HADMÉRNÖK

VII. Évfolyam 4. szám - 2012. december

Puskás Béla

THE RISKS OF NETWORKS' COMPLEXITY

Abstract

"We live in an accelerated world" sounds one of the most common truisms of our age. Comparing to the previous decades this feeling is mainly caused by the dynamic flow of information, fast traffic and transportation means and the globalization, which have been resulted by the booming technical development. Nowadays a journey from Hungary to the United States does not resemble the risky and long-run adventure as it was at the wake of the last century. We also can keep connection with our relatives living on another continent easily. Consequently the people have got closer to each other but at the same time they loosened their connections as well. We live in the virtual space and rarely contact our friends physically. This gap between the individuals and their physical reality is getting so wide, that they don't realize the devastation of environment or the natural disasters.

Az előző évtizedekhez képest a dinamikus információáramlás, a transzport eszközök fejlődése, a globalizáció eredményeként a műszaki fejlődés felgyorsult. Napjainkban már nem számít kockázatos és hosszú kalandnak átutazni az Egyesült Államokba, mint ahogy ez a múlt század elején volt. Mi is, mint humán szféra könnyen tarthatunk kapcsolatot rokonainkkal, ismerőseinkkel, akik akár egy másik kontinensen is élhetnek. Következésképpen az emberek az IT hálózatok segítségével közelebb kerültek egymáshoz, de ugyanakkor lazított is a kapcsolatuk. Virtuális térben élünk, amit az is bizonyít, hogy csak ritkán találkozunk személyesen ismerőseinkkel, barátainkkal. Ez a különbség az egyének és a fizikai valóság egyre növekvő eltávolodását hozhatja, miközben környezetünkben jelentős változások, természeti katasztrófák játszódhan le.

Keywords: *network attack, future IT warfare, structure of networks ~ hálózati támadások, a jövő informatikai hadviselése hálózatok szerkezete*

"We have built our future upon a capability that we have not learned how to protect! "[1]

HOW HAS THE REVOLUTIONARY ELECTRONIC DEVELOPMENT CHANGED OUR COMMON LIFE?

On the 4th of September in 1837 the inventor, Samuel Morze introduced his electromagnetic telegraph. In order to use it two things were essential. One of them was the Morze alphabet, while the other was the telegraph network itself. At that time the bit rate was "only" at around 5 bit/sec.

In 1876 Alexander Graham Bell had the telephone patented. He also had to establish and operate a network thus he founded the Bell Telephone Company in 1877. Presently it is the well-known American Telephone and Telegraph Co. (AT&T).

Between 1895 and 1901[2], based on James Clerk Maxwell's theory regarding the radio waves, Nikola Tesla, Guglielmo Marconi and Alexander Popov "independently" from each other invented the radiotelegraph.

In 1957 the Soviet Union launched "Sputnik", the first satellite of mankind. As a response, the President of the USA and the Department of Defense founded ARPA[3] in 1958. In 1969 an experimental network was established and some others joined in later. Five years earlier Paul Baran had already pointed out: in order to create a minimum risk level communication channel, a partitioned network had to be established instead of the decentralized ones. According to his theory the separated packets used on the Internet had to be sent through individual nodes toward their destinations. Nevertheless his idea was rejected.

IN THE SEVENTIES THE INTERNET STARTED ITS OWN LIFE.

More and more institutions joined the network, but not on the way as Baran thought. Instead of the partitioned network a scale-free model was evolved. Due to its extension and rapid development the network couldn't be controlled exclusively. The dominant original goal of an operational network, which is protected against attacks, was not taken into account any more. On the contrary THE INTERNET, which is highly resistant against random errors, was born. It is quite similar to the other networks of our life, such as social networks, networks of the human bodies (nerve system, connections between cells etc.) but it resembles the networks of spreading epidemics and many other else.

Do we really know what has come to life by the Internet?

The main problem is that not only the simple common user doesn't understand it, but the IT professionals are not able to clear up the matter as well. We don't have proper knowledge about the network structure and we can't obtain it by our way of thinking. We have to apply the theory of networks. For example documents are being prepared faster on Internet than the search engines can locate and index them. Nowadays they don't even try it and only the 30-40 % of the whole document is mapped even by the most effective search engines. In case of cell phones, especially the smart phones, the situation is quite the same. Their development is so fast that their effect to the hardwares, softwares and the other system can't be measured. Recently 10 % of the Internet data flow is going through mobile networks.

Then how the USA, NATO or Hungary can prepare themselves for the future IT warfare and how can we protect our critical IT systems against the hackers and terrorists?

---

[1] George Tenet Former CIA director

[2] In 1901 Marconi introduced his invention for what the Nobel Prize in Physics was awarded to him in 1909-ben. Tesla had already introduced his patent in 1896, while Popov had done so in 1895.

[3] Advanced Research Projects Agency

Today the real task is not to understand the occurrences going on the Internet or the Internet itself as an entity. Today when it became a part of our life we have to insert it into our complex world.

The terrorist organizations and other criminal groups sometimes hide secret messages in the chaos of the Internet. They can communicate on the network or exploiting its and the users' weaknesses in order to gain money.

Against whom do we have to protect our systems?

In most of the cases the attackers are completely unknown. They hide their sources and even their homeland can't be identified properly. Usually not the owners of the concept execute the attack, but they get "innocent" prying men to do the messy job. They provide only the method and pattern of the attack. The communication channels and the logistics background are also given by someone else. They rarely have particular political or economical interests, the attack is simply considered as a challenge or a funny joke.

I think that in the future it will be very important to get familiar with the nodes of networks and their connections. We have to realize that the network is not just one-dimensional. The connections and effects of seemingly different social and electronic networks have to be researched. Not only the threatened system has to be examined but all the other linked networks as well. Besides the structures of networks we have to know the structures and the very details of the points (e.g. cells). From this point of view the node cannot be described as a mathematical concept because if today something is considered to be indivisible, tomorrow that can be a set. According to Albert-László Barabási the XXI century is going to be the age of complexity.

What has to be studied?

The matter is not so simple. Moreover it becomes more complex if we consider another dimension as well: the movements of nodes. The nodes can change continuously and dynamically. If the nodes are the critical infrastructures we have to count on their permanent movements. What has not been a node before that can become so and vice versa. This fact regards the Internet nodes especially.

In order to determine the items of networks we have to deal with complexity as well. Traditional telecommunication, television, informatics etc. networks and their nodes can be mentioned only within the category of electronic networks. All the network items such as routers, switches, modems, hubs, repeaters, transfer medias, servers, data storages, firewalls, adapters and their features influencing the functions of the "system" have to be studied. We also can test the linking "devices", for example printers, monitor-keyboard switches, different input devices, adapter interfaces (smart phones, TV, PDA, GPS etc.), medical equipment, control systems of critical infrastructures such as traffic lamps or airplanes. The device-free surveys concerning the physical and logical network topology, softwares, hardware and software settings, regulators, physical protection, the human factor, environmental effects are also very interesting of course. The parameters of these factors are quite sophisticated as well but their mutual effects and the quality of their linkage create a complex and immense system.

The Internet has become a complex network. Since it is continuously expanding it can be called scale-free network as well. While studying the network, Barabási and his team noted two facts: the expansion and the popularity.

The scale-free systems are highly resistant to random errors but a targeted attack against the centres can disintegrate them easily. Many vertices, which have only a few edges, can be eliminated but it doesn't have significant effect on the whole network. The destruction of the 80% of Internet nodes leaves the remaining 20% operational nodes working as an intact network.

There can be another practical question in connection with the networks: Do the malfunctions of devices, eruptions of social conflicts, devastations of biological or chemical disasters happen accidentally?

The segments of the network can be paralysed by a series of chance events or a well-organized, targeted attack.

It is easy to see, that as the drawing of the lottery, the malfunction of a random device is also not able to interfere the operation of the whole scale-free network. What is the probability that I can select that particular node, which has many links or especially important for the connection? In case of the Internet and other similar networks the degree exponent is less than three. Because of this fact there is no threshold, which prevents the network disintegration, when the nodes are removed continuously.

However a targeted attack is different. If the nodes with many links are destroyed firstly and it is carried on with the other nodes with less and less links, the network falls apart at a certain threshold. Usually this threshold can be reached quite soon and the attacker doesn't have to destroy too many nodes with many links. Although our system resistant to errors, but the removal of the nodes with many links (e.g. central routers) impose an almost unbearable burden onto the other important nodes and transfer medias. The other items can work for a while, but later packets are going to be lost and congestions are going to emerge, which is very similar to a DoS attack.

I am of the opinion that the nodes providing important links can cause similar problems. Although redundant connections are always installed within the systems these connections have smaller capacity.

Perhaps if the Internet would have not started to live its own "life" and in 1964 Baran would have succeeded in fulfilling his basic theory concerning the primacy of distributed models, we should not fear of the targeted attacks as much. But there is no point dealing with "what if..." questions because these processes are irreversible. We could consider the particular "systems" of evolution having similar networks instead. We may owe our life to it.

Consequently the items of the system, their mutual effects and links and the map of the network have to be known properly. I haven't mentioned the types of graphs, which make the structure of networks more difficult. For instance whether a graph is directed or not does make difference and the network structure modification effect of the relocation of the edge between two vertices can not be neglected either. The complex system can not be protected without this knowledge.

Based on data bases, data storages, documents and images some modern softwares are able to graphically depict the complicated networks and map the complex structures. By the assistance of these softwares false information and connections can be identified, forecasts and algorithms can be prepared. The different aspects (timeline, too many or few but highlighted connections) could reveal hidden, important information.

One of the most important part of the cognition is the obtainment and sorting of information. The concerning data can be obtained from unclassified and classified sources, for instance from the data bases of telecommunication ventures, social sites, Internet providers, manufacturers and many other sources.

If we know our system and lead a safety-conscious life we can avoid such unpleasant events[4], which occurred to the director of MI6, Sir John Sawer. It is obvious, that the problem of mapping the complexity is not only a matter of IT professionals. We have to realize that everything is linked with each other and the physical and logistical networks have mutual

[4] In 2009 Sir John Sawers's wife uploaded some family images onto a social site. By these pictures hostile organizations or individuals could obtain sensitive information, which could endanger Sawers and indirectly the MI6.

effects on each other as well. We can't be sure that the erased digital information really vanishes.

References

[1] Barabási, A.-L. (2003). *Behálózva.* Budapest: Magyar könyvklub.

[2] University of Debrecen. (without date). *Az Internet története.*, source: http://www.inf.unideb.hu/~bodai/internet/internet_tortenete.html; Download date: 30/09/2012

[3] Defense Technical Information Center. (2002). *Information Technology Industry Study Final Paper.*, source: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA425460; Download date: 30/09/2012

[4] ELTE. (2006). *Az elektronikus sajtó története.*, source: http://mmi.elte.hu: http://mmi.elte.hu/szabadbolcseszet/index.php?option=com_tanelem&id_tanelem=548&tip=0; Download date: 27/09/2012

[5] National Geographic Magyarország. (without date). *Samuel Morse, a távíró feltalálója.*, source: http://www.ng.hu/Civilizacio/2005/04/Samuel_Morse_a_taviro_feltalaloja; Download date: 28/09/2012

[6] Péter, B. (19/09/2012). A globális IT-rendszerek erdejében. *Computerworld*, page: 4.