CHALLENGES IN DATA COMMUNICATION AND CYBER SECURITY OF TUSAGA-Aktif (CORS-Tr)

Sedat BAKICI, Bilal ERKEK, Volkan MANTI and Alper ALTEKİN, TURKEY

Key words: Geoinformation/GI, GNSS/GPS, Data Communication, RTK GNSS Network, CORS-Tr, Data Security, Cyber Security

SUMMARY

There are three main activities of General Directorate of Land Registry and Cadastre; Mapping, Land Registry and Cadastre. Geomatic Department is responsible for mapping activities. Since 2005, the most important projects like TUSAGA-Aktif (CORS-Tr), Metadata Geoportal, Orthophoto Production and Orthophoto Web Services and preparation of Turkish NSDI Feasibility Report have been conducted and completed by this department's specialists.

TUSAGA-Aktif (CORS-Tr) System, gives position information at cm level accuracy in Turkey and TR Nortern Cyprus in a few seconds, if adequate numbers of GNSS satellites are observed and communication possibilities are present. Using of ground control points and benchmarks is not necessary in this system. CORS-Tr System has 146 permanent GNSS stations. Station data are transferred online to the main control center located in the Mapping Department of the General Directorate of Land Registry (GDLRC) and Cadastre and to the control center located in the General Command of Mapping. Currently CORS-Tr has more than 10000 users. Most of them are private companies working for governmental organization and remaining are universities, municipalities and GDLRC's regional cadastre offices.

Today technologies became more sophisticated and changes day by day. Consequently, data communication, security alternatives and security mentalities are changes too. In recent years, providing a safe data communication between control center and both GNSS station and users via trusted communication substructure has become an important issue. Additionally, protection of the real time working system and data against cyber attacks from domestic and foreign sources has become important. This paper focuses on data communication and security issues of GNSS network named CORS-Tr.

CHALLENGES IN DATA COMMUNICATION AND CYBER SECURITY OF TUSAGA-Aktif (CORS-Tr)

Sedat BAKICI, Bilal ERKEK, Volkan MANTI and Alper ALTEKİN, TURKEY

1. INTRODUCTION

A CORS is a Continuously Operating Reference Station. CORS can take the place of a traditional base station used in differential GNSS positing. They can give an instant position to an accuracy of a few cm and are used in many industries including Precision Agriculture, Construction, Mining, Surveying and in Scientific Research[1].

Continuously Operating Reference Stations GNSS Network Project called CORS-Tr (TUSAGA-Aktif in Turkish) has begun in 2006 as a research and development project of The Scientific and Technological Research Council Of Turkey (TUBITAK) by supporting financial side, Istanbul Kultur University (IKU) as a project implementer and The General Directorate of Land Registry and Cadastre (TKGM) and General Command of Mapping (HGK) including as joint customers. CORS-Tr project completed in 2009 and operated by TKGM and HGK collectively. Until 15 June 2011, it was operated free of charge for test purposes. Since then it has been operating as a paid service and price is determined by Inter Ministries Mapping Coordination and Planning Committee (BHİKPK) and confirmed by both Ministers who are Environment and Urbanization Minister and Defense Minister.

TUSAGA-Aktif (CORS-Tr) System, serves location information by cm level accuracy in Turkey and TR Nortern Cyprus in few seconds, where adequate numbers of GNSS satellites are observed and communication possibilities are present. No ground control points and benchmarks are necessary. CORS-Tr System includes 146 permanent GNSS stations. Station data is transferred online to the main control center located in the Mapping Department of the General Directorate of Land Registry and Cadastre and the second control center located in the General Command of Mapping.

Today CORS-Tr System has more than 10000 individual users which can be grouped as Land Registry and Cadastral Offices, Governmental İnstitutions, Licensed Surveyors, Universities and Private Companies. All users have chance to get good services from Geomatic Department via detailed web page, SMS and email message. More over call center (444) support is available in case of any problems on the field for 24/7.

This paper presents trusted data communication infrastructure and security issues of CORS-Tr system in Geomatic Departments.

2. CORS-Tr DATA COMMUNICATION

A GNSS network consists of several GNSS stations interconnected by reliable communications to enable real time computations and control. Each station has a cabinet which contains a receiver, an antenna, communication devices, small data storage, power supply, accumulator and so on. In most cases a computer is installed additionally for data transmission and control. It also contains a user interface which is required to configure and maintain the network. This may be realized remotely for example by radio communication , mobile phones or via internet connection.

In Turkey Turk Telekom Backbone for CORS-Tr data communication is available. CORS-Tr system has VPN tunel between reference station and control center as primary data communication and 3G APN tunnel as secondery. User connections are supported by APN tunnel by all three GSM Operators in Turkey. And all RTK correction send to user via an APN tunnel. Data communication structure is shown in section 3.3 Networks topic (Figure 3).

3. CORS-Tr SECURITY ISSUES

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity. Elements of cybersecurity includes[2]:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- End-user awareness and education.

3.1 Applications

In CORS-Tr system, we have Network RTK correction, networks DGPS correction, web online processing services and RINEX datas to provide our users. All applications are shown in Figures 1.a and 1.b.

Figure 1.a: TUSAGA-Aktif applications

CORS-Tr Main Applications			
RTO	Real Time Output	İScope	Realtime Visualization
TDC	Dynamic Control	TOP	Web Online Proces.
VRSNet	Corrections	TRI	Rover Integrity
TIC	Instrum. Config.	TED	Ephemeris Download.
TDS	Data Shop	TIM	Integrity Manager
TAC	Accounting	TSM	Streaming Manager
Atmo	Atmos. App.	TTG	Transformation Mang.

Figure 1.b: TUSAGA-Aktif applications

3.2 Information

CORS-Tr system works with 3 SQL databases which are ***TPPDB*** contains the history of the system, ***TPPAccounting*** contains the accounting information such as user, subscriptions, sessions, etc. and ***TPPDBRoverIntergrity*** is a separate database for the rover integrity results. Additionally we have RINEX datas, control center camera records and call-center recorded voices.

No	Information Type	Resp. Unıt	Backup Period	Where	Keeping Duration	Time Deliver to Achieve
Y 1	RINEX 1 Sec.	Geodesy	Weekly	Geodesy	3 Month	--------
Y 2	RINEX 30 Sec.	Geodesy	Monthly	Geodesy	1 Year	End of the Year
Y 3	Database Logs	Geodesy	Monthly	Geodesy	Endless	End of the Year
Y 4	Control Center Camera Records	Geodesy	Monthly	Geodesy	6 Month	----------
Y 5	Callcenter Recorded Voice	Data Mang.	Monthly	Geodesy	1 Year	----------

No	Information Type	Resp. Unıt	Achieving Period	Where	Keeping Duration	
A1	RINEX 30 Sec.	Data Mang.	Yearly	Data Mang.	10 Year	
A2	Database Logs	Data Mang.	Yearly	Data Mang.	Endless	

Figure 2-TUSAGA-Aktif Information to be backed up and to be archieved

3.3 Networks

We have two different networks in Geomatic Department. One of the network is CORS-Tr control center network, called METRO. Other is General Directorate of Land Registry and Cadastre (GDLRC) wide area network, called TAKBIS. TAKBIS network is under the responsibility of IT department of GDLRC. COSR-Tr network is an independent and special network. There is no connection or relation to TAKBIS network.

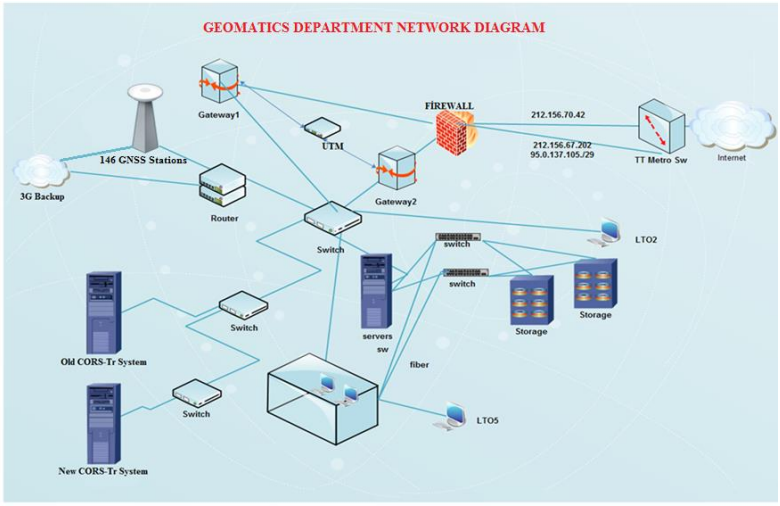

Figure 3- Geomatic Department Network Design

3.4 Our Experience and Business Continuity Planning

Of course CORS softwares including operating system and hardware, normally has their own firewall and some security issues with many applications. But we faced many problems since CORS-Tr established and these problems are briefly described below.

Lack of IT Personnel: Only Surveying Engineers and Surveying technicans were avaliable to operate CORS-Tr system, user membership and payment issues and to support users. There wasn't any IT staff to control system in case of a technical problem. Highly qualified geoinformatics personnel dealt with technical problems such as system freezing, communication bandwidth saturation or even exchange of broken harddisks.

DDOS Attacks: In summer season of year 2013 when mapping applications on the field by using CORS-Tr are very dense, we faced a very hard DDOS attack by an unknown source. DDOS attacks were continued for approximately 3 months , everyday between 10 a.m. and 12 a.m.

Awareness of Internal Users: Internal system users who use computers that has virüs, malware, trojan.etc. Internal users who used virus contaminated USB to connect system servers or unsafe remote desktop connection caused danger for the system . Unfortunately Institutional anti-virus system was unable to protect CORS-Tr system. Internal user's awareness on security issues should be increased.

Awareness of External Users: Some external users somehow adjusted their GNSS instrument settings to send more than five request in a second to connect CORS-Tr system. These requests interrupted other user connections and overloaded data communication bandwidth. Some external users shared their own password and user name with other users which cause conflict

between the users. An other problem caused by external users is unnecessary attempts for connection. Although their term has finished many external users, try to connect to the system.

4. IMPROVEMENTS

Measures taken to establish trusted service in CORS-Tr system usage in terms of security requirements after experienced problems are:

- One specialised Computer Engineer and a specialised Electrical and Electronics Engineer to operate COSR-Tr technical side were employed.
- UTM security device purchased for prevention from DDOS attacks. No DDOS attack detected since 2013.
- Directive about personal computer maintenance including software related security risks issued. Then data back-up and archiving directive for our employees in Geomatic Deparment issued.
- GNSS reference station data and information are stored in an SQL database. User information and activity log data are stored in an other SQL database. These two databases and other related data have been started to be backed up ever day regularly according to department directive.
- Data comunication bandwidth enlarged to 150mbps for giving good service to everyday increasing user count.
- VPN tunnel established between reference station and control center as primary data communiciation and a 3G APN tunnel as secondary. Reference stations data storage capacity increased.
- Current software updated to latest version including required moduls such as Realtime Visualization, Atmosphere, Transformation Generator and Online Web Processing.
- New hardware provided according to updated software requirements.
- Main applications like Network RTK correction, networks DGPS correction and provision of RINEX data to the our users and SQL databases are protected by extra security software for cyber attacks.
- In CORS-Tr network, servers and end points are protected by a software from inside and outside cyber attacks.
- User awareness of CORS-Tr usage was increased by 444 call center, SMS message, Social Media and Local trainings. And also customer satisfaction are surveyed regularly.
- A new software purchased using 3-factor authentication for connecting the system in order to avoid illegal usage of gnss devices by the employees of governmental institutions. The system uses user name-password, SIM card service number and gnss device's IMEI number for a match to connect the system. A user can only connect to the system with his own username-password, one SIM card authenticated to a one and only gnss device. No one can use some other user's ID or SIM card or GNSS device. This system also traces and logs the connections established to the system and give data about time-date , connection duration, used bandwidth.

5. CONCLUSION

At the beginning of TUSAGA-Aktif project we thought that project was considered geodesy related works only. Today we understood that TUSAGA-Aktif is not only a geodesic related work but also Information and Communication Technology work.

As a result today CORS-Tr have trusted data communication infrastructure, protected information and services by updated software and hardware including security devices and has more powerful user support.

REFERENCES

[1] URL1:http://www.sage.unsw.edu.au/currentstudents/ug/projects/Gowans/Thesis/What_is_it.html
[2] URL2: http://whatis.techtarget.com/definition/cybersecurity

CONTACTS

Mapping Department of General Directorate of Land Registry and Cadastre, 06550 Cankaya, ANKARA, TURKEY
sbakici@tkgm.gov.tr , berkek@tkgm.gov.tr , aaltekin@tkgm.gov.tr , vmanti@tkgm.gov.tr