxSignalsCount": 1000,

"streamsCount": 200000,

"streamPacketsIn": "streamPackets",

"streamPacketsOut": "streamPackets2",

"packetBuffer": "inputBuffer",

"signalsIn": "pairSignals\_converter",

"signalsOut": "signals\_selector",

"pairsOut": "pairSignals\_merger",

"hashlib\_path": "./libprocess\_hasher\_src\_port.so"

}

Параметры, на которые стоит обратить внимание:

* + streamPacketsIn - Входная очередь пакетов с идентификатором потока
  + streamPacketsOut - выходная очередь пакетов с идентификатором потока
  + signalsIn – Входная очередь сигналов с частичными признаками
  + signalsOut – Выходная очередь сигналов с полными признаками
  + pairsOut – Выходная очередь с информацией о связанности потоков
  1. **Конфигурационный файл для модуля StreamSaver**

{

"name": "StreamSaver",

"core": "AutomataTest",

"streamsCount": 200000,

"maxPacketSize": 65550,

"saveFullPackets": true,

"nanoPrecision": true,

"outputPath": "streams/",

"streamOut": "selectSignals\_merger",

"streamPacketsIn": "selectedFTPPackets",

"packetBuffer": "inputBuffer"

}

Параметры, на которые стоит обратить внимание:

* + outputPath – относительный путь, куда будет сохранены pcap файлы
  + selectedFTPPackets – Входная очередь отобранных пакетов
  + streamOut – Выходная очередь сигналов с информацией о готовности потока к объединению.
  1. **Конфигурационный файл для модуля StreamMerger**

{

"name": "StreamMerger",

"core": "AutomataTest",

"maxStreamsCount": 100,

"outputPath": "/home/zakhar/Desktop/process3\_qt/output/stream\_saver/merged/",

"inputPath": "/home/zakhar/Desktop/process3\_qt/output/stream\_saver/streams/",

"streamsIn": "selectSignals\_merger",

"pairSignalsIn": "pairSignals\_merger"

}

Параметры, на которые стоит обратить внимание:

* + streamsIn - Входная очередь сигналов с информацией о готовности потока к объединению.
  + pairSignalsIn – Входная очередь сигналов с информацией о связанности потоков
  + inputPath – путь до директории с сохраненными pcap файлами
  + outputPath – путь до директории куда будет сохранен объединенный pcap файл
  1. **Запуск программы**

Для запуска программы необходимо открыть терминал, перейти в директорию проекта, открыть папку scripts и ввести

./start.py

Запуститься программа и веб интерфейс для взаимодействия с ней доступный по адресу

localhost:8080/control/AutomataTest/

Для запуска модулей нужно нажать на кнопку Reload all

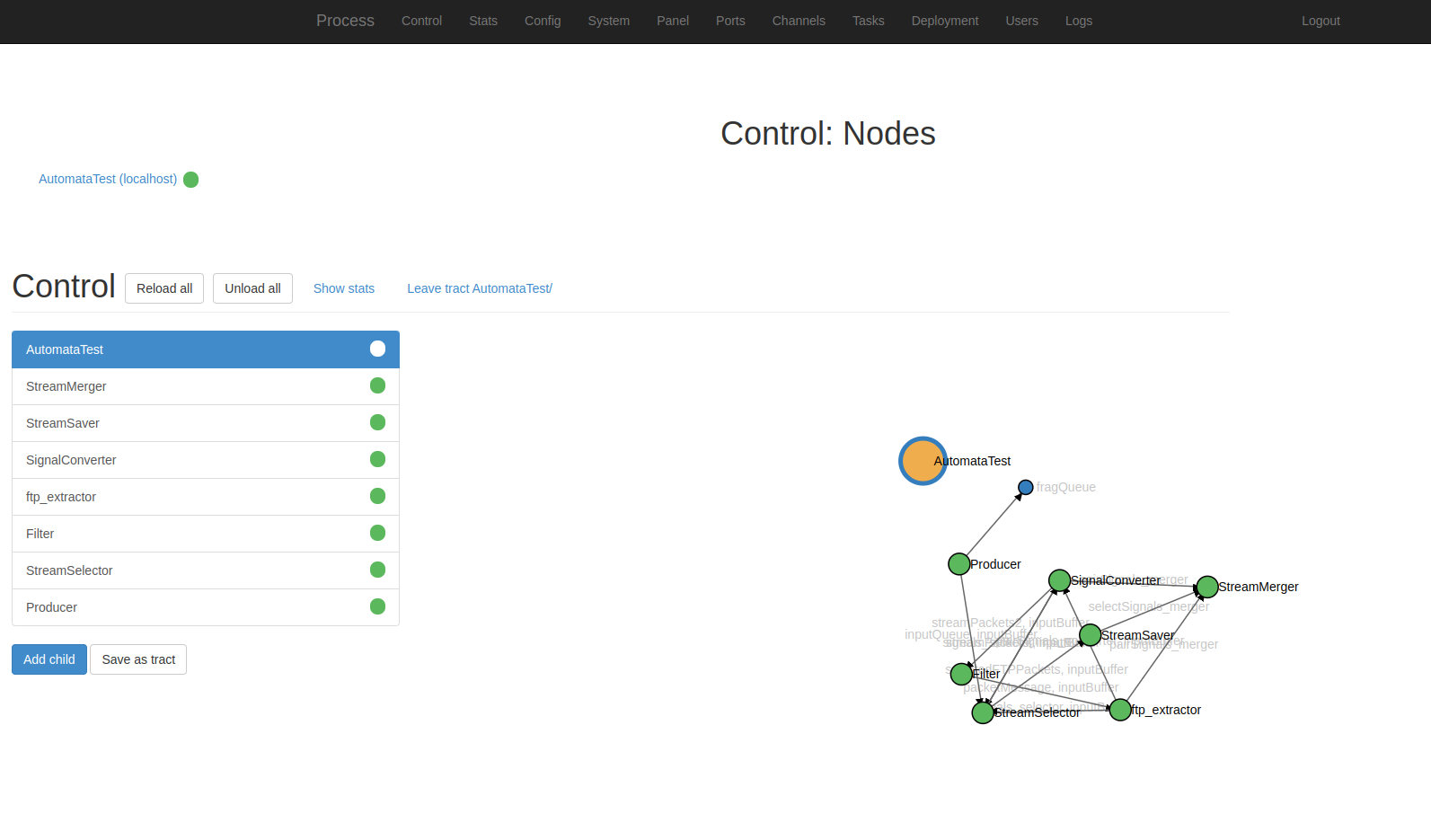


Рисунок 1. Панель управление

1. **Сообщение оператору**

Состав программной документации должен включать в себя следующие компоненты:

1. Техническое задание (ГОСТ 19.201-78)
2. Программа и методика испытаний (ГОСТ 19.301-78)
3. Пояснительная записка (ГОСТ 19.404-79)
4. Руководство оператора (ГОСТ 19.505-79)
5. Текст программы (ГОСТ 19.401-78)
6. **Приложение 1. Список используемой литературы**
7. ГОСТ 19.101-77 Виды программ и программных документов. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
8. ГОСТ 19.102-77 Стадии разработки. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
9. ГОСТ 19.103-77 Обозначения программ и программных документов. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
10. ГОСТ 19.104-78 Основные надписи. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
11. ГОСТ 19.105-78 Общие требования к программным документам. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
12. ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
13. ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
14. ГОСТ 19.603-78 Общие правила внесения изменений. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
15. ГОСТ 19.604-78 Правила внесения изменений в программные документы, выполненные печатным способом. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
16. ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды. – М.: Изд-во стандартов, 1997.
17. ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
18. ГОСТ 19.602-78 Правила дублирования, учета и хранения программных документов, выполненных печатным способом. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
19. Джеймс Куроуз. Компьютерные сети. Нисходящий подход. // Джеймс Куроуз, Кит Росс – 6-е изд., Москва, 2016

# **ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лист регистрации изменений | | | | | | | | | |
| Номера листов (страниц) | | | | | Всего листов (страниц в докум.) | № документа | Входящий № сопроводительного докум. и дата | Подп. | Дата |
| Изм. | Измененных | Замененных | Новых | Аннулированх |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |