НОРСИ-ТРАНС
Закрытое Акционерное Общество

ETSI
World Class Standards

Работа ЗАО НОРСИ-ТРАНС в области международной стандартизации связи.

Докладчик: Хохлов Роман

Дата: 17 апреля 2019 года

Международная деятельность ЗАО НОРСИ-ТРАНС в рамках работы по стандартизации в ETSI.

Группы по стандартизации ETSI:

- SmartM2M:Technical Committee (TC) Smart Machine-to-Machine Communications
- TC CYBER: Cyber security
- TC eHEALTH

Международная деятельность ЗАО НОРСИ-ТРАНС в рамках работы по стандартизации в ETSI.

Группы по стандартизации ETSI TC SmartM2M: Technical Committee Smart Machine-to-Machine Communications.

Presenter's Family Name: **Reznikov**	**Presenter's First name:** **Mikhail**
Company **CJSC "Norsi-Trans"**	**Presenter's email address:** **mikerez@norsi-trans.ru** **Presenter's mobile number:** **+79637198596**
Authors: **Mikhail Reznikov**	
Abstract title: **M2M fair queuing using SDN-switch capabilities**	
Select which related agenda item you are referring to in the call for Presentation: **Data Models and Ontologies and interworking**	

Международная деятельность ЗАО НОРСИ-ТРАНС в рамках работы по стандартизации в ETSI. Группы по стандартизации ETSI: TC CYBER

Работы ЗАО Норси-Транс в ETSI TC CYBER:

1. Denial Of Service threat impact on ISP/MNO security
2. Hardware and software systems for protection against DDoS attacks as a DPI analysis solution to be integrated in telecom operator's channels
3. Feasibility Report on LI provisions to the Russian market
4. Technical methods and recommendations to implement content traffic filtration
5. Universal platform for Data Collection and Analysis

Международная деятельность ЗАО НОРСИ-ТРАНС в рамках работы по стандартизации в ETSI.

Группы по стандартизации ETSI: TC eHealth

Международная деятельность ЗАО НОРСИ-ТРАНС в рамках работы по стандартизации в ETSI.

Работа ЗАО Норси-Транс в ТС SmartM2M: M2M fair queuing using SDN-switch capabilities

Presenter's Family Name: **Reznikov**	**Presenter's First name:** **Mikhail**
Company **CJSC "Norsi-Trans"**	**Presenter's email address:** **mikerez@norsi-trans.ru** **Presenter's mobile number:** **+79637198596**
Authors: **Mikhail Reznikov**	
Abstract title: **M2M fair queuing using SDN-switch capabilities**	
Select which related agenda item you are referring to in the call for Presentation: **Data Models and Ontologies and interworking**	

M2M fair queuing using SDN-switch capabilities / Аппаратно Программное обеспечение QoS SDN, обеспечивающее приоритетную постановку в очередь потока команд M2M из разных источников, отдавая приоритет некоторым устройствам или службам, или замедляя работу наиболее активных пользователей.

НТ НОРСИ-ТРАНС Закрытое Акционерное Общество

ETSI World Class Standards

Presentation description:

Traditionally, general purpose IP-channels are suggested as the main carrier at network level for M2M interaction. Furthermore, the most common TCP transport protocol is used for creation of a session for the majority of M2M functions.

As is widely known, traditional TCP/IP stack comes with the set of specific problems related to Quality of Service needs. Basically there is no mechanism for prioritization or queueing in upper network layers of the Internet, and QoS abilities have to appear at physically-dependent layers. From the point of clear TCP/IP function one user can simultaneously make plenty of connections forcing other users out. As a result, deliberate or spontaneous Denial of Service could occur.

Since M2M concept notably requires QoS feature, this possibility has been examined in several works regarding different bearer types and generations. Due to the 5G network and IoT era, SDN QoS functions should be considered.

Besides, the case of M2M Gateway standing out of Core/Access Network should be investigated.

The demonstration shows SDN QoS hardware and software realization that provides fair queuing of M2M command flow from different sources, giving priority to some devices or services or slowing down the most active users.

Denial Of Service threat impact on ISP/MNO security.

The Denial of Service (DoS) threat was investigated in TISPAN TS 102 165-1 V4.2.3 (2011-03) and basic classification was made.

DoS/DDoS attacks are a threat that is approaching with a plenty of new Internet users and devices that have become online.

There are different ways to provide harmful traffic propagation or service disturbance and with widely distributed big network this problem increases several times.

Considering ISP/MNO, there are such problems as local service disturbance, channel bandwidth consumption and abuse users control.

Each problem impacts network security and several ways are commonly used to avoid.

The main goal of the document is to consider general models of impact and estimate the effectiveness of possible countermeasures.

Detailed security impact for different ISP/MNO devices should be described.

The most difficult DoS defence tasks should be brought out and investigated.

The general pitfalls and bottlenecks should be highlited.

Finally, the 5G/SDN and NFV/Cloud approaches are to be focused as possible DDoS carrier and victim.

This activity will also help working on different WIs related to network attacks threat.

Hardware and software systems for protection against DDoS attacks as a DPI analysis solution to be integrated in telecom operator's channels

DDoS attacks blocking/filtering is a complicated undetermined task. In contrast to other kinds of attacks, for network system attacks all entrances are open and violator very likely is already in the system before we decide to block him.

Finally, detecting traffic belonging to exact attack is difficult because often it looks like usual activity and there is high possibility of innocent users blocking.

As result, the powerful algorithms or big databases are required for effective DDoS attack blocking otherwise solution could just minimize attack impact.

As one of possible defense application point the channel could be considered.

The benefits are clear: there is no impact to ISP's routers and services while protection works.

This is very useful when ISP does not want to change routers/BGP configuration or does often changes or upgrades in configuration.

While in-channel solution is comfortable it requires fast DPI engine, fault-safety and redundance capabilities.

The other general feature of such solution is possibility of blocking large source-distributed attacks at the top of hierarchy with no need to forward all traffic to remote filtration units.

Feasibility Report on LI provisions to the Russian market

Technical methods and recommendations to implement content traffic filtration

- Methods and recommendations on connection of the content filtering complexes to the networks of telecom operators and Internet service providers (inline bypass connection scheme and BGP traffic capture);
- Methods and recommendations on realization of hardware and software complexes to enable legality in networks of telecom operators and Internet service providers in a cloud format;
- Methods and recommendations on normative documents describing requirements to the content filtering solutions on the basis of normative documents of the Russian Federation;
- Methods and recommendations on development, support and operation of the databases containing the forbidden materials;
- Standardization of the protocol of exchange of information between the content filtering solutions and databases containing the forbidden materials;
- Methods and recommendations on creation of electronic services providing content filtering;
- Methods and recommendations on realization of DPI (Deep Packet Inspection) solutions;
- Methods and recommendations on realization of DCI (Deep Content Inspection) solutions;
- Methods and recommendations on application of the content filtering solutions in educational and healthcare organizations, public wireless networks.

Universal platform for Data Collection and Analysis is a tool for achievement of the greatest efficiency of analysis of large volumes of various information. Special mechanisms of universal platform data visualization provide quick search of solutions and rapid assessment of facts.

The work will focus on the following issues:

- description of structure and features of Universal platform for Data Collection and Analysis;
- analytical requests to Big Data Appliance systems from Universal platform;
- requests to external DBMS from Universal platform,
- statistics on results of analytical requests;
- geoinformation system - visualization of analytical request results, target's path and movement location;
- use of reference information;
- data sources and their information value.

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Спасибо за внимание!

ЗАО «Норси-Транс»

email: info@norsi-trans.ru

тел: +7 495 748-74-83