Archives of
Transport System
Telematics

Volume 9

Issue 2

May 2016

Mobile and reliable data access to telematics data systems

D. LASKOWSKI, P. LUBKOWSKI
MILITARY UNIVERSITY OF TECHNOLOGY, Gen. S. Kaliskiego 2, 00 – 908 Warsaw, Poland
EMAIL: dariusz.laskowski@wat.edu.pl

ABSTRACT

The perspective of use the Bring Your Own Device (BYOD) model in telematics environment which ensure a reliable access to network resources is presented in the paper. The BYOD model is a future-proof solution which applies in areas related to database systems. It provides the user wireless access with the use of 802.11n/ac/d standard, mobile access via WiMax-2 or LTE-A networks and wired with the use of Gigabit Ethernet technology.
The research network which reflects the events representative for the telematics environment was established for the verification of functional capabilities of BYOD model. Services that offer a user the synchronization of files between mobile terminals and data server were implemented in testbed. A detailed set of test scenarios and criteria for assessment of the declared properties model BYOD were also defined. The article presents the results of research that confirm the use of this type of networking solutions for mobile and reliable access to data in a telematics environment.

KEYWORDS: data transfer, mobile access, reliability of telematics system, BYOD

1. Introduction

In the recent years a very dynamic development of technologies, including mobile technology is noticeable. Solutions, which on this occasion arise, make mobile devices become inherent to the human life. Mobile devices, such as laptops, tablets or smartphones, are used for different purposes. Lately, more and more frequently private devices are also used to perform the tasks in the workplace. This is due to the fact that the devices available to employees are more advanced and more efficient than those offered to them by the employer. The result of this situation is the creation of the concept of Bring Your Own Device (BYOD) model. This model is dynamically developed and is used in almost every field. Studies of this model are created by different companies, among others: Cisco Inc., IBM and Air Watch, providing solutions in the area of ICT.

Bring Your Own Device is a model that enables the user execution of the tasks, regardless of the place of dislocation and conditions of the network, using private devices [1,2]. Model BYOD provides the user access to the network using wireless (mobile) as well as wired technologies. This access is implemented using currently available the latest standards and techniques. The wireless support of user can be achieved in two ways. The first of these is available through WLAN network, using standard 802.11n and 802.11ac/d, through the access point in place of work. The second approach is access through the mobile network (e.g. 3G/4G, WiMAX, WiMAX-2, LTE, LTE-A, etc.). Wired access can be implemented using standard such as Fast Ethernet or Gigabit Ethernet. In addition to the undeniable advantages the model can also be characterized by some drawbacks. An example would be inadequate protection of mobile devices as well as the lack of security policy.

Appropriate configuration of IT network and the use of security equipment can significantly increase the level of network security and so called "sensitive data" that are stored in network data bases. An example solution may be the use of advanced router with firewall functionality (e.g. CISCA ASA) as well as configuring connections within the Virtual Private Network (VPN) with SSL (Secure Socket Layer) or IPsec (Internet Protocol Security) protocols. Another solution that can be considered is use a virtual router or BGP (Border Gateway Protocol) router with MPLS (Multiprotocol Label Switching) functionalities between border network devices.

In nowadays transportation systems that are widely using the IT networks there are often real-time needs for "fast" access (transmission) to the "large" amounts of data [3]. Using the latest

standards it is possible to transmit data at a throughput of up to 1Gbps of wired or wireless links.

As mentioned BYOD model is widely used and can be implemented in many different ways depending on demand. The BYOD model dynamically adapts the access to network resources and allocates the transfer rate over the time, e.g. for a service of file synchronization between the server and the client using the Work Folders. This is particularly important target service conditioning the functionality of the current work of the organization and supporting the process of archiving data repositories. An additional and essential advantage of BOYD model, distinguishing it from others is that the data are stored in a redundant manner.

In order to better analysis model can be divided into 3 main sections. The first concerns the data center, a place where data or applications from which the user can remotely use are stored. The second area is the area of the network, which carried out the functions of routing and access to services. This area includes network infrastructure, e.g. company, architecture of the Internet Service Provider (ISP) and network access infrastructure - wired or wireless. The third area is the user's device - a device specification, security methods, characteristics of network application, etc. Each of these areas can be analyzed from various perspectives - safety, performance, reliability or QoS. Later in the paper these areas were subjected to a comprehensive analysis, in particular in terms of reliability.

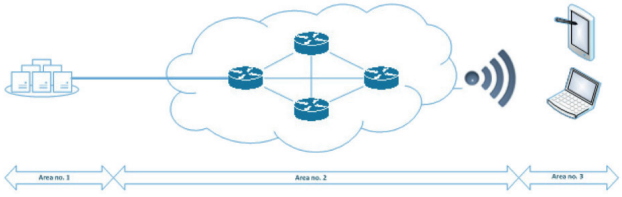

Fig. 1. General architecture of Bring Your Own Device model [own studies]

2. Architecture of research environment

The research environment model is shown in the Fig.2 [4]. Architecture of telecommunications network used during the research uses a commonly used network equipment, of which more important are: the Cisco 28xx and 29xx routers, 3COM family Baseline 22xx 24 port switches, Dynamode R-ADSL-411N wireless routers and two Hewlett-Packard family Proliant DL 360 5 generation servers with Windows server 2012 R2 with Active Directory, DNS and Work Folders service among others. Confidentiality of communication provides VPN tunnels that use SSLv3.0 protocol. This architecture provides the user wired and wireless access.

The Windows 8.1 operating system was installed on the client device. Wired communication network takes place through interface Gigabit Ethernet, and wireless communication interface using 802.11n. The IPv4 address plan and OSPF routing were used as well. The Work Folders service was the main service implemented in research network. This service allows synchronization files between the server and the users. The principle of operation is similar to applications such as OneDrive or Dropbox. The difference is that in the case Work Folder data is stored on the local server rather than on a server belonging to others. Authentication is based on account and domain password. Work Folders uses HTTPS and SSL certificate to ensure the confidentiality of data. The server administrator can delete the files in the user working directory and secure them in such a way as to minimize the risk of use of files in an unauthorized way [5, 6]. The research environment contains also the device which is generating background traffic within communication network (LANforge-FIRE Stateful Network Traffic Generator/LANforge ICE) and tools for valuation of traffic (*iperf*). Example settings are included in the table 1.

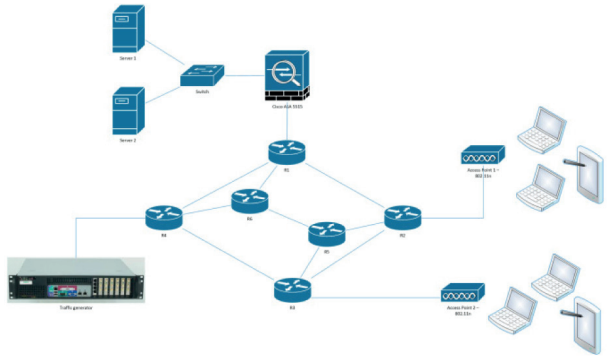

Fig.2. The research architecture of BYOD model [own studies]

Table 1. The parameters of client and server in iperf application [own studies]

Parameter	Client	Server
The *iperf* mode of operation	generator of demands	executor of the demands
Server address	192.168.1.2	-
Port	5001	5001
Parallel streams	1	-
Transmission time [sec]	300	-
Protocol	TCP	TCP

Allowing for the characteristics of the network environment outlined above, it is proposed to adopt the following requirements for testing environment:

1. Split the users into groups and assigning them permissions (Table 2).
2. Provision of:
   - access control to network resources, consisting of distinguishing and managing access rights for different groups,
   - identification and authentication of network users while using the services covered by the access control,
   - security of information upon which decisions are made about granting access rights to the resources and services performed in a network.
3. Events recording, this allows for creation of ongoing statistics of the network, through:

- the use of identification and authentication mechanisms,
- user activities associated with the use of access rights.

4. The elimination of possibility of changes associated with the logical network architecture, user rights and the classification of information.

Table 2. Users and services allocation [own studies]

Users \ Resources	E-mail	Printer	Data base	Educational resources	Server	HTTP server
Administrator	✓	✓	✓	✓	✓	✓
Employee	✓	✓	✓	✓	✓	✓
Other crew	✗	✗	✗	✓	✗	✓
Guest	✗	✗	✗	✗	✗	✓

The research architecture of BOYD model was used to conduct the following tests:

- Determine the service realization probability as a function of the number of running services. The number of services was increased from 1 to 100. To ensure a high level of credibility of the obtained results, each test was repeated 65 times. It was assumed that the time of service realization is equal to 60 seconds. Research was carried out for three standards of wireless network: 802.11g, 802.11n and 802.11ac.
- Bandwidth and network delay variation for the user who has access to the network using 802.11n was examined. Based on the results from a previous study, it was assumed that it will be performed for the network in which 10 services is running. A packet loss for the network was tested as well.

3. Analysis of results

As a result of studies performed and the results obtained a set of graphs showing the probability of services realization depending on the number of running services were made. The probability of services delivery is defined as the ratio of the number of provided services to the number of service needed. For such defined probability a subjectively acceptable and critical level of services realization was determined (Fig.3).

On the basis of analyzes and assessments it was determined that the acceptable level is equal to 0.8, while the critical level to 0.7. In practice, this means that failure of 1 from the 5 available services it is acceptable. As can be seen from the graph (Fig. 3), the best results were obtained for 802.11ac standard. Noticeable is also the fact that the probability of service realization in the case of standard 802.11ac started to decrease when running 35 services, while for 802.11g standard it was 8 services. This gives more than four time larger network reliability. This also means that the use of the latest standard of Wi-Fi, creates the possibility of use the network resources by four times number of users. Therefore it can be conclude that the introduction of the latest standards, and thus higher bandwidth, provides also greater network reliability and increases the probability of access to network resources. It is also worth noting that the probability of the service delivery for three studied standards does not fall below 0.2 (802.11g). This means that there is always a probability that the demand for the service will be executed even at a very busy network.

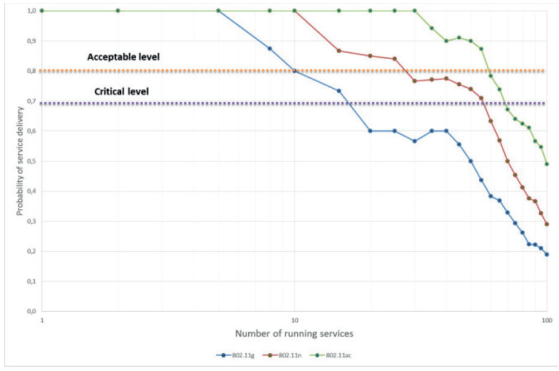

Fig.3. Probability of the service delivery depending on the number of running services [own studies]

Another study is related to examining network performance in terms of available bandwidth and delay variation. The study use the application *iperf* configured to work in research network of BOYD model. The obtained results are presented in the following figure (Fig.4).

As can be seen the average throughput for 802.11n reached 220 Mbps. This is a satisfactory result, in particular, that at the same time the system was used by 10 users. Jitter at an average value of 150 msec. is acceptable for the considered research network. The maximum values recorded in the range 500 - 1000 msec. are instantaneous values which are practically no noticeable for the user. Due to the fact that the services provided in the network are non-real time services, the jitter value is not so significant for the provided services.

A recent study included measurements of packet loss (Fig.5). Just like before *iperf* application was used. The observation period was set for 60 minutes in order to increase the reliability of the results. As can be seen, the average packet loss does not exceed 1%, which is a very satisfactory result.

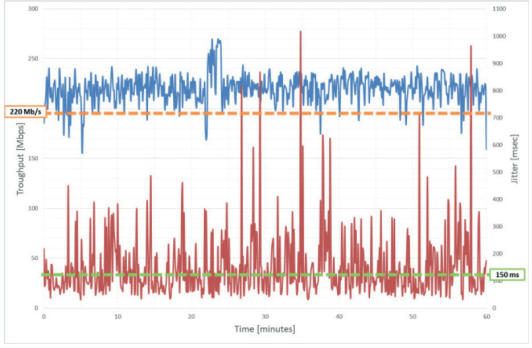

Fig.4. Throughput and delay variation as a function of time for 802.11n network [own studies]

However, within the first 10 minutes of the study, the results achieved significantly deviating from the expected packet loss level. The reason for this may be caused by the traffic associated with the establishing of connections and launching services. In the subsequent time intervals the losses normalized, which created the conditions for reliable data transmission.

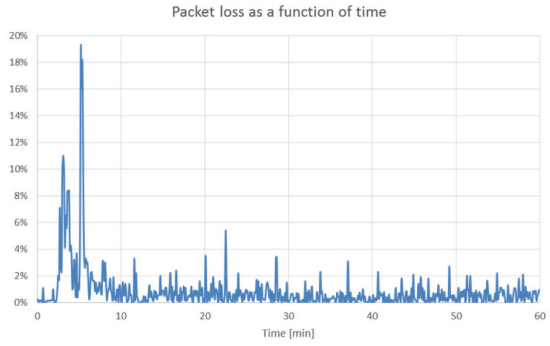

Fig.5. Packet loss as a function of time for 802.11n network [own studies]

5. Conclusion

The paper presents the test results of BYOD model reliability in terms of access to network resources using mobile standards. The test results show that, depending on the used standard of wireless network it is able to handle user with the probability depending on the number of simultaneously running network services. The user using the services of BYOD model has assured reliable access to network resources at a satisfactory level of bandwidth and latency variation, enabling continuous use of the services. Packet losses are so low, that they are not noticeable by the user.

The results indicate that the dynamically developing new techniques and technologies are solutions ensuring network reliability. The network architecture of BYOD model presented here is a very good example of this. Thanks to the described model, users can use private mobile devices, e.g. in the workplace and use them for the accomplishment of tasks.

It can be used in telematics environment for provision of mobile and reliable access to database system.

Bibliography

[1] LASKOWSKI D., STAPOR P.: Bring Your Own Device – model of safe and efficient access to the IT network. ICT engineering models - Volume 10. Politechnika Koszalińska, 2015.

[2] ANDERSON N.: Cisco Bring Your Own Device - The freedom of choice devices without exposing computer networks, Cisco Systems Inc., August 2013.

[3] KOWALSKI M., et al.: Exact and approximation methods for dependability assessment of tram systems with time window, European Journal of Operational Research, vol. 235, Issue: 3, pp. 671-686, 2014.

[4] LUBKOWSKI P., LASKOWSKI D.: Test of the multimedia services implementation in information and communication networks, Advances in Intelligent Systems and Computing, Vol. 286, Springer, pp. 325-332, Poland 2014.

[5] https://technet.microsoft.com/en-us/library/dn528861.aspx [date of access: 06.01.2016].

[6] https://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html [date of access: 06.01.2016].