PhD Days

Cyber Sécurité en Réalité Virtuelle : améliorer le processus de détection d'intrusion, d'investigation et de décision via l'utilisation de techniques de visualisations 3D immersives

Présenté par Nicolas Delcombel
Encadré par Thierry Duval et Marc-Oliver Pahl

24 Juin 2021

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

chairecyber-cni.org/

Sommaire

Présentation

Représentation de données temporelles multivariées

- Etat de l’art
- Prototype
- Expériences envisagées

Représentation de réseaux

Interaction multimodales

Planning

Objectif de la thèse

Proposer de **nouveaux moyens** d'aide à la **gestion d'intrusion** basés sur la détection de **signaux dits « faibles »**

Définitions

Signaux faibles :

Avertissements difficiles à détecter, trop incomplets pour permettre des estimations précises

Pour la cyber :

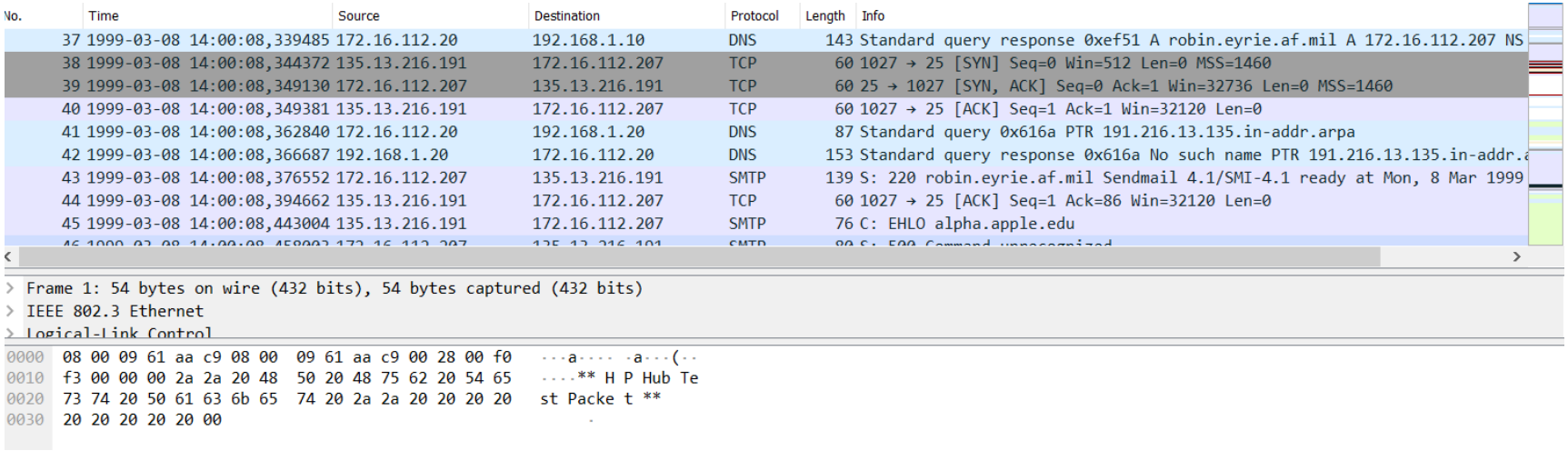
La plupart des attaques perturbent la “périodicité” du réseau [Anh Huynh, 2016]

Elles restent difficiles à détecter car noyées dans le bruit

Cybersécurité

Grande quantité de données hétérogènes venant de capteurs différents

Des outils pas adaptés pour les afficher



Wireshark

Visualisations pour la cybersécurité

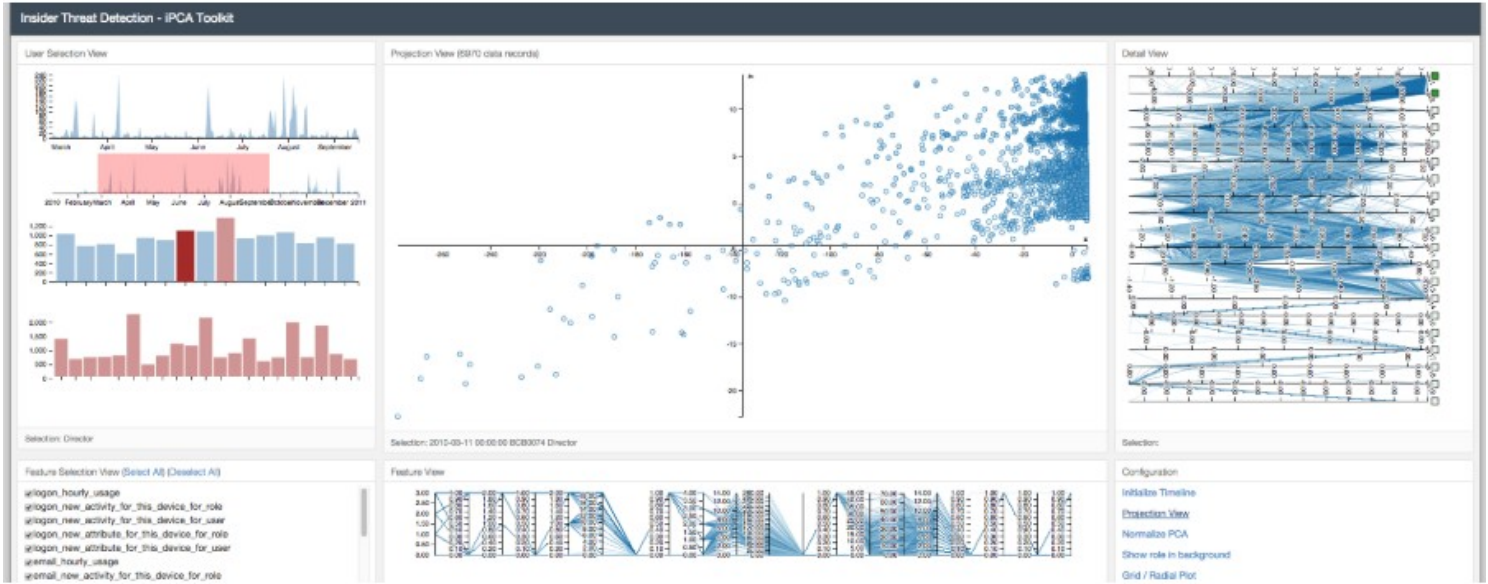
Interactives

Mantra de Schneidermann : Overview First, Zoom and Filter, Details on Demand

Limitées en taille et en méthodes d'interactions

Visualisations pour la cybersécurité

Exemple : Legg, 2015 [1]

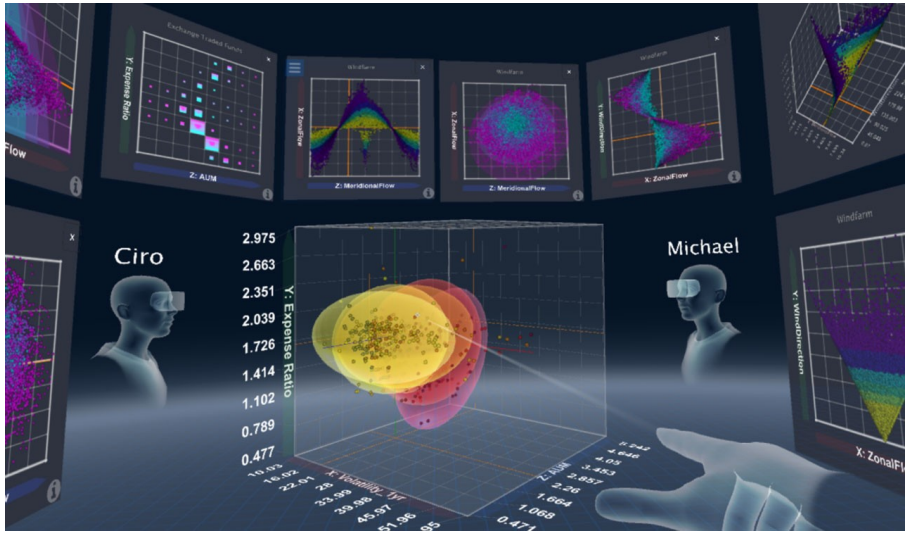


L’immersive Analytics

Étudie comment les nouvelles interactions et technologies d'affichage peuvent soutenir le raisonnement analytique et la prise de décision.

Offre des interfaces multi-sensorielles pour les approches analytiques favorisant la collaboration et l’immersion.

Chandler et al., 2015 [2]



Questions de recherche

Comment l’Immersive analytics peut-elle se mettre au service de la cybersécurité ?

Quelles représentations et interactions choisir pour quel problème ?

- En particulier celui des signaux faibles
- En fonction du type de données

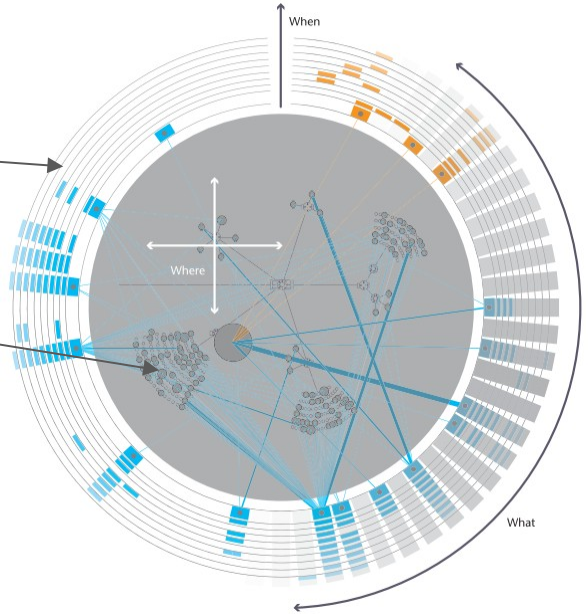
Quelles sont les bonnes pratiques de l’Immersive Analytics ?

Etat de l’art : représentation de données temporelles multivariées

Représentations 2D pour la cybersécurité: exemple 1

Alertes au cours du temps

Noeuds du réseau

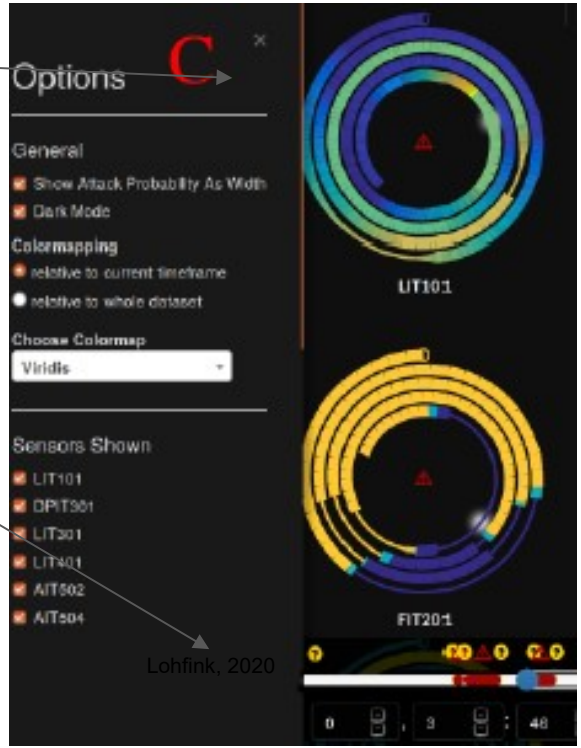


Foresti, 2006
[3]

Etat de l’art : représentation de données temporelles multivariées

Représentations 2D pour la cybersécurité: exemple 2

- Visualisations des différents capteurs
- Des alertes sont levées et affichées sur la timeline



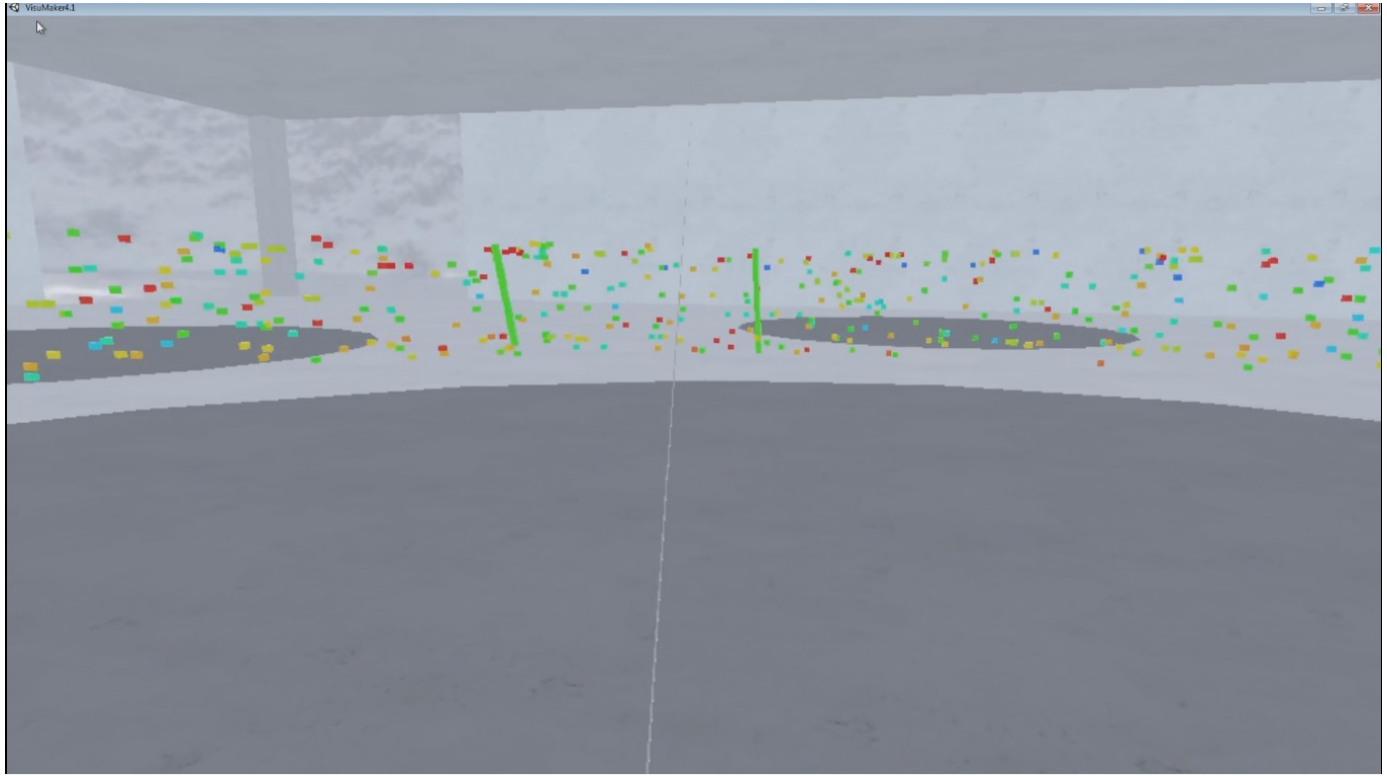
Besoins :

- comparaison entre capteurs
- lien avec le monde réel
- manque de place

Lohfink, 2020 [4]

Etat de l’art : représentation de données temporelles multivariées

Représentation 3D pour la mise en valeur de signaux périodiques



Cantu, 2018 [5]

Synthèse

- Des spirales ou cercles concentriques mettent en valeur les motifs périodiques en 2D
- En 3D, l’équivalent de ces représentations est l’hélice
- La représentation doit permettre de croiser les données

- Il est acceptable d’utiliser plusieurs dimensions de la représentation pour représenter une dimension du jeu de données si cela permet de détecter les motifs qui s’y trouve
- L’Immersive Analytics peut ignorer les guidelines 2D, et créera les siennes une fois qu’assez de visualisations pourront être analysées

Cybercopter

Jeu de données

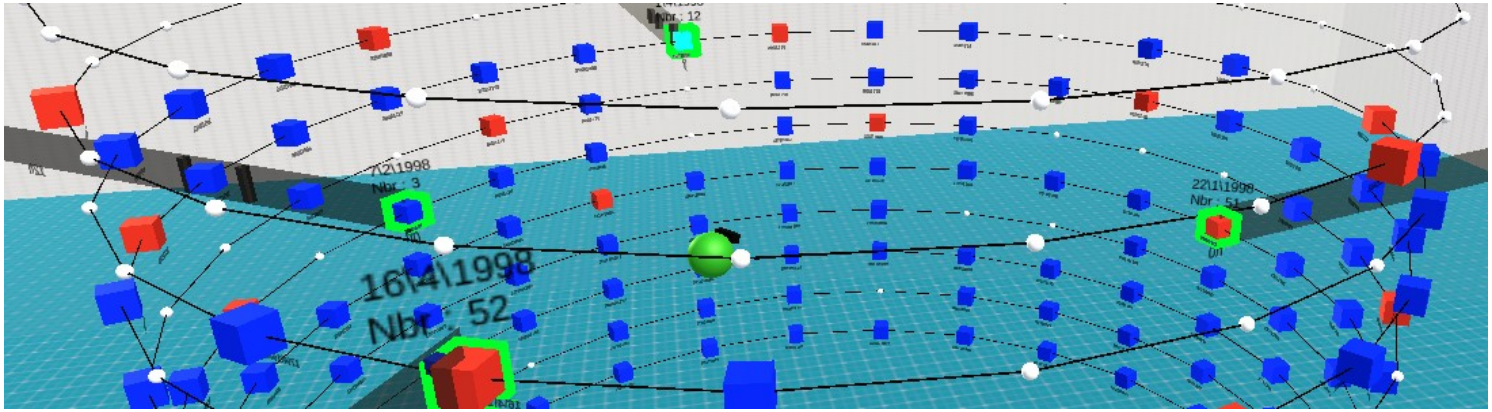
- SWaT
- Données issues de capteurs physiques d'une usine de traitement d'eau
- Plusieurs attaques sont menées afin de nuire au fonctionnement de l'usine
- Cela perturbe le fonctionnement périodique de l'usine

	Timestamp	FIT101	LIT101	MV101
0	28/12/2015 10:00:00 AM	2,427057	522,8467	2
1	28/12/2015 10:00:01 AM	2,446274	522,886	2
2	28/12/2015 10:00:02 AM	2,489191	522,8467	2
3	28/12/2015 10:00:03 AM	2,53435	522,9645	2
4	28/12/2015 10:00:04 AM	2,56926	523,4748	2
5	28/12/2015 10:00:05 AM	2,609294	523,8673	2
6	28/12/2015 10:00:06 AM	2,637158	524,1028	2

SWaT (2015) [6]

Cybercopter

Présentation



Chaque hélice représente un capteur

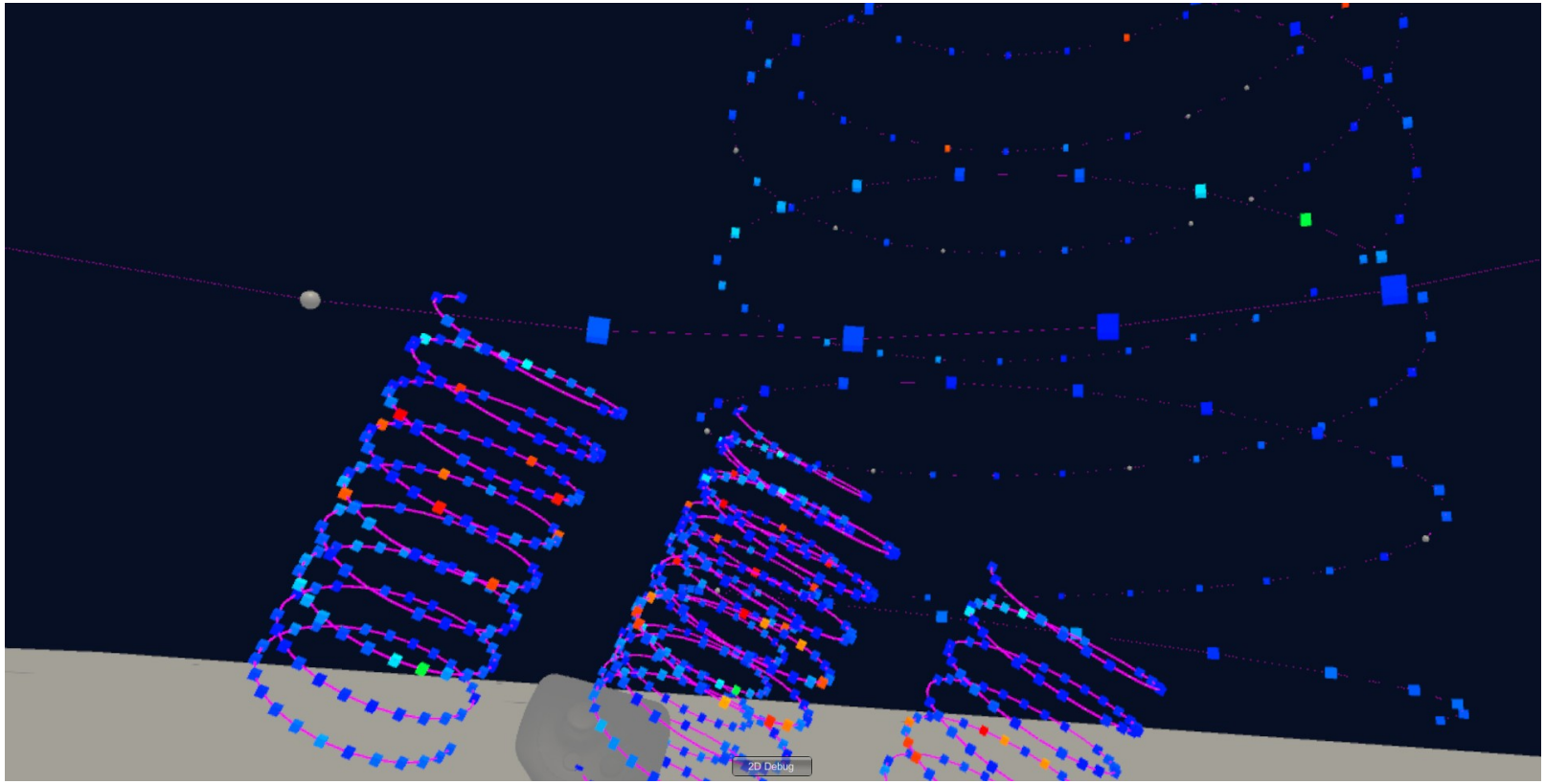
Chaque cube représente un pas de temps, sa couleur dépend de la valeur du capteur

L'utilisateur peut faire varier la périodicité des hélices

La 3D permet la comparaison et le positionnement géographique

Cybercopter

Démo



Cybercopter

Expérience envisagée

Comparaison 2D vs 3D

Utiliser un scénario similaire à celui utilisé par Lohfink

Hypothèses :

- la 3D facilite la comparaison
- la 3D permet d’afficher un plus grand nombre de capteurs dans la scène sans “perdre” l’opérateur
- L'environnement immersif augmente le sentiment de présence, la situational awareness et l’engagement.

Cybercopter

Expérience envisagée

L’environnement immersif permet de mieux se souvenir des scénarios effectués sur le long terme.

Cybercopter

Synthèse

- Les représentations hélicoïdales permettent d’afficher des données temporelles multivariées en mettant en valeurs les signaux périodiques
- Elles permettent de croiser plusieurs informations entre elles

MAIS

- Elles ne permettent pas d’afficher des réseaux

Etat de l’art : représentation de réseaux

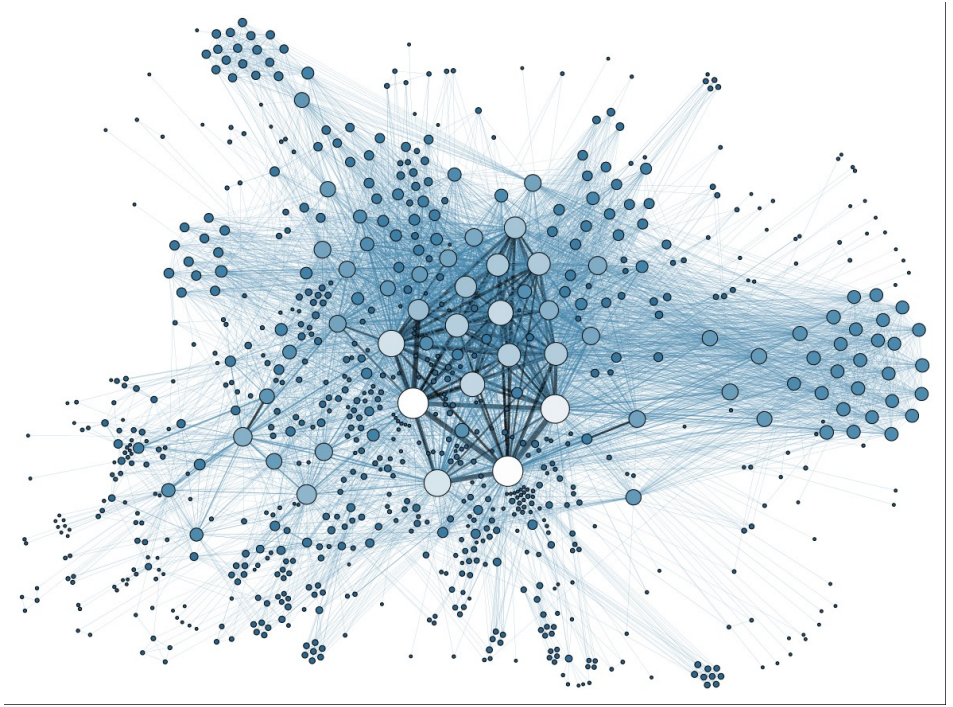
Graphes

Les Cahiers du Numérique 10, 2014

Etat de l’art : représentation de réseaux

Graphes

- Les graphes ne permettent pas une exploration temporelle facile.
- Pour représenter le temps : soit on affiche une multitude de graphes, soit on utilise des animations.
- Fatiguant

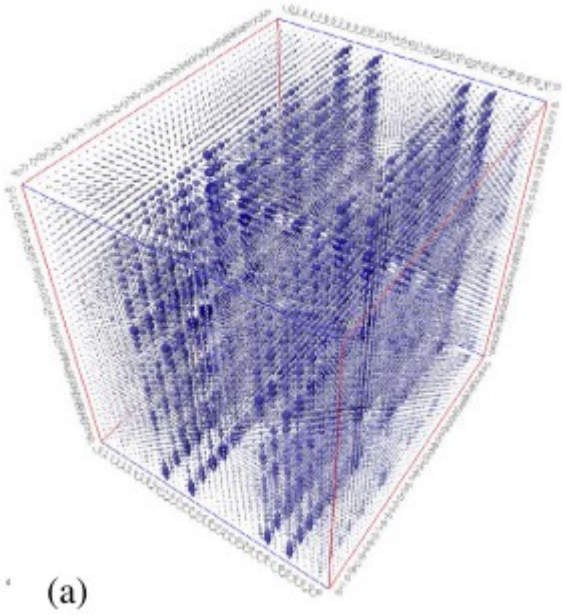


Les Cahiers du Numérique 10, 2014

Etat de l’art : représentation de réseaux

Matrice 3D de corrélation

- Solution : matrice 3D de corrélation
- Permet de faire apparaître des motifs temporels
- Nécessite des interactions pour être utilisable



Bach,2014 [7]

Etat de l’art : représentation de réseaux

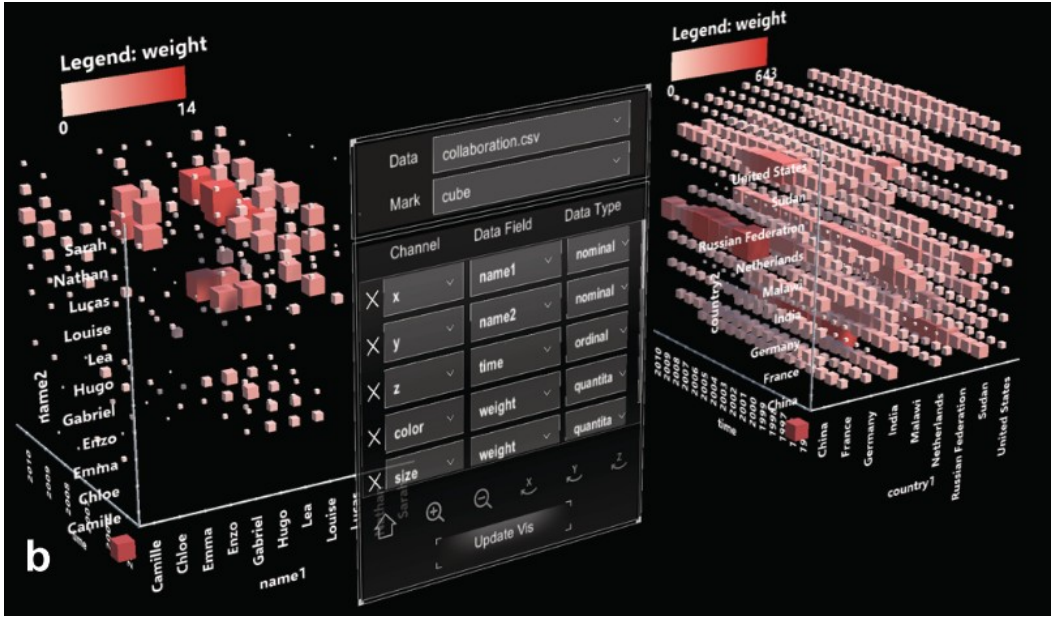
Matrice 3D de corrélation

Problèmes :

- occlusion
- représentation avec un volume important

Solution : multimodalité

- vibrations et sons en sortie
- voix en entrée

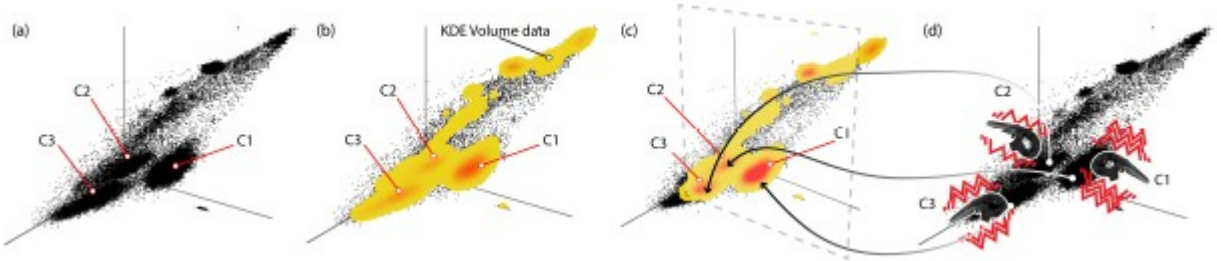


DXR, 2019 [8]

Etat de l’art : Multimodalité

- Les interfaces multimodales améliorent les performances de l'utilisateurs [9]
- Elles peuvent être utilisées pour immerger et guider l’utilisateur dans les jeux de données
- La multimodalité permet de représenter d’autres dimensions du jeu de données sans surcharger la mémoire de travail. [9]
- La voix permet de faire facilement des requêtes [12]

Christos Papadopoulos, 2004 [10]



Arnaud Prouzeau, 2019 [11]

Etat de l’art : Multimodalité

- Les interfaces multimodales améliorent les performances de l'utilisateurs [9]
- Elles peuvent être utilisées pour immerger et guider l’utilisateur dans les jeux de données
- La multimodalité permet de représenter d’autres dimensions du jeu de données sans surcharger la mémoire de travail. [9]
- La voix permet de faire facilement des requêtes [12]

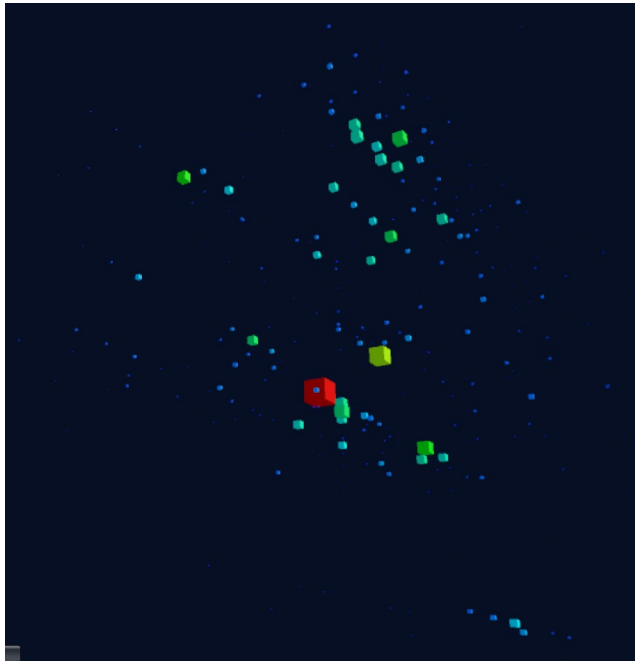
Synthèse

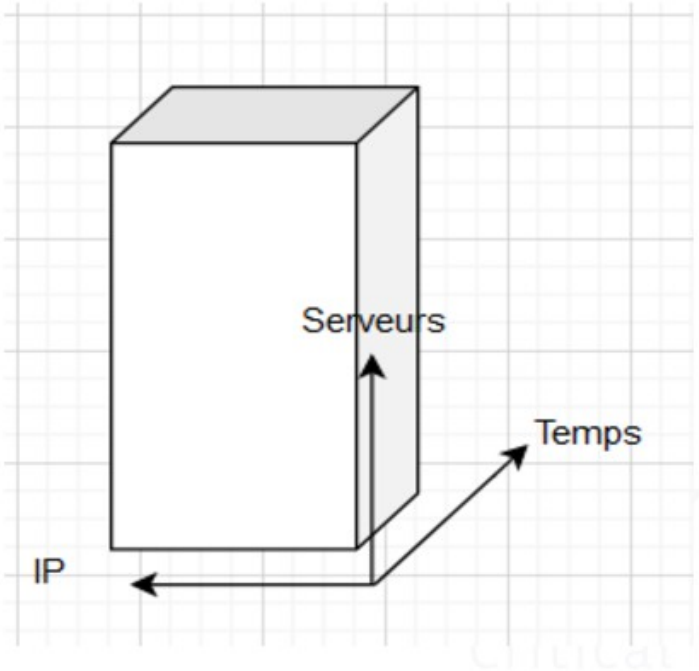
- Les matrices 3D de corrélation permettent d’afficher un réseau en mettant en valeur des évènements périodiques
- La multimodalité peut permettre d'interagir plus efficacement avec les représentations 3D

- L’immersive Analytics peut s’inspirer des travaux des psychologues pour trouver les bonnes représentations

Cubernêtikê

Présentation





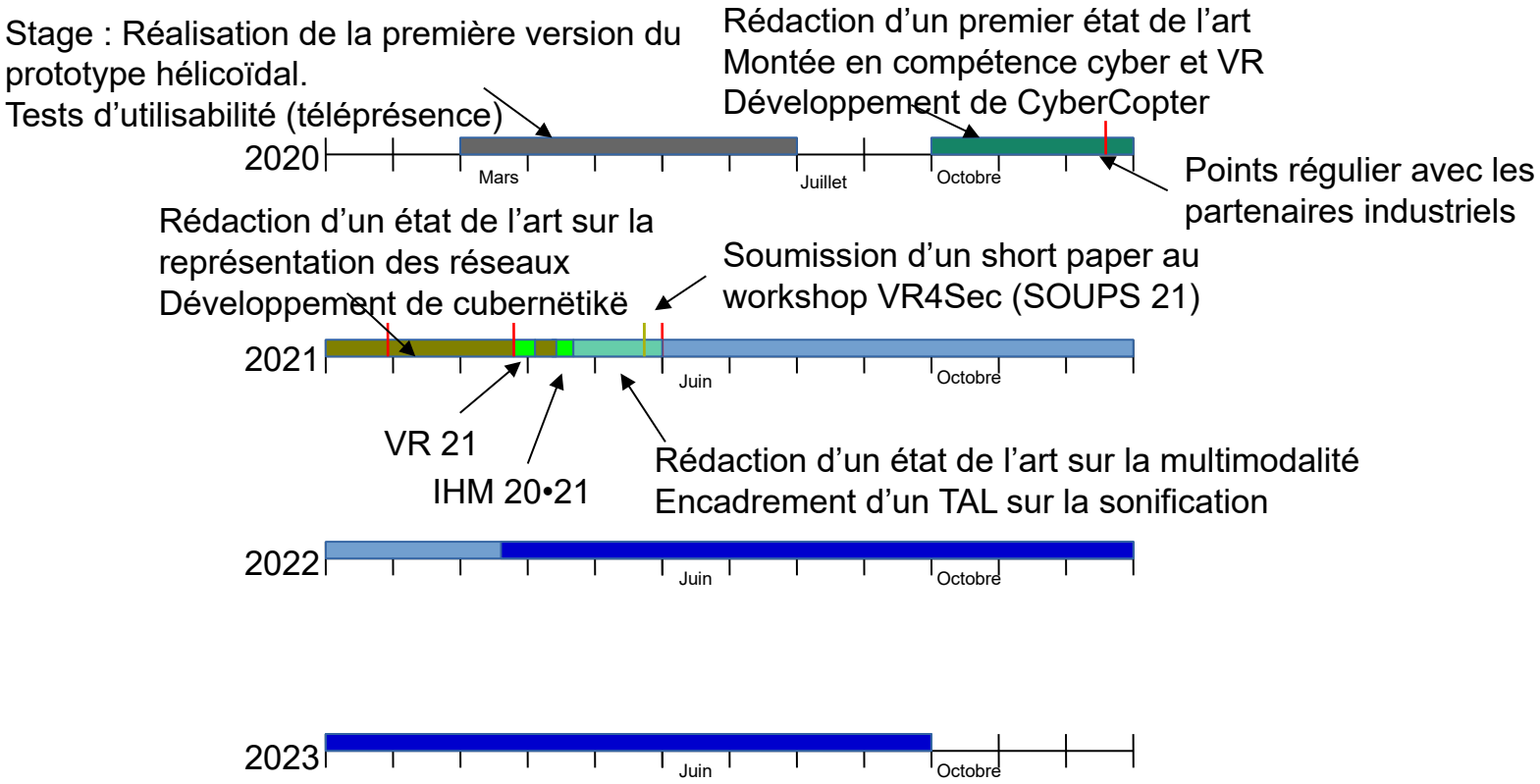
Cubernêtikê

Expérience envisagée

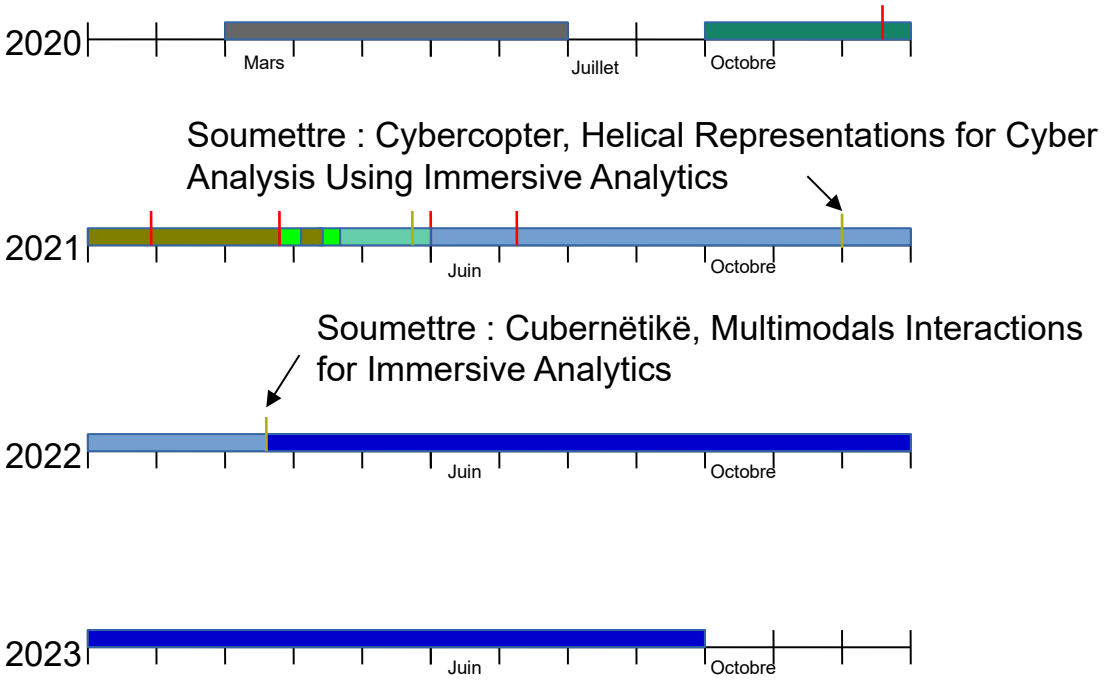
Comment utiliser la multimodalité afin de faciliter l’exploration de données ?

- Comparer différentes méthodes de sonification

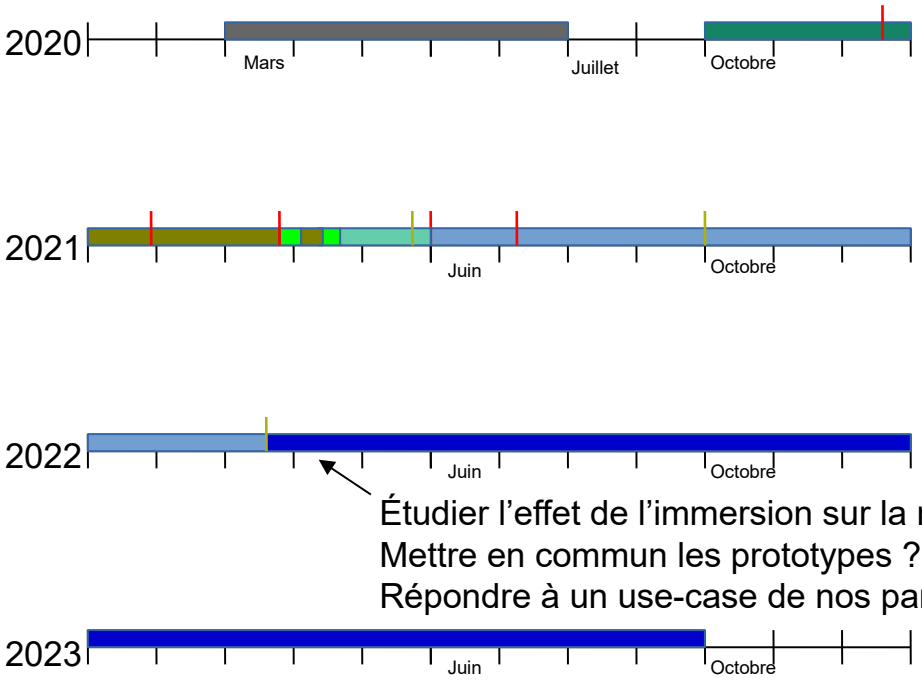
Planning


Stage : Réalisation de la première version du prototype hélicoïdal.
Tests d'utilisabilité (téléprésence)
Rédaction d'un premier état de l'art
Montée en compétence cyber et VR
Développement de CyberCopter
2020
Mars
Juillet
Octobre
Points régulier avec les partenaires industriels
Rédaction d'un état de l'art sur la représentation des réseaux
Développement de cubernëtikë
Soumission d'un short paper au workshop VR4Sec (SOUPS 21)
2021
Juin
Octobre
VR 21
IHM 20•21
Rédaction d'un état de l'art sur la multimodalité
Encadrement d'un TAL sur la sonification
2022
Juin
Octobre
2023
Juin
Octobre

Planning


2020
Mars
Juillet
Octobre
Soumettre : Cybercopter, Helical Representations for Cyber Analysis Using Immersive Analytics
2021
Juin
Octobre
Soumettre : Cubernëtikë, Multimodals Interactions for Immersive Analytics
2022
Juin
Octobre
2023
Juin
Octobre

Planning


2020
Mars
Juillet
Octobre
2021
Juin
Octobre
2022
Juin
Octobre
Étudier l'effet de l'immersion sur la mémoire à long terme
Mettre en commun les prototypes ?
Répondre à un use-case de nos partenaires ?
2023
Juin
Octobre

Références

[1] Philip A. Legg. Visualizing the insider threat: Chal-lenges and tools for identifying malicious user activity.2015 IEEE Symposium on Visualization for Cyber Secu-rity, VizSec 2015, (October 2015), 2015

[2] Tom Chandler, Maxime Cordeil, Bongshin Lee, Ben-jamin Bach, Tim Dwyer, and Kim Marriott. ImmersiveAnalytics.IEEE Computer Graphics and Applications,39(3):16–18, 2019

[3] Stefano Foresti, James Agutter, Yarden Livnat, ShaunMoon, and Robert Erbacher. Visual Correlation of Net-work Alerts.IEEE, (8):1275–1279, 2006.

[4] Anna Pia Lohfink, Simon D.Duque Anton, Hans DieterSchotten, Heike Leitte, and Christoph Garth. Security in Process: Visually Supported Triage Analysis in Industrial Process Data.IEEE Transactions on Visualization and Computer Graphics, 26(4):1638–1649, 2020.

[5] Alma Cantu, Thierry Duval, Olivier Grisvard, and GillesCoppin. HeloVis: A Helical Visualization for SIGINTAnalysis Using 3D Immersion.IEEE Pacific Visualiza-tion Symposium, 2018-April:175–179, 2018

[6] Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo,and Aditya Mathur. A dataset to support research inthe design of secure water treatment systems.LectureNotes in Computer Science (including subseries LectureNotes in Artificial Intelligence and Lecture Notes inBioinformatics), 10242 LNCS(October):88–99, 2017

Références

[7] Benjamin Bach, Emmanuel Pietriga, and Jean DanielFekete. Visualizing dynamic networks with matrix cubes. In Conference on Human Factors in Computing Systems - Proceedings, pages 877–886. Association forComputing Machinery, 2014.

[8] Ronell Sicat, Jiabao Li, Junyoung Choi, MaximeCordeil, Won Ki Jeong, Benjamin Bach, and HanspeterPfister. DXR: A Toolkit for Building Immersive DataVisualizations.IEEE Transactions on Visualization andComputer Graphics, 25(1):715–725, 2019

[9]] Bruno Dumas, Denis Lalanne, and Sharon Oviatt. Mul-timodal interfaces: A survey of principles, models and frameworks.Lecture Notes in Computer Science (in-cluding subseries Lecture Notes in Artificial Intelligenceand Lecture Notes in Bioinformatics), 5440 LNCS(May2014):3–26, 2009

[10] Christos Papadopoulos, Chris Kyriakakis, AlexanderSawchuk, and Xinming He.CyberSeer.(March2014):90, 2004.

[11] Arnaud Prouzeau, Maxime Cordeil, Clement Robin, Bar-rett Ens, Bruce H. Thomas, and Tim Dwyer. Scapticsand highlight-planes: Immersive interaction techniquesfor finding occluded features in 3D scatterplots.Con-ference on Human Factors in Computing Systems - Pro-ceedings, 2019

[12] Arjun Srinivasan and John Stasko. Orko: FacilitatingMultimodal Interaction for Visual Exploration and Anal-ysis of Networks.IEEE Transactions on Visualizationand Computer Graphics, 24(1):511–521, 2018