

REPUTATION-BASED SECURITY FOR HETEROGENEOUS STRUCTURALLY COMPLEX SYSTEMS

O.M. Kussul

National Technical University of Ukraine “Kyiv Polytechnic Institute”,
Institute of Physics and Technology, 37 Prospect Peremogy,
Kyiv 03056, Ukraine, olgakussul@gmail.com

In this paper we present the service-oriented infrastructure within the Wide Area Grid (WAG) project that was carried out within the Working Group on Information Systems and Services of the Committee on Earth Observation Satellites (CEOS). The study focuses on enabling trust for this infrastructure using certificates and reputation-based model.

В даній роботі розглянуто сервіс-орієнтовану інфраструктуру обробки супутникових даних, яка розроблена в межах міжнародного проекту Wide Area Grid (WAG) робочої групи WGISS комітету супутникових спостережень CEOS. Розглянуто питання забезпечення довіри в таких структурно-складних системах, зокрема на основі сертифікатів та репутації.

Introduction

At present, the solution of applied problems in many domains such as climate change, environment monitoring, disaster management is impossible without extensive use of Earth observation (EO) data. A system of systems (SoS) is required in order to enable solution of these problems at both regional and global scale. Such an approach envisages the integrated use of satellite data and corresponding products and services, and integration of existing regional and international satellite monitoring systems. It is particularly important for the area of disaster management where different space agencies collaborate in order to timely provide necessary data and services in case of emergency.

A considerable need therefore exists for an appropriate infrastructure that will enable the integrated and operational use of multi-source data for different applications domain. From technological point of view, Grids can provide solutions to the above-mentioned problems. In this case, a Grid environment can be considered not only for providing high-performance computations, but, in fact, can facilitate interactions between different actors by providing a standard infrastructure and a collaborative framework to share data, algorithms, storage resources, and processing capabilities [1–7].

There have been several studies on evaluating and using Grids for the EO domain. In particular, we may refer to the GENESI-DR project (www.genesi-dr.eu) that aims at building a grid-based infrastructure supporting the Global Earth Observation System of Systems (GEOSS) architecture. The European Space Agency (ESA) and the European Space Research Institute (ESRIN) developed the Earth Observation Grid Processing on-Demand infrastructure (G-POD) [4, 6]. FAIRE is another Grid-based application that is operationally used by ESA in the context of flood mapping. The application takes advantage of Grid technology for near real-time (NRT) data access, calibration, orthorectification, map projection, co-registration. The application is operationally used in the context of the International Charter “Space and Major Events” (<http://www.disasterscharter.org>). DEGREE (Dissemination and Exploitation of GRids in Earth science) project was a European-funded project that aimed to build a bridge linking the Earth Science and Grid communities throughout Europe. Grid was considered to be the appropriate platform for integration of heterogeneous data resources, processing tools, models, algorithms, and so on. The following applied problems were within the scope of DEGREE: earthquake analysis, floods modelling and forecasting, and influence of climate changes on agriculture.

In this paper we present the service-oriented infrastructure within the Wide Area Grid (WAG) project that was carried out within the Working Group on Information Systems and Services (WGISS, <http://www.ceos.org/wgiss>) of the Committee on Earth Observation Satellites (CEOS). The study focuses on enabling trust for this infrastructure using certificates and reputation-based model.

1. The WAG project

The WAG project was initiated by the French Space Agency (CNES) within the CEOS WGISS activities with main contributions from Space Research Institute (SRI) NASU-NSAU (Ukraine) and CEODE-CAS (China). The project objective was to develop the “horizontal” infrastructure in order to integrate computational, human, intellectual, and informational resources of the space agencies within a distributed system. In order to create such an infrastructure Grid technologies were used. An application that was tackled within the project is flood monitoring and prediction. Within the infrastructure services were developed in order to enable fast acquisition, processing and delivery of geo-information products based on optical and synthetic-aperture radar (SAR) satellite data in case of emergency. The WAG project is considered as CEOS WGISS contribution to GEOSS. Description of the infrastructure, technologies used and case-study applications are given in details in the following sections.

2. Service-oriented system for satellite data processing

Overall architecture. To enable automatic processing of satellite data, a service-oriented infrastructure was implemented (Fig. 1). We followed the approach used in the Earth System Grid [8]. The four major components of the system are as follows:

1. *Client applications.* Web portal is a main entry point, and provides interfaces to communicate with system services.

2. *High-level services.* This level includes security subsystem including services for managing reputation, catalogue services, metadata services (description and access), automatic workflow generation services, and data aggregation, sub-setting & visualisation services. These services are connected to the Grid services at the lower level.

3. *Grid services.* These services provide access to the shared resources of the Grid system, access to credentials, file transfer, job submission and management. The Grid services include: Globus Security Infrastructure (GSI), GridFTP, Grid Resource Allocation Management (GRAM), MyProxy, Replica Location Service (RLS), and OGSA-DAI.

4. *Database and application services.* This level provides physical data and computational resources of the system.

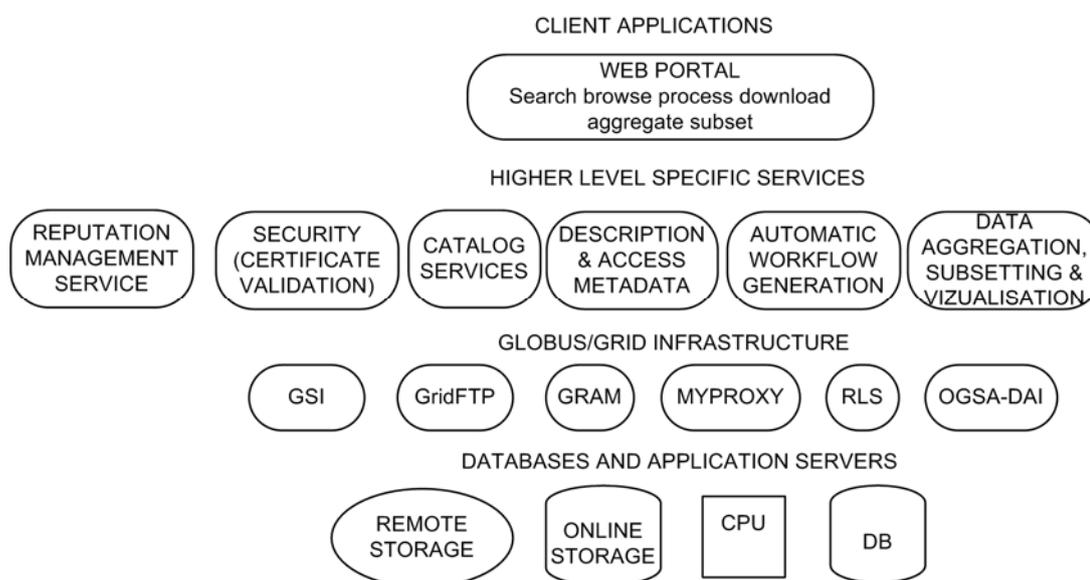


Fig. 1. Overall architecture of service-oriented structurally complex system for satellite data processing

The WAG Services. Using the described approach we implemented a service-oriented system for disaster monitoring using satellite data. The system integrates geographically distributed resources of the SRI NASU-NSAU (Ukraine), Institute of Cybernetics of NASU (IC NASU, Ukraine) and CEODE-CAS (China) [1-3, 5]. The system is applied for disaster monitoring and management, in particular floods. In order to benefit from data of different nature (for example, optical and radar) and provide integration of different products in case of emergency, SRI NASU-NSAU flood mapping service was integrated with the flood mapping services provided by the CEODE-CAS. SRI NASU-NSAU flood mapping service uses radar satellite data (Envisat/ASAR, Radarsat-2) while CEODE-CAS service is based on the use of optical data acquired by MODIS instrument onboard Terra and Aqua satellites. Figure 2 shows the architecture of the China-Ukrainian service-oriented system for disaster management.

The following Service Level Agreement (SLA) was delivered:

- *geospatial products should be available within 24 hours after satellite image acquisition;*
- *spatial resolution of satellite images and corresponding products should be no less than 250 m.*

The integration of the Ukrainian and Chinese systems is done at the level of services. The portals of SRI NASU-NSAU and CEODE are operated independently and communicate with corresponding brokers that provide interfaces to the flood mapping services. These brokers process requests from both local and trusted remote sites. For example, to provide a flood mapping product using SAR data the CEODE portal generates a corresponding search request to the broker at the SRI NASU-NSAU side based on user search parameters. This request is processed by the broker and the search results are displayed at the CEODE portal. The user selects the SAR image file to be processed, and the request is submitted to the SRI NASU-NSAU broker which generates and executes workflow, and delivers the flood maps to the CEODE portal. The same applies to the broker operated at the CEODE side that provides flood mapping services using optical satellite data. In order to get access to the portal the user should have a valid certificate. The SRI NASU-NSAU runs the VOMS server to manage with this issue.

Workflow for flood mapping from satellite SAR imagery. Within the infrastructure an automated workflow of satellite synthetic-aperture radar (SAR) data acquisition, processing and visualization, and corresponding geospatial services for flood mapping from satellite SAR imagery were developed. The data are automatically downloaded from

the ESA rolling archives where satellite images are available within 2-4 hours after their acquisition. Both programming and graphical inter-faces were developed to enable search, discovery and acquisition of data. Through the portal a user can perform a search for the SAR image file based on geographical region and a time range. A list of available SAR imagery is returned and the user can select a file in order to generate a flood map. The file is transferred to the resources of the SRI NASU-NSAU and a workflow is automatically generated and executed on the resources of the infrastructure (Fig. 3).

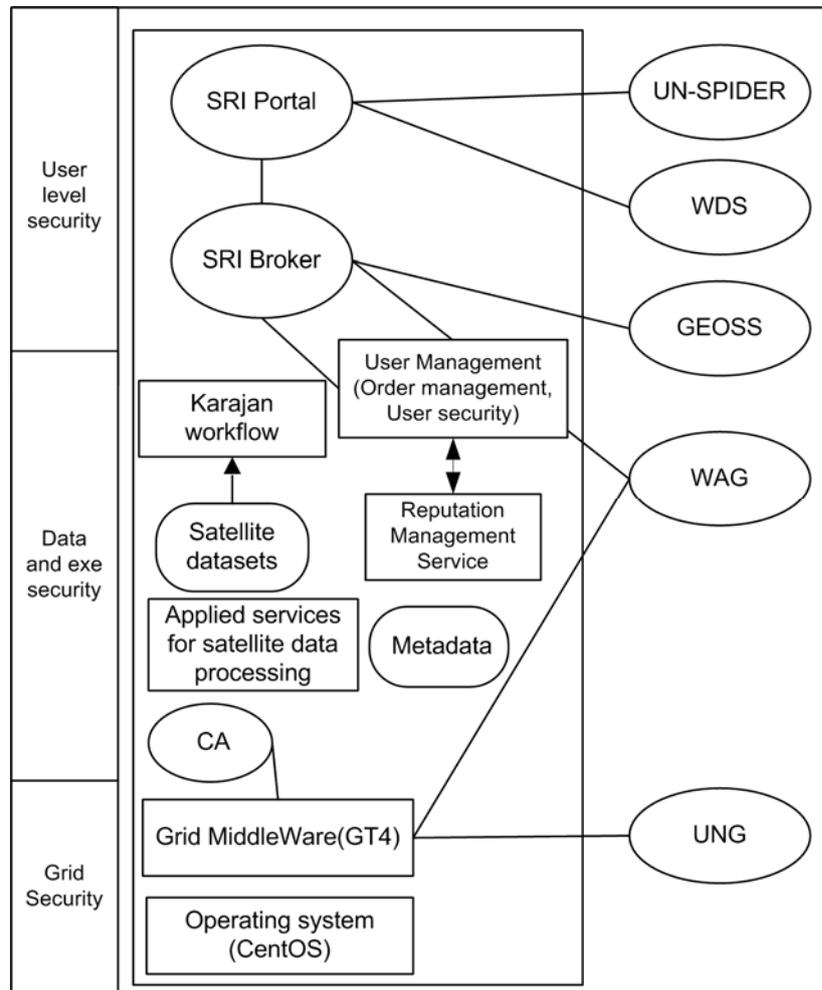


Fig. 2. Architecture of service-oriented Ukrainian-Chinese system for disaster management

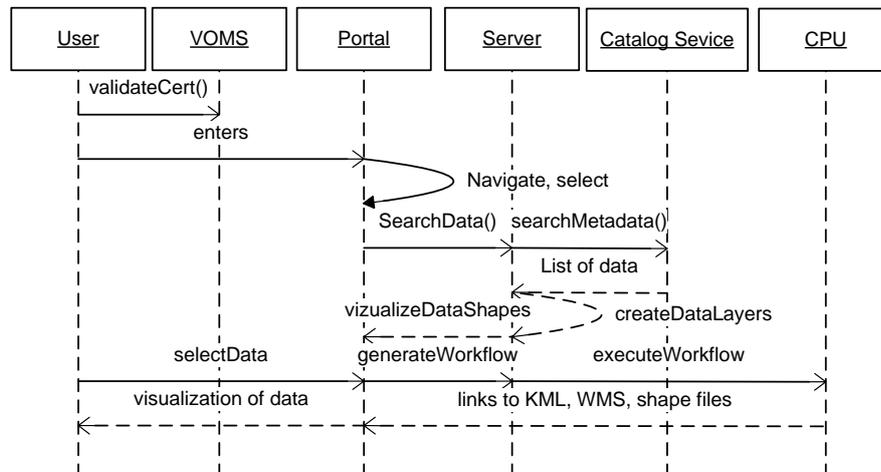


Fig. 3. UML sequence diagram of workflow for flood mapping from satellite SAR imagery

A neural network approach to SAR image segmentation and classification was developed [5, 9, 10]. The workflow of data processing is as follows:

1. Geometric (orthorectification) and radiometric correction of the SAR image using digital elevation model (DEM). Regions with shadows and layover are identified at this stage as well.
2. Processing of SAR image using a neural network classifier. The neural network assigns to each pixel of the output image a binary value corresponding to one of two classes (“Water” and “No water”) taking as input a moving window of image pixel intensities.
3. Removal of those regions that were detected as shadow/layover at the stage No. 1, since the pixel values in these regions are not related to physical conditions of the environment.
4. Geocoding, i.e. transformation to geographical projection using ground-control points (GCPs) incorporated in the SAR image;

Visualization of the results using ESRI shape files, KML (Keyhole Markup Language) files, and OGC WMS. To benefit from the use of the Grid a parallel version of the method for flood mapping from satellite SAR imagery has been developed. The parallelization of the image processing was implemented in the following way: a SAR image is split into the uniform parts that are processed on different nodes using the OpenMP Application Program Interface (www.openmp.org). The use of such infrastructure allowed us to considerably reduce the time required for image processing and service delivery. In particular, it took approximately more than 1.5 h (depending on image size) to execute the whole workflow on a single workstation. The use of Grid computing resources allowed us to reduce the computational time to less than 20 minutes.

3. Enabling trust in service-oriented system for satellite data processing

Enabling security trust between different parties within a heterogeneous structural-complex system is one of the main prerequisite for such integration. We investigated and applied two approaches: Public Key Infrastructure (PKI) and reputation-based trust management. First, we review a general approach to integrating reputation management system into the service-oriented structurally complex systems.

Integrating reputation into service-oriented structurally complex systems. Figure 4 shows a general framework for integrating reputation management system into the service-oriented structurally complex systems.

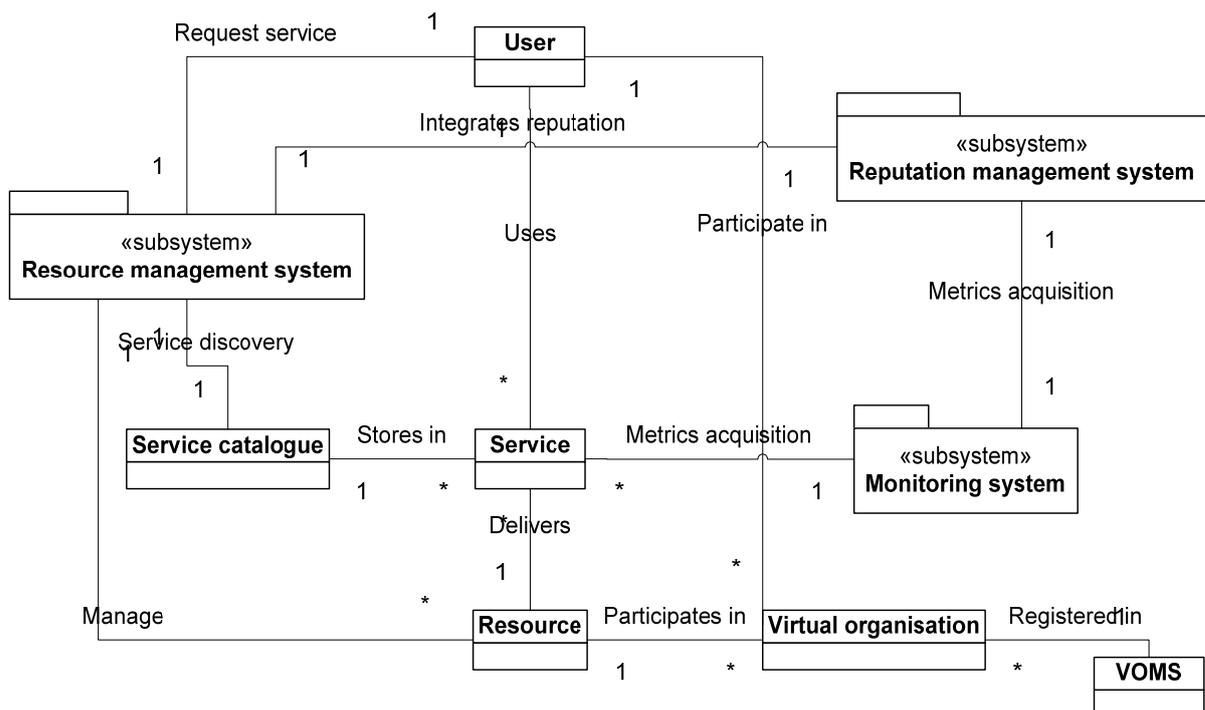


Fig. 4. Integrating reputation into service-oriented structurally complex systems

The main components and system of this architecture are as follows:

- **Users.** They utilize services. The users can be human beings who get access to services through portals but also can be third-party systems that utilize APIs. Users also form and participate in virtual organizations.
- **Resource.** Resources deliver services, form and participate in virtual organisations.
- **Virtual organisations (VO).** VO is a temporary or permanent coalition of geographically distributed individuals, groups, organizations that share resources, capabilities (databases, computing resources etc.) and information to reach common goals.
- **Virtual Organisation Membership Service (VOMS).** VOMS is a system for managing authorization data within multi-institutional collaborations.
- **Service.** Service is a functionality provided by resources and system components.
- **Catalogue service** provides a list of services that resources provide.

— **Resource management system** processes request from users, performs service searching based on user requirements, and select appropriate resource to deliver a service. For selecting resources reputation acquired from reputation management system is utilized.

— **Reputation management system** assess, stores and updates resource reputation. This system interacts with monitoring system to acquire data on quality of service (QoS) metrics to calculate resources reputation. It also interacts with resource management system to deliver resource reputation.

— **Monitoring system** is used to acquire data on user and service interactions.

Certificates. X.509 is the most widely used format which is supported by most of the existing software. To get access to resources of the Grid system, a user should make a request to a Certificate Authority (CA) which is always a known third party. The CA validates the information about the user and then signs the user certificate by the CA's private key. The certificate can thus be used to authenticate the user to grant access to the system. To provide a single sign on and delegation capabilities the user can use the certificate and his private key to create a *proxy certificate*. This certificate is signed not by CA but rather the user himself. The proxy certificate contains information about the user's identity and a special time stamp after which the certificate will no longer be accepted.

In order to enable Grid system integration with different middleware installed and security mechanisms and policies used the following solutions were tested:

1. To create our own CAs and to enable the trust between them.
2. To obtain certificates from a well known CA, for example the European Policy Management Authority for Grid Authentication (EUGridPMA, <http://www.eugridpma.org>).
3. To use a combined approach in which some of the Grid nodes accept only certificates from the local CA and others accept certificates from a well known third party CAs.

Within the integration of the UASpaceGrid and the CEODE-CAS Grid the second and the third approaches were verified. In such a case, the UASpaceGrid accepted the certificates issued by the local CA that was established using the TinyCA, and certificates issued by the UGRID CA (<https://ca.ugrid.org>).

It is worth mentioning that Globus Toolkit v.4 and gLite v.3 middleware implement the same standard for the certificates, but different standards for describing the certificate policies. That is why it is necessary to use two different standards for describing the CA's identity in a policy description file.

Reputation model. In order to enable trust between different parties, we also focused on estimating resources reputation based on QoS metrics and SLA. In particular, we extended the existing utility-based reputation model for virtual organizations in Grids [11] to address threats scenarios in the area of trust and reputation management [12]–[16]. These modifications included: assigning initial reputation to a new entity in VO, capturing alliance between consumer and resource, defining a time decay function, and score function. The proposed reputation model was analyzed against the existing security threat scenarios and how the model overcomes them. In particular, the model was effective in countering such threats as individual malicious peers, malicious collectives, driving down the reputation of a reliable peer, while there were some limitations in countering malicious collectives with camouflage.

The proposed model was evaluated not only in terms of countering security threats but also resource management in service-oriented systems. A problem of on-line job scheduling was considered, and a general procedure for integrating reputation into the scheduler using a non-linear trade-off scheme was presented. The advantage of using such a scheme is that it provides a Pareto-optimal solution partially satisfying criteria with corresponding weights. The experiments showed that the scheduler with knowledge of reputation using a non-linear trade-off scheme outperformed a scheduler without knowledge of reputation on average 45% for all performance metrics used in the study. A non-linear linear trade-off scheme for incorporating reputation into the scheduler of resource management system was compared to a multiplication scheme, and showed better performance with a factor of 2. Currently, we are evaluating the use of such a model for the GEOSS infrastructure.

4. Earth observation applications

Flood monitoring and risk assessment for Ukraine. The severe 2010 winter in Ukraine that was characterized by large amount of snow and ice on rivers posed a high threat of floods during the melting period. In order to provide flood risk assessment both synthetic-aperture radar (SAR) and optical satellite imagery were used. In particular, we acquired more than 30 Envisat/ASAR scenes during the 2010 winter-spring period, and more than 50 archived scenes during autumn 2009 to monitor the snow cover. These images were processed using resources of the service-oriented infrastructure.

Satellite optical images were acquired using the EO-1 Sensor Web System. In particular, the OGC Sensor Planning Service (SPS) was used for tasking the EO-1 satellite [17]–[19]. Through the UN-SPIDER RSO in Ukraine a request was made from local authorities to acquire satellite images over the Kyiv city area due to a high risk of a flood in spring 2010. The use of the Sensor Web and the Grid ensured a timely delivery of products to end-users. A sequence of events starting from the notification of satellite tasking and ending with generation of final products is as follows:

- | | | |
|-----------------------------|---|---|
| Mon Apr 12, 2010 @ 10:33 pm | — | Notification on EO-1 tasking through Sensor Planning Service (SPS) |
| Tue Apr 13, 2010 @ 10:33 am | — | Image taken |
| Tue Apr 13, 2010 @ 04:30 pm | — | Image available at the NASA ftp server and automatically transferred to the Grid system resources |
| Tue Apr 13, 2010 @ 11:30 pm | — | Generation of geospatial products using Grid computing resources |

It took less than 12 h after image acquisition to generate geospatial products that were delivered to the Ukrainian Ministry of Emergency Situations, the Council of National Security and Defence, and the Ukrainian Hydrometeorological Centre. The information on river extent that was derived from the EO-1 image was used to calibrate and validate hydrological models to produce various scenarios of water extent for flood risk assessment.

Flood mapping for China. In July 2007, following the flooding on the river Huaihe (China), SRI NASU-NSAU and CEODE-CAS processed Envisat/ASAR and Radarsat-1 images that were acquired 15 and 19 July 2007, respectively. The images were processed using computational resources of the service-oriented infrastructure. The resulting flood maps were delivered using OGC WMS services.

Conclusions

In this paper we presented results that were achieved within the Wide Area Grid (WAG) project. In order to benefit from using data from multiple sources, integration of the Ukrainian and Chinese flood mapping services that use radar and optical satellite data was carried out. The paper discussed the use of certificate-based and reputation-based trust enabling issues. The particular advantages of such integration are as follows: the system will benefit from the use of services that are provided by different partners within the system; data resources are distributed within the system at different sites (Ukrainian and Chinese), so this allows us to improve the quality of services delivered within the system; the use of Grids enables the use of high-performance computing resources that in turn will decrease the time required for satellite data processing and delivery of service which is critical for disaster management domain; the use of unified Grid and OGC services provides scalability of the system while adding new components and services; such collaboration provides valuable contribution and impact to the on-going large-scale international activities such as creation of the GEOSS infrastructure.

1. *Lecca G., Petitdidier M., Hluchy L., Ivanovic M., Kussul N., Ray N., Thieron V.* "Grid computing technology for hydrological applications" // *J. of Hydrol.* – 2011. – Vol. 403, No. 1-2. – P. 186–199.
2. *Kussul N., Shelestov A., Skakun S.* "Grid Technologies for Satellite Data Processing and Management within International Disaster Monitoring Projects" in *Grid and Cloud Database Management*, S. Fiore, G. Aloisio, Eds. Springer-Verlag: Berlin Heidelberg. – 2011. – P. 279–306.
3. *Kussul N., Shelestov A., Skakun S.* "Grid and sensor web technologies for environmental monitoring" // *J. Earth Sci. Inf.* – 2009. – Vol. 2, No. 1-2. – P. 37–51.
4. *Cossu R., Schoepfer E., Bally P., Fusco L.* "Near real-time SAR-based processing to support flood monitoring" // *J. of Real-Time Image Proc.* – 2009. – Vol. 4. – P. 205–218.
5. *Kussul N., Shelestov A., Skakun S.* "Grid System for Flood Extent Extraction from Satellite Images" // *J. Earth Sci. Inf.* – 2008. – Vol. 1, No. 3-4. – P. 105–117.
6. *Fusco L., Cossu R., Retscher C.* "Open Grid Services for Envisat and Earth Observation Applications" in *High performance computing in remote sensing*, 1st ed., A. J. Plaza, C.-I. Chang, Eds.: Taylor & Francis Group: New York. – 2007. – P. 237–280.
7. *Shelestov A., Kussul N., and Skakun S.* "Grid Technologies in Monitoring Systems Based on Satellite Data" // *J. of Automation and Inf. Sci.* – 2006. – Vol. 38, No. 3. – P. 69–80.
8. *Williams D. N. et al.* "Data management and analysis for the Earth System Grid" // *J. Phys.: Conf. Ser.* 125 012072 – 2008.
9. *Kussul N., Shelestov A., and Skakun S.* "Flood Monitoring on the Basis of SAR Data" in *Use of Satellite and In-Situ Data to Improve Sustainability*, F. Kogan, A. Powell, and O. Fedorov, Eds. NATO Science for Peace and Security Series C: Environmental Security. – 2011. – P. 19–29.
10. *Skakun S.* "A Neural Network Approach to Flood Mapping Using Satellite Imagery" // *J. Comput. and Inf.* – 2010. – Vol. 29, No. 6. – P. 1013–1024.
11. *Arenas A., Aziz B., and Silaghi G. C.* "Reputation management in grid-based virtual organizations," in *Proc. Int. Conf. on Secur. and Cryptogr. (SECURITY 2008)*. – 2008. – P. 538 – 545.
12. *Kussul O., Novikov O.* "Utility-based reputation model for VO in GRIDs" // *J. Herald of NTUU "KPI". Informatics, control and computer science.* – 2009. – Vol. 50. – P. 137 – 145.
13. *Skakun S., and Kussul N.* "An Agent Approach for Providing Security in Distributed Systems" in *Proc. International Conference Modern Problems of Radio Engineering, Telecommunications, and Computer Science (TCSET 2006)*. – 2006. – P. 212 – 215.
14. *Shelestov A., Kussul N.* "Using the fuzzy-ellipsoid method for robust estimation of the state of a grid system node" // *J. Cybernetics and Systems Analysis.* – 2008. – Vol. 44, No. 6. – P. 847–854.
15. *Kussul N., Shelestov A., Sidorenko A., Skakun S., Veremeenko Y.* "Intelligent multi-agent information security system" in *Proc. the Second IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.* – 2003. – P. 120–122.
16. *Kussul N., Skakun S.* "Neural network approach for user activity monitoring in computer networks" in *Proc. IEEE International Joint Conference on Neural Networks.* – 2004. – Vol. 2. – P. 1557–1561.
17. *Moe K., Smith S., Prescott G., Sherwood R.* "Sensor Web Technologies for NASA Earth Science" in *Proc. of 2008 IEEE Aerospace Conf.* – 2008. – P. 1–7.
18. *Mandl D., Frye S. W., Goldberg M. D., Habib S., Talabac S.* "Sensor Webs: Where They are Today and What are the Future Needs?" in *Proc. Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006)*. – 2006. – P. 65–70.
19. *Mandl D.* "Experimenting with Sensor Webs Using Earth Observing 1" in *IEEE Aerospace Conf., Big Sky, MT* – 2004.