# Adaptive Visualization of Complex Networks with FocalPoint: A Context Aware Level of Details Recommender System

Catherine Inibhunu and Scott Langevin
Uncharted Software, Toronto, Canada

Maintaining situational awareness of a dynamic global computer network that consists of ten to hundreds of thousands of computers is a complex task for cyber administrators and operators looking to understand, plan and conduct operations in real time. Currently, cyber specialists must manually navigate complex networks by continuous cycles of overviews, drilldowns and manually mapping network incidents to mission impact. This is inefficient as manually maneuvering of network data is laborious, induces cognitive overload, and is prone to errors caused by distractive information resulting in important information and impacts not being seen. We are investigating "FocalPoint" an adaptive level of detail (LOD) recommender system tailored for hierarchical network information structures. FocalPoint reasons about contextual information associated with the network, user task, and user cognitive load to tune the presentation of network visualization displays to improve user performance in perception, comprehension and projection of current situational awareness. Our system is applied to two complex information constructs important to dynamic cyber network operations: network maps and attack graphs. The key innovations include: (a) context-aware automatic tailoring of complex network views, (b) multi-resolution hierarchical graph aggregation, (c) incorporation of new computational models for adaptive-decision making on user tasks, cost/benefit utility and human situation awareness, and (d) user interaction techniques to integrate recommendations into the network viewing system. Our aim is to have a direct impact on planning and operations management for complex networks by; overcoming information overload, preventing tunnel vision, reducing cognitive load, and increasing time available to focus on optimum level of details of the global network space and missions.

## INTRODUCTION

Cyber attacks against network systems are becoming increasingly prevalent. Businesses and government agencies alike place great value on increasing and maintaining the security of their networks. The primary approach used to achieve this goal is human auditing and monitoring of network system displays. Today's state of the art network analysis and monitoring tools provide largely manual interactions, with limited ability to effectively navigate through complex networks at varying resolutions and fail to account for operational goals or business processes and their inherent uncertainty (Jones & Horowitz, 2011). Efficiency and effectiveness is only achieved with highly trained experts in cyber security and network administration. This approach does not scale to the number of operations, operational complexity, or rapid response required for the dynamic nature of cyber space. User performance in perception, comprehension, and projection of the cyber network situation suffers tremendously under these conditions, and must be improved to ensure effective system monitoring and, consequently, heightened cyber security.

In order to take effective actions and decisions in cyber space an operator needs to have a clear view of the current state of the network, potential attack paths, vulnerabilities, assessment of risks and mitigation strategies without cognitive overload.

Research on cyber situation awareness (Cyber SA) is focused on analyzing large volumes of data captured from complex cyber networks such as Best and Cox (2015) and mapping out threats from vulnerabilities on the overall network space using network maps and attack graphs in Cheng (2015). Visualization methods have been suggested to better understand results generated from monitoring and analysis systems (Angelini, Prigent & Santucci, 2015). However, visualization systems have several challenges as noted in Fink, North, Endert and Ros (2009) that these systems are not able to handle complex volumes of cyber data, do not allow cross correlation, perform poorly when trying to reason on context changes and lack the ability to manage multiple informational displays which leads to cognitive overload for users.

To increase the effectiveness of information visualization, Carenini, Conati and Hoque (2013) indicated there is a need to pay attention to the needs and abilities of the user with the concept of adaptability. Adaptive systems have been utilized on web interfaces, human learning tools and desktop assistance where systems learn about users then create adaptive models that generate user tailored recommendations (Jameson, 2008). However, when dealing with a dynamic cyber space where uncertainty is hard to detect and quantify, deciding what information is most relevant to the user is not a trivial exercise. Adaptive level of detail systems are needed to improve user performance when monitoring complex networks thus enhance decision-making and allow focus on critical issues and understand impacts that would be impossible with existing systems.

To address these challenges we are investigating "FocalPoint", a real-time adaptive system for determining appropriate LOD views tailored for hierarchical network information structures. FocalPoint reasons about contextual information associated with the network, user task, and user cognitive load to tune the presentation of network visualization displays to improve user performance in

perception, comprehension and projection of current cyber situational awareness.

The rest of this paper presents related work, followed by a technical objective of FocalPoint, and finally some concluding remarks.

## RELATED WORK

Our work draws on research from various fields: cyber situation awareness, adaptive systems, human computer interfaces, user modeling and adaptive visualization. The need to understand complex networks through Cyber SA has been studied extensively, in particular on the need to understand large amounts of data from network flows, detect anomalies and infer interesting patterns (Best & Cox, 2015). A comprehensive review of Cyber SA is detailed in Franke and Brynielsson (2014).

There are many challenges as noted in Best, Endert and Kidwell (2014) when trying to provide situation awareness to cyber analysts; big data, heterogeneous information sources, network linkage, data quality, cyber space threat progression, and balancing risk and reward. Approaches for handling large amount of data look to build data intensive architectures with visualization capability as described in Best and Cox (2015) where a combination of storage and statistical analysis for network behavior characterization is done, others use moving target defense as outlined in Fink et al. (2014) to understand CPU utilization and network bandwidth, while use of packet level data for modelling network behaviors is proposed in Pike, Scherrer and Zabriskie (2011).

Another approach aimed at providing Cyber SA on complex computer networks is the creation of attack graphs which are used to formulate potential paths an attacker might exploit to compromise a system (Homer, Varikuti, Ou & McQueen, 2008). Various techniques have been utilized from machine learning and data mining to represent, generate and understand interesting behaviors among nodes with attack graphs; probabilistic approaches (Noel, 2004; Wang, 2010), Neural Networks (Kotenko & Stepashkin, 2006), Stochastic and spatiotemporal methods (Abraham, 2015; Chen, 2015). A comprehensive review on attack graphs is presented in Shandilya, Simmmons and Shiva (2014).

The number of potential attack paths generated grows exponentially even on a network with a small amount of nodes. This becomes a difficult challenge when trying to analyze and understand any relationships among the different nodes. Visualization is suggested in Noel and Jajodia (2004) as a way to show the attack graph relationships to a user. However, current visualization systems are not able to scale to large networks resulting in cognitive overload on users thus ineffecive to providing Cyber SA. To overcome this, adaptive systems can be built to fit users specific knowledge, background and objective (Fischer, 2001).

Studies on adaptive systems present varying techniques looking to improve human computer collaboration (Fischer, 2001). These systems are able to adapt their behaviors based on user interaction, tasks and changes on context and the environment. Several researchers have looked at how such adaptive systems can be modeled such that human-computer interaction is integrated seamlessly, bayesian networks to infer user focus (Horvitz, 1999; Bencomo, 2013), adaptation by content, presentation and navigation in Zarikas (2007), and using adaptive interfaces to adapt user behavior, recommendations and smart menus in Jameson (2008). Others use taxonomies to identify adaptation levels and their triggers such as Feigh, Dorneich and Hayes (2012), agent-based simulations using weights to evaluate tasks and goals for adaptation in Topcu (2014), models to automate user tasks with minimal interaction between human and machine in Soh, Sanner and Jamieson (2015), and ontology based concept trees, hierarchies to link concepts and functions then reasoning on possible adaptation states in Vassev and Hinchey (2015).

Common understanding among researchers is that systems can change and reorganize their components to adapt themselves to the system and user context. The challenges lies on the ability to accurately perceive and interpret users current cognitive state, integrating state of the environment, system, user task and predict users current needs (Feigh et al., 2012).

Adaptive visualization research looks to enhance visualization thus reducing information overload (Nazemi, Stab & Kuijper, 2011). Techniques applied includes content delivery adaptation using parameterization, cache, and network neighborhoods detailed in Papadakis, Zahariadis and Nikolaouet (2015), fuzzy logic to infer context, incoming data, human concepts and real world situations in Haghighi et al. (2010), probabilistic approaches to identify user anomalies, similarities and deviation from norm in Nazemi et al. (2014) and inclusion of human attributes in Steichen (2013). Ontologies have been used to depict visualization paradigms as described in Ryabinin and Chuprin (2015).

In addition to existing challenges on systems that try to use visualization to provide situation awareness in cyber space such as cognitive overload, adaptive visualization systems are faced with several problems; ability to appropriately adapt on details, changing evolving knowledge context allowing user to modify or customize thus enhance visualization. Furthermore, in an attempt to be dynamic, the systems lack contextual knowledge of the visualization paradigm and effective methods to address changing requirements and user interaction with the system.

## FOCALPOINT TECHNICAL OBJECTIVE

Providing situation awareness on large and complex cyber networks is a research area studied extensively in statistical analysis and information visualization (Best & Cox, 2015). However, the amount of information generated that a human can synthesis and manage effectively becomes a huge challenge (Fink et al., 2009). Novel approaches to understand the contextual information about the environment, the user and tasks/missions, and accurately infer users viewing intention is needed to provide effective situation awareness (Nazemi et al., 2011).

To address these challenges, our research on FocalPoint investigates the integration of; cyber situation awareness, human computer interfaces, user modeling and context-aware adaptive visualization to develop an adaptive system for recommending LOD views of large-scale and dynamic

network environments leading to enhanced decision making in cyber space. To the best of our knowledge, no system exists addressing these research areas.

Using data captured from complex cyber networks representing hundreds to tens of thousands of nodes, FocalPoint reasons about contextual information associated with the network, user task, and user cognitive load to tune the presentation of network visualization displays to improve user performance in perception, comprehension and projection of current situational awareness.

FocalPoint is applied to two complex information constructs related to cyber operations: network maps and attack graphs. Adaptive LOD recommendation is used to tailor cyber views to summarize normative aspects of the network and focus attention on abnormal activity, prioritizing and linking to potential risks.

FocalPoint provides:

(a) Context-aware automatic tailoring of cyber network views by utilizing knowledge bases of, networks, tasks, assets, health and status information to increase situational awareness in cyber space.

(b) Multi-resolution hierarchical graph aggregation of network maps to present heterogeneous level of detail that varies with relevance to operator task and system state. Automatic link filtering allowing users to focus on critical tasks and works with larger networks.

(c) Invention of new methods for usable adaptations thereby mitigating adaptive usability issues such as balancing unsolicited automation that disrupt user workflow vs. recommending adaptations in context using previews.

**Automatic Context Reasoning**

Inclusion of automatic context reasoning into information visualization systems has been identified as a Grand-Challenge in Thomas and Cook (2005). FocalPoint is looking to addresses this by providing context aware reasoning services that adapt views of key elements in cyberspace, including node-link visualizations of network maps, and attack graphs. This is done by integration of advanced visualization and adaptive user interfaces similar to Nazemi, et al. (2011) combined with machine learning principles for network reasoning in Jensen and Nielsen (2007) and context-aware computational intelligence techniques detailed in Abbas, Zhang and Khan (2015).

**Proactive Decision Support**

A challenge with monitoring and decision-making in complex dynamic environments is getting the "right information" at the "right time". To address this challenge, a system needs to be able to determine information relevance, overcome operator's cognitive overload, prevent tunnel vision and adapt visual displays of network assets accordingly thus provide proactive decision support (PDS). FocalPoint aims to address PDS by; (a) increasing scale, scope and mission plans on systems that are managed and understood by human operators, (b) overcoming information overload hence quickly make sense of highly complex networks and vulnerabilities by seeing critical structures and the most important information, (c) preventing tunnel vision where the operator's attention resources become mis-engaged with lower priority detail and (d) reducing the cognitive load required of planners and operators, lowering fatigue and increasing awareness levels.

**Adaptive Level of Detail Reasoning Service**

FocalPoint provides automatic and context-aware adaptation of the LOD to tailor cyber views dynamically. We use an attack graph-based knowledge representation to represent all potential attack paths between nodes and provide visual representation of the attack process (Swiler, 2001; Sheyner, 2002; Noel, 2004). The representation can be used offensively or defensively to understand the relationship between vulnerabilities and threats (Barik, 2011; Wang, 2006). Attack graphs are augmented with attributes from network maps to represent device and network attributes, health and status information such as bandwidth, utilization and latency. Reasoning services are integrated to infer where uncertainty or risk is high and draw attention to these areas. User and system activity logging together with user models infers the current user task as it relates to view requirements, represents the user operational role, and estimates user cognitive load. Together these models provide machine decision-making on when to tailor or recommend views, presentation changes and the level of detail most effective to support the user.

**Adaptive Display of Network Details**

To understand network connectivity among related nodes, FocalPoint aggregates exploits shared among these nodes by adopting monotonicity principles in Noel and Jajodia (2004) and allowing the simplification of views by removing steps determined to be unnecessary to understand attack goals as noted in Homer, et al. (2008). With this, the user can focus efficiently on exactly the information they require. In addition, FocalPoint performs level of detail adjustments automatically as the user's task and cyber situation context changes.

Our focus on adaptive display of network details is on two user-system interactions; (1) User requests for information, the system retrieves the requested information and tailors the associated level of detail, e.g. query for sub-graph, task plan, navigating network map or attack graph. (2) The display system receives new information from sensors or analytic services, and the current display is updated, e.g. updates to network properties such as latency, utilization, or connectivity.

**Automation and Recommendation methods for Usable Adaptations**

The phenomenon of information overload is noted as a huge challenge by many researchers who are trying to reduce cognitive overload, interaction cost and collaborative viewing (Nazemi, et al., 2011). To address this problem, we are investigating new methods to communicate to the user on

adaptive LOD changes. In particular we are looking at the ability to determine triggers, when to make recommendations for usable adaptations and when to automate thus enhance user computer interactions and reduce cognitive overload. We are utilizing similar principles in (Nazemi, 2011, 2014; Zorzal, 2014) to derive user interactions and behaviors for appropriate automation and recommendations.

**FocalPoint Architecture**

Input to FocalPoint is network maps, attack graphs, streams of sensor alerts, and user activity events. The context-aware reasoning component performs high-level reasoning over the cyber space and current user task. The decision component receives information from the reasoner and makes adaptation decisions that signal the adaptation execution modules to tailor the level of detail. Execution modules receive adaptation parameters from the decision component and using state information from the reasoner, adapt the level of detail accordingly. The gray components facilitate integration to other systems.

*Activity Monitor.* This component gathers information on user and system activity. An event logging system similar to tacit collaboration and recommendation services for intelligence analysts is tailored for cyber planner and operator activities (Schroh et al, 2009). Events captured are high-level indicators of activity and are used by user modeling services to build models of individual context. Interaction with operations and elements in the network or attack graphs signal interest in investigation or monitoring user tasks. Events provide evidence to the user and task reasoning component.

*User and Task Reasoning.* Utilizing probabilistic Hidden Markov Models (HMM) principles similar to work in MacInnes et al. (2008), temporal context models infers the task or subtask the user is currently engaged in given a sequence of activity events received from the user activity sensors. Inferred user tasks are part of the system context necessary to effectively provide context-aware adaptive user interfaces.

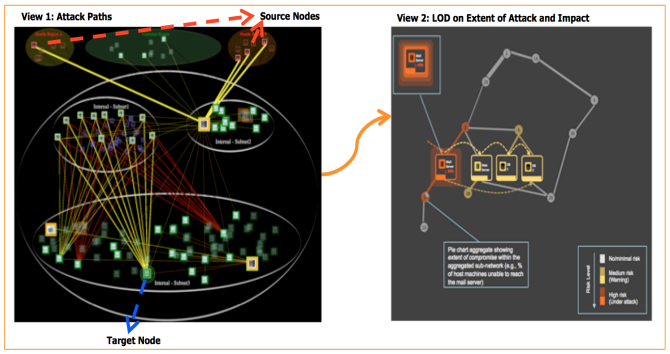
*Context Reasoning.* Gathering relevant information on the state of the environment, the user and tasks/missions, this component evaluates any changes to context using computational intelligence techniques similar to works in (Nazemi, 2011; Zhang, 2015) and network reasoning in Jensen and Nielsen (2007) to derive new facts from existing context. The resulting contextual information is used to increase visual prominence of potential attack path threats or bring information to the forefront when mission risk is increased. This information highlights key network components where uncertainty and risk is greater, and provide the relevant details.

*Adaptive Decision.* Influence diagrams encode adaptation decisions as detailed in Zarikas (2007). These are decision theoretic models that utilize graphical probabilistic models, augmented with decision and utility nodes in Jensen and Nielsen (2007). Our utility models provide a trade off view on interaction cost/benefit vs. user cognitive load to guide adaptive decision-making. FocalPoint predicts the consequences of possible system actions using prior empirical learning, and evaluates the possible actions, taking into account situation-dependent priorities and the tradeoffs between the consequences (Jameson, 2001). Our decision model determines the value of new information vs. the cognitive load cost of the operator and whether it warrants an adaptation of visual display.

*LOD Adaptation Modules.* These modules tailor level of details presented in cyber visualizations to satisfy adaptation decisions. Parameters that govern the adaptation module control how to perform the adaptation, such as level of detail to present, and modality for the adaptation (recommend or automate). Each module is associated with one or more domain objects such as network maps or attack graphs. Adaptation instructions convey the necessary information for the view display to alter the presentation of its information.

*Adaptive Display Details for Attack Graphs.* A sample of an attack graph is shown in Figure 1, this depicts a network that contains several subnets (clusters), 3 internal and 3 external (machines as nodes, links as edges). 2 of the external subnets represent potential hostile regions (attackers) and there are some machines in these hostile regions sending communication to several machines in the internal subnets. FocalPoint allows one to clearly see the various paths the attackers can take to compromise the internal subnets, probabilistic weights on paths are used to highlight risk.

**Figure 1: Attack Graph.** View 1 represents the various paths that the attackers (source nodes) might take to compromise several machines if they have access to the target node. FocalPoint aggregates exploits shared among the different machines and as shown in view 2 machines with similar exploits are grouped together thus allowing a user to focus on important information. View 2 also includes attributes necessary to assess severity.




## CONCLUSION

Our research on FocalPoint presents an innovative approach to understanding complex space. We integrate techniques drawn on research from various fields: cyber situation awareness, adaptive systems, human computer interfaces, user modelling and adaptive visualization.

Using data captured from complex cyber systems, FocalPoint reasons about contextual information associated with the network, user task, and user cognitive load to tune the presentation of network visualization displays to improve user performance in perception, comprehension and projection of current situational awareness. We anticipate that with proactive decision-making and context aware reasoning, user,

tasks and system cognitive states are appropriately managed leading to adaptive LOD views that are effective.

In future work we plan to conduct component level tests and user experimentation to measure the effectiveness of FocalPoint using representative Cyber SA scenarios and compare against a baseline.

## Acknowledgement

This work is supported by Office of Navy Research (ONR) Command Decision Making (CDM) Program under Contract No. N00014-15-C-5033 to Uncharted Software Inc. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflects the views of ONR. The ideas presented here reflect discussions with many people, especially from Uncharted Software and University of Toronto's Cognitive Engineering Laboratory.

## References

Abraham, S., & Nair, S. (2015). A Predictive Framework for Cyber Security Analytics using Attack Graphs. *International Journal of Computer Networks & Communications , 7* (1).

Abbas S. Zhang L. & Khan S.U (2015) A survey on context-aware recommender systems based on computational intelligence techniques. *Computing 97(7) 667-690*

Angelini, M., Prigent, N., & Santucci, G. (2015). PERCIVAL: Proactive and rEactive attack and Response assessment for Cyber Incidents using Visual AnaLytics. *VizSec 2015.* IEEE.

Barik, M., & Mazumdar, C. (2011). A novel approach to collaborative security using attack graph. *IMSAA* (pp. 1-6). IEEE.

Bencomo, N., Belaggoun, A., & Issarny, V. (2013). Dynamic Decision Networks for Decision-Making in Self-Adaptive Systems: A Case Study. *SEAMS.* San Francisco: ICSE.

Best, D. M., & Cox, B. A. (2015, July/August). Clique: Situational Awareness through Behaviour. (K. Evans, Ed.) *Smart Systems* , 66-68.

Best, D. M., Endert A., Kidwell D. (2014). 7 key Challenges for Visualization in Cyber Network Defense VizSec. Paris, 33-40.

Carenini, G., Conati, C., Hoque, E., & et al. (2013). Highlighting Interventions and User Differences: Informing Adaptive Information Visualization Support. *CHI.* Paris: ACM SIGCHI.

Chen, Y.-Z., Huang, Z.-G., Xu, S., & Lai, Y.-C. (2015, May). Spatiotemporal Patterns and Predictability of Cyberattacks. *PLOS One* , 1-19.

Cheng, Y.-Z., Huang, Z.-G., Xu, S., & Lai, Y.-C. (2015, May). Spatiotemporal Patterns and Predictability of Cyberattacks. (Z.-K. Gao, Ed.) *PLOS ONE* .

Endsley, M. (2008) Situation Awareness: A Key Cognitive Factor in Effectiveness of Battle Command, Battle for Cognition, Praeger, CT.

Feigh, K. M., Dorneich, C. M., & Hayes, C. C. (2012, December). Toward a Characterization of Adaptive Systems: A Framework for Researchers and System Designers. *Human Factors* .

Fink, G. A., Haack, J. N., & McKinnon, D. (2014). Defense on the Move: Ant-Based Cyber Defense. *IEEE Security & Privacy , 12* (2), 36-43.

Fink, G. A., North, C. L., Endert , A., & Rose, S. (2009). Visualizing Cyber Security: Usable Workspaces. *6th International Workshop on Visualization for Cyber Security* (pp. 45-56). VizSec.

Fischer, G. (2001). User Modeling in Human - Computer Interaction. *User Modeling and User-Adapted Interaction , 11*, 65-86.

Franke, U., & Brynielsson, J. (2014). Cyber situation awareness - A systemic review of the literature. *Computers & Security* , 18-31.

Haghighi, P. D., Gillick, B., Krishnaswamy, S., Gaber, M. M., & Zaslavsky, A. (2010). Situation-Aware Adaptive Visualization for Sensory Data Stream Mining. *Sensor-KDD.* Berlin: Springer-Verlag.

Homer, J., Varikuti, A., Ou, X., & McQueen, M. (2008). Improving Attack Graph Visualization through Data Reduction and Attack Grouping. *VizSec.* IEEE.

Horvitz, E. (1999, September). Uncertainty, Action, and Interaction: In Pursuit of Mixed-Initiative Computing. *Intelligent Systems* , 17-20.

Jameson, A. (2008). Adaptive Interfaces and Agents. In A. S. Jacko (Ed.), *Human-computer interaction handbook: Fundamentals, evolving technologies and emerging applications* (2nd ed.). New York.

Jameson, A. B.-H. (2001). When actions have consequences: Empirically based decision making for intelligent user interfaces. *14*, 1-2.

Jensen, F. V. & Nielsen T. D. (2007). *Bayesian networks and decision graphs.* NY.

Jones, R..A & Horowitz B. (2011). (2013). System-Aware Cyber Security. *8th International Conference on Information Technology: New Generation.*

Kotenko, I., & Stepashkin, M. (2006). Attack Graph Based Evaluation of Network Security. In H. L. Markatos (Ed.), *CMS* (pp. 216-227). IFIP.

Langevin, S., Valtorta, M., & Bloemeke, M. (2010). Agent-Encapsulated Bayesian Networks and the Rumor Problem. *Int. Conf. on Autonomous Agents and Multiagent Systems.* Toronto: International Foundation for Autonomous Agents and Multiagent Systems.

MacInnes, J., Santosa, S., Kronenfield, N., McCuaig J. et al. (2008). nAble Adaptive Scaffolding Agent– Intelligent Support for Novices. *International Conference on Web Intelligence and Intelligent Agent Technology.* IEEE.

Nazemi, K., Retz, W., Kohlhammer, J., & Kuijper, A. (2014). User Similarity and Deviation Analysis for Adaptive Visualizations. In S. Yamamoto (Ed.), *HIMI* (pp. 64-75). LNCS.

Nazemi, K., Stab, C., & Kuijper, A. (2011). A Reference Model for Adaptive Visualization Systems. *HCII* (pp. 480-489). Orlando: Human-Computer Interaction.

Noel S., J. S. (2004). Managing Attack Graph Complexity Through Hierarchical Aggregation. . VA: CCS Workshop on Visualization and Data Mining for Computer Security.

Noel, S., & Jajodia, S. (2004). Managing Attack Graph Complexity Through Visual Hierarchical Aggregation. *CCS Workshop on Visualization and Data Mining for Computer Security.* Fairfax VA: ACM.

Papadakis, A., Zahariadis, T., & Nikolaou, N. (2015). Adaptive content caching simulation with visualization capabilities. *Telecommun Syst* , 531-539.

Pike, W. A., Scherrer, C., & Zabriskie, S. (2011). Putting Security in Context: Visual Correlation of Network Activity with Real-World Information.

Poolsappasit. (2012). Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing , 9*, 61-74.

Ryabinin, K., & Chuprina, S. (2015). Development of ontology-based multiplatform adaptive scientificvisualization system. *Journal of Computational Science* .

Schroh, d., et al. (2009). nCompass Service Oriented Architecture for Tacit Collaboration Services,. *International Conference on Information Visualization.* IEEE.

Shandilya, V., Simmons, C., & Shiva, S. (2014). Use of Attack Graphs in Security Systems. *Journal of Computer Networks and Communications* .

Sheyner, O., Haines, J., Jha, S., Lippmann, R., & Wing, J. (2002). AAutomated Generation and Analysis of Attack Graphs. *Symposium on Security and Privacy* (pp. 273 - 284). IEEE.

Soh, H., Sanner, S., & Jamieson, G. (2015, December). A Decision-Theoretic Approach for Adaptive User Interfaces in Interactive Learning Systems. *NIPS*

Steichen, B., Carenini, G., & Conati, C. (2013). User-Adaptive Information Visualization - Using Eye Gaze Data to Infer Visualization Tasks and User Cognitive Abilities. *IUI.* Santa Monica: ACM.

Swiler, L. P., Phillips, C., Ellis, D., & Chakerian, S. (2001). Computer-Attack Graph Generation Tool. *DISCEX.* IEEE.

Thomas, J. J., & Cook, K. A. (2005). Visualization Viewpoints. (T.-M. Rhyne, Ed.) *IEEE Computer Graphics and Applications* .

Topcu, O. (2014). Adaptive decision making in agent-based simulation. *Simulation , 90* (7), 815-832.

Vassev, E., & Hinchey, M. (2015). KnowLang: Knowledge Representation for Self-Adaptive Systems. *Software Technologies* , 81-84.

Wang, L., Jajodia, S., Singhal, A., & Noel, S. (2010). k-zero day safety: measuring the security risk of networks against unknown attacks. *Proceedings of the 15th European conference on Research in computer security.* ESORICS.

Wang, L., Noel, S., & Jajodia, S. (2006). Minimum-cost network hardening using attack graphs. *Computer Communications , 29*, 3812-3824.

Zarikas, V. (2007). Modeling decisions under uncertainty in adaptive user interfaces. *Inf Soc , 6*, 87-101.