Integration of modified Security Service Vector to the MANET

Anton Čižmár, Ľubomír Doboš and Ján Papaj
Department of Electronics and Multimedia Communications,
Faculty of Electrical Engineering and Informatics, Technical University of Košice,
Letná 9, 042 00 Košice, tel. 055/602 4220, E-Mail: anton.cizmar@tuke.sk, lubomir.dobos@tuke.sk, jan.papaj@tuke.sk.

Abstract *– A mobile ad-hoc network (MANET) is infrastructure-less, self-organized networks that either operate autonomously or as an extension to the wired networking infrastructure. MANET is expected to support new QoS and security-based applications and new services. Nowadays, the QoS and security are very important areas of research in MANET, but are consider separately with different objectives and architectures. No protocols or systems are designed to integration QoS and security to the integrated compact system in MANET. We design new complex user-based model to interaction between User, QoS, Security and Dynamic Source Routing protocol (DSR) via Security Service Vector (SSV). The main challenge is provide the ability to configure own level of QoS and security, and provides user's new abilities of configuring requirements to QoS and security. This paper examines the integration of modified SSV to the MANET. The DSR is modified to implement SSV. We show and simulate basic principle and operations of this process.*

Keywords: *MANET, QoS, Security, Security Service Vector*

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of mobile nodes that are self configuring and capable of communicating with each other, establishing and maintaining connections as needed. Nodes in MANET are both routers and terminals. These networks are dynamic in the sense that each node is free to join and leave the network in a random way.

The notion of QoS is a guarantee provided by the network to satisfy a set of predetermined service performance constraints for the user in terms of the end-to-end delay statistics, available bandwidth, probability of packet loss, and so on [1]. In literature, the researches QoS support in MANETs include ***QoS models***, ***QoS resource reservation signaling***, ***QoS routing*** and ***QoS Medium Access Control (MAC)*** [1].

Security is an area that 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 following: Confidentiality, Authentication, Availability, Integrity and Non-repudiation. In literature, the researches security support in MANETs includes ***Secure routing***, ***Key management*** and ***Intrusion Detection System*** [2].

Security and QoS are very important areas of research. It's interesting that area of QoS is not as old as security but has been extensively addressed by researchers and practitioners. In QoS literature, security is interpreted as a dimension QoS, but 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 [3].

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 at al. [3].

Today in MANET, Security and QoS related systems have different objectives and architectures, but security mechanisms may severely affect QoS mechanisms in terms of network performance and data confidentiality. A security service vector (SSV) has been presented to describe functional requirements of security policies. The 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.

We provide basic idea how we could integrate security as a QoS parameters to the MANET via SSV. The integration provides the user new abilities to configure QoS and security requirements via routing protocol. The integration implies that users have opportunity to configure their own level of security and QoS parameters for services. A necessary component in a SSV is the service model which contains the provided services and their QoS and security parameters. The Dynamic Source Routing protocol (DSR) is used to integration SSV to the new designed model.

II. CONCEPT OF SECURITY SERVICE VECTOR

Concept of Security Service Vector (SSV) is introduced in [4]. QoS system controls numbers of requirements and incoming traffic. When it receives very large amount of incoming traffic from the same source or same destination, system alerts the security

system to verify whether the network is being under attack. Report log is stored for subsequent analysis. Quantitative zone is deployed to keep some packets as suspicious attacking packets while waiting for the user's confirmation.

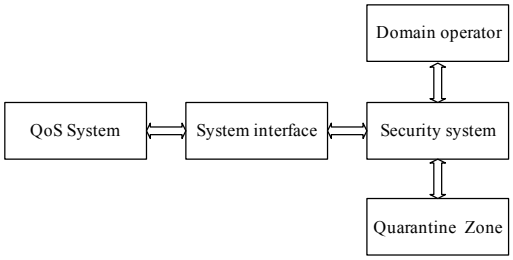


Fig. 1. The SSV architecture in wired network

The SSV architecture was proposed to cooperation between QoS and security mechanisms in wired networks (Fig.1) [5].

Security vector (SV) was proposed to determine a number of customizable Security Services (SSs) with choices of customizable Service Degrees (SDs) [6]. Let be a security service vector, consisting of j security service vector portions, where each vector portion is dedicated to every node. The SSV portions of each intermediate node are in the form of

$$\|SSV\| = \bigcup_{j=1}^{J} \|SSV\|_j \equiv \{(SS^1, SD_m), ..., (SS^N, SD_m), [x]\}_1, ..., \{(SS^1, DS_m), ..., (SS^N, SD_m), [X]\}_J \quad (1)$$

Where X denotes other information that can be attached, for example estimated cost, time and data length. There are two communication phases taken place for data transmission: ***probing phase and data transmission*** (Fig.2).

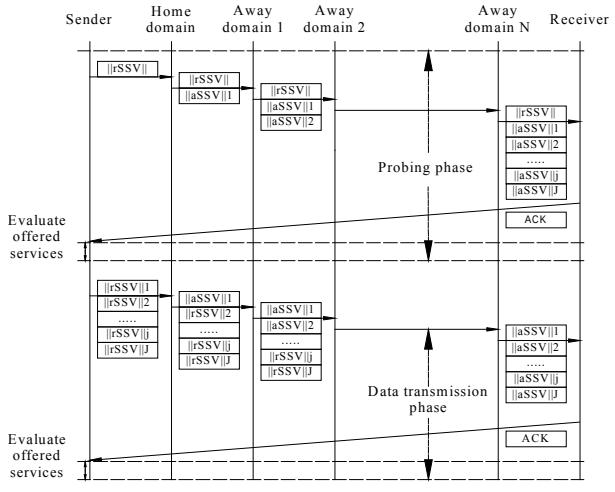


Fig. 2. The SSV transition diagram

The probing phase happens during connection establishment and the data phase starts after the connection has been set up. During the probing phase, the sender who wants to exercise security service options sends the probing packet through all domains along the path. The probing packet verifies whether satisfied security services can be offered along with sufficient resources for the following data packets. This probing packet contains the same requested SSV (rSSV) for every domain. The rSSV portion in the probing phase is:

$$\|\text{rSSV}\| = \{(SS^1, SD_m), ..., (SS^N, SD_m), [\text{data\_leng ht}]\} \quad (2)$$

Along with the requested services, the size of data sample is attached so that intermediate routers can estimate delay and processing cost. Any edge router performs the following basic tasks: verifying the sender's identity; examining the rSSV; verifying whether the sender has a privilege to request the services; checking available resources; writing down its aSSV portion; and forwarding the probing packet to the next hop. The probing packet is repeatedly forwarded through intermediate routers to the receiver, who replies to the querying user with an acknowledgement (ACK) packet. The receiver replies with an ACK packet containing all available SSV (aSSV) portions to the sender. The sender then evaluates all services offered and concludes whether to proceed to the data phase or to drop this connection and try again later. If there are J intermediate edge routers along the path, the ACK packet carries J aSSV portions, one for each router, denoted as

$$\|aSSV\| = \bigcup_{j=1}^{J} \|aSSV\|_j \equiv (SS^1, SD_m), ..., (SS^N, SD_m)\{(SS^1, SD_m), ..., (SS^N, SD_m), [delay, time\_process, cost]estimated\}_1, ..., (SS^1, SD_m), ..., (SS^N, SD_m)\{(SS^1, SD_m), ..., (SS^N, SD_m), [delay, time\_process, cost]estimated\}_J \quad (3)$$

At the end of the probing phase, the querying user retrieves information from all aSSV portions carried in the ACK packet. Information in each portion includes a pair of service and the degree offered by each router, the estimated delay, processing time, and cost with regard to the sample data length (in bytes). Then, both security-related and non security-related utility functions are used to evaluate and maximize the user's benefits subject to several constraints. If the benefits are not satisfied, the connection request is discarded. Otherwise, the user proceeds to the data transmission phase.

Satisfied with the evaluation result, the user starts the data transmission phase during which the data flow is attached with security-related information and sent through the network. In other words, the rSSV portions, one for each intermediate router, are attached to each data flow [6]. The rSSV portions in the data transmission phase are denoted as

$$\|rSSV\| = \bigcup_{j=1}^{J} \|rSSV\|_j \equiv \{(SS^1, SD_m), ..., (SS^N, SD_m)\}_1, ..., \{(SS^1, DS_m), ..., (SS^N, SD_m)\}_J \quad (4)$$

Upon arrival at each router, a router picks up its associated rSSV portion and executes the security services requested individually. The requested services may be rejected if the service degree is downgraded from the one chosen by the querying user or if the service is entirely unavailable due to insufficient resources. After the security services were served, each router records the results by replacing the corresponding

rSSV portion with the aSSV portion to report the querying user. Upon arrival of the data packet, the receiver may reply either immediately upon arrival of a data packet or after a delay for several data packets with an ACK packet. The user evaluates whether the packet has received the records of served services and other QoS requirements, along with the total cost, which will be charged to the user's account. The service provider also records the network performance to improve future services. The querying user retrieves information from the ACK packet, containing all aSSV portions, denoted as

$$\|aSSV\| = \bigcup_{j=1}^{J} \|aSSV\|_j \equiv$$
$$\{(SS^1, SD_m), \ldots, (SS^N, SD_m),$$
$$[delay, time\_process, cost]served\}_1, \ldots,$$
$$(SS^1, SD_m), \ldots, (SS^N, SD_m)\{(SS^1, SD_m), \ldots, (SS^N, SD_m),$$
$$[delay, time\_process, cost]served\}_J \quad (5)$$

The SSV consists of two sides: ***user*** and ***network sides*** and it is beneficial to both [5]. From the user side, users have the possibility to specify their own security and QoS requirements to the traffic flow, and can define set of parameters divided into two groups: ***security-related parameters*** (data rate, loss rate, and delay) and ***security-related parameters*** (processing rate, delay, and service and degree blocking rate). These parameters should maximize the user's benefits, subject to the user's budget and transmission QoS requirements, as well as to optimize the network performance. Another advantage of SSV is that the user has possibility to analyze report message if a problem occurs. From the network side, the cooperation between security and QoS mechanism boosts the network performance. Also the SSV and cooperation mechanism can prevent and reduce some types of security attacks.

II. PROCESS OF INTEGRATION SSV TO THE MANET

The new architecture is designed to cooperation between users, services, QoS, security and routing mechanisms via SSV in MANET (Fig.3).

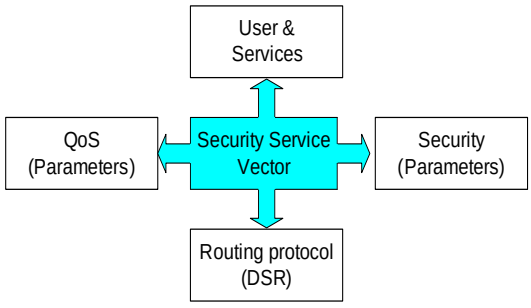


Fig. 3. New architecture to integration SSV to the MANET

In this model, the user specify QoS and security-related requirements on services or applications via SSV and then the routing protocol selects an appropriate route to the destination, and consequently the network can provide the user-requested services. The 'appropriate' means that all nodes around the selected way can fulfill selected requirements to QoS and security requirements. In this work, the services are divided to the three classes: High SSV, middle SSV and standard SSV and consequently each class can have one of the three service degrees: high, middle and low. Service level is common title used for classes and service degrees. High SSV service is services very sensitive to QoS and security parameters. Middle service provides service with specified QoS or security requirements. Standard service is service without special QoS and security requirements. Each services have own service degree. High degree mean the service can't change service degree to the lower level, the node can provide only service with specify requirements. Middle degree means the service can operate on required level of QoS and security but one of the parameters can be change in the case the node couldn't provide requested service. Low degree provides service with possibility to change QoS and security based on current states of the nodes. After process of collecting SSV information, the decision process of routing protocols is started as it shows Fig.4.

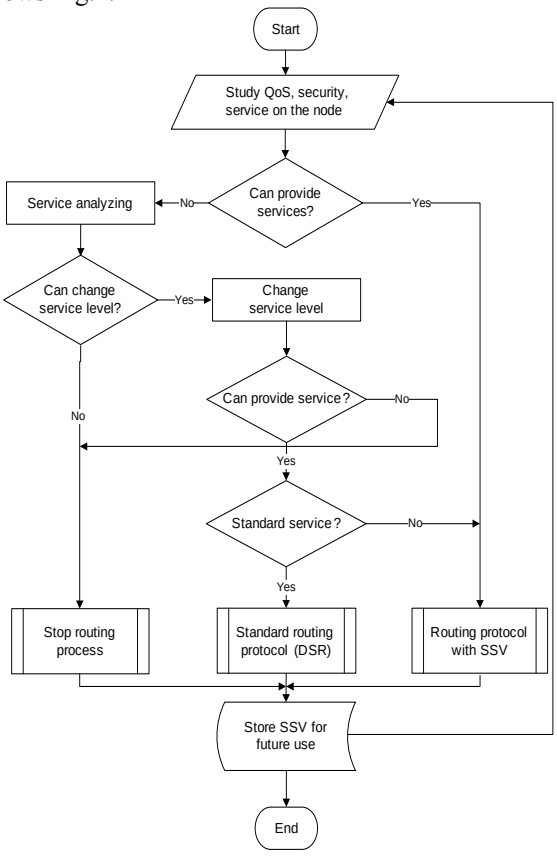


Fig. 4. Selection process of the routing protocol in MANET

The SSV is implemented to the modified DSR. DSR protocol is a simple and robust routing protocol designed for use in multi-hop wireless ad-hoc networks of mobile nodes [7]. Process of integration SSV to MANET is divides to following phases [8]:

- ***Probing phase (route discovery RREQ) and route replay RREP***
- ***Data transmission phase***

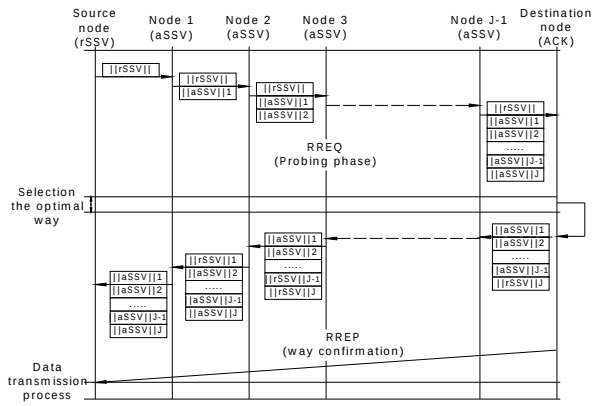


Fig .5. Implementation of SSV to the MANET

Fig. 5 illustrates the main idea of implementation SSV to the MANET. In first phase, the user (source node) defines its own requirements for QoS and security and then start proces of selection of the routing protocol (Fig. 4). The QoS and security related parameters and services are studied on each MANET nodes. The collected information are stored to the SSV cache and are available for future use, when probing (RREQ) packets are arrived. If node change service level, the new values rewrite corresponding value SSV in SSV cache on the nodes.

In second phase, the user (source node) who wants to make security-related service with another user (destination node) or server, sends the modified route request packet to the all-intermediate nodes along the source. Request packet contains requirements specified for QoS and security-related services (aSSV and rSSV portions) as it shows Fig. 6.

Option Type	Opt.Data Len	Indentification
Target Address + rSSV		
Address[1] + aSSV		
Address[2] + aSSV		
……		
Address[n] + aSSV		

a)

Option Type	Opt.Data Len	L	Reserved
Target Address + rSSV			
Address[1] + rSSV			
Address[2] + rSSV			
……			
Address[n] + rSSV			

b)

Option Type	Opt.Data Len	F	L	Reser.	Salvage	Segs . Lft
Target Address + rSSV						
Address[1] + aSSV						
Address[2] + aSSV						
……						
Address[n] + aSSV						

c)

Fig. 6. Modification of DSR header packet a) route request RREQ, b) route replay RREP, c) source route packet

If intermediate node is not the destination node, added is information about possibilities of provisioning requested services. This information is added to the relevant aSSV and then is sent to another intermediate node. This process is called route discovery and corresponds with Probing phase.

Process of collecting aSSV information is executed till the destination node is found. When destination node is found, route is written to the source node route cache memory and destination node rewrites all aSSV information into the rSSV information. This packet is then called ACK packet.

The ACK packet is sent back to the source node. Fig. 7 shows RREQ phase from source to destination node, describes how source and intermediate nodes behave when RREQ packet is arrived.

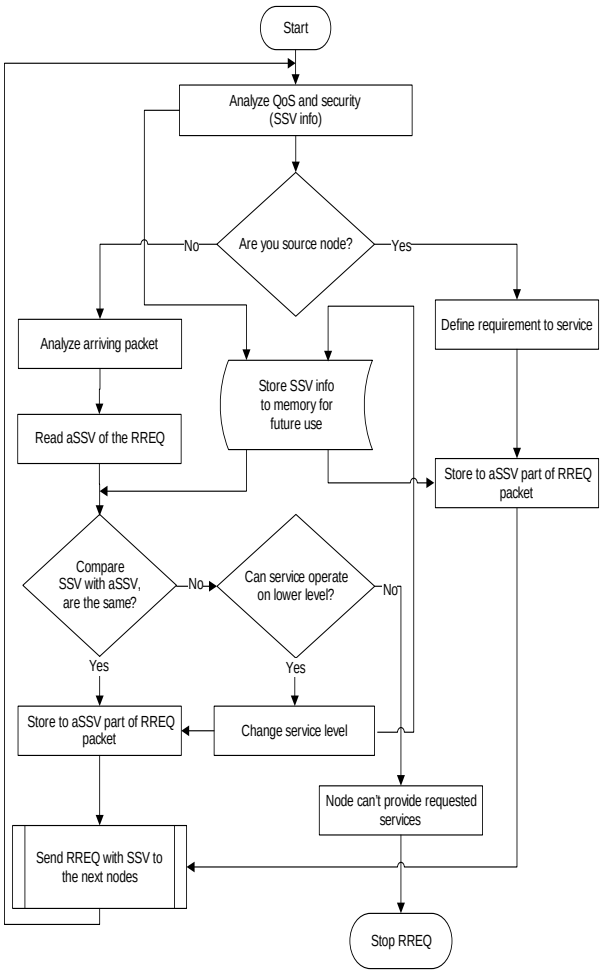


Fig. 7. Modified DSR Probing phase RREQ

III. SIMULATION AND RESULTS

The simulations are performed in OPNET simulator. The integration process SSV to the MANET is simulated. The SSV is implemented to DSR routing protocol. The DSR and modified DSR with SSV are used to compare of acquired data. For simplification of simulations, we simulate only probing phase (RREQ) as it shows Fig. 4 and Fig. 7. We create simple project with two scenarios. All scenarios contain 10 MANET nodes. On each node random information about QoS, security and service level was generated. In first scenario the standard MANET with DSR is simulated. In second, the modified DSR with SSV is simulated.

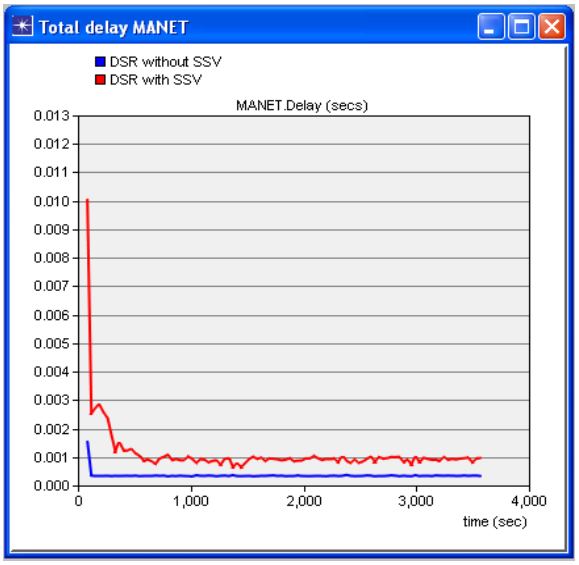


Fig. 8. Total delay of the MANET

Delays caused by adding process SSV was an observed parameter of simulation. Total delay of MANET network illustrates Fig.8. We can see the integration of SSV to DSR influence minimaly the total delay of the tested MANET network.

Fig.10 shows how the SSV integration process affects delay of the DSR routing process on different nodes (source node, intermediate node and destination node).

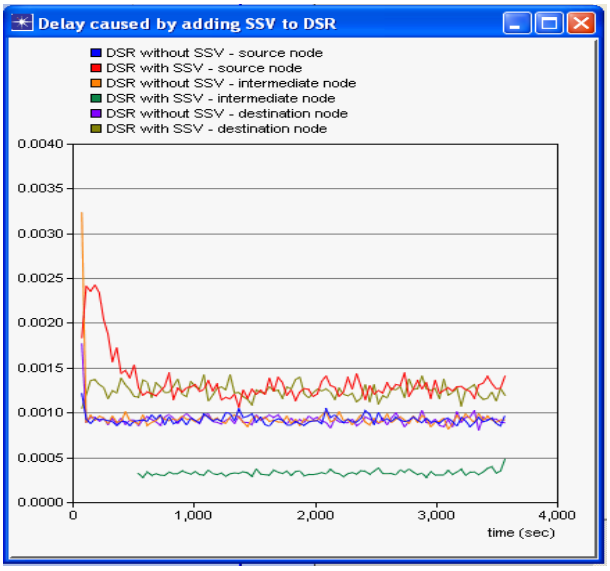
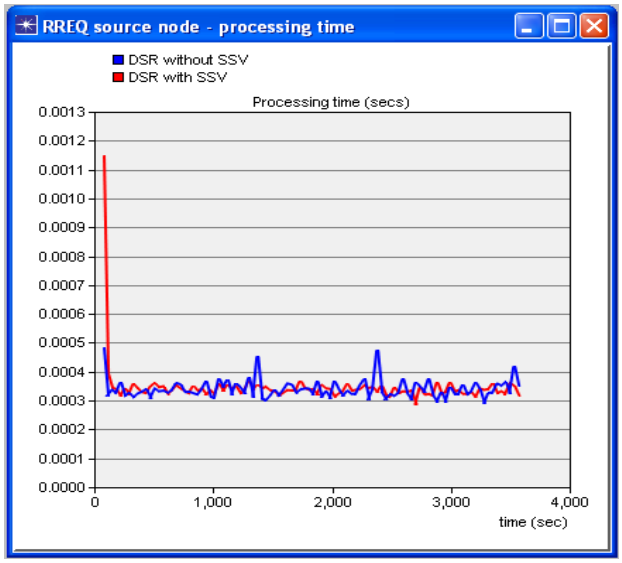


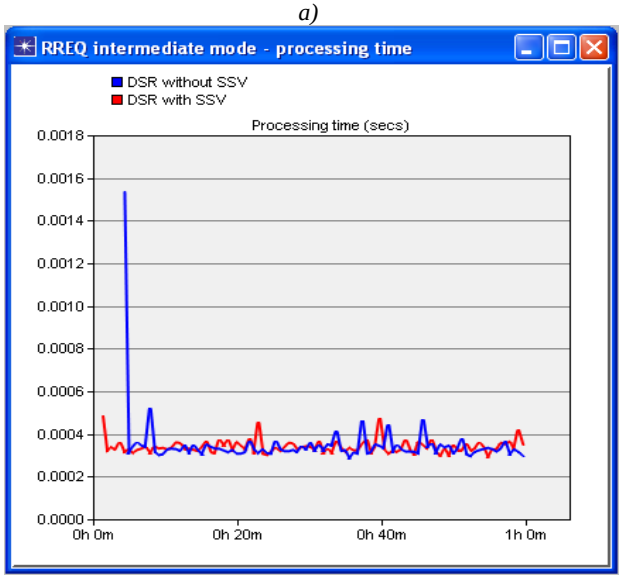
Fig.9. Delays on source, intermediate and destination node

Next parameter is processing time. It is time necessary to execute all SSV processes to integrate to the DSR on the nodes.

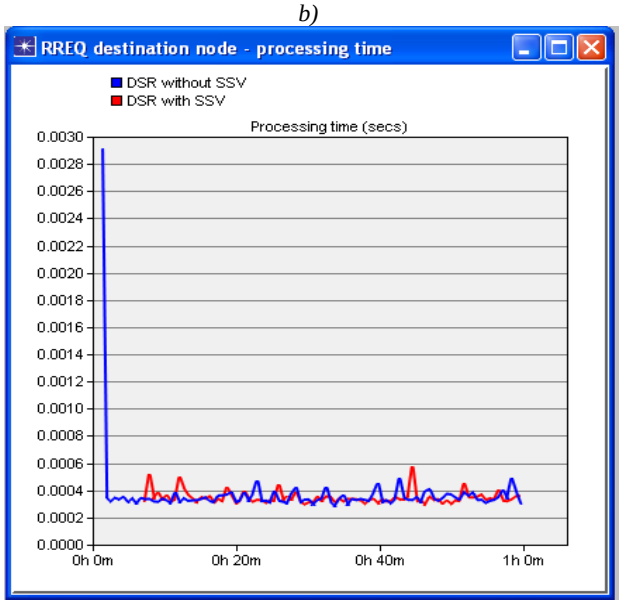
Fig. 10 shows the processing time of the process adding SSV on source, intermediate (router) and destination node.



a)



b)



c)

Fig. 10. Processing time a) source node, b) intermediate node, c) destination node

IV. CONCLUSIONS

Today, The QoS and security are very important areas of research in MANET and QoS and security related mechanism or models don't provide user's ability to change level of requested parameters or services. In the present work we overview new, user-oriented QoS and security related model, in which the user specifies its own requirements on QoS and security. All components are interactive cooperated via SSV. We show the integration do not extremely increase total delay of sending probing packet between source and destination node as we can see on the Fig.8-10. Next part of our work will be dedicated to implement SSV as a part of new model. In the foreseeable future we will specify methods for extending architectures, including QoS and security and services. We will define new evaluation paradigm of integration security as one of QoS parameters to the MANET. Users will have the ability to select levels of QoS that reflect their actual requirements, and the new model will reflect users demand to QoS and security.

ACKNOWLEDGMENTS

Research described in the paper was financially supported by VEGA No.1/4054/07, also by COST 2100 - Pervasive Mobile & Ambient Wireless Communications and INDECT (FP7-No.218086).

REFERENCES

[1] S. Chakrabarthi, A. Mishra, "QoS Issues in Ad Hoc Wireless Networks", IEEE Communications Magazine, pp. 142 –148, Feb. 2001.

[2] H. Yang, Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions (2004)". IEEE Wireless Communications. 11 (1), pp. 38-47. Postprint available free at: http://repositories.cdlib.org/postprints/618.

[3] C. E. Irvine and T. E. Levin, " Toward quality of security service in a resource management system benefit function." In Proceedings of the 2000 Heterogeneous Computing Workshop (HCW'00), pp. 133–139, Cancun, Mexico, May 1, 2000.

[4] P. Sakarindr, N. Ansari, R. Rojas-Cessa, S. Papavassiliou, "Security-enhanced quality of service (SQoS) networks", IEEE Sarnoff Symposium on Advanced in Wired and Wireless Communications, pp. 129-132, , April 2005.

[5] J. Yang, J.Ye, S. Papavassiliou, "A new differentiated service model paradigm via explicit endpoint admission control", in Proc. SCC2003, pp. 299–304, Jun. 2003.

[6] P. Sakarindr, N. Ansari, R. Rojas-Cessa, S. Papavassiliou, "Security-enhanced quality of service (SQoS) networks: a network analysis", IEEE Military Communications Conference, October 2005.

[7] D. Johnson, D. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks in Ad Hoc Networking", Addison-Wesley, pp. 139–172, 2001.

[8] J.Papaj, Ľ.Doboš, A.Čižmár, "Security service vector in MANET", In: AEI '2008: International Conference on Applied Electrical Engineering and Informatics: September 8-11, Greece, Athens 2008. Košice, FEI TU, pp. 130-138. ISBN 978-80-553-0066-5, 2008.