AUGMENTED REALITY AND CYBER CHALLENGES EXPLORATION

Assoc. Prof. Zlatogor Minchev PhD[1], Assoc. Prof. Luben Boyanov PhD[2,1]
Institute of Information and Communication Technologies, Bulgarian Academy of Sciences [1]
University of National and World Economy, Sofia, Bulgaria [2]

zlatogor@bas.bg, lboyanov@unwe.bg

Abstract: *Digital environment progress towards real and virtual realities mixing is reasonably producing new understandings for ICT progress expectations. In todays' mobile web world, augmented realities are practically integrating 'Internet of Things' (IoT) mobile concept and 3D visualization technologies into a new evolving smart world. This changes our everyday life concepts, adding capabilities with innovative functionalities. However, it also is generating multiple challenges from cybersecurity perspective. This paper studies the problem for human-machine interaction, accentuating on the multifaceted understanding of possible threat sources and attack vectors in the new augmented reality research area. In this context, a system model with prognostic analysis is proposed. The necessity of obtained results validation is finally discussed.*

Keywords: AUGMENTED REALITY, IOT, HUMAN-MACHINE INTERACTION, CYBER THREATS, MODELLING, ANALYSIS

1. Introduction

The term "virtual" has become more and more popular in recent years. In general something **virtual** has the attributes of something that exists in reality but that "virtual something" is replicated or presented by something else. In computing the term "virtual memory" exists for a long time and means an approach of using a big amount of memory, which does not exist as hardware memory chips, so that the programmer can use amount of memory without bothering for its existence. Another popular term in the last decade is "virtual machine". This is an emulation of a particular computer system and working on a virtual machine allows someone to work as if doing so on a real (hardware) machine, which does not exist physically. In general, we can assume that any "virtual" object refers to a specific type of emulation of some real object.

The approach of using the properties of a real object has been used very successfully in training and education. The virtual reality technology was introduced in the form of a flight simulator by Thomas A. Furness III, who is often referred to as the 'Grandfather of Virtual Reality' [1]. According to Sherman and Craig [2] there are four key elements of Virtual Reality - Virtual World, Immersion, Sensory Feedback and Interactivity. The first element is the content of a given medium which may exist only in the mind of the creator and there are ways to be shared with others. The second element means that a user is immersed into alternative point of view – i.e. the feeling of being in an environment. The Sensory Feedback allows the system to track actions/movements of the participant in the emulated system. The forth element is the response of the system to the actions of the participant. Summarizing the concepts above illustrates that the term "Virtual Reality" is used to describe a computer generated environment, in all possible dimensions, in which a human can be part of and interact with the surrounding environment.

The advance of computing power and computer based system allowed the creation of complex and powerful systems. In addition to training of pilots (well-known flight simulators), virtual systems are used in combat training for the military. Using head-mounted display (HMD), gloves, weapons and other items allows proper training for combat. The virtualization makes possible repetition of various situations in a wide variety of terrains and situations [3].

As shown above, Virtual Reality replaces the real environment with a computer generated. Unlike it (but having similarities) the Augmented Reality has a direct view of the real environment, where its elements are supplemented, or **augmented** by computer-generated sensory input such as sound, video, graphics or GPS data [4]. Generally, in this concept, a view of reality is modified by a computer system and program. As a result, the technology functions by enhancing the presented perception of reality. Similarly to the Virtual Reality, the Augmented Reality uses head-mounted displays, computers and specialized software. In Augmented Reality popular hardware are also accelerometer, GPS and solid state compass. As in Virtual Reality, Augmented Reality is applied in military, industrial, educational, medical and commercial applications. It is used to visualize building projects; to see a content of a packed commercial product; to interact educational content (like historical events, engineering concepts, etc.) with the students; provide otherwise hidden information to doctors or surgeons; provide battlefield data onto a soldier's goggles in real time [5], etc.

A key technology that became wide spread is the mobile computing and communication – smart phones, tables and other devices are already inseparable part of our everyday life. Another important technology, which is emerging and will have an enormous impact on the future according to almost all forecasts and to the most influential companies in the IT sector, is the Internet of Things (IoT). It is very likely that those technologies will integrate with Virtual and Augmented Reality approaches.

2. Dangers of Augmented and Virtual Reality

Having all those gains and benefits does not come without concerns. Using this technology one may not be able to correctly estimate the speed of an object or a car or ignore some of the threats of the real, surrounding environment. And there are serious concerns about those technologies – some can be physical threats, other – behavioral, privacy, security and some can be placed even at a level of "National security threat" [6]. In Table 1 we present a classification of threats in Augmented and Virtual Reality.

Table 1: *Classification of threats in Augmented and Virtual Reality.*

Types of threats	Examples	Effect	Level of threat
Physical threats	Devices (like head mounted displays) and sensors do not respond quickly or accurately in the simulated environment	On the health or even life of humans – immediately or in later situations in real environment	High
Security threats	Criminals or terrorist acquiring those technologies and getting hold of software or communication	Exposure of the security holes of important sectors (police, military, industrial, communication)	High
Behavioral threats	Using avatars (instead of real person) for destructive behavior – harassing and stalking	Annoying, bullying and stressing others	Medium
Educational or training threat	Acquiring improper skills and knowledge of environment	Trainees can not cope in real-life situations	Medium to high
Bad investment	Developing augmented/virtual reality platform can be very expensive	Projects on augmented/virtual reality can bankrupt major developers	Medium

The physical threats may come from the imperfection of devices like head-up displays, or their non-interference with the peripheral vision of the pilot/users as the displays present information only in the central field. Also there is the threat of misjudging relative motions, due to the poorer (or absent) peripheral field.

In regard to the security threats there are significant risks in the way augmented or virtual environments are deployed. The communications used in such platform - voice, position, messages have to be protected and encrypted.

As mentioned above, virtual/augmented reality is often used in training. There is also the issue that those technologies help reducing social and cultural barriers, giving the chance of some to participate at higher level in the educational process. And often this is done using avatar. Here come the behavioral threats, where some individuals can assert a more destructive behavior, showing an non proper conduct of behavior.

Privacy threats are of concern even at present virtual societies like Facebook and Google+. Monitoring of presence, behavior and other issues of their users is alarming and stressful.

While those technologies can bring a great benefit, jumping on their use and development might be costly for a number of companies. It might be better to start with pilot virtual/augmented reality projects than spending a lot of money and not getting the expected advantage and value.

IoT has also a big security problem – sensors and other devices used in it are built with little or no security requirement. This could lead to serious vulnerabilities in applications in home, cities, industry, etc.

3. Cyber threats and challenges Exploration

Further on in the paper the problem with augmented and virtual reality mixing will be studied in a modeling context that allows to outline some tends and beliefs using experts' opinion, incorporated in a (3.1) system modelling approach and (3.2) probabilistic evaluation, following the approach proposed in [7].

3.1. System Modelling

The organization of this stage is based on the ideas of Vester's Dynamic System Theory generalization [8], successfully implemented for multiple cyber threats exploration [9], [10]. The modelling is performed, using experts' opinions, literature analysis data and I-SCIP-SA software environment [11].

A graphical interpretation of Chen's 'E-R' paradigm [12] is used, describing elements, as related entities in the model. All relations (uni- or bi- directional) are weighted in time (times equal to 0, concern static models, whilst – arrays of time values with certain functional – dynamic ones). Graphically, entities are marked with labeled rectangle or circle and relations, with arrows, labeled for both weight (yellow) and time (blue).

The resulting entities classification is obtained via generalization of relations weights visualized into a three dimensional Sensitivity Diagram (SD), using: influence (x), dependence, (y) and sensitivity (z) values. SD is providing four-sector entities classification (in accordance with x, y, z values): green – 'buffering', red – 'active', blue – 'passive' and yellow – 'critical'. Additional, 'active' (white, positive z values) and 'passive' (grey, negative z values) reassessment for each of the entities in a certain sector is also accomplished. This is also marked with elements' sensitivity evaluation towards the z axis. All entities from the model are visualized in SD with indexed balls.

A practical modelling implementation of '*IoT Gadgets*' into augmented and virtual - mixed '*Environment*' in the context of '*Users*' and Machine-To-Machine Artificial Intelligence developments – '*M2M AI Devts*', evolution together with the smart avatars '*Advanced Interface*' and '*Cloud Services*' for the modern connected by '*Network Comms*' web world is given in Figure 1.

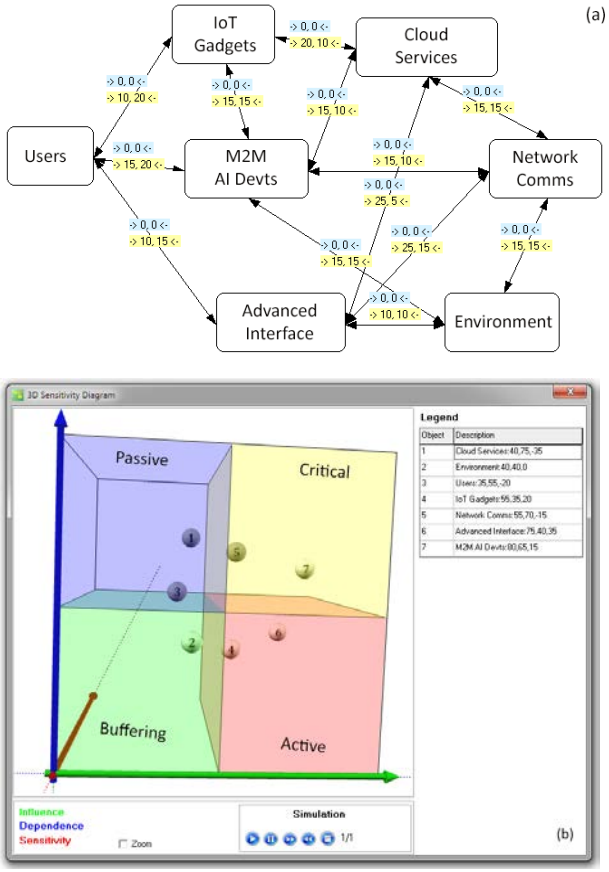

Figure 1. *A system model for cyber threats & challenges exploration in augmented reality (a) and the resulting sensitivity diagram (b).*

The resulting model SD (see Figure 1b) is defining the following classification for model potential sources of cyber threats: critical: '*Network Comms*' – '5' and '*M2M AI Devts*' – 7; active: '*IoT Gadgets*' – '4', '*Advanced Interface*' – 6; passive: '*Cloud Services*' – '1', '*Users*' – '3'; buffering: 'Environment' – '2'.

A further results probabilistic assessment is accomplished as the identified threats and challenges would be interesting for future dynamics trends evolution.

3.2. Probabilistic Assessment

Due to the prognostic nature of results from section 3.1, the studied processes have to be considered from multiple viewpoints. This practically, could be achieved combining selected system analysis entities classification from the SD (giving a priori assessment) with suitable probability distributions shapes. Thus, both experts' beliefs and development trends can be implemented as given in [7].

Additional further validation via agent-based simulation of cyberattacks towards selected relations of a certain entity of interest is performed. This provides a posteriori simulated probabilities change by assessing hypothetical evolution scenarios.

Five trends have been considered ('*Users*', '*IoT Gadgets*', '*Environment*', '*Network Comms*', '*Cloud Services*') for the most innovative entity '*M2M AI Devts*' from the presented model in section 3.1..

A resulting simulation from Matlab R2011b environment, using Beta distribution and cyberattacks probability defined after official statistics and experts' data beliefs [10], [13] with five-years' time horizon is provided in graphical form on Figure 2.

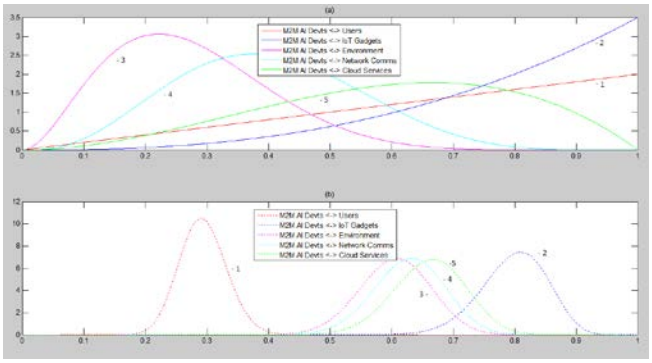

Figure 2. *A generalization of experts' a priori (a) and simulated a posteriori (b) probabilities for cyberattacks to 'M2M AI Devts'.*

According to the presented simulation results, '*IoT Gadgets*', '*Cloud Services*', '*Network Comms*' and smart 'Environment' (see Figure 2) are expected to be most probable (M > 0.5) for future cyberattacks in the new, mixed augmented reality environment.

4. Discussion

The presented analytical approach for exploration of innovative problems from modern digital world, like 'Augmented Reality', mixing in practice the real and virtual world is producing a useful solution towards the proper analysis of the present and future cyber security problems in this new media of human-machine interaction. When the proposed ideas are implementing experts' beliefs and simulation models, practical experimentation even within real laboratory environment will be of vital importance. Useful support in this sense could be obtained from hybrid simulations, like 'Academic Cyber CAX 2015' [14] and 'CYREX 2016' [15].

5. Acknowledgement

This study is partially supported by 'Creation of platforms for application studies in Internet of Things', UNWE Grant 1-5/2015-2016.

References

[1] HIT Lab, Thomas A. Furness III, http://www.hitl.washington.edu/people/person.php?name=tfurness [Online]

[2] Sherman W., Craig A., Understanding Virtual Reality: Interface, Application, and Design, Elsevier Science (USA), 2003, 608 p.

[3] Bymer L., Virtual reality used to train Soldiers in new training simulator, August 2012, http://www.army.mil/article/84453/ [Online]

[4] Mashable, Augmented Reality, http://mashable.com/category/augmented-reality/ [Online]

[5] Cameron C., Military-Grade Augmented Reality Could Redefine Modern Warfare, ReadWriteWeb, June 2010, http://www.readwriteweb.com/archives/military_grade_augmented_reality_could_redefine_modern_warfare.php [Online]

[6] Niiler E., Virtual Reality Is a National Security Threat, February 2016, http://news.discovery.com/tech/gear-and-gadgets/virtual-reality-is-a-national-security-threat-160212.htm [Online]

[7] Minchev, Z., et al. Cyber Intelligence Decision Support in the Era of Big Data, In ESGI 113 Problems & Final Reports Book, Chapter 6, FASTUMPRINT, 2015, pp. 85-92

[8] Vester F., The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity, München, MCB-Verlag, 2007.

[9] Minchev Z., Human Factor Role for Cyber Threats Resilience, In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare, IGI Global, 2015, pp.377-402

[10] Minchev Z. & Boyanov, L System Modelling & Experimental Assessment of IoT Cyberthreats in Future Smart Homes, In Proceedings of ICAICTSEE – 2015, Sofia, UNWE, November 13-14, 2015 (in press)

[11] Minchev Z., & Petkova M., Information Processes and Threats in Social Networks: A Case Study, In Proceedings of Conjoint Scientific Seminar 'Modelling and Control of Information Processes', Sofia, Bulgaria, November 19, 2010, pp. 85-93

[12] Chen P., The Entity-Relationship Model-Toward a Unified View of Data, ACM Transactions on Database Systems, vol. 1, no.1, 1976, pp. 9-36

[13] Минчев, З. Прогнозни заплахи и предизвикателства в киберпространството, CSDM Views, No. 31, юли, 2015, http://it4sec.org/bg/article/prognozni-zaplahi-i-predizvikatelstva-v-kiberprostranstvoto [Online]

[14] Минчев, З. и к-в, Хибридни предизвикателства в киберпространството и ролята на човешкия фактор, Сборник доклади от Международна научна конференция „Югоизточна Европа: новите заплахи за регионалната сигурност", Поредица „Наука, образование, сигурност", том 3, София, НБУ, Планета 3, 2016, стр. 354-362

[15] CYREX 2016, Facebook News Post, https://www.facebook.com/zlatogor/media_set?set=a.10205930490366187.1073741836.1377246688&type=1&l=ddca0a3fcc [Online]