Computing and Informatics, Vol. 31, 2012, 1025–1044

SECURITY AND QOS INTEGRATION MODEL FOR MANETS

Anton Čižmár, Ján Papaj, Ľubomír Doboš

Department of Electronics and Multimedia Communications
Faculty of Electrical Engineering and Informatics
Technical University of Košice
Letná 9, 042 00 Košice, Slovakia
e-mail: {anton.cizmar, jan.papaj, lubomir.dobos}@tuke.sk

Abstract. The new model used to integrating security and Quality of Service (QoS) as one parameter in mobile ad-hoc network (MANET) is introduced and studied in this article. Security and QoS represent a highly important field of research in MANET and they are still being considered separately with no mechanisms used to establish cooperation between them. This new model provides alternative to cooperation between QoS and security via cross layer design (CLD) and modified security service vector. Performance analysis of the new designed model is introduced too. It is also considered herein how processing of the new integrating model affects the performance of the MANET networks.

Keywords: QoS, security, cross layer design, security service vector, MANET

1 INTRODUCTION AND CURRENT STATE

A mobile ad-hoc network (MANET) represents a set of mobile devices and nodes with self-configuring features and with the ability to mutually communicate (Figure 1). MANET nodes can establish and maintain connections as needed without fixed infrastructure and central management. MANET is characterized as a dynamic network with ability of the nodes to join or leave the network at randomly set times and ways. Current research trends in MANET are oriented to the following categories: QoS, security, cross layer design.

The field of QoS provides a wide space for research. The notion of Quality of Service (QoS) is a guarantee provided by the network to satisfy a set of predeter-

mined service performance constraints for the user in terms of the end-to-end delay statistics, available bandwidth, probability of packet loss, etc. [1]. There are many applications and services that require specific QoS guarantees. In literature, the research of QoS support in MANETs includes:

QoS models – specifying an architecture in which some kinds of services could be provided.

QoS routing – a part of the network layer, searches for a path with enough resources but does not reserve resources.

QoS adaptation – hides all environment-related features from awareness of the multimedia application above and provides an interface for applications to interact with QoS control.

QoS signaling acts – a control centre in QoS support. Functionality of QoS signaling is determined by the QoS model.

QoS MAC protocols – essential components of QoS for MANETs. MAC protocols solve the problems of medium contention, support reliable communication, and provide resource reservation.

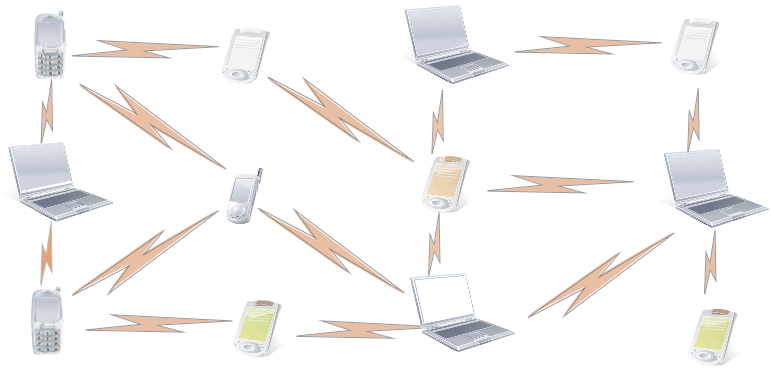


Fig. 1. Example of Mobile Ad-Hoc Network

Security has been studied since the beginning of computing, and some aspects, such as cryptography, were studied even earlier than that. The main goals of security requirements are: confidentiality, authentication, availability, integrity and non-repudiation [2]. The research of security support in MANETs includes [3]:

Secure Routing – there are two concepts regarding secure routing: one is exchanging routing information to keep the network connected and the other one involves secure data packet forwarding (SAAR, SAODV, ARIADNE).

Key Management – deals with secure key generation, key distribution, key storage and is to establish a shared secret between all participating parties.

Intrusion Detection System – collects and analyses audit data to detect unauthorized uses and misuses of computer systems. Intrusion detection is based on collection and analysis of system and network audit data.

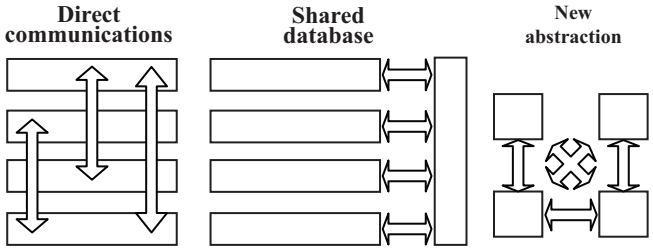


Fig. 2. Different types of cross layer design for MANET

The cross-layer design (CLD) approach is a new dynamic area of research into MANET networks. This approach provides new possibilities to increase the performance and adaptability of MANET [4]. Research of cross-layer networking is still at a very early stage, and no consensus exists on a generic cross layer infrastructure or architecture. The research carried out so far reflects diversity of the problems caused by the system dynamics in ad-hoc networks. Cross-layering is not simple replacement of a layered architecture nor is it a simple combination of layered functionality. Cross-layering tries to share information among different layers, which can be used as inputs for algorithms, for decision processes, for computations, and adaptations. There are 3 different architectures (Figure 2) [4]:

- Direct communication between non adjacent layers
- Shared database
- Heap architectures or completely novel approaches.

The specific characteristics of MANET leads to problems that the CLD is trying to solve, when the solutions can be divided into following areas [4, 5]:

Adaptation and self-organization – the system has included into the dynamics a wide range of communication conditions, a wireless node that can sense a number of features inside a MANET including changing topology, shared medium contention, varying traffic patterns and distributions.

Mobility – the nodes belonging to a MANET network may be mobile.

Energy control or power control – one of the greatest challenges in MANET is seen in solving the problems associated with low duration of terminal batteries.

Different QoS requirements – different kinds of media have different characteristics. QoS is responsible for distributing QoS requirements and restrictions along the whole protocol stack.

Security – the main purpose of a security task is to eliminate multiple layers of encryption. The other purpose is to eliminate security attacks.

Nowadays, in MANET the scientific community deals with the issues of QoS and security separately. Based on current understanding one can say that QoS and security present separate areas of research when one important fact is easily overlooked, namely that security and QoS as well as QoS and security mechanisms can affect, in negative sense, correct operation of the whole network and the overall network performance. In fact, it can affect the very functioning of QoS and security algorithms and may affect the provision of essential services required in the MANET. The issues of integrating QoS and security as a single parameter are just beginning to gain attention in MANET. So far, no ideas were designed that would enable the integration of QoS and security as a one parameter in MANET. In QoS literature, security is interpreted as a QoS dimension, but the process of integration has not been studied. The concept of security as a dimension of QoS has been suggested as a concept called variant security. The idea in this concept is that security mechanisms and services are considered to have a security range and a set of measurable security variables have been identified, which can be used to quantify a security attribute. The term *Quality of Security Service (QoSS)* has been coined by authors Irvine et al. [6]. A *security service vector (SSV)* has been presented to describe functional requirements of security policies. SSV was proposed to represent the level of services within the range of security services and mechanisms. The attributes of their security vector include security components, security services, level of security, and service area.

Basic ideas of the integration process are to provide QoS and security mechanisms at the same time, and that user or services had the possibilities to interact with system via CLD. Integration itself is necessary for proper functioning of both mechanisms in terms of QoS and security. Moreover, users can specify requirements for new services in MANET. In this article, we provide new model indicating how could security be integrated as a QoS parameter to the MANET via modified SSV and cross layer interface (CLI). CLI interface enables the user/system interaction and is also used to collect relevant information and to cooperate between application and network layers of the MANET layer model. Based on this information the system can evaluate and choose the optimum algorithms for achieving required parameters and guidelines. The modified SSV is used for cooperation between several blocks of the new model and also provides the decision algorithms for selection of routes. Model enables to specify requested parameters and the user has the ability to participate in the routing process. The advantage of this model is that it can be used for different services and not only for QoS and security.

2 QOS AND SECURITY INTEGRATION MODEL AS ONE PARAMETER IN MANET

2.1 Introduction of the New Integration Model of QoS and Security in MANET

We have designed a new model, which allows integrating security and QoS as a one parameter via modified SSV and CLD (Cross layer model) in MANET. Our model consists of 5 blocks as is shown in Figure 3 [7]:

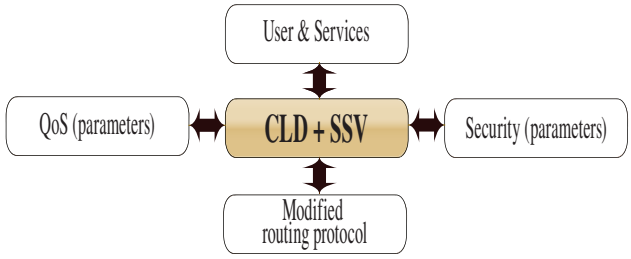


Fig. 3. Model of integrating QoS and security in MANET

The model includes all components for interactions between the user and system to integrate security as one parameter. The main block of our model is the block *SSV+ CLD*. CLD is used to create interactive environment between users and the system and, at a time, is used to support interactions between the routing protocol and modified security service vector (SSV). Block *QoS (parameters)* represents a mechanism for delivering of QoS in MANET network environments. It defines and specifies the QoS parameters necessary to provide the required services or information about what type of service a node can provide. Block *Security (parameters)* represents a mechanism to provide security-related services and also defines the necessary parameters used to process services providing. Block *User & Service* enables the interaction between the user and the system. The interaction with user means that user can define parameters for the type of service, which has to be achieved for services. Block *Modified routing protocol* represents the routing protocol with implemented modified SSV algorithm for selecting the optimal way based on user defined requirements (QoS and security).

2.2 Modified SSV for MANET

The main part of our model is modified SSV. Modified SSV is based on security service vector for IP networks [8, 9, 10]. Our modification takes into account all the requirements of MANET and MANET terminals and also MANET routing protocols. Modification of the SSV can be defined by two ideological parts: *user* and *system parts*.

The user part deals with process of collecting relevant data about requested services. In our case, these data are created by QoS and security parameters. Parameters can represent different QoS and security parameters or mechanisms for providing QoS and security processes [11]. In this model, users can specify the required parameters and using this approach can actively affect the system (routing) processes. The system part of modification represents the new method of processing collected data and also deals with routing processes of the routing protocol.

Based on requested parameters, nodes can accept/reject requested services or can provide service with lower degree of QoS and security. In MANET, there are three types of nodes: source, routing and destination. Each node has an implemented algorithm to process the routing packet (RP). Algorithms analyze the routing information stored in RP and analyze the information about requested parameters, QoS and security (rSSV). A main idea of modified SSV is shown in Figure 5. Proceeding and algorithm of modified SSV are shown in Figure 6.

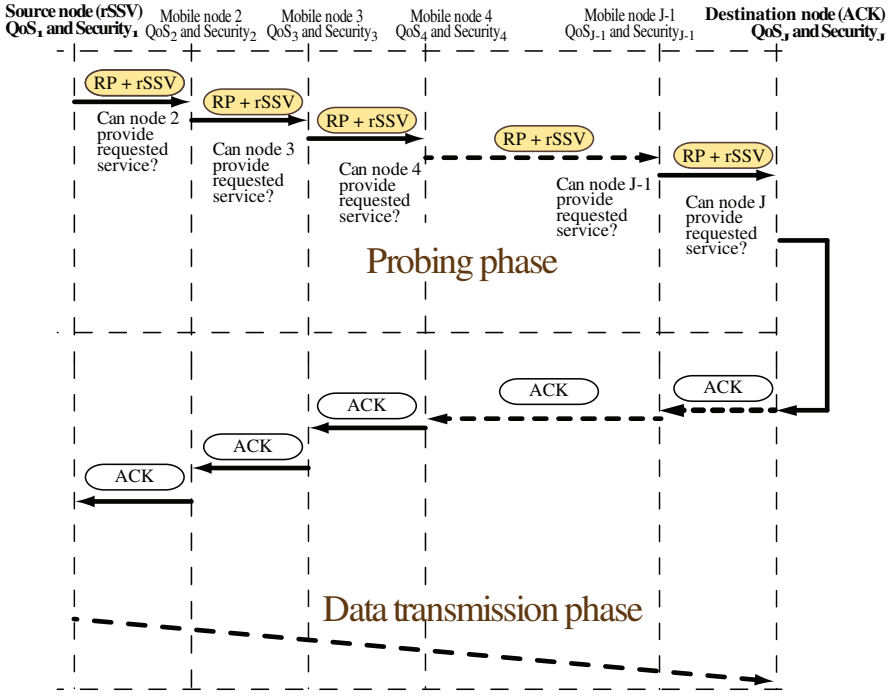


Fig. 4. Modified SSV in MANET

At the beginning, the source node collects information about QoS and security via cross layer interface (CLI). After collecting, data are stored to the modified route cache and routing packet (RP) is broadcast to the network. If the neighbor node receives a RP packet, the processing and analyzing phase is activated. This phase consists of two stages:

- Analyzing of arriving packet and collecting has the possibility to provide services.
- Application of the decision algorithm whether relevant node can provide requested service or not.

If a node cannot provide requested services, the complementary algorithm is activated. Next, the requested services (QoS_1 and $Security_1$, Figure 5) and own services on the routing nodes (QoS_J and $Security_J$, Figure 5) are analyzed. If the node can provide service on lower degree and data in the RP packet allow it, the node changes the level of service to a lower level and provides requested service. This alternation is stored to the modified route cache and then it is sent via RP to the next nodes. The process of analyzing is repeated till the destination node is found.

2.3 New CLI Model for Cooperation Between SSV and Routing Protocol in MANET

New cross-layer model (CLD) or cross layer interface (CLI) between non-adjacent layers was created for the purpose of interactions between the user and the system. This interface is used to collect QoS and security related data that are necessary for the modified SSV and modified routing protocol [11]. Modified SSV is also implemented in the dynamic source routing protocol (DSR). The task of our cross layer design is to enable transferring and collecting data from the application layer to the routing protocol operating on network layer. The collected SSV attributes consist of information about security and QoS parameter that a node is able to provide. The basic concept is shown in Figure 6.

In the CLD model, CLI interfaces are implemented in the network and application layers. CLI is used in three stages:

Control stage – is responsible for activating the processes of collecting QoS and Security related data.

Collecting stage – deals with processes of collecting and transmitting data from application/network layer.

Interaction stage – provides interaction between users and systems.

The process of collecting QoS and security related information is the same for all 3 types of nodes. In the case of source node, the user defines QoS and security via CLI interface located on the application layer (Figure 6). Collected data are marked as QoS_1 and $Security_1$, and are stored to modified route cache and to the RP (position rSSV) as well (Figures 4 and 5). In the case of routing and destination nodes, CLI interface collects QoS and security information from received routing packets (RP+rSSV) and collects information about QoS and security from modified route cache on the nodes and then activates decision-making process of SSV.

Function of modified SSV in MANET

Analyze type of node
Analyze QoS_j and $Security_j$ *mechanism on each node*
Create of the modified route cache memory
Storing of the QoS_j and $Security_j$ to the modified route memory by CLD interface

CASE type node is source node
Read QoS_1 and $Security_1$ from user by CLD
IF *QoS_j and $Security_j$ are the same or lower then can node provides* ***THEN***
Activation of CLI interface (CLI)
Send CLI request to CLD to activation of transition of the QoS_1 and $Security_1$
Storing of the QoS_1 and $Security_1$ to the modified route cache memory
Create modified RP with SSV (rSSV)
Storing QoS_1 and $Security_1$ to the packet and start routing processes

ELSE
Node can't provide requested service and stop routing on the node for this service
END
END

CASE node is routing node
Collects of RREQ Packets
Read parts SSV (QoS_1 and $Security_1$) from RREQ packets
Read QoS_j and $Security_j$ from modified route cache memory
Analyzing type of service from RREQ packets
IF *can provide requested services?* ***THEN***
Store route to the RREQ packet
Broadcast RREQ packet to the neighboring nodes
ELSE
Activate complementary algorithm to modify the QoS_j and $Security_j$
IF *is possible to provide service on other degree of service* ***THEN***
Decrease the level of service and store it to the modified route cache
Send RREQ packet with modified information about QoS_j and $Security_j$

ELSE
Stop routing and node can't provides requested services
END
END
END

CASE node is destination node
Read QoS_1 and $Security_1$ from RREQ packet
Read QoS_j and $Security_j$ from modified route cache memory
IF *node can provide QoS_j and $Security_j$*
Read route from packet
Select the route with respects to QoS_1 and $Security_1$
Send RP packet to source node
ELSE
Node can not provide requested services
Stop routing
END

Fig. 5. New designed CLD Model in MANET

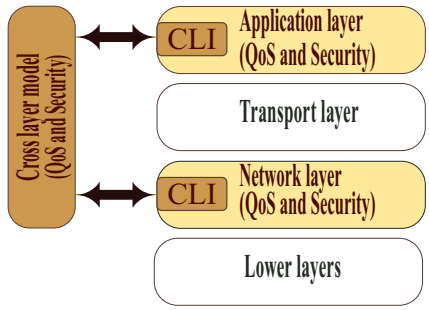


Fig. 6. New designed CLD model in MANET

3 EXPERIMENT SETUP

The main ideas of the simulations were to verify possibilities of implementing a new designed model in MANET terminals. All behavior of the proposed model was simulated in OPNET modeler 16.0 simulators and to evaluate effectiveness of integrating a new model with CLD and modified SSV three types of simulations were used:

- Model where the nodes used routing protocol DSR without modified SSV and CLD (DSR) – data are transmitted by each layer without CLD and modified SSV.
- Model where the nodes used modified routing protocol with implemented the modified SSV (DSR + SSV) – data are transmitted by each layer without CLD with implemented modified SSV.
- Model where the nodes used modified routing protocol with implemented modified SSV and CLD (DSR + SSV_CLD) – data are transmitted by new CLD interface and modified SSV is implemented.

To check functionality of the proposed model, modified SSV with CLD and the following parameters were used: time to processing, delay of MANET, total packet processing delay. The time to processing means the process time necessary to process all operations of data on nodes. Time is measured from the time of creation, from the application layer or from arrival on the physical layer. Delay of MANET represents the value of the average end-to-end delay measured from the network layer on the source node, where the MANET packet is created, to the delivery of the packet to the destination node and the processing time for SSV of information layers in source-target transport is also taken into account. Total packet processing delay represents the average delay in MANET networks from sending a packet to the adoption of the packet on the IP layer of the target node. The parameter does not reflect the time needed to process information SSV.

3.1 Simulations Setup

The 10 separated simulation scenarios that were formed of 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100 nodes were created to check the effectiveness of operation of the modified SSV and CLD in MANET. The size of the simulated area for simulations of 10, 20, 30, 40 and 50 nodes was $500 \times 500\,\mathrm{m}^2$ and for 60, 70, 80, 90 and 100 nodes $1\,000 \times 1\,000\,\mathrm{m}^2$. Simulated parameters were used to establish delay and total packet processing delay. Transmission power was set up to 1 mW.

The random mobility model was used to simulate the mobility of nodes. Speed ranged from 0 to $2\,ms^{-1}$. Simulation period was 1 000 seconds in all cases. Free environment without affecting interference was used as the simulation environment. The initial value of movement was a changing parameter, giving a different initial position of individual nodes in the simulated project. The result of each simulation was a set of values that were then statistically processed and evaluated. The number of values can be chosen in the simulator environment. In our case, each sample was made up of a set of 100 values from each simulation (10 000 values were recorded). All graphs showed the averages values.

3.2 Experiments

In order to compare the performance of real model and new designed model, CLD and modified SSV were implemented into MANET terminal and 5 types of experiments were simulated. The simulation setup was the same as that described in Section 3.1.

In the first experiment the processing time was analyzed. The first simulation was designed to measure the time of processing CLD and modified SSV activities on different type of nodes. This parameter represents the time required for processing and creating the modified packet. The term "processing", in the case of the source node, means the time since the creation of the requirements to transmit data at the application layer to the time of packet departure from the physical layer. It is the time of data arrival at the physical layer and of return to the physical layer in the case of routing node and the time necessary to perform required activities in the case of destination node. Simulation scenario consists of three nodes: source, destination and routing. Simulation was carried out 100 times and then the average processing time value was determined for different types of nodes. The main goal of simulations was to perform verification of the modified SSV for various types of nodes as well as verification of the activities proposed in the CLD model for MANET.

In the second experiment, the delay of MANET was analyzed. This parameter provides information about how long it takes to deliver a MANET packet from source to destination nodes, when it also includes the time that is essential for processing information and SSV for carrying out the activities of the SSV. Total delay of MANET presents an important parameter that refers to the time necessary to deliver a MANET packet from source to destination nodes and also includes

the time that is essential for processing information CLD and for carrying out the activities of the modified SSV.

The third experiment focuses on how SSV and CLD processing affects the total packet processing delay. This parameter represents the time necessary to transmit a packet from source to target through the MANET network, applied where a modified SSV algorithm and CLD are.

In the fourth experiment, it is monitored how increase in traffic, by applying the new designed model with modified SSV and CLD, can affect the network behavior. The burden in this case is seen as the number of nodes generating traffic (packets), thus becoming simultaneously the source, routing and destination nodes. To evaluate the impact the parameters of MANET network delay and delay time of service pacts were used, which represent averaged network values. The impact loading was studied for different networks consisting of 20, 40, 60, 80 and 100 nodes and randomly selected nodes to generate traffic. Simulation setup was the same as in 3.1.

In the fifth experiment it was studied how the process of increasing the nodes could affect the parameter of delay and total packet processing time. In each simulation, sets of nodes (20 %, 40 %, 60 %, 80 %) that could not provide user specified requirement for services were randomly generated. In this case, only two scenarios were compared, namely DSR + SSVD and DSR + SSV_CLD.

4 RESULTS

Results of monitoring the processing time depending on the type of node (first experiment) are shown in Figure 7. Processing time parameter is monitored on source, routing and destination nodes. Collected results showed that, in the case of source node, the implementation of the DSR + SSV increased the value of the processing time by 11.70 % as compared with DSR. When DSR + SSV_CLD was applied, values of the processing time were reduced by 19.09 % as against the DSR and by 24.89 % when compared with DSR + SSV. In the case of the routing node, the processing time increased slightly (by 4.76 %) as compared with the standard DSR protocol, and decreased after implementing DSR+SSV_CLD as compared with DSR (by 7.85 %) and DSR+SSV (by 12.14 %; Figure 7). When the DSR+SSV was implemented into the destination node, the processing time increased by 12.37 % as compared with DSR under the same conditions. Implementing DSR + SSV_CLD into the nodes represents processing time decrease when compared with DSR (by 16.80 %) and DSR_SSV (by 19.15 %). As shown, the implementation of CLD into the MANET model (DSR+SSV_CLD) provides time processing reduction compared with DSR model and model DSR + SSV.

Based on the obtained results we can conclude that the highest processing time reductions were achieved after integrating the DSR+SSV_CLD into the source node (about 24.89 %) and then into the destination node (about 16.80 %). The lowest reduction was recorded at the routing node (about 7.85 %). From this perspective,

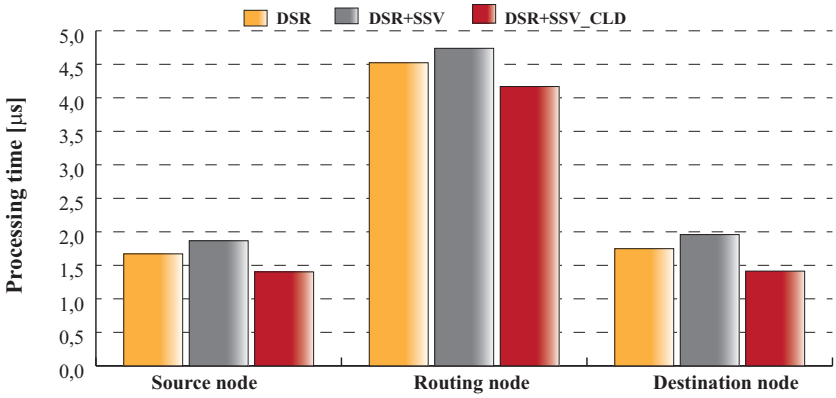


Fig. 7. Processing delay of MANET nodes

the integration of CLD appears to be an effective tool for acquiring and implementing the required activities mainly on the source and destination nodes.

Results of the second experiment, in which the delay of the MANET network was analyzed and studied, showed that the delays of the MANET increased by 20.21 % after implementation of DSR + SSV_CLD as compared with the standard DSR and by 27.24 % when using DSR + SSV (Figure 8).

However, applying DSR + SSV_CLD reduced the delay by 5.52 % as compared with DSR + SSV. The lowest increase of the delay value (comparison with standard DSR) was achieved for 50 nodes – the average delay after applying DSR + SSV_CLD increased only by 2.41 % and by 11.36 % using DSR + SSV as compared with the standard DSR protocol, and applying DSR + SSV increased by 11.36 % (Figure 8).

In the third experiment the total packet processing delay was analyzed. The obtained results are shown in Figure 9. Conversely, when DSR + SSV_CLD was applied in MANET consisting of 50 nodes, the total packet processing delay was reduced by 3.13 % against the standard DSR protocol. On the other hand, the application of the SSV + DSR meant achieving an increase (about 3.13 %).

In the fourth experiment, the performance of implemented modified SSV and CLD model in MANET in simulated real activities was studied. We analyzed how the changed numbers of nodes that generate traffic could change the parameters delay of MANET.

Figures 10 and 11 show the comparative delay of MANET and the total processing delay analyses when the numbers of nodes that generated the traffic (%) for different networks consisting of 20, 40, 60, 80 and 100 nodes were changed. Based on collected results, it can be concluded that the integration of modified SSV (DSR + SSV) into MANET layer model represented an increase in the values as compared with standard layer model (DSR). After applying cross layer model to MANET the delay was reduced, as compared with DSR + SSV. These situations could be caused by the following factors:

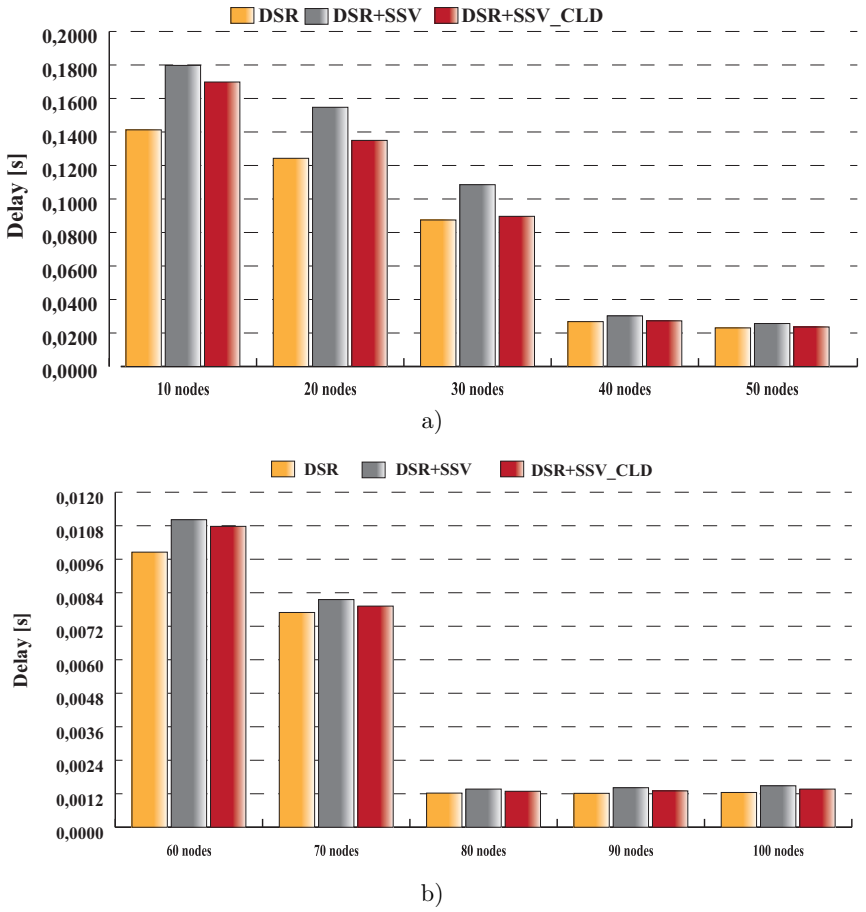


Fig. 8. Delay of MANET depending on the number of the nodes on the area: a) $500 \times 500\,\mathrm{m}^2$, b) $1\,000 \times 1\,000\,\mathrm{m}^2$

1. density distribution of nodes and their mobility – the values depended on the distribution and movement of nodes and
2. activity modified SSV and CLD – the delay would increase mainly by the decision algorithms at routing nodes.

The main idea of the fifth experiment was to determine the impact of the increasing number of nodes that fail to provide the required services to activity of modified SSV algorithm and the activity of MANET network itself. The effect of delays in the MANET network on timely delivery of packets when transmitting from the source to the destination node was analyzed. Since the standard DSR protocol does not allow comparison of this information, only two types of simula-

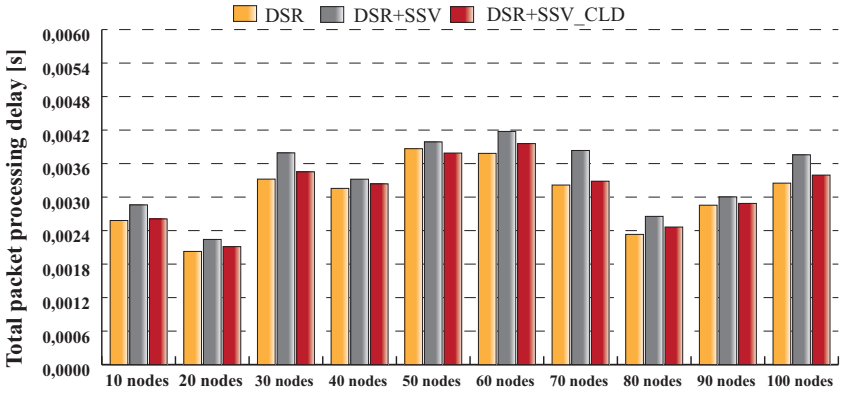


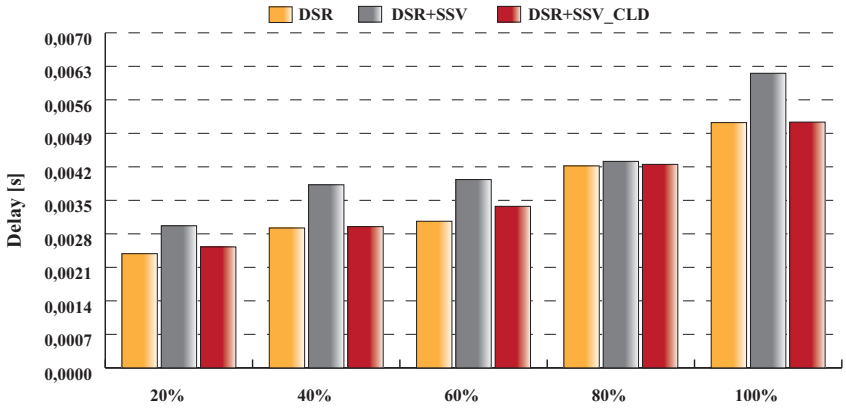
Fig. 9. Total packet processing delay for different MANET

Number of nodes	Model	20 %	40 %	60 %	80 %
20	DSR + SSV	0.00284	0.00174	0.00387	0.00452
	DSR + SSV_CLD	0.00253	0.00139	0.00326	0.00326
40	DSR + SSV	0.00220	0.00197	0.00263	0.00330
	DSR + SSV_CLD	0.00186	0.00181	0.00245	0.00299
60	DSR + SSV	0.00235	0.00261	0.00359	0.00431
	DSR + SSV_CLD	0.00229	0.00225	0.00306	0.00410
80	DSR + SSV	0.00243	0.00191	0.00157	0.00310
	DSR + SSV_CLD	0.00213	0.00173	0.00140	0.00389
100	DSR + SSV	0.00180	0.00164	0.00185	0.00200
	DSR + SSV_CLD	0.00147	0.00147	0.00175	0.00185

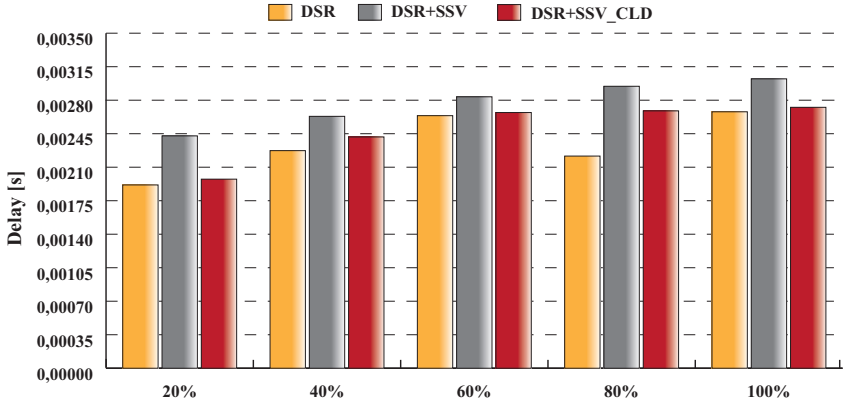
Table 1. Delay of MANET depending on the number of nodes incapable of providing the required services

Number of nodes	Model	20 %	40 %	60 %	80 %
20	DSR + SSV	0, 00267	0, 00943	0, 00334	0, 00385
	DSR + SSV_CLD	0, 00205	0, 00706	0, 00309	0, 00288
40	DSR + SSV	0, 00189	0, 00193	0, 00216	0, 00280
	DSR + SSV_CLD	0, 00175	0, 00158	0, 00195	0, 00266
60	DSR + SSV	0, 00257	0, 00244	0, 00227	0, 00314
	DSR + SSV_CLD	0, 00241	0, 00229	0, 00215	0, 00299
80	DSR + SSV	0, 00372	0, 00327	0, 00332	0, 00317
	DSR + SSV_CLD	0, 00316	0, 00301	0, 00320	0, 00299
100	DSR + SSV	0, 00125	0, 00135	0, 00158	0, 00604
	DSR + SSV_CLD	0, 00114	0, 00125	0, 00138	0, 00498

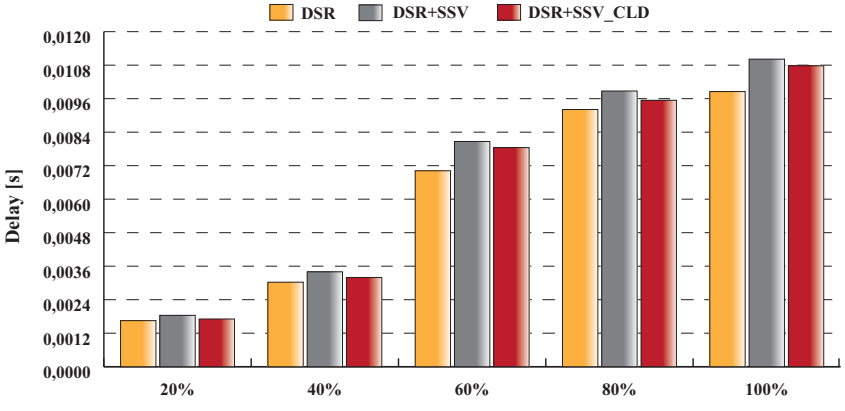
Table 2. Total packet processing delay of MANET depending on the number of nodes incapable of providing the required services


DSR
DSR+SSV
DSR+SSV_CLD
Delay [s]
0,0070
0,0063
0,0056
0,0049
0,0042
0,0035
0,0028
0,0021
0,0014
0,0007
0,0000
20%
40%
60%
80%
100%

a)


DSR
DSR+SSV
DSR+SSV_CLD
Delay [s]
0,00350
0,00315
0,00280
0,00245
0,00210
0,00175
0,00140
0,00105
0,00070
0,00035
0,00000
20%
40%
60%
80%
100%

b)


DSR
DSR+SSV
DSR+SSV_CLD
Delay [s]
0,0120
0,0108
0,0096
0,0084
0,0072
0,0060
0,0048
0,0036
0,0024
0,0012
0,0000
20%
40%
60%
80%
100%

c)

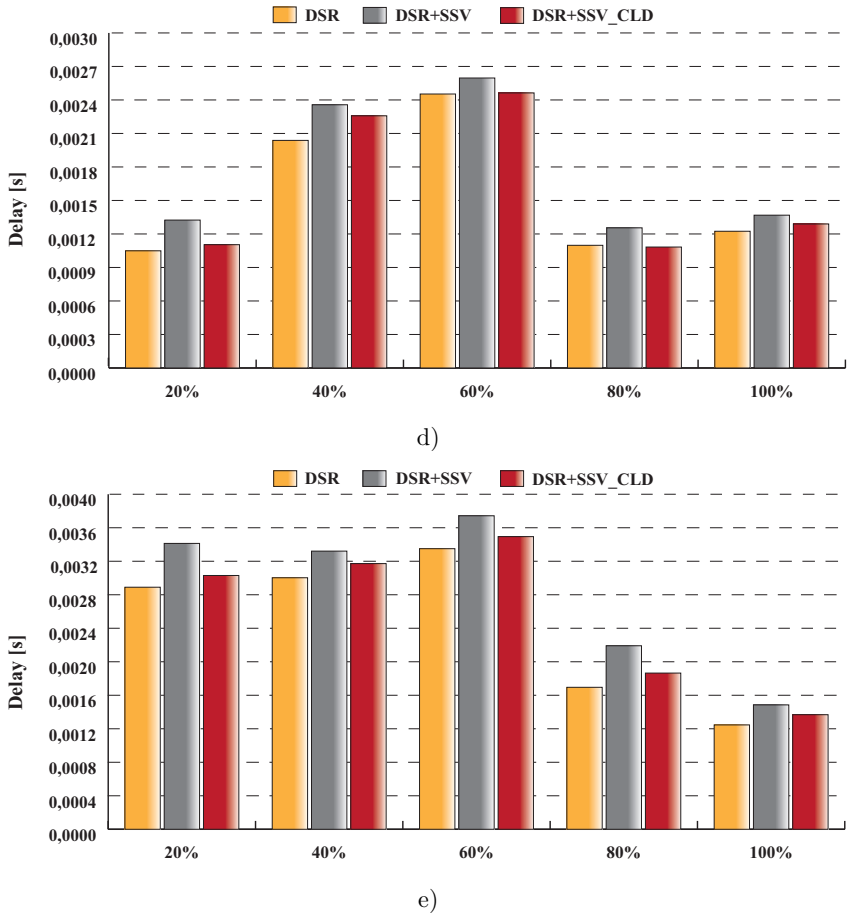
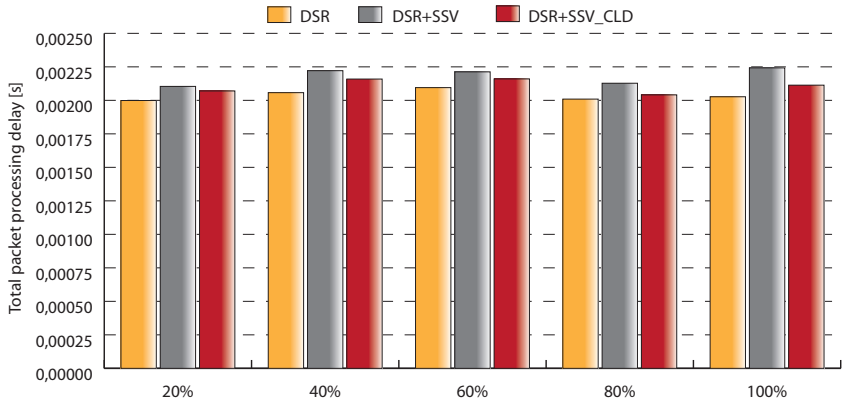


Fig. 10. Delay of MANET analysis depending on the number of nodes generated traffics: a) 20, b) 40, c) 60, d) 80, e) 100 nodes

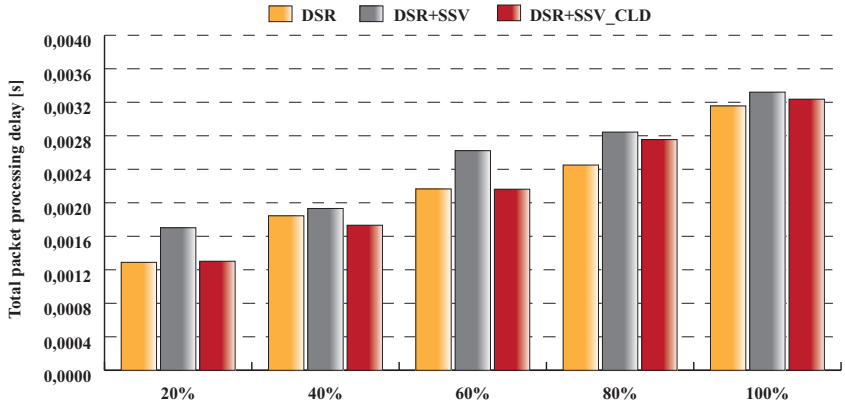
tions – using DSR routing protocol implemented with a modified SSV (SSV + DSR) and using a modified routing protocol implemented with a modified SSV and CLD (DSR + SSV_CLD) were compared. Table 1 indicates the values of the delay of MANET for different numbers of nodes that can not provide requested services and Table 2 shows total processing delay of MANET under the same conditions. In all cases the DSR + SSV_CLD provides better results than the model DSR + SSV.

5 CONCLUSIONS

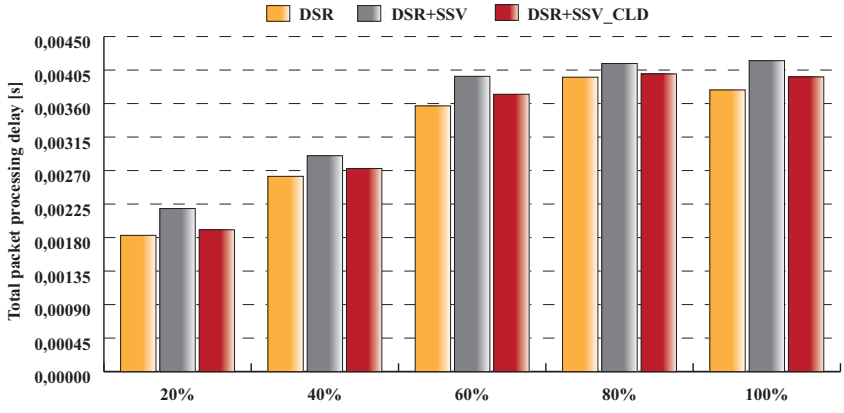
The article presents a newly designed model, which can be used to integrate QoS and security as a one parameter in MANET. The performance analysis was introduced


DSR
DSR+SSV
DSR+SSV_CLD
Total packet processing delay [s]
0,00250
0,00225
0,00200
0,00175
0,00150
0,00125
0,00100
0,00075
0,00050
0,00025
0,00000
20%
40%
60%
80%
100%

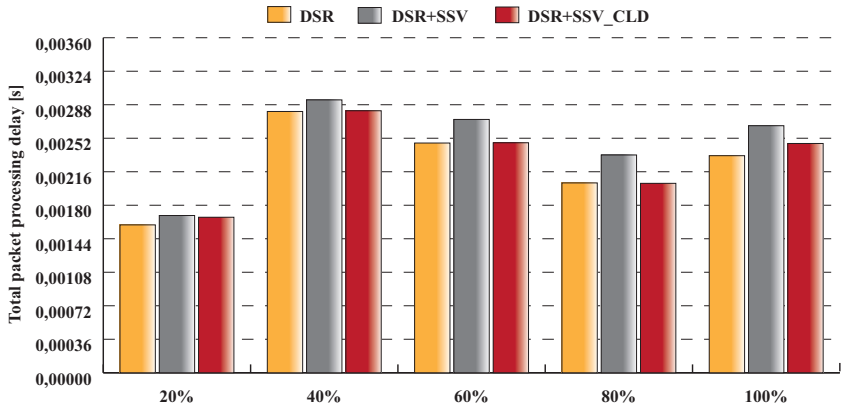
a)


DSR
DSR+SSV
DSR+SSV_CLD
Total packet processing delay [s]
0,0040
0,0036
0,0032
0,0028
0,0024
0,0020
0,0016
0,0012
0,0008
0,0004
0,0000
20%
40%
60%
80%
100%

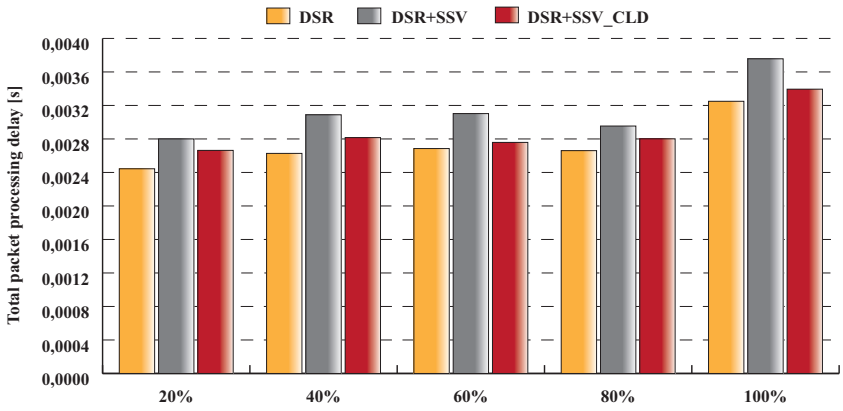
b)


DSR
DSR+SSV
DSR+SSV_CLD
Total packet processing delay [s]
0,00450
0,00405
0,00360
0,00315
0,00270
0,00225
0,00180
0,00135
0,00090
0,00045
0,00000
20%
40%
60%
80%
100%

c)



d)



e)

Fig. 11. Total packet processing MANET analysis delay depending on the number of nodes generated traffics:a) 20, b) 40, c) 60, d) 80, e) 100 nodes

and tested too. This new integration model provides a new way how QoS and security related services could be provided in parallel and also provides new ideas as to how new models could be designed to provide different service types. Our designed model can be used for different service types or for different applications. Based on collected results, we can state that the new model that integrated the new modified SSV model with CLD (DSR + SSV_CLD) reduced the processing time as compared with standard DSR model and the DSR + SSV model. The results obtained in delay and total packet processing delay indicate that to integrate the modified SSV with CLD resulted in insignificant increase of delays of the MANET network and of total processing delay. When performance of implemented modified SSV and CLD model in MANET was simulated, comparable results were achieved in

the DSR model. Deviations were caused by that activity modified SSV and physical parameters MANET network.

Acknowledgment

The research described in the paper was financially supported by INDECT (FP7 No. 218086) and by the Ministry of Education of Slovak Republic under VEGA 1/0386/12 and MŠ SR 3928/2010-11.

REFERENCES

[1] Gerla, M.: Ad Hoc Networks: Emerging Applications, Design Challenges and Future Opportunities. Ad Hoc Networks: Technologies and Protocols, Vol. 1, 2004, pp. 1–45.

[2] Djenouri, D.—Khelladi, L.—Badache, A. N.: A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks. Communications Surveys & Tutorials, IEEE, Vol. 7, 2005, No. 4, pp. 2–28.

[3] Patwardhan, A.—Parker, J.—Joshi, A.—Karygiannis, A.—Iorga, M.: Secure Routing and Intrusion Detection in Ad Hoc Networks. Third IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, 2005, pp. 8–12.

[4] Srivastava, S.—Motani, M.: The Road Ahead for Cross-Layer Design. Proceedings of 2005 2nd International Conference on Broadband Networks. IEEE, 2005, pp. 551–556.

[5] Carneiro, G.—Ruela, J.—Ricardo, M.: Cross-Layer Design in 4G Wireless Terminals. IEEE Wireless Communications Magazine, Vol. 11, 2004, No. 2, pp. 7–13.

[6] Irvine, C. E.—Levin, T. E: Toward Quality of Security Service in a Resource Management System Benefit Function. Proceedings of the 2000 Heterogeneous Computing Workshop (HCW '00),Cancun, Mexico, May 2000, pp. 133–139.

[7] Papaj, J.—Doboš, Ľ.—Čižmár, A.: Performance Analysis of New Integration Model of Security and Qos as One Parameter in MANET. Journal of Electrical and Electronics Engineering, Vol. 4, 2011, No. 1, ISSN: 1844-6035, pp. 169–172.

[8] Sakarindr, P.—Ansari, N.—Rojas-Cessa, N.—Papavassiliou, S: Security-Enhanced Quality of Service (SQoS) Networks: A Network Analysis. Military Communications Conference MILCOM, IEEE, Vol. 4, 2005, pp. 2165–2171.

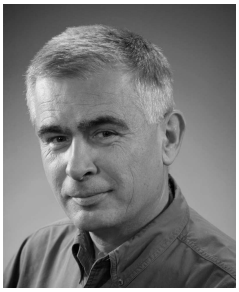
[9] Yang, J.—Ye, J.—Papavassiliou, P.: A New Differentiated Service Model Paradigm via Explicit Endpoint Admission Control. Eighth IEEE Symposium on Computers and Communications (ISCC 2003), 2003, pp. 299–304.

[10] Sakarindr, P.—Ansari, N.—Rojas-Cessa, N.—Papavassiliou, S: Security-Enhanced Quality of Service (SQoS) Networks. IEEE Sarnoff Symposium on Advances in Wired and Wireless Communications, 2005, pp. 129–132.

[11] Papaj, J.—Čižmár, A.—Doboš, Ľ.: Implementation of the New Integration Model of Security and QoS for MANET to the OPNET. Communications in Computer and Information Science, 149 CCIS, ISSN: 1865-0929, 2011, pp. 310–316.

Anton Čižmár works as the Rector of the Technical University of Košice (FEI TU) and as Full Professor at the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics. His research interest includes broadband information and telecommunication technologies, multimedia systems, telecommunication networks and services, man-machine communication. His scientific research topics include broadband information and telecommunication technologies, multimedia systems, telecommunications networks and services, 4^{th} generation mobile communications systems, localization algorithms.

Ján Papaj works as a researcher at the Faculty of Electrical Engineering and Informatics of the Technical University of Košice (FEI TU) and his research interests are in mobile ad-hoc network (MANET), routing protocols and techniques, QoS and security in MANET, cross layer design, sensor networks, opportunistic and cooperative networks.



Ľubomír Doboš works as a Vice Dean of the Faculty of Electrical Engineering and Informatics of the Technical University of Košice (FEI TU). His scientific research topics include broadband information and telecommunication technologies, multimedia systems, telecommunications networks and services, 4^{th} generation mobile communications systems, localization algorithms.