Proceedings of the 17th International Conference on Research in Telecommunication Technologies 2015

9th – 11th September 2015

Ostravice, Czech republic

Editors: Marek Dvorsky, Martin Mikulec
Proceedings of the 17th International Conference on Research in Telecommunication Technologies 2015

© Marek Dvorsky, and Martin Mikulec
Preface

This year, the RTT conference is organized by the Department of Telecommunications by Faculty of Electrical Engineering and Computer Science, VSB-TU Ostrava.

The conference will held in Wellness Hotel Sepetna near Beskydy mountains.

The conference RTT is an occasions to share new information, recently advances and knowledge in the field of telecommunications.

The proceedings of the conference will be published at the conference website

We wish you to have a great time during the RTT 2015 conference.

On behalf of the organizing crew
Marek Dvorsky and Martin Mikulec

Committees

RTT 2015 CHAIRMEN
Marek Dvorský VSB–TUO Ostrava, Czech Rep
Miroslav Vozňák VSB–TUO Ostrava, Czech Rep

RTT 2015 PUBLICITY CHAIR
Pavel Bezpalec, CVUT, Czech Republic

RTT 2015 PROGRAMME COMMITTEE
Ivan Baroňák, STUBA Bratislava, Slovakia
Milan Dado (University of Žilina, Slovakia)
Lubomír Doboš (Technical University of Košice, Slovakia)
Jaromír Hrad , CVUT, Czech Republic
Erik Chromý (Slovak University of Technology in Bratislava, Slovakia)
Jozef Juhař (Technical University of Košice, Slovakia)
Viktor Klekovkin (Izhevsk State Technical University, Russian Federation)
Jaroslav Koton (Brno University of Technology, Czech Republic)
Jiří Mišurec (Brno University of Technology, Czech Republic)
Pavel Lafata , CVUT, Czech Republic
Dušan Levický (Technical University of Košice, Slovakia)
Dušan Maga , CVUT, Czech Republic
Beata Mikovičová (Institut supérieur d’électronique de Paris, France)

Yuri R. Nikitin (Izhevsk State Technical University, Russian Federation)
Bohumil Pšenička (National Autonomous University of Mexico, Mexico)
Rastislav Róka (Slovak University of Technology in Bratislava, Slovakia)
Santiago Silvestre (Technical University of Catalonia, Spain)
Jan Skapa (Technical University of Ostrava, Czech Republic)
Zdeněk Směkal (Brno University of Technology, Czech Republic)
Boris Šimák , CVUT, Czech Republic
Sergej A. Trefilov (Izhevsk State Technical University, Russian Federation)
Yuri V. Turygin (Izhevsk State Technical University, Russian Federation)
Adrian Ulvan (Lampung University, Indonesia)
Martin Vacullík (University of Žilina, Slovakia)
Jiří Vodrážka , CVUT, Czech Republic
Kamil Vrba (Brno University of Technology, Czech Republic)
Andrzej Wac-Włodarczyk (Lublin University of Technology, Poland)
Tatjana Welzer Družovec (University of Maribor, Slovenia)
Vladimír Weser (University of Žilina, Slovakia)
Tomáš Zeman , CVUT, Czech Republic
Index

Energy Consumption of Wireless Sensor Network .................................................................5
Amr Awamri, Dusan Maga and Tarek Nahdi

Quality Management Of Large Pedagogical Projects.........................................................9
Tomas Zeman and Jaromir Hrad

Dependable Ict Systems ......................................................................................................13
Stefania Sobotova

A New Design Of The Detail Description For Objects Recognition In The Key Frame Using Ontology ..........15
Martina Radilova, Patrik Kamencay, Robert Hudec, Miroslav Benco, Slavomir Matuska, Jan Hlubik

Model For Detecting Wild Animals Based On A Photogrammetry .......................................19
Andrej Satnik, Jozef Talapka, Jan Hlubik, Patrik Kamencay, Robert Hudec, Martina Radilova, Miroslav Benco

Electronically Controlled RF Switch For UWB Application ..................................................25
Stanislav Slovak, Pavol Galajda

Optimalizace Dynamického Rozsahu Vstupního Signálu Pásmové Propusti S Obvody Cci+ ...............29
Zdenek Tesar and Iva Petrikova

Comparison Of BB84 And B92 Protocol In Terms Of The Length Of The Final Key .......................35
Miralem Mehic

A Novel Social Based Opportunistic Routing in MANET ...........................................................40
Martin Matis, Lubomir Dobos and Jan Papaj
Energy Consumption of Wireless Sensor Network

Amr Awamri¹, Dusan Maga² and Tarek Nahdi²

¹ Benha University, Faculty of Electrical Engineering, Department of Telecommunication, Fareed Nada Street, Benha, Qalubiya Governorate, 13511, Arab Republic of Egypt, amr.awamri@bhit.bu.edu.eg
² Czech Technical University in Prague, Faculty of Electrical Engineering, Department of Telecommunication Engineering, Technicka 2, 166 27, Prague, Czech Republic: dusan.maga@fel.cvut.cz, tareknah@fel.cvut.cz

Abstract — Sensor networks are formed from a collection of sensing nodes which communicate with one another, typically through wireless channels, in order to collect spatially distributed data about their environment. Sensor nodes are operating on battery power with a limited energy resources. The energy consumption is one of the most important issues and the designing of the energy consumption protocol is very critical for prolonging the lifetime. This paper introduces the LEACH routing protocol in Homogenous & Heterogeneous system supported by simulation and analysis of the results. From the brief analysis of the simulation we have come to the conclusion that LEACH Heterogeneous System provides a good performance in energy consumption and increasing the level in lifetime of the wireless sensor networks than LEACH Homogeneous System.

Keywords — Wireless Sensor Networks; Network Lifetime; Energy Consumption; LEACH protocol.

I. INTRODUCTION

With the popularity of laptops, cell phones, PDAs, GPS devices, RFID, and intelligent electronics in the post-PC era, computing devices have become cheaper, more mobile, more distributed, and more pervasive in daily life. It is now possible to construct, from commercial off-the-shelf (COTS) components, a wallet size embedded system with the equivalent capability of a 90s PC. Such embedded systems can be supported with scaled down Windows or Linux operating systems. From this perspective, the emergence of wireless sensor networks (WSNs) is essentially the latest trend of Moore's Law toward the miniaturization and ubiquity of computing devices.

Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components. These components are integrated on a single or multiple boards, and packaged in few cubic inches. With state-of-the-art, low-power circuit and networking technologies, a sensor node powered by 2 AA batteries can last for up to three years with a 1% low duty cycle working mode. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. WSNs can be deployed on a global scale for environmental monitoring and habitat study, over a battle field for military surveillance and reconnaissance, in emergent environments for search and rescue, in factories for condition based maintenance, in buildings for infrastructure health monitoring, in homes to realize smart homes, or even in bodies for patient monitoring [1], [2], [3], [7] and [8].

After the initial deployment (typically ad hoc), sensor nodes are responsible for self-organizing an appropriate network infrastructure, often with multi-hop connections between sensor nodes. The onboard sensors then start collecting acoustic, seismic, infrared or magnetic information about the environment, using either continuous or event driven working modes. Location and positioning information can also be obtained through the global positioning system (GPS) or local positioning algorithms. This information can be gathered from across the network and appropriately processed to construct a global view of the monitoring phenomena or objects. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission.

Since the nodes in a WSN are battery powered, minimizing the energy consumption of the WSN is key to ensuring that WSN can operate for the longest period of time possible. Much research has been done to develop different types of routing protocols and examine their effect on energy efficiency [5], [6], [10].

II. LOW-ENERGY ADAPTIVE CLUSTERING HIERARCHY (LEACH)

LEACH is a single-hop routing protocol that divides the WSN into clusters and assigns a leader to each cluster (cluster heads). The sensor nodes within a cluster regulate their energy used to transmit data and only use as much energy as is required to reach the leader of the cluster. The cluster heads (CH) then aggregates the data and expends a larger amount of energy to transmit the data directly to the sink. To increase total network lifetime, LEACH periodically rotates the leader responsibility to other nodes. LEACH researchers found that the optimal number of nodes to make CH is 5 percent of the total number of nodes in the WSN. Cluster heads (CH) have many tasks: firstly they are responsible of collecting data from the member nodes; secondly, they transmit the aggregated data to the base station; and thirdly they are responsible for creating a time division multiplexed access (TDMA) schedule which specifies the time slots allocated for each member of the cluster.

Initially, when clusters are being created, each node decides whether or not to become a cluster-head for the current round. This decision is based on the suggested percentage of cluster heads for the network (determined a priori) and the number of times the node has been a cluster-head so far. This decision is
made by the node $n$ choosing a random number between 0 and 1. If the number is less than a threshold $T(n)$, the node becomes a cluster-head for the current round. The threshold is set as:

$$T(n) = \begin{cases} 
1 - p \left( r \bmod \left( \frac{1}{p} \right) \right), & n \in G, \\
0, & n \notin G.
\end{cases}$$  \(1\)

Where $P = \text{the desired percentage of cluster heads (e.g., } P = 0.05\), $r = \text{the current round, and } G$ is the set of nodes that have not been cluster-heads in the last $1/P$ rounds. Using this threshold, each node will be a cluster-head at some point within $1/P$ rounds. During round 0 ($r = 0$), each node has a probability $P$ of becoming a cluster-head. The nodes that are cluster-heads in round 0 cannot be cluster-heads for the next $1/P$ rounds. Thus the probability that the remaining nodes are cluster-heads must be increased, since there are fewer nodes that are eligible to become cluster-heads. After $1/P - 1$ rounds, $T=1$ for any nodes that have not yet been cluster-heads, and after $1/P$ rounds, all nodes are once again eligible to become cluster-heads.

The cluster-head node receives all the messages for nodes that would like to be included in the cluster. Based on the number of nodes in the cluster, the cluster head node creates a TDMA (time division multiplexed access) schedule telling each node when it can transmit. This schedule is broadcast back to the nodes in the cluster.

Once the clusters are created and the TDMA schedule is fixed, data transmission can begin. Assuming nodes always have data to send, they send it during their allocated transmission time to the cluster head. This transmission uses a minimal amount of energy (chosen based on the received strength of the cluster-head advertisement). The radio of each non-cluster head node can be turned off until the node’s allocated transmission time, thus minimizing energy dissipation in these nodes. The cluster-head node must keep its receiver on to receive all the data from the nodes in the cluster. When all the data has been received, the cluster head node performs signal processing functions to compress the data into a single signal. Fig.1 shows the structure of an evolutionary algorithm in LEACH protocol [13].

The simulations of LEACH protocol mainly performed with assumption that all sensor of networks are charged homogeneously. There is also another type of simulation. In this simulation the sensor of networks are charged heterogeneously where some advanced nodes with different energy capabilities [6]. Usually CHs die faster than other nodes because CHs need more power capabilities to aggregate data to base station [10]. Thus it’s important to study CH death rate and power consumption, over all network life time can be increased if we increase CH life time.

III. CALCULATION OF ENERGY CONSUMPTION

For the calculation of the energy consumption a communication model is used (fig. 2) [13]. In this model the transmitter dissipates energy to run the radio electronics and the power amplifier, and the receiver dissipates energy to run the radio electronics [13], [14]. Using the radio model an estimation of energy consumed in transmission or reception by a sensor node at each cycle is given.

In our work, we assume a simple model where the radio dissipates $E_{\text{elec}} = 50 \text{nJ/bit}$ to run the transmitter or receiver circuitry and $E_{\text{amp}} = 100 \text{pJ/bit/m}^2$ for the transmit amplifier to achieve an acceptable $E_b / N_o$. These parameters are slightly better than the current state of-the-art in radio design. We also assume an $r^2$ energy loss due to channel transmission. Thus, to transmit a k-bit message a distance d using our radio model, the radio expends:

$$E_{\text{Tx}}(k,d) = E_{\text{Tx-elec}}(k) + E_{\text{Tx-amp}}(k,d)$$

And to receive this message, the radio expends:

$$E_{\text{Rx}}(k) = E_{\text{Rx-elec}}(k)$$

IV. ANALYSIS OF RESULTS FOR LEACH PROTOCOL IN HOMOGENEOUS & HETEROGENEOUS SYSTEM

In this paper, an analysis of the power consumption for CH’s in case of LEACH protocol is made. The analysis take into consideration the percentage of heterogeneous nodes, the analysis has been performed for homogeneous (0% heterogeneous nodes), 10%, 20% heterogeneous nodes.

During the study of LEACH protocol important parameters are taken into consideration the round number vs the number of Dead Cluster Heads and round number vs the average energy of CH.

With the nodes being deployed, some assumptions were made concerning the node features and these are as follows:

- Nodes always have to send data.
- All nodes start with the same initial energy.
- Clusters and nodes are static.
- Nodes are assumed to have a limited transmission range after which another equation for energy dissipation is used.

```
Initial network

Divide into cluster

Selection of CH

Calculation of energy consumption of every node

Threshold

No

Yes

Output

Figure 1. Steps in LEACH
```
A. LEACH Protocol in Homogeneous System

Fig. 2 shows the results of setup stage in LEACH protocol, CH has been randomly selected. The simulations were configured with a network size of 100 x 100 meters and with 200 nodes randomly distributed; the base stations were located at position (150, 50). All of the sensor nodes periodically sensed the environment and transmitted the data to the cluster heads. Every result shown is an average of 50 experiments. O indicates Normal nodes and dark O indicates CHs. X indicates BS.

B. LEACH Protocol in Heterogeneous System

A heterogeneous network is a network where part of the sensor nodes namely advanced nodes, are equipped with more initial energy than the rest of the normal nodes and these advanced nodes with extra energy can improve the lifetime of the network [10]. The same procedure as in the normal LEACH protocol is followed i.e., the formation of the clusters is same in this heterogeneous system and also the cluster head selection by comparing the residual energy of the individual in every round. The structure of the LEACH Heterogeneous system for wireless sensor networks is shown in Fig. 3; Here 200 nodes are distributed in 100x100 meters area. BS is located at the (150, 50). ‘O’ indicates Normal nodes and ‘red o’ indicates Normal nodes CHs. ‘+’ symbol indicates Advance Node and ‘red +’ indicates Advance Node CHs. X indicates BS.

The results of the simulation are presented on Fig. 4 and 5. Fig. 4 and 5 describe the comparison between the Leach Homogeneous and Leach-Heterogeneous System in terms of number of dead nodes and average energy of each Node. Simulation results using MATLAB shows that the LEACH heterogeneous system significantly reduces energy consumption and increases the total lifetime of the wireless sensor network.

C. CONCLUSION

It can be seen that nodes remain alive for a longer time (rounds) in Leach-Heterogeneous system than LEACH - Homogeneous system.

In this paper, we evaluated LEACH routing protocol for Wireless Sensor Networks. The main reason of the evaluation of LEACH protocol is the study of the energy consumption due to the limited amount of energy in the sensor nodes. From the brief analysis of the simulation we have come to the conclusion that LEACH Heterogeneous System provides a good performance in energy consumption and increasing the level in...
lifetime of the wireless sensor networks than LEACH Homogeneous System.

The analysis of the energy consumption of wireless sensor network shows the importance of powering nodes from non-renewable energy sources, such as batteries and fuel cells. This method of powering has improved over the years, this improvement is fairly gradual compared with other areas of electronics and cannot satisfy all of the simultaneous demands for long life, low volume, low weight and limited environmental impact. Therefore Wireless sensor networks can be powered by environmentally scavenged energy (Energy Harvesting). There are a great many sources of energy and conversion devices which have been considered for energy harvesting. Energy harvesting device can provide the level of the power required by the sensor node in Wireless sensor network.

ACKNOWLEDGMENT

This work has been supported by an Institutional support for development and research.

REFERENCES

QUALITY MANAGEMENT OF LARGE PEDAGOGICAL PROJECTS

Tomáš ZEMAN1, Jaromír HRAD1

1Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague
Technická 2, Praha 6, Czech Republic
zeman@fel.cvut.cz, hrad@fel.cvut.cz

DOI: 10.15598/aeee.v13ix.xxxxx

Abstract. The paper deals with procedures necessary to maintain quality standards during the simultaneous development of numerous learning objects with the involvement of different authors. We have to take into account formal rules (structure, extent, text formatting), but also the content quality (correctness, consistence, modern concept). If we should adhere to these quality standards, it is necessary to develop quite complex system of quality management based on a well-defined workflow and clear methodology.

Keywords

Education, quality management, learning content development, international cooperation.

1. Introduction

A large number of learning objects is being successively developed within the project TechPedia under the framework of Erasmus+ program. The authors are affiliated with different institution in several European countries. The outputs will include:

1. 100 learning modules (20 topics, each of them available in 5 languages),
2. 200 worksheets,
3. 2000 explanations of key terms (in a form of encyclopaedia),
4. 3000 entries of professional terminology in a translation dictionary,
5. 100 tests for classes,
6. 100 tests for students’ competition.

These learning objects are being developed in electronic form in several formats that allow practical use on different platforms (e-book readers, LMS, printed, and of course on computers, tablets or smartphones).

With respect to the large number of learning objects, authors and target platforms, there have to be implemented unified regulations, which is the only way to achieve high quality of the outputs.

2. Standard development procedures

2.1. Learning content development

1) Goals

During the development process we work with the following elements: authors of the content (often lecturers) on one side, and electronic development tools with their functionalities on the other one. We also must not forget about the support team (graphics designers, programmers, reviewers, etc.).

The goal of the learning content development is to harmonize all elements so that the result has unified nature, regardless of the different authors and environments of origin.

2) Methodology

The basic methodology that we decided for – after many (mostly negative) experiences – consists in detailed specification of clear and unambiguous procedure for the development of learning materials.

3) Basic conditions

We adhered to the following basic conditions when formulating the rules for the development of electronic courses:

- Modular concept – the individual topics (learning modules) may be suitably composed into comprehensive courses; the modules consist of individual screens;
• One screen roughly corresponds to a half of a standard A4 page, one module typically contains 40 explanatory screens (text, pictures) and a test,
• The explanation is accompanied by encyclopaedic explanations of many professional terms, worksheets and key vocabulary for the translation dictionary;
• The individual authors have different capabilities and experiences in the areas of ICT and electronic support of education – therefore the authors should not care about the final form of the courses; the authoring process must be easy and straightforward, with clearly defined rules;
• Supervision and unified conception of all modules in all stages of the authoring process have to be guaranteed;
• The particular procedures of the authoring process have to be standardized;
• The authoring is performed in several languages, with English version as the primary/reference one.

2.2. Authoring of texts

Authoring of texts is the key to the success of the entire project. Practical experience says that most authors do not obey the given formal rules. However, only strict adherence to the rules (i.e. using the styles, keeping the maximum extent of texts, their proper structure, etc.) allows step-by-step development of complex courses with contributions from different authors, providing unified outputs from heterogeneous primary materials.

The authoring is based on a text processor and its functions. The authors use a special document template that contains approximately 40 defined styles, each of them representing an element with a specific meaning in the final learning material. Authors can use the styles e.g. to insert pictures in a unified way (specifying a link to an external file) into any place in the text, not worrying about their placement in the final version of the learning material.

Authors fill some basic metadata (names of the authors, annotation, objectives, keywords, etc.) in the introductory section of every module. Then during the writing they define – by applying the appropriate styles – what the function of the respective text part is (screen beginning, headline, numbering, bullets, important text, definition, note, typical block, etc.).

Authors are – to certain extent – involved also in the development of graphics, usually collaborating (as the originators of the fundamental idea) with a graphic designer (who gives the idea its visible representation, respecting the given graphic standards manual). Alternatively, the authors can develop the graphics for their learning materials personally, provided that they are able to strictly comply with the given standards.

3. Quality management

The highest possible quality of the content is the primary requirement for any learning material. We have developed procedures that we apply to all learning objects so that we can achieve high quality of the outputs, but also to conclude all project-related activities in a realistic time horizon given by the approved schedule.

3.1. Module outline

There are two main stages of the development process. The first one consists in specification of module outline, as illustrated in Fig. 1.

The quality management is based on several aspects, one of them being the real importance of the topic for the prospective users, i.e. the teachers as well as their students. [1] So, the authors should firstly make a list of topics they are able to elaborate; then the chief quality manager (see below) selects out of this quite long list (about 100 items) 50 topics that are considered to be the most current. This selection is offered to teachers who are going to use the developed learning materials in the future. It is important to ask a representative sample of teachers from different types of schools dealing with different areas of technology in different countries. The final selection of 20 specific topics is based on the results of an online survey.

![Fig. 1: Development of an outline for a module](image)

When the list of topics is finalized, the authors of the respective modules propose short outlines (10 lines each), and the teachers are requested to comment them again. Then authors consider the feedback and decide, which suggestions should be reflected in the (almost) final version of the outlines – as the final decision is the responsibility of the chief quality manager. At this moment we have defined specific authors and final outline for each considered topic.

3.2. Module content development

The content of a module (see Fig. 2) is strictly based on the approved outline (see above). The author firstly develops the content of the learning module itself, but working also on the other types of supplementary
learning objects (worksheets, tests, explanatory dictionary, etc.) at the same time, so that they together form a compact unit. Graphic designer works simultaneously with the author, developing graphics for the module (and for its accompanying learning objects) according to the author’s instructions.

As soon as the author and the graphic designer finish this stage, the intermediate results are passed to a reviewer. The reviewer must be independent from the authoring team – definitely from another institution, preferably also from a different country. The review has two parts:

- Evaluation – using an electronic evaluation form, the basic parameters of the learning materials are briefly and clearly rated in the following categories: relevant expression, professional level, language level, graphics level, overall evaluation, brief summarizing comments, and conclusion/recommendation;
- Suggestions – using reviews in the original document, the reviewer proposes to the author what modifications, corrections, amendments etc. should be made.

![Fig. 2: Development of a module](Image)

Both results of the review are then returned to the author who is expected to reflect the reviewer’s remarks and suggestions in the new version. After making the necessary modifications, the author submits the learning objects to a quality manager.

The quality manager has to decide whether the reflections of the reviewer’s recommendations is satisfactory; if so, the materials are passed for technical processing; if not, the author is requested to make the desired changes to the content.

However, in order to proceed with the next stage, the evaluation from the reviewer has to be positive. There are given some minimum standards that must be kept – if not, the entire material must be returned to the author to be thoroughly revised. Quality manager is the person responsible for this procedure.

Technical processing begins with formal check of proper formatting. If the format is not correctly applied, it has to be fixed in order to enable automated further processing of the material.

When the formatting is correct, the authoring in the reference language (i.e. English) is finished. The subsequent processing is divided into two independent branches. The first one consists in localization: the learning objects (including graphics etc.) are translated from the reference language into the national ones (returning to the stages marked 5, 6 and 7 in Fig. 2). The translation is followed by reviewing and other procedures (stages marked 8, 9 and 10 in Fig. 2), as described above.

The second branch is a technical one, consisting in automated conversion of the completed source learning objects into the finalized electronic form, which may be:

- suitable for e-book readers (various formats),
- LMS-compatible – transparent SCORM package,
- printable format (e.g. PDF).

This is not the end of the entire process yet. Now we have all the learning objects prepared in electronic form, ready for pilot testing. The pilot testing involves dozens of schools, dozens of teachers and hundreds of students using the developed learning objects during six months.

The final stage of the pilot testing includes evaluation of the developed learning materials by their users, i.e. teachers and students. Quality managers should summarize the collected feedback into an evaluation document for the content authors and translators. Such document is the basis for one more modification, resulting, at last, in the final version of all learning objects, which can be included in standard study plans.

### 4. Quality managers

Besides reviewers and users, quality managers are another group that can influence the quality of the developed learning objects. The roles of quality managers are defined for the respective tasks and responsibilities (of course, one person may have several roles).

Quality managers guarantee that if the quality control processes described above (based on reviewers, users, evaluation and feedback) fail for any reason, the learning objects will be returned to the proper stage of the developed process. Another responsibility of quality managers consists in supervision over the approved time schedule, including negotiations concerning its necessary modifications, as in some specific cases it may be more appropriate to deliver the outputs later but in substantially higher quality.

Quality managers are permanently in contact with content authors (not only during the review and evaluation), which helps to identify various types of problems in the early stages of the development process.
While the reviewers focus only on some specific topics of their interest, quality managers have to supervise all topics (and modules), and therefore they can prevent, for example, duplication of explanations in the learning objects or other types of inconsistencies.

5. Conclusion

The system described in this paper is based on many years of experience with development of heterogeneous as well as homogeneous learning objects. It involves three stages of reviewing performed by:

- users,
- professionals,
- quality managers.

Each of these three stages focuses on different aspects of quality to be guaranteed for the final output.

Besides that, there is available a set of sophisticated software tools that support the management of learning objects development with the desired quality.

At present time (summer 2015) a large-scale development of learning objects within the TechPedia project is in progress. The system of quality management described in this paper is being applied. We assume that during the coming year – when the project shifts into its next phase – we will get enough relevant data showing to what extent the introduced quality management system will have been able to fulfil our expectations.

Acknowledgements

This paper has originated thanks to the grant support obtained from the Erasmus+ program within the project No. 2014-1-CZ01-KA202-002074 “European Virtual Learning Platform for Electrical and Information Engineering – TechPedia”.

References


About Authors

Tomáš ZEMAN was born in Praha, Czech Republic. He received his M.Sc. from the Czech Technical University in Prague in 1989; he received his PhD from the Czech Technical University in Prague in 2001. His research interests include impulse noise, multimodal systems, data transmission and e-learning.

Jaromír HRAD was born in Přerov, Czech Republic. He received his M.Sc. from the Czech Technical University in Prague in 1994; he received his PhD from the Czech Technical University in Prague in 2003. His research interests include data transmission, power line communication and innovations in pedagogy.
DEPENDABLE ICT SYSTEMS

Stefania SOBOTOVA

1Department of Telecommunication Engineering, Faculty of Electrical Engineering, Czech Technical University in PragueTechnická 2, Praha 6, Czech Republic

misagste@fel.cvut.cz

Abstract. Current development of Information and Communication Technologies (ICT) systems is too demanding, because in the new service or system design is necessary to meet in addition real needs of users and technical requirements. From a technical and economical point of view the system’s elements must be interoperable, user friendly, affordable, scalable and portable by design in the long term and managed to fast technical progress and development. The most common problems are isolated development of not only ICT systems, advanced technologies, duplicated development and ending in pilot stage. The main point of service design is to select the right procedure which ensures: interoperability with other systems, create or keep standardization rules (in defining standards, which will result into a reduction of prices and thus facilitate mass deployment of new service), integration technologies, extending functionality of “common used systems and equipments” and include in the context of users' routines. For the system or service to be successfully deployed they must meet several criteria - in one word service must be dependable.

Keywords

Reliability, dependability, service design, SLA, ICT system.

1. Introduction

The solution in the creation of the dependable system is handling ontology, which means to define concepts and relations between them. The second point is to describe the various processes and use ontology to create interoperable links between individual processes that the system has performed and described them as interlinked business processes. These processes should be simulated and validated. If the simulation results are not acceptable, it is necessary to go back at the beginning and examine what the problem is. Measured values of all attributes in the simulation represents how dependable the system is designed. Generally, this key step in system design is underestimated, which later causes that the system does not meet all the defined requirements and finally leads into much more expensive development.

2. Dependable system

ICT system dependability is the quality of the delivered service such that reliance can justifiably be placed on this service. The service delivered by a system is its behavior as it is perceived by another special system(s) interacting with the considered system: its user(s) [1].

Measuring dependability to be defined of several attributes: availability, reliability, safety, confidentiality, integrity, maintainability. This attributes are defined within Laprie’s Dependability Tree [2].

Fig. 1: Dependency Tree

Relationships between attributes result from definitions and the literature is quite divergent. Thus, we consider the following characteristics of individual parameters dependability.

Availability is the ability of the system to in fact deliver its service and it is related with SLA (Service Level Agreement) [2][3].

Reliability is defined as the probability by which a component, device, system, or process will perform its intended function without failure for a given time when operated correctly in a specified environment. Reliability deals with reducing the frequency of failures over a time interval and it measures of the probability for failure-free operation during a given interval, i.e., so it measures the success for a failure free operation:

\[ R(t) = \exp\left(\frac{-t}{MTBF}\right) = \exp(-\lambda t) \]  \hspace{1cm} (1)

where \( \lambda \) is constant failure rate and MTBF is mean time
between failure. MTBF measures the time between system failures and is easier to understand than a probability number. For exponentially distributed failure modes, MTBF is a basic figure-of-merit for reliability (failure rate \( \lambda \), is the reciprocal of MTBF) [3][6].

Safety denotes the system’s ability to fail in such a way that catastrophic consequences are avoided. Thus, safety is reliability with respect to catastrophic failures [3].

Confidentiality means a security principle that requires that the data should be only accessed by authorized person [5]. Confidentiality is the ability of the computing system to prevent disclosure of information for unauthorized parties [3].

Integrity - a security principle that ensures data and configuration items are modified only by authorized personnel and activities. Integrity considers all possible causes options of modification, including software and hardware failure, environmental events, and human intervention [5]. Integrity is the ability of the computer system to prevent unauthorized withholding, modification or deletion [3].

Maintainability is expressed as a measure of how quickly and effectively an IT service or other configuration item can be restored to normal working after a failure. Maintainability is often measured and reported as MTRS. Maintainability is also used in the context of software or IT service development to mean ability to be changed or repaired easily [5]. Maintainability attribute denotes the system’s ability to undergo modifications and repairs [3].

3. Problems and solutions

Develop dependable system represents several problems coping. Today's ICT is a pile of different software for which it is possible to ensure perfection without error. Makes designing error-free systems an illusion if we consider the interaction of hardware and software and the fact that the most current ICT systems are distributed. Ever decreasing feature size of hardware components increases the chances possibility of errors caused by hardware. Communication is more space over error-prone wireless links. ICT systems not only used by professionals; in practice, this means that errors may be caused by the human operator or system user.

As the solution for ICT systems guarantees the reliability of the systems modeling and analysis as part of the process of designing information and communication technologies. When assessing the reliability we need to focus on ICT system as a whole which represents both hardware and software, because it has a lot of weight. An indispensable part of the solution is the integration of methods and techniques for the verification of the model (model checking) and classical techniques for assessment of the dependability (stochastic processes).

4. Conclusion

This article provides some kind of basic procedure for design of any ICT system, which is expected to have a certain reliability. The actual processes that are the basis for development ICT services carry out simulation in the simulation tools, debug and validated. Based on the above classification of the main attributes of dependable system and the dependencies between them it is possible to verify that the proposed system satisfies the requirements of the system, and possibly to be further improved.

5. Acknowledgements

This work was supported by the Grant Agency of the Czech Technical University in Prague; grant number SGS OHK3-027/15.

References


A NEW DESIGN OF THE DETAIL DESCRIPTION FOR OBJECTS RECOGNITION IN THE KEY FRAME USING ONTOLOGY

Martina RADILIOVA¹, Patrik KAMENCAY¹, Robert HUDEC¹, Miroslav BENCO¹, Slavomir MATUSKA¹, Jan HLUBIK¹

¹Department of Telecommunications and Multimedia, Faculty of Electrical Engineering, University of Zilina, Univerzitna 8215/1 010 26 Zilina, Slovakia

martina.radilova@fel.uniza.sk

Abstract. In this article, we deal about the research on question: “How to obtain detail information’s about recognition and classification objects in key frame of video?”. Detailed description can be achieved based on ontology. For this paper the ontology for animals is designed. The ontology is created in three basic steps. Firstly, the ontology editor is chosen. Secondly, schema is designed. Third, based on schema, the animal ontology is created in ontology editor. Couple of editor types are introduced and finally our software selection for creation animal ontology is described. Each ontology is named by a Uniform Resource Identifier (URI). This ontology has a hierarchical structure of classes, subclasses and relations between classes. The animal’s kingdom was divided into sub-realms (unicellular and multicellular organisms), phyla, classes, orders, families, genera, species and subspecies. The hierarchical division of animals was realized by internet encyclopedia called “BIOWEB”.

Keywords

Ontology, Uniform Resource Identifier, hierarchical structure.

1. Introduction

Currently, the detection of objects in static or dynamic images improved as well as access to information about the objects in the image.

This value is continually growing. Along with the increased volume of available data from the image there are increased demands on the ease of searching, processing and evaluating the information. A possible solution is a semantic description that enriches the description of the objects in the image about metadata. Appropriate means of assigning semantic description of objects are ontologies. The aim is to create a semantic description of the machine-readable ontology and assign a description of the object in the image [4].

This article is the extension of article called “Semantic Description of Static Images based on Support Vector Machine classification”[5]. The outline of the paper is as follows. In the next section, description based on ontology is introduced. Ontology design and ontology testing is described in section 3 and section 4. Finally the brief summary is discussed in section 5.

2. Ontology

In the past, it was the term used exclusively by philosophers. However, today finds application in the field of informatics and knowledge engineering. Ontology is seen as a data model that represents the terms and various entities and relations between them. We know describe the individual ontology situations and real relations, such as family relations, division of animals and so on. Large ontologies maximize the number of occurring information and relations between various concepts. to comprehensively describe and model real world situations. This allows us to avoid more sensuality and more significance of terms. A simplified outline of ontology is shown in Fig. 1. This figure shows the animal kingdom and their interrelationships [1].

All information, terms, ideas, properties and different relationships, which includes ontology can be classified by tagging information. We can designate the documents or parts of documents keywords. Using this machine will be able to distinguish semantically related or different expressions. Open up the possibility of the automatic data processing machine.
3. Ontology Design

The practical part consists of two basic parts:

- selection ontology editor - using this editor we will implement the ontology of animals,
- design, implementation and creation of ontologies.

3.1. Selection of the Ontology Editor

Protégé is a most widely used free, open-source ontology editor designed and developed at Stanford University in collaboration with the University of Manchester.

Protégé offers a friendly user interface. Enable the creation of classes and their hierarchical structure. We enter the restrictions classes, determine the different classes, and add classes individually. Particularly define the properties that assign classes using restrictions. Protégé can graphically display ontology created using a card "Jambalaya Tab". There is also an alternative view using the card OWL VizTab.

Ontology editor Protégé also, besides creating ontologies allows checking logic errors by using the tool "Reasoner". Protégé has no dedicated ontology language and therefore we can save the created ontology in several languages. There is a possibility of opening and editing previously created ontologies. Protégé application is a useful helper in creating OWL ontologies.

3.2. Ontology Design and Specific Ontology Design of Animals

The proposal itself was inspired ontology free encyclopedia "Bioweb". We have created a classes animal, we defined them a place in the hierarchical tree division animals and we assign them basic characteristics.

Editor Protégé creates OWL ontology, which consists of the following basic components [2, 3]:

1) OWL Classes

The basis of the each ontology is classes and their hierarchical structure. Each class to another class or group classes in object-oriented environment is tied. The final class is on top of the class hierarchy, which in Protégé predefined class owl: Thing. Class "owl: Thing" is fixed and can not be deleted. Come out from it all created class. Protégé can express the different classes using the tool "Disjoint classes". Different classes are identified and selected to the list. Classes difference is expressed using a list of classes (Disjoint classes). Axiom is generated, which affect other classes. By using the logical operator "or" we can say that a given class is a subclass of only one class and by using the logical operator "and" again we determine that a class is a subclass of several classes simultaneously.

The first class of animals was created as follows:

- switch on card „Classes”,
- click on the button add subclass,
- selected class is called.

Class of animals, what is a tree has subclasses respectively subkingdom "Unicellular" and "Multicellular". Every subkingdom is further divided into phylums, classes, ords, etc. The class hierarchy is also called taxonomy. After completing a complete class hierarchy division animals was created class of properties that is related to the class for a class of animals. Class Properties include a plurality of individually which detailed description on individual animal species. This means that it does not subclasses, but has only individual.

2) Properties

Properties represent relationships between classes. There are three main types of properties:

- object properties – class joining with another class,
- properties of the data type – class joining with the data type of integer literals,
- annotations – class joining with a data type of string literals. Is used for add information, metadata (data that describes other data).

The majority of properties that we defined and used in this ontology will object properties. For the creation and application properties in Protégé, it is necessary to switch on the card "Properties" and create a new property. We will name property using the dialog box that appears at the top of the Properties card. In the Protégé, we can enter properties and also their sub-properties so that it is possible to create a hierarchy of properties.

In the ontology we defined 22 object and data properties "má_počet_nôh" and "má_počet_buniek".
Each property was named. According to the hierarchical structure of "regnum, subregnum, phylum, subphylum, class, subclass, superorder, ordo, suborder, family, genus, species" we first created a few object properties "má_podrišu" and inverse property "patrí_do_ríše" which we have defined the properties.

Then we created all the 11 pairs of object properties "má_podrišu" - "patrí_do_ríše", "má_kmeň" - "patrí_do_podrišu", "má_podkmeň" - "is_to_kmeňa", "má_telo" - "patrí_do_podkmeňa", "má_druh" - "patrí_do_rod".

Finally, we defined the animal through the data properties "má_počet_nôh". We have applied it to different types of animals using restrictions and the dialog box "Create restriction" as cardinality. Object class of ontologies have been assigned property "má_počet_nôh" the number data type integer.

**Fig. 3:** Properties determining the relations between classes, card "jambalaya".

Using the same procedure we describe the all classes in ontologies division animals. Each class except for the species and regnum "animal" has a two restrictions composed of the restriction property of the type "má_" and "patrí_do_" and restrictions "someValuesFrom".

**Fig. 4:** Data property.

### 3) Individuals

In the next step we create individually. Protégé allows defining individual and describing properties of classes. Aid individually, we describe individual objects (classes) ontologies, such as the environment in which they live, what they eat, whether they are protected by law, etc. We used limitation "HasValue" for this. Procedure of creation individually:

- Creation of Class "Properties".
- Selection the card for the creation of "Individuals".
- Clik on button "Create instances" was created by individuals who were unambiguously defined "Asserted".
- Give a name for a new individual.

We can now describe the class of animals after creating individual instances.

### 4) Datatype

Datatype associated classes respectively objects with data type value (literal). Using data properties we express the data limitations for the selected class. Domains, differences and range can be defined. Its can be defined after assigned the object properties. In our ontology, we selected data type string and a string of characters. However, it is necessary to define data types. Their presence is required in difficult extensive ontology.

### 5) Limitations

The limits are divided into:

- Limitations using properties

At this limit, we proceed by switching to the card 'Classes'. Furthermore, we which class we want to describe by restriction. In the central part of Protégé environment, there is "Asserted Conditions" which offers the possibility to create limitations, restrictions. Finally, press the button "Create Restriction" a window opens in which for selected class choose the property in the "Restricted Property", select the restriction using "Restriction" and in the window "Filter" write respectively we choose a class that is associated with the selected class currently selected restriction property and restrictions.

Using the same procedure we describe the all classes in ontologies division animals. Each class except for the species and regnum "animal" has a two restrictions composed of the restriction property of the type "má_" and "patrí_do_" and restrictions "someValuesFrom".

- Limitations using the cardinality

The procedure is almost the same as with limitations using properties. It differs only by making how restriction the property we choose a data property. We use restriction "cardinality" and assigns the selected class in the window "Filter" number data type integer. In addition to data property "má_počet_nôh", we used the property "má_počet_buniek", which we created restrictions for subregnum "unicellular".

- Individuals limitations

We realize their restriction "HasValue", designated by the symbol 3. Suppose we want to determine the coverage of the animal's anatomy in ontology. For example, I want to say that the kind of "Vlk obyčajný" has a body covered with hair and we have already created individually in class "Properties" including individually 'hair'. So we can use limitation the "HasValue" along with this individually for the specification, whereby has an animal covered body. To generate limitations using instances:

- 1. We chose card "Properties" and we have created a new object property and named it "má_telo_pokrytý".
- 2. We switch on the "Classes" and we have chosen class "Vlk obyčajný".
3. Press a button to create restriction "Create Restriction" and we have chosen "ma_telo_pokryte" as restriction property.

4. We have specified restriction "HasValue" with the symbol ∈.

5. We chose "hair" into the field "Filter" as an Individual to complete restrictions. The value can be written individually or embeds the using the "Insert individual".

6. Finally, we pressed the "Enter", close the dialog box and created a limitation.

By such a procedure, we have created additional properties on the card "Properties", which by combination with the appropriate instances describe the individual species in the ontology created. Each animal species can be described unlimited number of individual's limitations. Individual's limitations are metadata that help us to characterize semantically animals OWL ontology.

![Hierachy structure classes and single ontologies](image.png)

**Fig. 6:** Hierarchy structure classes and individual of ontologies.

**4. Ontology testing**

Ontology division animals underwent test ontologies. Simulation result was successful without reporting errors in the code, warning messages, or conflicting definitions and relationships.

We created classes of animals, defined them places in hierarchical tree division animals, which were realized under the web encyclopedia BIOWEB. Through this division animals managed to assign them semantic description. For example, species "Loxodonta africana" belongs into a specific order, classes, subphylum, phylum and regnum. The next section is assigned classes of properties that describe their interrelationships. We then created individually, which characterize the species of animals. In the last step was an applied class’s limitation (restrictions), which completes the overall relational image of each class ontology.

Ontology has been deployed also the system SIIT (Semantic Inclusion of Image and Textual segments). This method is for creating short web abstract based on an analysis of static images [5]. And thanks ontology was improved creation abstracts from 62.92% to 79.59%.

The future we will expand about to other sorts, properties and other modality, which will be required for the development of software.

**Acknowledgements**

The work presented in the paper was supported by the University Science Park of the University of Zilina (ITMS: 26220220184) supported by the Research &Development Operational Program funded by the European Regional Development Fund.

**References**


MODEL FOR DETECTING WILD ANIMALS BASED ON A PHOTOGRAMMETRY

Andrej SATNIK¹, Jozef TALAPKA¹, Jan HLUBIK², Patrik KAMENCAY¹, Robert HUDEC¹, Martina RADILOVA¹, Miroslav BENCO¹

¹Department of Telecommunications and Multimedia, Faculty of Electrical Engineering, University of Zilina, Univerzitna 8215/1, Zilina, Slovakia

Abstract. In this article, the problematic about detecting of wild animals based on a photogrammetry is presented. Recently, a lot of pressure is exposed to environmental protection by government and also independent organisations. Many funds are given to nature protection and species which are in danger in their natural habitats mainly because of the road construction. First, the photos of animal in graphic environment Cinema 4D were created. Next, these photos into three different photogrammetry software solutions (Agisoft PhotoScan, Autodesk Memento and 3DF Zephyr) were inserted. Finally, the comparisons between these three photogrammetry software solutions are presented. The best method for the reconstruction of 3D model will be chosen. The obtained experimental results demonstrate that the best results were obtained by Autodesk Memento.

Keywords

3D reconstruction, eco-duct, photogrammetry, 3D model, wild animals.

1. Introduction

In the past, the eco-ducts were built without any knowledge, where the animal’s paths were. These eco-ducts influence badly the environment or the potential of migration is insufficient. The solution is the planning of the migration corridors for the eco-ducts already being built. Migration corridor is the 50 meter long line of trees, which will linked to the traditional animal’s path. The animals will be easily guided to the nearest eco-duct. The tree planting is cheaper than bridge construction. Migration corridors should be building alongside the new communications as well as alongside the existing one.

Nowadays, the data about wild animals is being used for planning the eco-ducts. This data is from the standard sources (direct observation of animals, tracking of animals, etc.). These sources are not efficient for long time period and are very time consuming. The developed integrated system the data about wild animals in exact area will provide. The solution for the confident data source is that the camera system will be used to supervise the area and evaluate the data. The system for recognition from video-recordings should recognize quantity, distance and direction of migrating animals. Based on this data the planning of the eco-ducts should be more efficient. For testing the algorithm, the test video recordings of moving animals are needed. It is very difficult to make these recordings because we are focused on wild animals. That’s reason why the 3D models of animals for the test video-recordings are needed. The 3D scene like this is fully under control. We can change the amount of animals, the location, the speed of migration, etc.

2. Selection of suitable object for reconstruction

For 3D reconstruction, the model of deer was chosen, because it contains a simple body surface and complicated shape of antlers. It is likely that most mistakes will be entitled to the antlers. Deer as an object of reconstruction is useful because it does not contain long fur which will reduce the computation time.

2.1. Creation of reference model

To compare reconstructed models, a creation of reference model is needed. As a reference model, free high resolution 3D model of deer with detailed texture map was chosen [1]. However this model is symmetrical,
mesh and texture was modified.

For simplest adjustment of the origin, scale and coordinate system for calculating of the Hausdorff distance, the base board with grayscale chessboard pattern was used. To avoid the error of calculating the position of cameras in the 3D reconstruction, the base board was rotated by 45 degrees (Fig. 1). Thus we avoid the image mirroring between left and right image. The reference 3D model was saved in the Wavefront (.obj) format with texture file (4096x4096 pixel (.png)).

![Fig. 1: Asymmetric reference model.](image1)

### 2.2. Camera images rendering

The reference model was edited and rendered in the environment Cinema 4D R15. Reference model was placed in the geometrical center of the sphere. Camera was moving around the upper hemisphere in five different levels ranging from 0 to 360 degrees incremented by 10. It can be seen in the Fig. 2. It ensure constant camera distance from the scanned object.

![Fig. 2: Camera position in five levels.](image2)

During the scanning process, all parameters of cameras were constant. The use of virtual camera ensures perfectly focused images. Recorded images were rendered with 4096x3112 pixels resolution in 24-bit bit depth. In this way, the database of 180 images was created.

### 3. 3D model reconstruction by stereo geometry

A classical problem of stereo computer vision based on a stereo geometry is the extraction of 3D information from stereo views of a scene. To solve this problem, knowledge of view properties and feature point between views is needed. However, finding these points is notoriously hard to do for natural scenes. The fundamental idea behind stereo computer vision is the difference in position of a unique 3D point in two different images. As the object moves closer to the cameras, the relative position of object will change, and the positions in each image will move away from each other. In this way, it is possible to calculate the distance of an object, by calculating its relative positioning in the two images. This distance between the same objects in two images is known as disparity. Disparity map computation is one of the key problems in 3D computer vision. A large number of algorithms have been proposed to solve this problem [6].

First, radial and tangential lens distortion are removed by camera calibration, which gets intrinsic and extrinsic camera parameters. Knowledge of the camera parameters is utilized to rectify both images. The image rectification is necessary for reducing complexity of calculations for left and right images pixel correspondence. This approach is used to reduce a search space for disparity and depth map computation algorithms. Then, the stereo matching problem is reduced to one-dimensional search along horizontal lines, instead of two-dimensional search. Finally, stereo matching algorithm is applied on the left and right images with the aim to find all correspondences (matching points) and assign depth. Output of the stereo matching algorithm is the depth map [6], [7].

However, the method based on a stereo geometry is very time-consuming. Therefore, this method will not be further used in our final comparison.

### 4. 3D model reconstruction by photogrammetry

In nowadays, a lot of software solutions for 3D model reconstruction by photogrammetry are available. For reconstruction purposes, three best known environments, namely, Agisoft PhotoScan 1.1.6 Professional Edition [2], Autodesk Memento 1.1.0.1 beta [3] a 3DF Zephyr Pro 2.0 [4] were chosen.

#### 4.1. Agisoft PhotoScan based reconstruction

Agisoft PhotoScan [2] is an advanced image-based 3D modeling solution for creating professionals quality 3D content from still images. Agisoft PhotoScan uses Structure from Motion (SFM) as the algorithm to determine the orientation of the cameras and to position object points. This SW is preferable over other 3D photo-modelers because it supports projected coordinate systems which make it suitable for photogrammetric and remote sensing applications. Based on the latest multi-
view 3D reconstruction technology, it operates on arbitrary images and is efficient in both controlled and uncontrolled conditions. 3D reconstruction SW automatically builds textured 3D models using digital photos of the real scene [2].

In the first phase sparse point cloud is produced. In close range photogrammetry, sparse point modeling is essentially a digitizing process on the oriented photos [7]. Parameter settings were set: Accuracy to high and Pair selection to disabled. Image pair selection may speed up process due to selection of a subset of image pairs to be matched [2], but may cause errors in alignment. Point limit were set to 40 000 and Constrain feature by mask was disabled.

In the second phase dense point cloud is created. Dense point modeling employs automatic image matching algorithms to compute the 3D coordinates of thousands of points from a pair of oriented photos [7]. Additionally, accuracy and quality of created model is higher than from sparse point cloud. Settings for dense point cloud were set: Quality to High, Depth filtering to Aggressive, Reuse depth maps was disabled.

Thereafter, from dense point cloud the mesh is created. Settings were set: Source type to Arbitrary, Interpolation was enabled and Face count was set to High. Number of polygon count is based on number of points given from dense point cloud. The texture is obtained from selected cameras, which are mapped on created mesh. Settings for this process were set: Mapping mode to generic, textures were given from all cameras. Blending mode was set to mosaic, texture size was set to 4096x4096 px. and Texture count to 1.

4.2. Autodesk Memento based reconstruction

Autodesk Memento is software for converting 2D images into high 3D meshes which can be edited, retopologized, analyzed, 3D printed and exported. After importing photos Autodesk Memento uploaded photos to server. It is possible to set only Quality: Draft/Best and model name. Reconstructed 3D model is downloadable from server after some time. Waiting time depends on the number of requests in the server queue. 3D model is exported to .obj format with texture size 4096x4096 in .jpg format.

4.3. 3DF Zephyr based reconstruction

After images importing and cameras calibrating, these parameters were set: Keypoint Density – High, Matching Type – Fast, Matching Stage Depth – High, Reprojection Error Tolerance – Normal, Bundle Adjustment – Local And Restained, Photo Ordering – Sequential. In first step, the 3DF Zephyr uses 3DF Samantha core technology for automatic camera orientation process [5]. Next, the dense point cloud generation is processed. The following parameters: Category - Close Range Presets - Hight Details were set. In this step, 3DF Zephyr uses the algorithm 3DF Stasia which extract a very accurate high-poly mesh from a set photos [6]. This algorithm for each pixel of input images generates the 3D surface. The 3D mesh creation is the third step. For the surface reconstruction: Category - Close Range Presets – Hight were set. For the export of 3D model, Export Format - .obj and texture resolution - 4096x4096 in .png file format was used.

4.4. Analyze of 3D reconstruction models

For further model processing (sculpting, retopology, rigging and animation), the structure and the number of polygons of the model are very important. Based on our subjective comparison it is possible to say that the 3D model created by Autodesk Memento provide best precision with details of the face and antlers.

The worst performances was achieved by 3DF Zephyr, because the density of polygons is uniform across the surface of the model and details of antlers was not preserved (Fig. 4). The largest number vertices was reached by 3DF Zephyr, but the surface area had the least surface which was caused by faulty reconstruction base board (Tab. 1).

<table>
<thead>
<tr>
<th>Verticles</th>
<th>Faces</th>
<th>Surface area [mm²]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference model</td>
<td>Agisoft Photoscan</td>
<td>Autodesk Memento</td>
</tr>
<tr>
<td>Verticles</td>
<td>355 265</td>
<td>101 920</td>
</tr>
<tr>
<td>Faces</td>
<td>408 476</td>
<td>179 999</td>
</tr>
<tr>
<td>Surface area [mm²]</td>
<td>16 492 237</td>
<td>15 238 402</td>
</tr>
</tbody>
</table>
Fig. 3: Solid models with wireframe.
The texture mapping is also important for further texture editing and the fur creation. Based on our experiments, the best editable texture was created by Autodesk Memento, because it creates the largest block of texture mapping. Also, good editable performances of texture were obtained by Agisoft PhotoScan because it uses all texture pixels.

5. Comparison of reference model with reconstructed

For comparison of the reference and reconstructed models, the Hausdorff distance, which computes how far two subsets of a metric space are from each other, was used. To analyze difference between two models, the Autodesk Memento was used. Since each exported model has a different size and orientation we have to manually set its origin, coordinates and scale. Origin and coordinates was set the middle of top side of the baseboard (Fig. 4) and was set to scale 2x1x0.4 meter.

Hausdorff distance colorfully illustrates the difference between a reference and reconstructed model (Fig. 5). Range of Hausdorff distance is ±10 mm. We consider that the exact model should have distance less than 1% of this. This distance is displayed by green in Figure 6. The most accurate reconstructed 3D model is created by Autodesk Memento.
6. Conclusion

In this paper we described a method of creation 3D model of animal by photogrammetry. The photos of animal, which were created in graphic environment Cinema 4D, were inserted to three different photogrammetry software solutions. The best results were obtained by software Autodesk Memento. The details of mesh were preserved better than the other compared software, which is proven in section 4. The other solutions have high differences especially in area of antlers and face. These obtained details can be used for further graphic processing.

Acknowledgements

This work was supported by EUREKA project no. E!6752 – DETECTGAME: R&D for Integrated Artificial System for Detecting the Wildlife Migration.

References

Electronically Controlled RF Switch for UWB Application

Stanislav SLOVÁK, Pavol GALAJDA

Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 040 20 Košice, Slovakia

{Stanislav.slovak, pavol.galajda}@tuke.sk

Abstract. The article deals with the implementation of CMOS switch for the purposes of electronically controlled calibration systems for different applications operating in the ultra-wide frequency band (UWB). The realization has been carried out in two steps. Design of the calibration module based on the available RF CMOS switch PE42540 was the goal of the first phase, described in the introductory part of the article. This module has been designed for the operational bandwidth from a few tens of MHz to 8GHz and has been realized using two layers Rogers Printed Circuit Board RO4003C whose design has been customized to 50Ω impedance environment. Within the frame of this solution the electronically controlled calibration unit was realized, in order to carry out evaluation of required parameter by means of measurements. Second phase which is being developed comprises the design of electronically controlled calibration unit with application specific integrated circuit (ASIC). This design is implemented in 0.35um SiGe BiCMOS technology by Austria Microsystems (AMS) using the most advanced solutions in the form of NMOS transistors connected as a RF switch. The main objective of this paper is the design and realization of a CMOS switch, which can be implemented in a wide spectrum of various RF, microwave and UWB applications as for example switching signals from different directions (multiple antennas) or switching between different applications such as calibration of sensor systems, which requires a reference elements [1].

In order to effectively obtaining the most accurate data on a specific device under test (DUT) it is necessary to accurately calibrate the entire system. Our objective was to design a low-cost device that could meet these requirements without the need for external intervention to the system (i.e. in-situ electronically controlled calibration). According to [2] for the realization of calibration the confrontation with the four known states i.e. SOLT (short, open, load, thru), is required. In the first phase a commercially available chip PE42540 [3] has been selected. The IC contains four internal RF switches (four RFx ports) and one RFC port in the architecture known as a Single Pole- Four Throw (SP4T). Its basic features include bandwidth up to 8GHz and high linearity, the IIP3 is 58dBm, isolation is 31dB @ 8GHz, insertion loss is 1.2dB @ 8GHz and maximum power handling is 30dBm @ 8GHz. Because the maximum bandwidth in which the switch has acceptable properties is just to 8GHz, we decided to realize a new solution of the Application Specific Integrated Circuit (ASIC) RF switch, which is capable to operate at full UWB frequency band defined by as Electronic Communication Committee (ECC) and Federal Communications Commission (FCC). The proposed switch was implemented in 0.35um SiGe BiCMOS technology by Austria Microsystems (AMS) using the most advanced solutions in the form of an NMOS transistors connected as a RF switch.

The article is divided into several chapters, where the second is devoted to the design, realization and testing of the calibration module based on the available RF CMOS switch PE42540. The reconfiguration of the measurement plane with the four known states i.e. SOLT (short, open, load, thru), is required. In the first phase a commercially available chip PE42540 [3] has been selected. The IC contains four internal RF switches (four RFx ports) and one RFC port in the architecture known as a Single Pole- Four Throw (SP4T). Its basic features include bandwidth up to 8GHz and high linearity, the IIP3 is 58dBm, isolation is 31dB @ 8GHz, insertion loss is 1.2dB @ 8GHz and maximum power handling is 30dBm @ 8GHz. Because the maximum bandwidth in which the switch has acceptable properties is just to 8GHz, we decided to realize a new solution of the Application Specific Integrated Circuit (ASIC) RF switch, which is capable to operate at full UWB frequency band defined by as Electronic Communication Committee (ECC) as Federal Communications Commission (FCC). The proposed switch was implemented in 0.35um SiGe BiCMOS technology by Austria Microsystems (AMS) using the most advanced solutions in the form of an NMOS transistors connected as a RF switch.

Keywords

Calibration, RF switch, CMOS, UWB, ASIC

1. Introduction

With the development of modern silicon technology, more and more high-frequency circuits can be implemented in CMOS processes. Radio frequency (RF) integrated circuits (ICs) in CMOS technology have proven manufacturing and the trend of System-on-Chip (SoC) requires further integration of semiconductor switch for different applications.

The main objective of this paper is the design and realization of a CMOS switch, which can be implemented in a wide spectrum of various RF, microwave and UWB applications as for example switching signals from different directions (multiple antennas) or switching between different applications such as calibration of sensor systems, which requires a reference elements [1].

In order to effectively obtaining the most accurate data on a specific device under test (DUT) it is necessary to accurately calibrate the entire system. Our objective was to design a low-cost device that could meet these requirements without the need for external intervention to the system (i.e. in-situ electronically controlled calibration). According to [2] for the realization of calibration the confrontation with the four known states i.e. SOLT (short, open, load, thru), is required.

In the first phase a commercially available chip PE42540 [3] has been selected. The IC contains four internal RF switches (four RFx ports) and one RFC port in the architecture known as a Single Pole- Four Throw (SP4T). Its basic features include bandwidth up to 8GHz and high linearity, the IIP3 is 58dBm, isolation is 31dB @ 8GHz, insertion loss is 1.2dB @ 8GHz and maximum power handling is 30dBm @ 8GHz. Because the maximum bandwidth in which the switch has acceptable properties is just to 8GHz, we decided to realize a new solution of the Application Specific Integrated Circuit (ASIC) RF switch, which is capable to operate at full UWB frequency band defined by as Electronic Communication Committee (ECC) as Federal Communications Commission (FCC). The proposed switch was implemented in 0.35um SiGe BiCMOS technology by Austria Microsystems (AMS) using the most advanced solutions in the form of an NMOS transistors connected as a RF switch.

The article is divided into several chapters, where the second is devoted to the design, realization and testing of
the CMOS switch module based on the commercially available chip PE42540. The third chapter deals in detail with the design of ASIC calibration unit based on NMOS switch operating in the UWB frequency band. The last chapter is dedicated to the layout and to the simulation results of the specific parameters of designed ASIC RF switch.

2. Calibration Unit Based on PE42540

For years, the RF switch has been dominated by discrete components using PIN diodes and III-V MESFETs. Recently due to miniaturization, CMOS front-end switch designs have been explored and manufactured, that are appropriate for different RF applications.

2.1. Design of CMOS Calibration Unit for UWB Applications

The first solution of the calibration unit based on CMOS switch can be implemented in RF or UWB applications. The general connection of the module is based on the abovementioned commercially available integrated circuit PE 42540 whose block diagram is shown in Fig.1.

![Block Diagram of the CMOS Switch, PE42540](image)

This switch belongs in a group of absorptive switches developed on Ultra CMOS process technology [3]. It is designed specifically to support the requirements of the test equipment and development activities. The chip is comprised of four symmetrical RFx (RF1-RF4) ports and one RFC port, all controlled by CMOS decoder, by which it is possible to link the RF input to the output.

The complete design of the electronically controlled calibration unit is shown on Fig.2. The CMOS switch circuit is mounted on a two-layer printed circuit board (PCB) consisting of RO4003C material with $\varepsilon_r = 3.38$ and thickness of 0.203mm. RF switch chip was connected via customized 50Ω transmission lines to miniature SMP connectors mounted on the top layer of the PCB (see Fig.2).

Fig. 2: Final version of RF switch module based on PE42540 chip

2.2. Testing and Measurement Results

In the testing of calibration units the most prominent parameters such as insertion loss, isolation and third-order intercept point (IP3), where measured. Based on these measurements the parameters of the switch where compared with the data that are guaranteed by the manufacturer. The measurements of transient response for all six possible states (RFC to RF1, RF2 and RF4- OFF, ON) of the switch, necessary for three states i.e. short, open and load was made. Port RF3 is not used and therefore it is not shown. Figure 3 shows the dependence of the insertion loss for the case, the RF ports (RF1, RF2 and RF4) are activated (switch ON).

![Insertion loss vs. frequency performance, RF1, RF2 and RF4-ON](image)

Fig. 3: Insertion loss vs. frequency performance, RF1, RF2 and RF4-ON

Figure 4 shows the measured insertion loss when the individual RF switch ports (RF1, RF2 and RF4) are closed (switch OFF).
Measurement results on the PE42540 (see Fig.5) exhibit approximately 56dBm input third-order intercept point (IIP3) which is a value close as specified by the manufacturer. These measurements were carried out by Vector Network Analyzer Agilent PNA-X N5241A, Generator Anritsu MG3700A and MXA Signal Analyzer N9020A.

Isolation was measured on the closest neighbor RF ports, thus according to Fig.1 between and RF2-RF4. Calibration unit with the switch PE42540 reached the insulation values as introduced by the manufacturer in the data sheet and are shown in Fig.6. These measurements were made for activated (switches RF2-ON, RF4-OFF and RF4-ON, RF2-OFF) and deactivated (both RF2 and RF4 switches OFF) RF ports.

Fig. 6: Isolation between ports RF2 and RF4

Proposed RF semiconductor switch is based on the fundamental principle of NMOS transistor connected as switch [4], [5] and [6]. This is so called Single Pole, Single Throw (SPST) connection, which passes or blocks an RF and microwave signals between two devices. Schematic of the basic NMOS switch is shown on Fig.7.

Source V2 is an input signal in the UWB frequency band and DC sources V1 and V4 represent the bias voltages that control the states of the switch. Appropriately selected transistors types and their interconnections realize the circuitry that meets the requirements of the most important parameters such as switch linearity, insertion loss and isolation. If the transistor M1 is open (switch ON) the transistor M2 is closed and vice versa. The transistor sizing have to be selected as a compromise between the bandwidth and the attenuation [7] and [8].

3.1. Design of the ASIC as SP3T NMOS Switch

The primary function of the designed switch is it’s realization in calibration RF or UWB systems. One way to achieve calibration of the UWB system is to connect know references, often open, short, load and defined through and consequently to calculate the system specific corrections [2]. In the first phase of the ASIC design it was necessary to implement electronically three states: open, short and load by means of a switch, which contains one RF port and three- symmetrical Rfx (RF1- RF3) ports.

The whole concept of this switch is realized for the 50Ω impedance matching environment. Figure 8 shows the complete circuit diagram of Single Pole- Three Throw
(SP3T) ASIC switch. In this case it is the extended version of the basic diagram SPST switch by two additional ports. The switching NMOS transistors M1, M3 and M6 where connected by another group of parallel connected transistors (M2, M4 and M5) in order to achieve the best parameters relating to the frequency range and attenuation. The change of the number of additional ports and Width-to-Length (W/L) ratio of the transistors rapidly change attenuation and bandwidth of signal. Therefore, choice of the number and size of transistors is a compromise between these two parameters. Comparison of the effective bandwidth of a different number of ports (SPST and SP3T) is shown in Fig.9.

Fig. 9: Comparison of the frequency band of the switches

3.2. Layout and final version of the SP3T NMOS switch

The active layout of the chip was implemented on an area 180,5x120µm. The proposed layout is shown in Fig.10, where one can see three symmetrical RF switching blocks and a CMOS control logic block. ASIC works with negative logic and the supply voltage thus represents -3.3V.

Fig. 10: Layout of the NMOS UWB ASIC RF switch

4. Conclusion

The first part of this article was dedicated to the implementation of low-cost RF CMOS switch based on commercially available solution. After the module evaluation, the measurement results are in accordance with the values specified by the manufacturer, but as we expected it do not meet FCC frequency bandwidth requirements. Therefore we decide to design of the customized NMOS based RF switch, sketched in the second part of this article. Its final realization in AMS technology is preparing for manufacture. As simulation shown, it will be appropriate for application in the UWB frequency band not only defined by ECC but also FCC. This design is customized implemented with the aim of implementation of proposed structure in system on chip (SoC) applications.

5. Acknowledgment

This work was supported by the projects implementations: University Science Park TECHNICOM for Innovation Applications Supported by Knowledge Technology, ITMS: 2622020182, supported by the Research & Development Operational Programme funded by the ERDF; the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic under the contract No. 1/0563/13 and No. 1/0766/14.

6. References

OPTIMALIZACE DYNAMICKÉHO ROZSAHU VSTUPNÍHO SIGNÁLU PÁSMOVÉ PROPUSTI S OBVODY CCII+

Zdeněk TESAŘ, Iva PETŘÍKOVÁ

Katedra telekomunikačních techniky, Fakulta elektrotechniky a informatiky, VŠB-TU Ostrava, 17. listopadu 2172/15, Ostrava-Poruba, Česká Republika

Abstrakt. V článku je provedena analýza vlivu nelinearit aktivních prvků na maximální velikost vstupního signálu elektronických filtrů. Jsou zde uvedena kritéria pro hodnocení obvodových řešení filtrů a z nich plynoucí doporučení pro návrh filtrů s ohledem na maximální dynamický rozsah vstupního signálu. Je zde uvedena pro pásmové propusti univerzální metoda využívající podkritické kladné zpětné vazby pro zvýšení dynamického rozsahu zpracovávaného signálu.

Klíčová slova

Aktivní prvky VFA, CFA, OTA, CCII+, dynamický rozsah vstupního signálu, elektronický filtr, pásmová propust, podkritická zpětná vazba, statická a dynamická nelinearita.

1. Úvod

V současné době je při návrhu elektronických filtrů možno volit z celé řady obvodových řešení využívajících klasické a moderní aktivní prvky, které mohou pracovat v napěťovém, smíšeném nebo proudovém módu. Aktivní kmitočtové filtry mají řadu výhodných vlastností, ale jejich nevýhodou je omezený kmitočtový rozsah a rozsah úrovní vstupního signálu. Pokud je překročena dovolená úroveň vstupního signálu, filtr přestává být lineárním obvodem a se začíná degradovat, pro kterého byl navržen. K této degradaci dochází vždy, když kterýkoliv aktivní člen přestane pracovat v lineárním oblasti svých charakteristik. Pro dosažení maximální úrovni vstupního signálu (maximální vstupní dynamický rozsah) je u filtrů pracujících v napěťovém, smíšeném a vlastně i proudovém módě nutno zajistit, aby přenosy ze vstupu na kritické uzly a větve měly optimální velikost.

2. Nelinearity aktivních prvků

Podmínkou, aby filtr mohl být považován za lineární obvod je, že všechny pasivní a aktivní prvky pracují v lineární oblasti a neuplatňují se jejich nelineární parametry. Obecně lze elektronický obvod, tzn. i filtr rozdělit na pasivní a aktivní část. Pasivní část budeme pro uvažované signálové úrovně považovat za lineární (prakticky vždy splněno) a nelinearity filtru budou určovat nelinearity aktivních prvků. Blíže si pro potřeby analýzy dynamického rozsahu vstupního signálu definujeme nelinearity komerčně dostupných aktivních prvků, jedná se o klasický operační zesilovač VFA, transadmitanční zesilovač OTA, transimpedanční zesilovač CFA a konvenční proudový konvejor CCII+.

Nelinearity aktivních prvků se dělí na statické nelinearity (omezení rozmístění) a dynamické nelinearity (omezení rychlosti změn signálů), [1].

U standardního operačního zesilovače VFA jsou statické nelineární parametry závislé na velikosti napájecího napěti a na velikosti výstupního proudu (proudová limite), viz. Fig. 1. Dynamický nelineární parametr rychlost přeběhu $SR$ je vázán s mezní výkonovou frekvencí $f_p$ a s amplitudou výstupního napětí $U_0$ (harmonický signál) vztahem

$$SR = \frac{\Delta U_0}{\Delta t} = 2\pi f_p U_0$$ (1)

$U_{omax}$ je největší hodnota výstupního napětí v lineární oblasti.

$I_{omax}$ je největší hodnota výstupního proudu v lineární oblasti.

$U_{cmmax}$ je největší hodnota souhlasného vstupního napětí v lineární oblasti.

$SR_{max}$ (rychlost přeběhu) je největší rychlost změny výstupního napětí v lineární oblasti.
3. Kritéria určující velikost vstupního signálu

Základní kritéria pro srovnávání a hodnocení jednotlivých obvodových řešení filtrů z hlediska dynamického rozsahu vstupního signálu jsou odvozeny na základě analýzy obecné struktury operační sítě se zesilovači VFA uvedené na Fig. 5. a její modifikace pro další uvedené aktivní prvky OTA, CFA a CCII+ na Fig. 6.

Kritérium č. 1

Urhčíme maxima frekvenční závislost napěťových přenosů ze vstupu do kritických uzlů zapojení filtru (vstupy a výstupy aktivních prvků).

\[
\begin{align*}
\text{IN} F_n(f) &= \frac{U_{\text{cmn}}}{U_{\text{VST}}} \\
\text{OUT} F_n(f) &= \frac{U_{\text{dmn}}}{U_{\text{VST}}} 
\end{align*}
\]

(2)

(3)

Kritické uzly zapojení se stanoví na základě analýzy konkrétního zapojení a pro rozhodující nelinearity použitých aktivních prvků, Fig. 1. až Fig. 4. Pro maximální úroveň vstupního napětí pak platí

\[
U_{\text{VST max}} < \frac{U_{N \text{max}}}{F_{\text{n max}}(f)}
\]

(4)

kde \(U_{N \text{max}}\) je největší hodnota vstupního – výstupního napětí v lineární oblasti a \(F_{\text{n max}}(f)\) je největší hodnota
přenosu v daném frekvenčním rozsahu.

Kritérium č. 2
Určime maxima frekvenční závislost přenosových admitancí ze vstupu do kritických větví zapojení filtru.

\[ Y_n(f) = \frac{I_{0n}}{U_{VST}} \quad (5) \]

Kritické větve zapojení se stanoví zase na základě analýzy konkrétního zapojení a pro maximální úroveň vstupního napětí pak platí

\[ U_{VST\max} < \frac{I_{0n\max}}{Y_{n\max}(f)} \quad (6) \]

kde \( I_{0n\max} \) je největší hodnota vstupního – výstupního proudu v lineární oblasti a \( Y_{n\max}(f) \) je největší hodnota přenosové admitance v daném frekvenčním rozsahu.

Kritérium č. 3
Zjistíme při jakých frekvencích \( f_{\max} \) dochází k maximu napěťového přenosu ze vstupu na napěťové výstupy aktivních prvků a kontrolujeme, zda je pro danou rychlost SR přeběhu aktivního prvku splněna podmínka

\[ SR > 2\pi f_{\max} F_{0n}(f_{\max})U_{VST\max} \quad (7) \]

Podrobně jsou kritéria zpracována v lit. [6].

Pouzoucí zapojení filtru pomocí uvedených kritérií, především kritérií č. 1 pro filtry pracující v napěťovém režimu, je nutno provést hlavně při návrhu filtrů s větším počtem aktivních prvků, filtrů s vysokým činitelem jakosti a u filtrů vyšších řádů realizovaných pomocí kaskádní a nekaskádní syntézy.

Při optimalizaci zapojení filtru provádíme takové úpravy obvodového řešení nebo takové znění hodnot součástek, aby se všechny kritické přenosy blížily hodnotě jedna, a následně provedeme hodnocení pomocí dvou zbývajících kritérií.

4. Experimentální ověření

Metodu podkritické kladné zpětné vazby aplikujeme na pásmovou propust druhého řádu s obvyky CCII+, lit. [2], která má tyto parametry \( F_{PP}(f_0)=1, \quad Q=10, \quad f_0=100kHz \). Schéma zapojení je na Fig. 7.

Fig. 7: Pásmová propust PP1 \( Q=10 \).

Z průběhu frekvenční závislostí přenosů \( F_{21} \) a \( F_{31} \) je vidět, že maximální hodnota přenosu \( F_{21} \) je v souladu se zadáním rovna jedné, ale u přenosu \( F_{31} \) je jeho maximální hodnota desetkrát větší, je určena vztahem (10) a s rostoucím činiteljem jakosti \( Q \) propusti roste, tzn., že maximální dovolený rozkmit vstupního signálu klesá.

Zjednodušeně řečeno, v případě, že vstupní napětí pásmové propusti bude mít rozkmit \( U_{pp}=1V \) bude mít stejný rozkmit i výstupní napětí \( U_{pp}=1V \), ale rozkmit napětí uzlu (3) bude \( U_{pp}=10V \), což při napájecím napětí \( \pm 5V \) znamená, že konvejor IO2 již nebude pracovat v lineární oblasti. Z uvedeného vyplývá, že dané zapojení pásmové propusti bude mít pro větší činitele jakosti malý rozkmit vstupního napětí. Zvětšíte dynamický rozsah
vstupního signálu optimalizací hodnot pasivních
součástek není u tohoto zapojení možné, viz návrhové
vztahy v Tab. 1. Optimálním řešením by nebylo ani
použití odporového děliče na vstupu filtru a následné
zesílení signálu na jeho výstupu. Řešením je využití
podkritické napěťové kladné zpětné vazby (bootstrap)
tvořené rezistory $R_A$, $R_B$, která zvyšuje činitel jakosti
filtru, lit. [3], [4].

Tab.1: Návrhové vztahy a přenosy pro PP1.

$$F_{21}(f_0) = \frac{C_2}{C_1}$$  \hspace{2cm} (7)

$$Q = \frac{R_1 C_2}{\sqrt{R_1 C_1}}$$  \hspace{2cm} (8)

$$f_0 = \frac{1}{2\pi \sqrt{R_1 R_2 C_1 C_2}}$$  \hspace{2cm} (9)

$$F_{31\text{max}} \approx \sqrt{Q^2 + 1}$$  \hspace{2cm} (10)

$$F_{21} = \frac{U_2}{U_1} = \frac{\frac{1}{p R_2 C_1}}{p^2 + \frac{1}{R_1 C_2} + \frac{1}{R_1 R_2 C_1 C_2}}$$  \hspace{2cm} (11)

$$F_{31} = \frac{U_3}{U_1} = \frac{\frac{1}{p R_2 C_2} + \frac{1}{R_1 R_2 C_1 C_2}}{p^2 + \frac{1}{R_1 C_2} + \frac{1}{R_1 R_2 C_1 C_2}}$$  \hspace{2cm} (12)

Modifikované zapojení PP se stejnými parametry, ale
s podstatně větším dynamickým rozsahem (cca 10x) je
na Fig. 9., návrhové vztahy a přenosy $F_{21}=U_2/U_1$, $F_{31}=U_3/U_1$ a $F_{71}=U_7/U_1$ jsou uvedeny v Tab. 2. Na Fig. 10
jsou frekvenční charakteristiky přenosů ze vstupu uzel (1)
do kritických uzlů (2) – výstup PP, (3) a (7).

Fig. 8:  Frekvenční charakteristiky PP1 $Q=10$.

Fig. 9:  Modifikovaná pásmová propust PP2 $Q=10$

Fig. 10:  Frekvenční charakteristiky PP2 $Q=10$.

Princip zvětšení rozkmitu vstupního signálu
modifikované pásmové propusti PP2 spočívá
ve vyrovnání napěťových přenosů ze vstupu
do kritických uzlů tak, aby se blížily k hodnotě jedna.
Z porovnání vztahů (17), (21) a (22) plyne, že největší
vliv na rozkmit vstupního signálu má maximální velikost
přenosu $F_{31\beta}$, která závisí na činiteli jakosti pásmové
propusti bez zpětné vazby, vztah (21). Při návrhu volíme
činitel jakosti propusti bez zpětné vazby malý, v našem
případě byl volen $Q=0,5$ tím minimalizujeme přenos $F_{31\beta}$.
Potřebnou hodnotu činitele jakosti $Q_\beta$ nastavíme pomocí
podkritické kladné zpětné vazby, rezistory $R_A$ a $R_B$, vztah
(16).
Zde je potřeba dát pozor na stabilitu filtra, podmínkou nutnou je, že člen
\[ 1 - \frac{C_2}{C_1} \beta > 0 \] (23)

Na průběhu frekvenčních charakteristik jednotlivých přenosů Fig. 10. je vidět, že maximální hodnoty přenosů se blíží požadované hodnotě jedna (0 dB) a dynamický rozsah vstupního signálu je maximálně využit.

**Tab.2:** Návrhové vztahy a přenosy pro PP2

\[ f_0 = \frac{1}{2\pi \sqrt{R_1 R_2 C_1 C_2}} \] (13)

\[ \beta = \frac{R_A}{R_A + R_B} \] (14)

\[ 1 - \beta = \frac{R_B}{R_A + R_B} \] (15)

\[ Q_\beta = \frac{1}{1 - \frac{C_2}{C_1} \beta} \sqrt{\frac{R_2 C_2}{R_1 C_1}} = \frac{1}{1 - \frac{C_2}{C_1} \beta} Q \] (16)

\[ F_{21\beta}(f_0) = \frac{C_2}{C_1} \frac{1 - \beta}{1 - \frac{C_2}{C_1} \beta} = F_{21}(f_0) \frac{1 - \beta}{1 - \frac{C_2}{C_1} \beta} \] (17)

\[ F_{21\beta} = \frac{1}{p R_2 C_1} (1 - \beta) \] (18)

\[ F_{31\beta} = \frac{1}{p R_2 C_2} \left( 1 - \frac{C_2}{C_1} \beta \right) + \frac{1}{R_1 R_2 C_1 C_2} \] (19)

\[ F_{31\beta} = \frac{1}{p R_2 C_2} \left( 1 - \frac{C_2}{C_1} \beta \right) + \frac{1}{R_1 R_2 C_1 C_2} \] (20)

\[ F_{31\beta_{max}} \approx \frac{1 - \beta}{1 - \frac{C_2}{C_1} \beta} \sqrt{Q^2 + 1} \] (21)

\[ F_{71\beta_{max}} \approx \frac{1 - \beta}{1 - \frac{C_2}{C_1} \beta} \] (22)

Další výhoda metody podkriticke kladné ZV je vidět na průběhu frekvenčních charakteristik původní Fig. 11. a modifikované Fig. 12; pásmové propusti, kde při ladění frekvence \( f_0 \) filtrů dochází s rostoucí frekvencí \( f_0 \) ke zvyšování přenosu \( F_{31} \) a tím k poklesu dynamického rozsahu vstupního signálu. Z porovnání frekvenčních charakteristik je vidět, že pokles úrovně vstupního signálu je u upravené pásmové propusti výrazně nižší něž u původního zapojení.

**Fig. 11:** Frekvenční charakteristiky PP1 (ladění \( f_0 \)).

**Fig. 12:** Frekvenční charakteristiky PP2 (ladění \( f_0 \)).

5. **Závěr**

Problematicka maximálního dovoleného dynamického rozsahu vstupního signálu je z hlediska správné funkce filtrů velmi důležitá a ne vždy je při návrhu filtrů dostatečně respektována. V příspěvku jsou stanovena základní kritéria pro posuzování obvodových řešení filtrů s různými komerčně dostupnými aktivními prvky (VFA, CFA, OTA a CCCI+) s ohledem na dynamický rozsah vstupního signálu. Na řešení návrhu pásmové propusti je ukázána metodika postupu optimalizace dynamického rozsahu.
úpravou zapojení filtru zavedení podkritické kladné ZV. Další způsob optimalizace je metoda optimální volby hodnot pasivních součástek filtru, podrobně je praktický postup uveden v lit. [5], která je u laditelných pásmových propustí méně vhodná.

Poděkování

Tento výzkum, který vedl k těmto výsledkům, byl financován z projektu TA03020439 - Bezpečnost optických přenosových sítí a vývoj optických součástek pro sílovou energetiku a energovody (2013-2016, TA0/TA).

Literatura


About Authors


COMPARISON OF BB84 AND B92 PROTOCOL IN TERMS OF THE LENGTH OF THE FINAL KEY

Miralem MEHIC, Miroslav VOZNAK

VŠB-Technical University of Ostrava 17.listopadu 15, 708 00 Ostrava-Poruba, Czech Republic

miralem.mehic.st@vsb.cz; voznak@ieee.org

Abstract. Quantum Key Distribution (QKD), often called in a more general context Quantum Cryptography, is a technology that uses the properties of quantum mechanical systems in combination with information theory to achieve unconditionally secure distribution of secret keys. BB84 and B92 are the oldest QKD protocols. These protocols consist of several phases in which initial key is significantly reduced: secret key exchange, extraction of the raw key (sifting), error rate estimation, key reconciliation, privacy amplification and authentication. In this article we explained the reduction of the initial key in each of QKD phases.

Keywords

B92, BB84, Symmetric Cryptography, Quantum Key Distribution.

1. Introduction

Until recently, cryptography was the point where security engineering meets mathematics. Today, this definition is extended to include the principles of quantum physics. Quantum cryptography uses quantum physical principles to establish symmetrical binary keys between legitimate users that will use these keys to encrypt theirs communication data. Therefore, this technology can be better described as “Quantum Key Distribution” or just QKD.

The concept of quantum cryptography was originally proposed in 1960s by Stephen Wiesner, a student of Columbia University, and finally published in 1983 [1], thought its real development is recorded from 1984 when Charles Bennett (IBM) and Gilles Brassard (University of Montreal) presented BB84, the first QKD protocol [2]. Five years later they made a first practical demonstration of QKD by establishing secret key over 30cm through the air. This protocol is even today most widely used. Eight years later Bennet developed B92 [3] protocol that is simpler and faster than its predecessor. BB84 and B92 are the oldest QKD protocols which consist of several post-QKD operations in which initial key is significantly reduced. In this article, we analyzed these phases and we compare BB84 and BB92 protocol on the basis of the length of the final key.

2. Secret key exchange

At the beginning of communication, the sender hereinafter named Alice and the recipient hereinafter named Bob must agree on the same alphabet. BB84 assumes that the polarization of photons is used as a carrier of information, so Alice defines a random key with a length Q and uses a randomly selected polarization from the alphabet as a carrier of the key. For example, for the bit value 1 she can choose either vertical (x=90°) or diagonal polarization (x=45°), and for the bit value 0 she can choose either horizontal polarization (x=0°) or opposite diagonal polarization (x=-45°). On the receiving side of the quantum channel, Bob chooses a randomly selected basis for detection. Since Bob does not know which basis Alice has used, and he uses a randomly selected basis, he will be able to reliably detect only 50% of the sent key.

In order to establish a secret key using B92 protocol, Alice and Bob can use only two non-orthogonal polarizations, each one coding for one bit-value. Alice sends modulated photons over the quantum channel to Bob. Since Bob has no information about the sequence which Alice used, he will use randomly basis in order to measure the incoming photons. If Bob chooses the correct basis, he will measure the incoming photon. If he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure [4, p. 20]. However, the probability that Bob will choose correct basis is approximately 25%. All subsequent steps are identical for BB84 and B92 protocol.

3. Extraction of a raw key – Sifting

---

1 Sifting, Error-rate estimation, Key reconciliation, Privacy amplification, Authentication
4. Error rate estimation

The purpose of error estimation is to determine the percentage of errors in the key after quantum transmission and sifting have occurred. Errors may occur because of a disturbance of the quantum channel, noise in the detectors or an optical misalignment and other reasons. But errors may also occur due to eavesdropping by eavesdropper Eve. However, the threshold of bit error rate for optical channel without presence of Eve is known in forward so Alice and Bob must compare a small portion of their key in order to estimate the quantum bit error rate (QBER). If the error rate is higher than a given threshold, Alice and Bob revealed the presence of Eve and the key distribution process starts all over again.

If we mark n as the total length (Q) of the raw key then the number of bits k that will be used for the QBER estimation depends on the length of the sample block used for error rate estimation which is defined with a parameter we refer to as “level of security” Š(k). In [5], two levels of security are defined: basic and advanced. Alice and Bob must select the desired level of security Š(k), and use Equation (1) to calculate k.

However, Alice and Bob must delete the part of the key which they used for estimation of the error rate. It means that the raw key will be shortened even more. We use notation R to mark the length of the key after this phase.

\[
\hat{S}(k) = -\sum_{i=1}^{n} \frac{k - \log k}{n} \frac{1}{n}
\]  

(1)

5. Key reconciliation

When Alice and Bob are sure that the key distributed via the quantum channel has a low error rate, they must find and correct or delete all errors in the rest of the key. This phase is known to be highly interactive and time-consuming, since the discussion about the location of errors in the key is performed through the public channel. The cascade protocol [6] is the most widely used reconciliation protocol due to its simplicity and efficiency. It is run iteratively in the given number of iterations where random permutation of the key is performed with the objective to evenly disperse errors throughout the key. Next, the permuted key is divided into equal blocks of \(k_i\) bits, and after each iteration permutations are performed again and the block size is doubled: \(k_{i+1} = 2k_i\). For each block, Alice and Bob will exchange the results of the parity test and perform a binary search to find and correct errors. Instead of going through all the iterations continuously, the Cascade protocol investigates errors in pairs of iterations. The process is recursive.

However, the length of the initial block \(k_i\) is a critical parameter, and should depend on the estimated error rate. An empirical result in [6] indicates that the optimal value of \(k_i\) is 0.73/p, where \(p\) is the estimated error rate (QBER) [6]. The Cascade protocol is modified in [7], with the aim of reaching the theoretical limit for protocol efficiency. From these results, it is clear that four iterations are sufficient for a successful key reconciliation, as was suggested in the [6]. Since the initial block length depends on the estimated error rate, it is necessary to perform all the iterations. The number of iteration \(i\) is increased to the value for which the length of block \(k_i\) can be used to split the raw key into two parts \(\{k_i < \frac{n}{2}\}\).

Now, let us go back to the parity check results. If the parity of a block disagrees between Alice and Bob, they perform a binary search on that block with the aim of identifying the single bit error. The binary search consists of dividing the block in half and comparing the parity check results for the divided block until the error is located. This means a maximum of \(\log_2 k\) parity bits are exchanged for each block with an error bit since \(\log_2 k\) is the maximum number of times block \(k\) can be divided, and one parity bit is exchanged for blocks without errors. In order to minimize the amount of information gained by Eve, it is advisable to discard the last bit of each block and sub-block for which the parity bit was exchanged. Now if we define \(L\) as the maximum number of leaked bits, and \(k_i\) as the length of the block in the \(i\)th iteration, it is clear that:

\[
L = \sum_{i=1}^{\log_2 k} \left( \sum_i^{k_i} \frac{n}{k_i} + \sum_{errors\ corrected} \left[ \log_2 k_i \right] \right)
\]  

(2)

where \(k_i = 2k_{i-1}\), \(k_i < \frac{n}{2}\) and \(n\) is the length of the initial key. Now it is clear that the number of leaked bits depends on the initial block size and error rate.
6. Privacy amplification

Alice and Bob finally have an identical key without errors, but since Eve may have gained significant knowledge of the key, Alice and Bob should strengthen their privacy. This is done by deleting some of the bits of the final key, so the raw key is shortened even more. The number of rejected bits during the privacy amplification process is defined in Equation (4) [8], where \( S \) is the number of bits that need to be discarded and \( n \) is the length of the key \( (B) \).

\[
\frac{n \cdot 2^{-S}}{\log 2} < 1 \tag{4}
\]

We mark the length of the final key after this phase as \( P \).

7. Authentication

Due to intended level of security of QKD which is unconditional (Information-theoretical) security in the presence of an adversary with unlimited computer power and memory, in QKD no restriction’s is put on adversary’s computational power and storage capability. Taking into account that QKD uses two channels, quantum, and public channel, it is necessary to protect communication from Eve’s influence. Public channel without authentication is like any other channel susceptible to a man-in-the-middle attack. In QKD, there are two types of authentication: immediate authentication and delayed authentication. Immediate authentication implies the authentication of messages immediately after they are received while the delay authentication implies the authentication for all messages exchanged during the session to be done at the end of the session. There are variations in the details, but all QKD protocols contain authentication. In this article, we follow the approach from [9] where authentication is performed two times. The first time, before error correction phase, where Alice and Bob authenticate the outcome of the measurement. This authentication is necessary to prevent intercept/resend attack [9]. Finally, the authentication is done at the end of the session in order to verify that the key is indeed identical on both sides.

Author in [10] divided authentication schemes into two categories: Information-theoretically secure (ITS) and computationally secure message authentication schemes. Then author performed a comparative analysis of Wegman-Carter, Sinson, den Boer, Bierbrauer et al., Krawczyk and a novel authentication scheme. In his document, author showed that Wegman-Carter [11] authentication which is based on ASU2 (Almost Strong Universal2) hashing is very well suited for authentication in QKD. To perform authentication it is necessary to sacrifice a certain part of the key and an upper bound for the key needed for authentication is defined with by the following equation [10]:

\[
k_{\text{auth}} = 4 \times \left( (b + \log_2 \log_2 a) \times \log_2 a \right) \tag{5}
\]

where \( a \) is the length of the message which needs to be authenticated and \( b \) is the length of authentication tag. Finally, it means that we need to exchange one authentication message to verify measurement on quantum channel where the length of the message which needs to be authenticated is \( \log_2 Q \) –bits, and it is necessary to verify key of length \( P \). The amount of key which need to be sacrificed for authentication is shown in Equation 6:

\[
k_{\text{auth}} = 4 \times \left( (b + \log_2 \log_2 a) \times \log_2 a \right) \times \log_2 \left( \frac{Q}{P} \right) + 4 \times \left( (b + \log_2 \log_2 P) \times \log_2 P \right) \tag{6}
\]

Now we can compare the length of the key in each previous step:

\[
Q > B > R > F > P > A \tag{7}
\]

Finally, this means that the raw key \( Q \) must be significantly longer than the key after being reduced in all phases explained above \( A \). The final key must be long enough to be used for the encryption and decryption of confidential data.

---

2. Often named as „continuous authentication“. More details about the continuous authentication can be found in [13]
8. Calculations

To summarize, we present the formula for calculating the length of the final key ($A$) from the length of the raw/initial key ($Q$), error rate and parameter “level of security” $\hat{S}(k)$.

$$A = m \times Q - \frac{\log m \times Q}{\log 2} - \hat{S} \times Q - L - k_{\text{auth}} \quad (8)$$

Where

- $\hat{S}$ – is the percentage of raw key ($Q$) used for calculating QBER
- $L$ - is the number of bits leaked during the key reconciliation phase
- $A$ - is the length of the final key
- $Q$ - is the length of the raw/initial key
- $m$ – is 0.25 for B92 and 0.5 for BB84

From Equation 8 it is easy to see that the noise in the quantum channel is included only in the calculation of the number of leaked bits $L$ during the error reconciliation phase. Also, the parameter $\hat{S}$ has a significant impact on the final length of the key, but with the increase of $\hat{S}$ the possibility that Eve gain information about the key decreases.

![Fig. 2. Comparison of the length of the final key; red line – B92; blue line – BB84](image)

![Fig. 3. The length of the final key depending on the parameter $\hat{S}$ and error rate; $Q=10\ 000$; B92 protocol](image)

9. Calculations

In this article we present the Equation (8) which is used to calculate the length of the final key $A$ based on the length of the raw key $Q$, error rate in quantum channel and on security parameter $\hat{S}$. From Equation (8) and Figure 3, it is clear that the length of the final key increases with the parameter error rate ($p$) and the “level of security” $\hat{S}$. In [12] and [9] authors defined the upper bound for tolerated quantum bit error rate $p_{\text{max}}$ of 12.9% for BB84 protocol. However, we showed empirically that this error rate for B92 protocol is not acceptable. For minimal value of parameter $\hat{S}_{\text{min}}$ 8.16% the maximal error rate is 5.84% as it is shown in Figure 2. This value is the direct consequence of twice smaller number of photons that Bob detects in relation to the BB84 protocol.

It is important to underline that parameter $\hat{S}$ defines the amount of key which is needed to estimate QBER in the channel. Also, it is worth noting that the influence of eavesdropping is not included in the Equation (8) since the entire QKD process will be repeated if the estimated QBER is higher than maximally tolerated QBER.

References


A NOVEL SOCIAL BASED OPPORTUNISTIC ROUTING IN MANET

Martin MATIS¹, Lubomir DOBOS², Jan PAPAJ³

¹,²,³Department of Electronics and Multimedia Communications, Technical University, Košice, Slovakia

martin.matis@tuke.sk ¹, lubomr.dobos@tuke.sk ², jan.papaj@tuke.sk ³

DOI: 10.15598/aeee.v13ix.xxxx

Abstract. In this paper is proposed a new routing protocol for mobile environment - A Social Based Opportunistic Routing Algorithm (SBOR) based on social behaviour between nodes and single copy forwarding scheme for sparse or disconnected networks. This protocol is for network with intermitted connection between nodes, without end-to-end connections and for network, which is divided into two or more sub networks (islands). This one is fully decentralized and exchanges social information between nodes in the Mobile Ad-Hoc Network (MANET) environment based on opportunistic carrying, storing or forwarding for Delay-Tolerant Network (DTN). The scheme in simulation is evaluated by replaying real life traces which exhibit this highly dynamic connectivity. The SBOR algorithm is compared based on different levels of velocity. The results show that SBOR is possible to use in situations without infrastructure and for intermitted connectivity of the nodes. Increasing velocity of nodes is helpful for SBOR. The article also provides short performance analysis of the SBOR in MATLAB environment.

Keywords

MANET, DTN, Opportunistic routing, Social behaviour.

1. Introduction

Transport of data through MANET [1] is possible with using routing protocols, such as proactive, reactive or hybrid [3], with satisfying delay for many applications which require low delay. When the mobile nodes have high velocity or the network is very sparse and divided into many sub networks (islands), usage of standard MANET routing protocol is ineffective or impossible [4]. Node mobility is a big advantage for cases when the data are transported through a wireless mobile network with use of Delay/Disruption-Tolerant Network (DTN) [5], Chyba! Nenalezen zdroj odkazů. and [6] paradigm.

Mobile nodes may form small islands. Using MANET solutions within islands can make great improvements. When an island is relative small with well connected nodes through wireless link, then the topology information can be better distributed. Creating, maintenance and disintegration of path between nodes depend on velocity and movement. When the island is stable based on mobility and velocity, then nodes can make better forwarding decisions. When the velocity is higher in the network, than the life-time of actual paths is reduced and the path can be crashed or useless like initial end-to-end paths. However, MANET routing protocol can be still successful locally, using partial paths even if it fails globally. The result of using partial path can be finding edge of the island or new virtual source for the rest of unsent messages [4], [8], [9], [10] and [11].

There exist some algorithms for transfer of information and data through DTN based on social information as SimBet [12] or based on history information as PROPHET [13]. Other type of social-based algorithm is BUBLE Rap [14], which can improve forwarding performance of the previous solutions. Previous routing mechanisms do not take into account the mechanism for counting social relations among the mobile nodes.

For this reason, we proposed a Novel Social Based Opportunistic Routing Algorithm (SBOR) in this paper. The new one can be used in MANET environment based on DTN approaches and social-based information among nodes.

Proposed protocol tries to send data from Source (S) to Destination (D). Information about D, which owns S, are spread in an Extended Route Request Packet (E-RREQ) and the probability of delivery is calculated in each node based on information in the E-RREQ. This probability can be used by opportunistic routing. Decisions about message forwarding are made based on a
Social behaviour between mobile nodes. Opportunistic routing can provide delivery of message to destination or closer to destination for disconnected islands or in the sparse network.

The article is divided into following sections. The section 1 describes a MANET and DTN environment. In section 2, the social based interaction among nodes and a Novel of SBOR is introduced. The section 3 displays results of simulations for SBOR in MATLAB, especially success of delivery, delay, average number of attempts (NOA) for transfer of message through network and success of delivery depending on allowed number of attempts. At the end of the article the conclusions and future works are described.

2. New Proposal of Novel Social Based Opportunistic Routing

2.1. Overview

The main topic of this paper is a creation of routing protocol which can be used in MANET environment [1] and [2] based on DTN routing solutions [5] and [6]. This approach guarantees the delivery of messages between source node S and destination node D in MANET environment.

Network without end-to-end connection

The deployment of the mobile nodes in MANET is very sparse or consists of two or more sub networks (islands) without connection between them where destination and source nodes are from different islands (Fig. 1). It is impossible to find path between nodes S and D with basic MANET routing. In these situations it is possible to use an opportunistic sending of the information for message delivery. The DTN routing approaches can be used [8] and [15].

![Fig. 1 Network without end-to-end connection](image)

For these reasons, we proposed a Novel Social Based Opportunistic Routing Algorithm (SBOR), which can transfer a message from S to D based on social behaviour among nodes and single copy forwarding schema. We implement this proposal into Dynamic Source Routing (DSR) reactive routing protocol for MANET [1] and [3].

2.2. Social Based Inter-Node Relation Information

The proposal considers that every mobile device/node is owned by a particular person. It is assumed that the S has information about D (S owns some information about node D). This information can be obtained as follows:

- Adding contact’s information to address book in mobile device and/or;
- Exchanging personal profile between S and D at the first or later contact and/or;
- Personal profile can be synchronized and actualized between S and D at every meeting.

We defined, that relationship between nodes is calculated based on Nodes profiles. But there are many possible methods how to determine a probability of delivery. It can be based on number of contacts, on social relations, etc. and its combinations.

1) Nodes profiles

The approach of social relation was considered in described proposal. For this purpose was used Personal (private) profile of node and Contact profile of node, which the device has in its address book. Both types of profiles have the same Entries Tab. 1.

2) Personal (private) profile of node

It is an obligatory profile in every device and all Entries (Tab. 1) are necessary to be filled. These Entries are filled by the owner of the device, so this profile represents the device and its owner.

3) Contact profile of node

It is common set of entries about people, which the owner of device knows and its partial or full information has in its address book about them and one profile of contacts about one person is additional information, of which is extended route request packets (RREQ). Contact profile completes its owner using obligatory Entries (unique identifier of the device and name of the person) or other optional Entries (address where the person lives and works, how the person travels to work and home, where the person spends free time and other).

Every node has one Personal (private) profile (PP) and many Contacts profiles (address book) (CP). Every value and number of entries in PP and CP is changed to string of characters with same length using Hash mechanism MD5 [16]. Hash mechanism creates 128 bit length string of hexadecimal symbols of the Hash Functions (HF) from every row in PP and CP. These are called Personal Hash Functions and Contact Hash Functions. These HF are better for allocation of bits in the header of RREQ, in comparison with other node and secure transfer [17] and [18].
2.3. Determination of the Probability

Every node, which receives a RREQ packet with additional information about destination node, can calculate a probability of message delivery to D from CP and PP. This additional information is determined from social relation information between S and D.

Algorithm 1: Calculation of the probability of delivery.

**Assumption 1:** Personal profile (PP) and Contacts profiles (CP) exist in every device. PP is filled by owner of device and CP can be filled by owner or retrieved from other nodes/mobile devices.

**Assumption 2:** Personal profile are composed from created set of entries with the associated weight for each row.

**Assumption 3:** Plain text of entries is transformed using hash mechanism MD5 to unique Hash Function (HF) for every string in PP and CP.

**Initialization:** Extended RREQ (E-RREQ), PP and CP are used. Created set of entries are compared based on extended RREQ and PP.

1. If E-RREQ is received to some node, do
2. For \( r=1 \rightarrow 15, \text{do} \)
   - HF(r) is compared from PP and E-RREQ for row \( r \)
3. If HF(r)$_{PP}$ & HF(r)$_{REQ}$ are equal, do
4. The weight \( W \) from Common set of entries for the row \( r \) will be used for next calculations \( W_{\text{match}_\text{rows}}(r) = W(r) \).
5. Else \( W_{\text{match}_\text{rows}}(r) = 0 \)
6. End
7. End
8. \( P = \frac{\sum_{r=0}^{15} W_{\text{match}_\text{rows}}(r)}{120} \)
9. Else Calculation of probability is unnecessary for this cases
10. End

For example, rows 6 – 10 are the same from both profiles, so sum of Weights based on Tab. 1 is calculated (see Eq. 2).

\[
\sum_{r=0}^{15} W_{\text{match}_\text{rows}}(r) = 10101111010101011010101010101010 \approx 43_{10}
\]

and the probability of delivery is (3)

\[
P = \frac{43}{120} \approx 35.83\%
\]

2.4. Social Based Opportunistic Routing

DTN routing is typical routing for sparse networks with mobile devices and with intermittent connection. It can be used for disconnected networks, communication between islands and networks with high mobility too [6] and [19].

It is impossible to create an end-to-end path between S and D in those cases. DTN routing functions based on sending data from source to next node. Sending can be provided based on many criterions. Repeating sending or carrying will deliver the message to destination or closer to destination.

Proposal of SBOR (see Algorithm 2 and Fig. 2) assumes a flooding based routing [4] for sending “extended RREQ packet (E-RREQ)” and direct transfer of single copy forwarding based schema for sending of data. The selection of the next node neighbour from potential nodes is based on probability of delivery. This probability is calculated by information from E-RREQ packet (see Algorithm 1). That information is about social relation and behaviour about D. Every node, which receives an E-RREQ for SBOR, calculates a probability of delivery (it is the same process, which is described in

<table>
<thead>
<tr>
<th>No.</th>
<th>Entry</th>
<th>E</th>
<th>Weight (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ID</td>
<td></td>
<td>1111</td>
</tr>
<tr>
<td>1</td>
<td>Surname</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>2</td>
<td>Name</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>City (home)</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Street (home)</td>
<td>4</td>
<td>1101</td>
</tr>
<tr>
<td>5</td>
<td>Number (home)</td>
<td>5</td>
<td>1110</td>
</tr>
<tr>
<td>6</td>
<td>City (work)</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>Street (work)</td>
<td></td>
<td>1011</td>
</tr>
<tr>
<td>8</td>
<td>Number (work)</td>
<td>8</td>
<td>1100</td>
</tr>
<tr>
<td>9</td>
<td>Company</td>
<td>9</td>
<td>1010</td>
</tr>
<tr>
<td>10</td>
<td>Catering</td>
<td>A</td>
<td>1001</td>
</tr>
<tr>
<td>11</td>
<td>Shopping</td>
<td>B</td>
<td>100</td>
</tr>
<tr>
<td>12</td>
<td>Shopping</td>
<td>C</td>
<td>11</td>
</tr>
<tr>
<td>13</td>
<td>Travel</td>
<td>D</td>
<td>101</td>
</tr>
<tr>
<td>14</td>
<td>Bus (NO. of link)</td>
<td>E</td>
<td>111</td>
</tr>
<tr>
<td>15</td>
<td>Tram (NO of link)</td>
<td>F</td>
<td>110</td>
</tr>
</tbody>
</table>
section Determination of the Probability...) and sends E-RREQ for SBOR with probability of delivery, which was calculated during sending of E-RREQ. The source node receives probabilities from all neighbours and choses the next node with best probability to send all data packets. This next node will become new virtual source. New source tries to send data to another neighbour node with suitable probability with the same manner. If no neighbours of source or virtual source are in radio range or the node already had the data or the nodes have unfit probability, then the node, which has the message, will store and carries this message, as it find node with better probability of delivery. This process is repeated until the message will arrive at destination node.

Algorithm 2: New proposal of SBOR algorithm

Assumption_1: Personal profile (PP) and Contacts profiles (CP) exist in every device. PP is filled by owner of device and CP can be filled by owner or retrieved from other nodes/mobile devices.

Assumption_2: Personal profile composes from created set of entries with the associated weight for each row.

Assumption_3: Plain text of entries is transformed using hash mechanism MD5 to unique Hash Function (HF) for every string in the PP and CP.

Process of finding next node and transfer of message is shown on Fig. 2.

3. Simulations and Results

Proposed algorithm SBOR, based on social relation between nodes and probability of delivery was simulated, verified and compared with DSR protocol [20] and [21] in software MATLAB.

Set values of variable are possible to see in the Tab. 2.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area [m]</td>
<td>1000x1000</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100</td>
</tr>
<tr>
<td>Radio range [m]</td>
<td>130</td>
</tr>
<tr>
<td>Number of transmitted message</td>
<td>5</td>
</tr>
<tr>
<td>Limited number of attempts (NOA) for sending the message</td>
<td>200</td>
</tr>
<tr>
<td>Number of simulations repetitions</td>
<td>100</td>
</tr>
<tr>
<td>Velocity</td>
<td></td>
</tr>
<tr>
<td>- slow walking</td>
<td>1.4 m/s</td>
</tr>
<tr>
<td>- fast walking</td>
<td>2.8 m/s</td>
</tr>
<tr>
<td>- running/cycling</td>
<td>5.6 m/s</td>
</tr>
<tr>
<td>- driving in a city</td>
<td>11.2 m/s</td>
</tr>
<tr>
<td>- driving out of a city</td>
<td>22.4 m/s</td>
</tr>
</tbody>
</table>

Simulations were oriented on comparison of different level of velocity for SBOR. There was observed a success of delivery of message to D, delay of message transfer and message overhead using SBOR routing methods. Positions of 100 nodes were generated and deployed randomly in area 1000x1000m. Based on this deployment, four islands of connectivity were created. Number of islands were changed due to mobility of nodes during the time. S (node with number 9) and D (node with number 5) were selected from different islands (see Fig. 3). Transfer was provided by SBOR and then by DSR [20] with the same deployment and same mobility model for all nodes for SBOR as well as DSR.

Fig. 2: Process of finding and sending messages by SBOR

Messaging for SBOR routing works as follows. Mobile nodes are moving randomly and continuously. Every attempt to transfer full message to D or closer to D is created in one Time Slot including zero Time Slot. In this Time Slot the node, which carries the message, creates a decision, if the message will or will not be sent to next node based on probability of delivery. This process is repeated until the message reaches the D or maximum number of attempts is reached.

For example, in our simulations, duration of Time
Slots were set on 15 sec, but it is possible to be changed.

Length of Time Slot has direct impact on delay of transfer. If the transfer of message was created by 6 nodes, minimum of delay could be 5 x 15 sec, or more, when some node carried a message longer time due to various reasons (node with message does not have a neighbour, next node was used, next node have not suitable probability of delivery, etc.).

Every node is moving in specific area (see Fig. 3). The moving direction was random from range 0-2π.

We limited the number of attempts (NOA) for every simulation. The NOA mean, how many time periods can be used for communication, because in every Time Slot is an attempt to send data to destination, or next node which is closer to destination (with suitable probability). This limitation can be perceived as maximum delay, which can be reached during transfer in our simulations.

Number of attempts (200 allowed attempts) means, how many attempts (Time Slots) can be used for sending data to destination or more closely to destination. NOA was set to value 200 for our simulations, but it can be changed for other simulations. It depends on our decision. It had impact on success of message delivery. Every simulation of SBOR was repeated 100 times for every level of velocity. All results in tables are statistic values from these repetitions.

3.1. Success of Delivery

This result shows the average percentage of success of data transferred between the S (node with number 9) and D (node with number 5) in MANET environment. Only successfully attempts are evaluated. Result of SBOR is compared with DSR protocol by the same deployment of nodes and movement for both protocols.

Result of simulations is displayed on the Fig. 4. and represents success of delivery for SBOR and DSR for five velocities levels of nodes: (1,4 m/s, 2,8 m/s, 5,6 m/s, 11,2 m/s and 22,4 m/s).

SBOR routing reached low success of delivery (22%) for slowest velocity (1,4 m/s). Increasing velocity was helpful for this type of transfer, when the success of delivery obtained 48% of success for velocity level 11,2 m/s. Successes of deliveries were about the same (48%-30%) for high velocity level (11,2 m/s and 22,4 m/s) with decreasing tendency. Simulations for SBOR compared to the simulations for DSR reach much better success of message delivery for higher velocities. The success of delivery is very similar for velocity 1,4 m/s for both protocols. For the same movement and every velocity level is SBOR more usable as DSR routing protocol due to dynamically changing network. Lower success of delivery for SBOR, especially for higher velocity is caused due to the use of random movement. Higher velocity will be able to influence success of delivery for SBOR in positive form, when the movement will not be random, but social.

3.2. Message Delay

This simulation was orientated to identify an average delay for success deliveries for SBOR and to discover this velocity which has the lowest delay when the message is successfully delivered to destination.

Result of simulations is displayed in the Chyba! Nenalezen zdroj odkazů. and represents average delay for successful deliveries of message for SBOR for five velocities level (1,4 m/s, 2,8 m/s, 5,6 m/s, 11,2 m/s and 22,4 m/s). Results in the Chyba! Nenalezen zdroj odkazů. show Standard deviation (4), Minimum and Maximum of delay for success deliveries.

\[
\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{x})^2}
\] (4)

N in the equation 4 represents number of success transfer of message to D, x_i represents delay or NOA for i

Fig. 3 Positions of 100 nodes at start of simulation

Fig. 4 Success of delivery for SBOR and DSR
3.3. Average Number of Attempts

This simulation was focused to identify, which velocity have the lowest average number of attempts (message overhead) during a message transfer in simulations. We wanted to compare successful and unsuccessful attempts to deliver message to destination.

Result of simulations is displayed in the Tab. 4 and it represents average message overhead for all attempts of transfer of message for SBOR for five velocities level (1.4 m/s, 2.8 m/s, 5.6 m/s, 11.2 m/s and 22.4 m/s).

SBOR routing reached higher NOA for low velocities 1.4-5.6 m/s. The lowest average NOA from all transfers of message to destination is for velocity 11.2 m/s.

Standard deviation (4) of average NOA was the lowest for velocity 1.4 m/s. Better pattern of mobility can decrease standard deviation, especially for higher velocities.

Tab. 4 Average number of attempts, Standard deviation and Min NOA for all deliveries

<table>
<thead>
<tr>
<th>Velocity [m/s]</th>
<th>1.4</th>
<th>2.8</th>
<th>5.6</th>
<th>11.2</th>
<th>22.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average NOA</td>
<td>177.99</td>
<td>136.51</td>
<td>138.82</td>
<td>125.33</td>
<td>147.27</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>51.3816</td>
<td>78.94</td>
<td>82.59109</td>
<td>84.3392</td>
<td>81.5106</td>
</tr>
<tr>
<td>Min NOA</td>
<td>14</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

3.4. Success of Delivery – Allowed Number of Attempts

In this simulation was compared an impact of maximum number of attempts (NOA) to success of delivery for given velocities.

The maximum NOA was 200 attempts. It was increasing from 5 to max NOA with step 5 and the mobility model was the same in every simulation. It is possible to be seen on the Fig. 5.

The difference among simulations was only in NOA. When the NOA was low, the lowest success of delivery was for slowest velocity. When the velocity was increasing, the success for given NOA was increasing.

4. Conclusion and Feature Work

In this paper, the Novel Social Based Routing Algorithm for MANET (SBOR) was introduced. Algorithm is based on analyses of the MANET and DTN [18] and [19]. The Proposed protocol is based on social relations among nodes. This one reach better results for average success of delivery as DSR protocol for the same deployment of nodes at the start of simulations, for the same movement and for the same couple of nodes, Source and Destination. SBOR can reach better result with new model of social mobility which will correspond with probability of delivery based on social behaviour of nodes. This new routing algorithm can be used as backup free method for transferring message (text, voice, photos, etc.) in society, but knowing that the message will probably be delivered with a delay, because it is based on DTN and social relations among nodes. Mobile nodes are represented by people and they have repeating pattern of movement during the time. It can be used for future innovation of this proposal. Using social information among nodes can be helpful for calculations of probability of delivery for sparse or disconnected networks, where mobile nodes move based on social pattern of mobility. Today we are working on designing of the new mobility model based on the social context.
especially to social movement of the mobile nodes.

Acknowledgements

The research presented in this paper was supported by the Ministry of Education, Science, Research and Sport of the Slovak Republic under the project VEGA 1/0075/15.

References


About Authors

**Martin MATIS** was born in Krompachy, Slovak Republic in 1990. He received the Ing. (M.Sc.) the Faculty of Electrical Engineering, Technical University of Košice, in 2014. His research interests include mobile ad-hoc networks, opportunistic and delay tolerant networks.

**Lubomír DOBOS** was born in Vranov nad Topľou, Slovak Republic in 1956. He received the Ing. (M.Sc) degree and PhD. degree in Radioelectronics from the Faculty of Electrical Engineering, Technical University of Košice, in 1980 and 1989, respectively. His scientific research area is: mobile communications and services, 5G networks, opportunistic and delay tolerant networks.

**Jan PAPAJ** was born in Liptovský Mikuláš, Slovak Republic in 1977. He is graduated at the Department of Computers and Informatics in 2001 and obtained his PhD degree in Telecommunications in 2010 from the Faculty of Electrical Engineering and Informatics at Technical University in Košice. His research interests cover the fields of mobile ad-hoc networks, opportunistic and delay
tolerant networks.