Advances in Intelligent Systems and Computing 525

Ryszard S. Choraś *Editor*

Image Processing and Communications Challenges 8

8th International Conference, IP&C 2016
Bydgoszcz, Poland, September 2016
Proceedings

Springer

Advances in Intelligent Systems and Computing

Volume 525

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

More information about this series at http://www.springer.com/series/11156

Ryszard S. Choraś
Editor

Image Processing and Communications Challenges 8

8th International Conference, IP&C 2016 Bydgoszcz, Poland, September 2016 Proceedings

Springer

Editor
Ryszard S. Choraś
Institute of Telecommunications
and Computer Sciences
UTP University of Science and Technology
Bydgoszcz
Poland

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-319-47273-7 ISBN 978-3-319-47274-4 (eBook)
DOI 10.1007/978-3-319-47274-4

Library of Congress Control Number: 2016952533

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

We welcome you to the International Conference on Image Processing and Communications, IP&C 2016. The present volume contains the proceedings of the International Conference on Image Processing and Communications, IP&C 2016, held at Bydgoszcz, Poland, September 7–9, 2016.

IP&C 2016 was organized by the UTP University of Technology and Sciences and was hosted by the Institute of Telecommunications and Computer Sciences of the UTP University.

The IP&C 2016 brought together the researchers, developers, practitioners, and educators in the field of image processing and computer networks. IP&C has been a major forum for scholars and practitioners on the latest challenges and developments in IP&C.

The conference proceedings contain 37 papers which were selected through a strict review process, with an acceptance rate at 57 %. In all, 37 papers entered the review process and each was reviewed by two independent reviewers using the double-blind review method. There were also two invited talks by Massimo Ficco and by Damian Karwowski.

The presented papers cover all aspects of image processing (from topics concerning low-level to high-level image processing) and modern communications.

The organization of such an event is not possible without the effort and the enthusiasm of the people involved. The success of the conference would not be possible without the hard work of the local Organizing Committee.

We would like to thank all authors for the effort they put into their submissions.

Last but not least, we are grateful to Springer for publishing the IP&C 2016 proceedings in their Advances in Intelligent Systems and Computing series. Finally, we thank the Springer team for helping us in the final preparation of this AISC book.

I hope that all of the attendees found the conference informative and thought-provoking.

Ryszard S. Choraś
Conference Chair
IP&C 2016

Organization

Organization Committee

Conference Chair

Ryszard Tadeusiewicz	Poland
Ryszard S. Choraś	Poland

International Program Committee

Kevin W. Bowyer	USA
Dumitru Dan Burdescu	Romania
Christophe Charrier	France
Leszek Chmielewski	Poland
Michał Choraś	Poland
Andrzej Dąbrowski	Poland
Andrzej Dobrogowski	Poland
Marek Domański	Poland
Kalman Fazekas	Hungary
Ewa Grabska	Poland
Andrzej Kasiński	Poland
Andrzej Kasprzak	Poland
Marek Kurzyński	Poland
Witold Malina	Poland
Andrzej Materka	Poland
Wojciech Mokrzycki	Poland
Sławomir Nikiel	Poland
Zdzisław Papir	Poland
Jens M. Pedersen	Denmark

Jerzy Pejaś	Poland
Leszek Rutkowski	Poland
Khalid Saeed	Poland
Abdel-Badeeh M. Salem	Egypt

Organizing Committee

Sşawomir Bujnowski
Piotr Kiedrowski
Damian Ledziński
Zbigniew Lutowski
Adam Marchewka - Publication Chair
Beata Marciniak
Tomasz Marciniak
Ireneusz Olszewski
Karolina Skowron - Conference Secretary
Mścisław Śrutek
Łukasz Zabłudowski

Contents

Image Processing

20 Years of Progress in Video Compression – from MPEG-1 to MPEG-H HEVC. General View on the Path of Video Coding Development ... 3
Damian Karwowski, Tomasz Grajek, Krzysztof Klimaszewski, Olgierd Stankiewicz, Jakub Stankowski and Krzysztof Wegner

Automatic Tongue Recognition Based on Color and Textural Features ... 16
Ryszard S. Choraś

A First Attempt to Construct Effective Concept Drift Detector Ensembles ... 27
Michał Woźniak, Paweł Ksieniewicz, Andrzej Kasprzak, Karol Puchała and Przemysław Ryba

Quality Prediction of Compressed Images via Classification ... 35
Jevgenij Tichonov, Olga Kurasova and Ernestas Filatovas

Image Despeckling Using Non-local Means with Diffusion Tensor ... 43
Mariusz Nieniewski and Paweł Zajączkowski

Face Recognition with 3D Face Asymmetry ... 53
Janusz Bobulski

Best-Fit Segmentation Created Using Flood-Based Iterative Thinning ... 61
Adam Piórkowski

A Comparative Study of Image Enhancement Methods in Tree-Ring Analysis ... 69
Anna Fabijańska, Małgorzata Danek, Joanna Barniak and Adam Piórkowski

Key Frames Detection in Motion Capture Recordings Using Machine Learning Approaches 79
Tomasz Hachaj

Image Similarity in Gaussian Mixture Model Based Image Retrieval 87
Maria Luszczkiewicz-Piatek

A Flexible Software Architecture for a Network of Heterogeneous Smart Cameras 96
Dominik Pieczński, Marek Kraft and Michał Fularz

Quality Assessment of 3D Prints Based on Feature Similarity Metrics . . . 104
Krzysztof Okarma and Jarosław Fastowicz

Noise Objects Tracking Using Multiple Order Statistics and Spatio–Temporal Track–Before–Detect Algorithm 112
Przemysław Mazurek

Active Learning Algorithm Using the Discrimination Function of the Base Classifiers 120
Robert Burduk

The EOH Line Selector for Images with Downgraded Size for Mobile Robots Steering 128
Piotr Lech and Jarosław Fastowicz

Swipe-Like Text Entry by Head Movements and a Single Row Keyboard 136
Adam Nowosielski

The Feature Extraction From the Parameter Space 144
Adam Marchewka and Mirosław Miciak

Lossless Compression Method for Digital Terrain Model of Seabed Shape 154
Wojciech Maleika and Paweł Forczmański

On Combining Dual Morphological Binary Operators Using Median Set 163
Marcin Iwanowski

Subjective Image Quality Assessment Optimization 171
Anna Lewandowska (Tomaszewska)

Action Recognition Using Silhouette Sequences and Shape Descriptors 179
Katarzyna Gościewska and Dariusz Frejlichowski

Influence of Aggregating Window Size on Disparity Maps Obtained from Equal Baseline Multiple Camera Set (EBMCS) 187
Adam L. Kaczmarek

Combining Image Thresholding and Fast Marching for Nuclei Extraction in Microscopic Images 195
Marek Kowal, Przemysław Jacewicz and Józef Korbicz

Multiclass AdaBoost Classifier Parameter Adaptation for Pattern Recognition 203
Jerzy Dembski

Communications

CIPRNet Training Lecture: Hybrid Simulation of Distributed Large-Scale Critical Infrastructures 213
Massimo Ficco

Latin Multiplication in Telemetry Hot Potato Wireless Sensor Networks Analysis 215
Ireneusz Olszewski

Extreme Learning Machines for Web Layer Anomaly Detection 226
Rafał Kozik, Michał Choraś, Witold Hołubowicz and Rafał Renk

NEW QoS CONCEPT for Protecting Network Resources 234
Lukasz Apiecionek, Jacek M. Czerniak and Dawid Ewald

QoS Mechanism for Low Speed Radio Networks - Case Study 240
Robert Palka, Wojciech Makowski, Marcin Wozniak, Piotr Brazkiewicz, Krzysztof Wosinski, Pawel Baturo, Michal Terlecki and Tomasz Gromacki

IoT WiFi Home Network Stress Test 247
Piotr Lech and Przemysław Włodarski

Determining the Bit Error Rate for Redundant Transmission 255
Przemysław Włodarski and Piotr Lech

Power Consumption Optimization in Datacenters Using PSO Tuning in Fuzzy Rule-Based Systems 262
Rocio Perez de Prado, Jose Enrique Munoz-Exposito, Sebastian Garcia-Galan, C. Mora Garcia and Adam Marchewka

Considering Service Name Indication for Multi-tenancy Routing in Cloud Environments 271
Sebastian Łaskawiec and Michał Choraś

Author Index 279

NEW QoS CONCEPT for Protecting Network Resources

Lukasz Apiecionek(✉), Jacek M. Czerniak, and Dawid Ewald

Department of Computer Science, Institute of Technology,
Kazimierz Wielki University, ul. Chodkiewicza 30, 85 064 Bydgoszcz, Poland
lukasz.apiecionek@ukw.edu.pl

Abstract. Distributed Denial of Service attacks are one of the main problem of computer networks. There is no any method for protecting network user from source of the attack. Such attack could block network resources for many hours, while existing methods for protecting networks are using only firewalls and IDS/IPS mechanisms. Such solutions are not enough nowadays. This article presents the concept of Quality of Services methods and some well know network protocols for preparing network to fight with the DDoS attacks. This proposed concept lets the administrator to protect their network resources during the attack.

1 Introduction

Everybody knows that IT systems are nowadays omnipresent and users need a fast access to information from every part of the network. Nowadays Distributed Denial of Service attacks have become a problem as they cause network unavailability by blocking services via seizing system resources in computers in the network until they stop working. A user who has already started working in the system loses the connection and cannot even log out of the system, which has to do it for him after the connection timeout is reached or when a broken connection is detected. DDoS attacks are nowadays a serious obstacle for IT systems efficient functioning and they have to be eliminated. Common methods of fighting the DDoS attack problems [2–4,9,12] are usually limited to using the Intrusion Detection System and Intrusion Prevention System (IDS/IPS in short) solutions. Such systems are efficient provided that they have a description of well know attacks or some kind of Artificial Intelligence solution which could learn the actions in some specific scenarios of attack. Other solutions suggest using a firewall mounted on the network edge. However, this firewall will only block the incoming traffic on specific ports or IP address ranges, which is not sufficient. This paper presents a concept of the Quality of Services mechanisms which implemented in routers could eliminate the DDoS attacks.

The structure of this paper is as follows. Section 2 shortly describes the issue of the DDoS attacks and introduces the proposed method for fighting them. Section 3 provides a conclusion and discussion over the developed method.

R.S. Choraś (ed.), *Image Processing and Communications Challenges 8*,
Advances in Intelligent Systems and Computing 525, DOI 10.1007/978-3-319-47274-4_28

2 CONCEPT of QoS Method

2.1 Description of the DDoS Attacks

The DDoS attacks are widely described in the literature [4,5]. These attacks can be performed on various system resources: TCP/IP sockets [5,13] or DNS servers. Regardless of the method, the main principle is to simulate so many correct user connections that their number exceeds the actual system performance and drives it to abnormal operation. Papers [4,5,7–9] describe methods for dealing with the DDoS attacks by their global detection and the necessity of cooperation between network providers. The transmission of the attackers packets is done through the provider's network and if it cannot be blocked, it leads to data link saturation. Such saturation results in lack of connection to the server. The proposed solutions to prevent such situations are not specific and their implementation is associated with many problems. The most common concern is the limited performance of network devices. However, it is possible to limit the incoming traffic on a firewall and allow the servers to deal with the already established connection. This will let the users finish their work and the new users will be able to connect to the server. The QoS method implemented on routers are counting incoming traffic and decide which packet will be transferred to other network as first, and which will be the last. Such method are well known and implemented by network providers on their routers.

2.2 QoS Method Used on Routers

The QoS method implemented on routers are counting incoming traffic and decide which packet will be transferred to other network as first, and which will be the last. Such method are well known and implemented by network providers on their routers.

There were also some new QoS method ideas which could work on one routers and try to protect network resources locally [4]. But this solution will do not recognize the source of the attack and do not solve the problem. The hacker could still send their packet to the server.

Routers are exchanging lot of information between each other about reachability of the IP networks. This is done by routing protocols like OSPF, BGP or multicast routing protocols [10,11]. This mechanism could be used in new QoS method.

2.3 Proposition of the New QoS Method

Many QoS method are counting packets, but they do not know if the packet is a part of DDoS attack on some server. To fight with DDoS attack a new services for the network is required. Such services could use some well know mechanism like exchanging information between routers, SNMP protocols for getting another knowledge of traffic statistics. The proposition of the authors for new QoS Services which could works on routers has got a following steps:

- routers are collecting statistic of transferred traffic (1),
- statistics are divided into the counters of traffic to specific destination (2),
- routers are exchanging their statistic over SNMP (3),
- server which is an aim of the DDoS attack send a SNMP message to their router that it is under attack (4),
- routers are passing information between each other about the IP address of the aim of the attack (5),
- according to routers statistic they are looking for the source of the attack (6),
- when the sources of the attack are recognized, they are blocked (7).

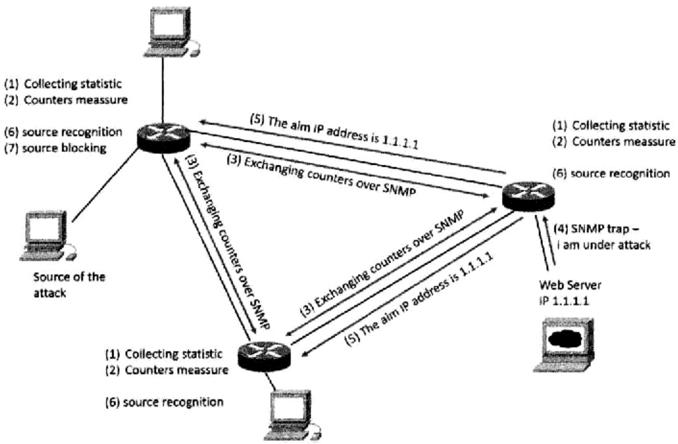

Fig. 1. QoS method concept in practice

This steps are presented on Fig. 1. This idea is very simple and could be implemented in easy way. The only thing to do is to implement it by network providers on their routers. All other proposed mechanism are well known.

2.4 Web Browsers Test

This method will not solve whole DDoS attack problems, but it will enable users to close their active connection when attack will start. Some test using Web browsers were made. Over 90 % of users used Internet Explorers (12 %), Mozilla Firefox (27 %) and Google Chrome (55 %) [1]. Using three most popular web browsers some test were made. Test procedure were to connect to web server which not exist and check how browser will send packets. Test condition:

- operating system Windows Vista,
- Internet Explorer version 9.0.8112.16421,
- Mozilla Firefox version 16.0.2,
- Google Chrome version 23.0.1271.64 m.

Table 1. Wireshark Web browsers connection test result

Number of packets	Delays before next packet is send from browsers [seconds]		
	Mozilla Firefox	Internet Explorer	Google Chrome
1	0	0	0
2	0,254	0,001	0,001
3	2,996	2,995	0,25
4	3,246	2,995	2,996
5	8,997	8,995	2,996
6	9,247	8,995	3,246
7	20,996	20,995	8,997
8	21,239	23,991	8,997
9	21,246	29,992	9,248
10	23,995		
11	24,235		
12	24,245		
13	29,998		
14	30,238		
15	30,248		
16	42,231		
17	45,23		
18	51,233		

Results of debug packets from Wireshark program are presented in Table 1. As it could be noticed, Mozilla Firefox browser tries to make a connection 18 times, while Google Chrome and Internet Explorer stops after 9 connection attempt.

Closing active connection and finishing work by users will be possible because of presented web pages browsers way of working. During browsers tests, authors recognize fact, that web page browsers made their work for user with some retransmission and they try to connect to web server more the once. Depending on browser which is chosen, there is nine chance to transfer appropriate data.

3 Conclusions

In this article a new concept of eliminating DDoS attacks was introduced. The methods suggested in the literature can block the access to the resources when the attack occurs, by using a firewall along with IDS/IPS mechanisms. During the time of the blockage no user from an external network can connect to the desired resources. The users who worked with the server lose their connection.

The method described in this article allows the network to find the sources of the attack. Then, such sources could be blocked and other users could still work with the server which was the aim of the attack. The part of this idea which has to be improved is a step 6 when routers are looking of the source of the attack. This is possible to do using for example fuzzy logic, which is described in literature [7]. Some other possibilities could be Kosinski's Fuzzy Numbers which are often better for some arithmetic reasons [6]. Besides the fact of the chosen algorithm for step 6, authors has a lot of idea which could be used [5,8]. This concept should be easy in implementation and during future test some algorithm will be implemented. Such idea should be considered to become some RFC standard. If there will be not any work on this topic, the DDoS attack will be huge problem in the future network.

References

1. http://www.w3schools.com/browsers/browsers_stats
2. Cert advisory ca-1996-21 tcp syn flooding and ip spoofing attacks, November 2000. http://www.cert.org/advisories/CA-1996-21.html
3. Cert advisory ca-1996-01 udp port denial-of-service attack, September 1997. http://www.cert.org/advisories/CA-1996-01.html
4. Apiecionek, L., Czerniak, J.M., Zarzycki, H.: Protection tool for distributed denial of services attack. In: Kozielski, S., Mrozek, D., Kasprowski, P., Małysiak-Mrozek, B., Kostrzewa, D. (eds.) BDAS 2014. CCIS, vol. 424, pp. 405–414. Springer, Heidelberg (2014). doi:10.1007/978-3-319-06932-6_39
5. Czerniak, J.M., Apiecionek, L., Zarzycki, H., Ewald, D.: Proposed CAEva simulation method for evacuation of people from a buildings on fire. In: Atanassov, K.T., et al. (eds.) Novel Developments in Uncertainty Representation and Processing. AISC, vol. 401, pp. 315–326. Springer, Heidelberg (2016). doi:10.1007/978-3-319-26211-6_27
6. Czerniak, J., Dobrosielski, W., Apiecionek, Ł., Ewald, D.: Representation of a trend in ofn during fuzzy observance of the water level from the crisis control center. In: Proceedings of the 2015 Federated Conference on Computer Science and Information Systems, Annals of Computer Science and Information Systems, pp. 443–447. IEEE (2015)
7. Dickerson, J.E., Juslin, J., Koukousoula, O., Dickerson, J.A.: Fuzzy intrusion detection. In: IFSA World Congress and 20th NAFIPS International Conference, vol. 3, pp. 1506–1510. IEEE (2001)
8. Kozik, R., Choraś, M., Renk, R., Hołubowicz, W.: Semi-unsupervised machine learning for anomaly detection in HTTP traffic. In: Burduk, R., Jackowski, K., Kurzyński, M., Woźniak, M., Żołnierek, A. (eds.) CORES 2015. AISC, vol. 403, pp. 767–775. Springer, Heidelberg (2016). doi:10.1007/978-3-319-26227-7_72
9. Moor, D., Shannon, C., Brown, D.J., Voelker, G.M., Savage, S.: Inferring internet denial-of-service activity. ACM Trans. Comput. Syst. (TOCS) **24**(2), 115–139 (2006)
10. Piechowiak, M., Zwierzykowski, P.: The evaluation of multicast routing algorithms with delay constraints in mesh networks. In: 8th IEEE, IET International Symposium on Communication Systems, Networks and Digital Signal Processing CSNSDP, Pozna'n, Poland (2012)

11. Piechowiak, M., Zwierzykowski, P.: The evaluation of unconstrained multicast routing algorithms in ad-hoc networks. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2012. CCIS, vol. 291, pp. 344–351. Springer, Heidelberg (2012). doi:10.1007/978-3-642-31217-5_36
12. Rocky, K., Chang, C.: Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE Commun. Mag. **40**, 42–51 (2002)
13. Schuba, C.L., Krsul, I., Huhn, M.G., Spafford, E.H., Sundaram, A.: Analysis of a denial of service attack on tcp. Computer Science Technical Reports. Paper 1327 (1996). http://docs.lib.purdue.edu/cstech/1327

QoS Mechanism for Low Speed Radio Networks - Case Study

Robert Palka(✉), Wojciech Makowski, Marcin Wozniak, Piotr Brazkiewicz, Krzysztof Wosinski, Pawel Baturo, Michal Terlecki, and Tomasz Gromacki

Teldat Sp.z o.o.sp.k ul., Cicha 19-27, Bydgoszcz, Poland
rpalka@teldat.com.pl

Abstract. A quick access to information is very important nowadays. Many systems exchange their data via radio links. These radio links are characterized by low bitrates and high bit error rate. In such situation, standard data exchange mechanisms cannot be used. In order to ensure the high quality for data transmission, other mechanisms have to be implemented. Such mechanism should be flexible and should adapt to the prevailing conditions of transmission. They should also allow to achieve optimum usage of the transmission medium. One of such mechanisms is the Battlefield Replication Mechanism. It has been adapted to work on mentioned radio links. This article presents the mechanisms for ensuring the delivery of the data used in the BRM - implemented and tested in practice.

Keywords: QoS · Radio replication mechanism

1 Instroduction

Data communications systems that transmit data through low bit rates links are a special case. Such links are mainly used by the public services: the police, military, medical and crisis staff [7]. In such systems, data rate transfer can be decreased even to 1200 bps. Sending IP packets which size is 1400 Bytes can last over 9 s and depends on the protocol which is used. The time required for different size of packets on mentioned link is presented in Table 1.

At these speeds, transmission packet queues may fill up relatively quickly, depending on the amount of data to be transmitted in a particular application. With an average packet size of 768 bytes, the system has 5.1 s to analyze the packets in the queue and decide which packet should be transmitted in the first place. This gives an opportunity to optimize the queues of data packets.

If the transmission is done by radio links, the radio waves reach all receivers which are in the range of the transmitter. Such transmission usually works in broadcast mode. This gives an opportunity for optimization. If there is a need to send the same data packet to all recipients, there is no need to transfer them separately and simply only one single packet could be transmitted to all of the radios. Moreover, when the transmission is made only to selected recipients, this

R.S. Choraś (ed.), *Image Processing and Communications Challenges 8*,
Advances in Intelligent Systems and Computing 525, DOI 10.1007/978-3-319-47274-4_29

Table 1. Time required for packet transferred over a link with data rate 1200 bps

IP Packet size [Bytes]	Transmission time [s]
51	0,4
255	1,7
510	3,4
768	5,1
1024	6,8
1400	9

can be done by indicating the recipients via the message in the radio network, but the transmission also is working in broadcast mode.

Data exchange in radio networks with low data rates is often characterized by a very high bit error rate. This is a challenge for the systems. One of the existing solutions which solve this problem is the Battlefield Replication Mechanism - BRM. The following sections of this article contains a description of this protocol with a mechanism which guarantees data packets delivery to the right destination.

2 A System with the BRM - Case Study

2.1 BRM Description

Battlefield Replication Mechanism is a data transmission protocol developed by engineers from TELDAT company [8]. BRM is using UDP (User Datagram Protocol), which is presented in Fig. 1.

As it is known, UDP uses a set of IP protocols and is a connectionless protocol which is not giving any guarantee that data packets will be delivered to the destination. The benefits of this protocol are: simplicity, lack of additional tasks (i.e. tracing session, establishing the connections) and the baud rate.

BRM protocol eliminates the disadvantages of using UDP, adds many new opportunities which improve its performance and ensures high security (encryption) of the transmission. BRM enables the exchange of operational data between databases (both version of the C2IEDM and JC3IEDM model can be used). BRM from its design phase was adapted to make the best and most effective work on low pass and unstable radio links, taking into account the current security requirements in ICT systems [1,2,4,5]. This protocol sends the minimum information required, ensures efficient bandwidth usage, adapting transmission parameters to the constantly changing environment. In order to ensure a high level of security of the transmitted information during various missions, the entire transmission is encrypted, and the data are further grouped, filtered and compressed (these treatments can increase the efficiency of transmission).

Each data transmission is encrypted using a symmetric key generated for this transmission. This key is exchanged (using the method of secure key exchange)

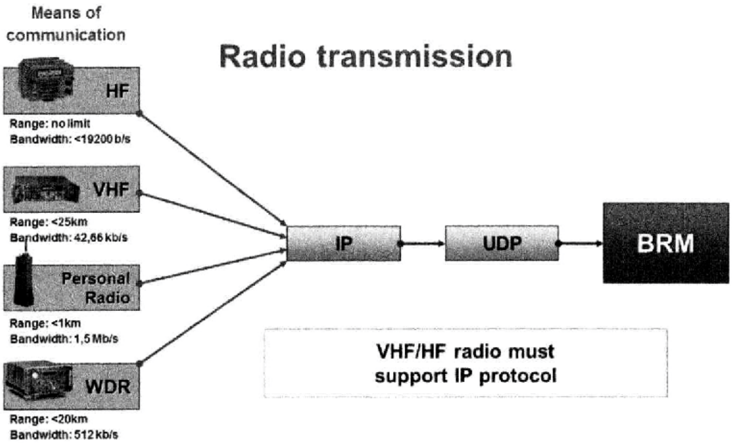

Fig. 1. Radio transmission with BRM protocol

between the points of replication during the connection phase, and is known only to the parties directly enumerating the data. Of course there is the ability to dynamically change it during runtime.

The most important features of the BRM protocol:

- uses a well-known and standardized UDP protocol;
- provides the delivery confirmation data;
- ensures high security - data encryption;
- operates on a low-throughput radio links;
- ensures an efficient use of the transmission links - additional compression;
- adatps the transmission depending on the transmission condition;
- provides a secure exchange of the encryption key;
- enables an automatic renewal of the encryption key;
- has a build-in mechanism for eliminating errors - integrity of the operational data;
- enables the replication of the data between C2IEDM and JC3IEDM databases of MIP program (sending the minimum required amount of data without loss of information).

2.2 Mechanisms Implemented in BRM

Sending information through the BRM mechanism consists of several steps, giving the assurance of delivering data (through the retry message). Data exchange mechanism guarantees delivering the data to the point of replication to which the connection exists. A confirmation mechanism is shown in Fig. 2. In this scenario, it is assumed that the first mobile vehicle is going one way, and at this time the BRM sends the position to the second mobile vehicle in the following manner:

- position is transmitted as a data packet called light, which means that it consists of minimal amount of data for passing information about the position and movement,
- if the packet will not reach the destination (second vehicle) in the configured amount of time (according to data errors or some other problems in the transmission) which in the presented situation lasts 15 s and is called AwaitingTimeOut, there will be a retransmission started till the situation when vehicle 1 will get an acknowledge from the second vehicle.

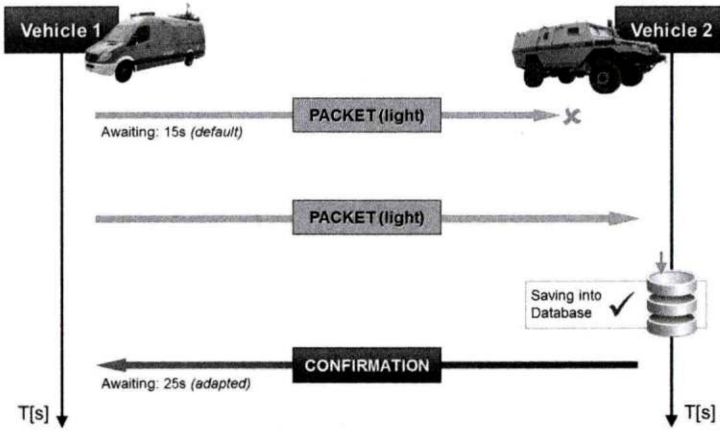

Fig. 2. Data confirmation mechanism

BRM is also equipped with a mechanism of missing data analysis and their replenishment. Figure 3 illustrates the operation of the mentioned mechanism. In the same situation as mentioned previously:

- the first vehicle sends a packet in light version(which consist of minimum information about position and movement) to the second vehicle over the radio link;
- second vehicle tries to save the data into the database;
- if the procedure of saving data fails (the second vehicle will not have the information about the first vehicle), there will be a special packet generated, which informs the first vehicle that the procedure of saving data failed;
- if the first vehicle gets the information about problems in saving data, it will generate new packets which consist of all of the required information for saving data into the database.

The mechanism of data exchange can operate with any radio station: from HF via VHF, Personal Radio to Wide Digital Radio. It should be noted that the radio used to transmit data, has to support IP and UDP transmission, which the BRM protocol uses.

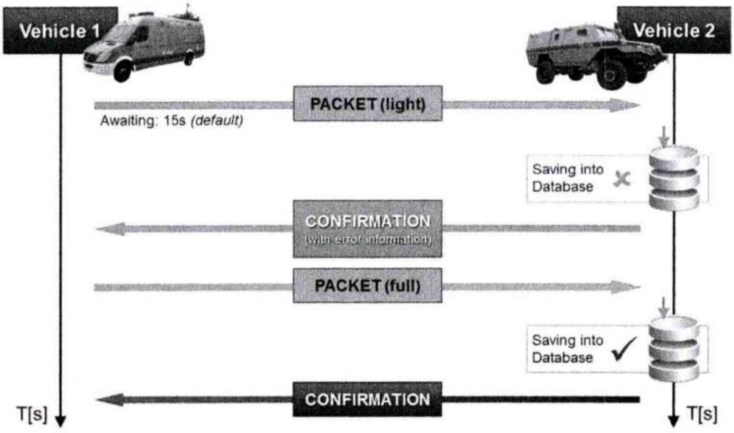

Fig. 3. Data analysis mechanism in BRM

The format of BRM package is shown in Fig. 4. In order to optimize the performance, the BRM protocol sends the data as tasks and identifies the appropriate task by the header added in the package.

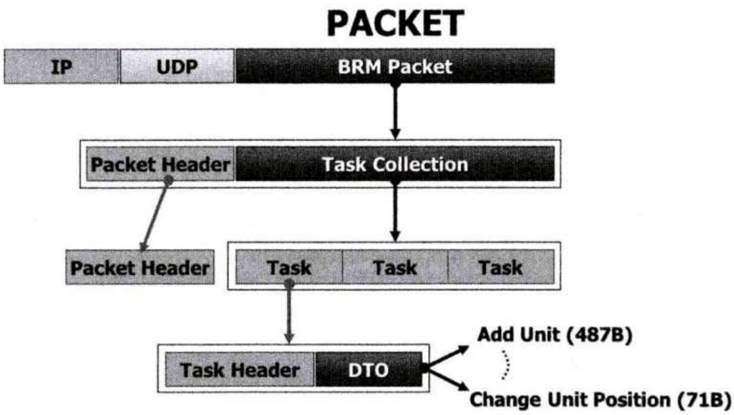

Fig. 4. BRM package structure

In accordance with the principle of this operation, the data can be transferred in full, standard or limited version. The types of packages are shown in Fig. 5.

If the average packet size is about 136 bytes and the transmission speed is at 1200 bps, the packet transmission time is 906 ms. The transmission system has got almost one second in average for the optimization of the queues.

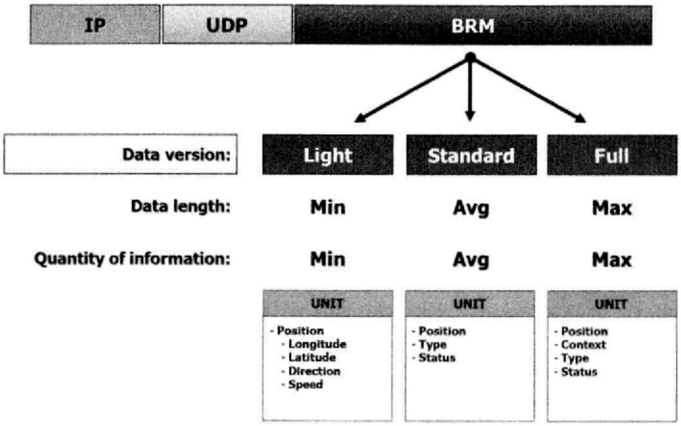

Fig. 5. Types of BRM packages

2.3 Queues Mechanism in BRM

The BRM protocol uses queue optimization mechanisms, based on the experience gained in the study of routing protocols [9]. The first step of the optimization is dropping packets consisting the same information. This could be made because packet flow to the queue could be faster than the transmission from the queue over the radio link. The transmission of the packet which consist the same data is unnecessary.

When the radio works in broadcast mode, all of the receivers get the same data. There is no requirement for sending packets in unicast mode if the packets are consisting the same data. In such situation the queue is optimized and data are exchanged by only one packet which consists the same information. This mechanism is changing unicast transmission to multicast mode and works also in some specific situations in broadcast mode.

The above mentioned mechanisms are used for queues optimization which lets us save data throughput and is separated from the application layer in that fact, so there are no requirements for any additional task to do in the application. The above mentioned mechanism could be also used in any type of transmission medium.

3 Conclusions

This article presents the practical implementation of the transmission mechanism of data within links with low data rates. This mechanism is using optimization procedures for the queues. The devices have got a lot of time for queues optimization in the network with low data rates links. When they poses some free computing power it gives very good results, while simple packet dropping can cause increasing of data flow and finally blocking the network. BRM mechanism is widely used in data transmission for the military systems [6] and also could be successfully used for communication with aircrafts [3].

References

1. Apiecionek, Ł., Czerniak, J.M., Zarzycki, H.: Protection tool for distributed denial of services attack. In: Kozielski, S., Mrozek, D., Kasprowski, P., Małysiak-Mrozek, B., Kostrzewa, D. (eds.) BDAS 2014. CCIS, vol. 424, pp. 405–414. Springer, Heidelberg (2014). doi:10.1007/978-3-319-06932-6_39
2. Apiecionek, Ł., Makowski, W.: Firewall rule with token bucket as a DDoS protection tool. In: 2015 IEEE 13th International Scientific Conference on Informatics, pp. 32–35. IEEE (2015)
3. Apiecionek, Ł., Makowski, W., Biernat, D., Łukasik, M.: Practical implementation of AI for military airplane battlefield support system. In: 2015 8th International Conference on Human System Interaction (HSI), pp. 249–253. IEEE (2015)
4. Apiecionek, Ł., Motylewski, R., Stosik, P.: Bezpieczenstwo transmisji danych w systemach monitorowania wyposażenia straży pożarnej, problemy monitoringu eksploatacji sprzetu i wyposażenia straży pożarnej. CNBOP-PIB, pp. 41–48 (Jozefow 2015). doi:10.17381/2015.2
5. Apiecionek, L., Romantowski, M.: Security solution for cloud computing (2014)
6. Kruszyński, H.: Możliwości mobilne systemu JASMIN. Wsparcie teleinformatyczne dowodztw w dzialaniach wojsk ladowych, pp. 119–129
7. Kruszyński, H., Kosowski, T.Z.: Zarzadzanie wsparciem wspolpracy cywilno-wojskowej w dzialaniach kryzysowych, public managmenet 2013, wyzwania i dylematy zarzadzania organizacjami publicznymi 1, pp. 521–542 (2013)
8. Muchewicz, K., Sierakowski, L.: Sposoby wymiany danych operacyjnych w systemie jasmin, materiały konferencyjne xvii automatyzacja dowodzenia (2009)
9. Piechowiak, M., Zwierzykowski, P., Hanczewski, S.: Performance analysis of multicast heuristic algorithms. In: Third International Working Conference on Performance Modelling and Evaluation of Heterogeneous Networks, p. 41. Networks UK Publishers (2005)

Advances in Intelligent Systems and Computing 525

Ryszard S. Choraś *Editor*

Image Processing and Communications Challenges 8

8th International Conference, IP&C 2016 Bydgoszcz, Poland, September 2016 Proceedings

This book collects a series of research papers in the area of Image Processing and Communications which not only introduce a summary of current technology but also give an outlook of potential feature problems in this area. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in image processing and communications. The book is divided into two parts and presents the proceedings of the 8th International Image Processing and Communications Conference (IP&C 2016) held in Bydgoszcz, Poland September 7–9 2016. Part I deals with image processing. A comprehensive survey of different methods of image processing, computer vision is also presented. Part II deals with the telecommunications networks and computer networks. Applications in these areas are considered.

Engineering
ISSN 2194-5357
ISBN 978-3-319-47273-7
9 783319 472737
▸ springer.com