Building a usable visual analytics tool for network security[1]

Mike Just
Heriot-Watt University
Edinburgh, UK

12 July 2016
@ Dalhousie University
Halifax, NS, Canada

[1] Joint with Muhammad Adnan (Leeds) and Lynne Baillie

Network security challenges

- Increase in
  - Number of users
  - Variety of connecting devices
  - Diversity of communicating applications
  - Amounts of network data
- Layered security model
  - Firewalls, IDS/IPS, ...
  - Active monitoring typically supported by textual or semi-visual tools as well as home-made scripts
  - Efficiency and effectiveness of these tools is challenged by the high volume and complexity of data that is being generated

Visual analytics for network security

- State-of-the-art still necessitates computer+human solutions
- Visual analytics has emerged as a promising approach to deal with the data overload
  - Network data is processed and presented in a visualisation
  - Visualisation is interpreted by human, perhaps to identify possible attack traffic for further analysis
- Unfortunately, many proposed VA tools have failed to gain wide acceptance among network security professionals

Visual analytics for network security

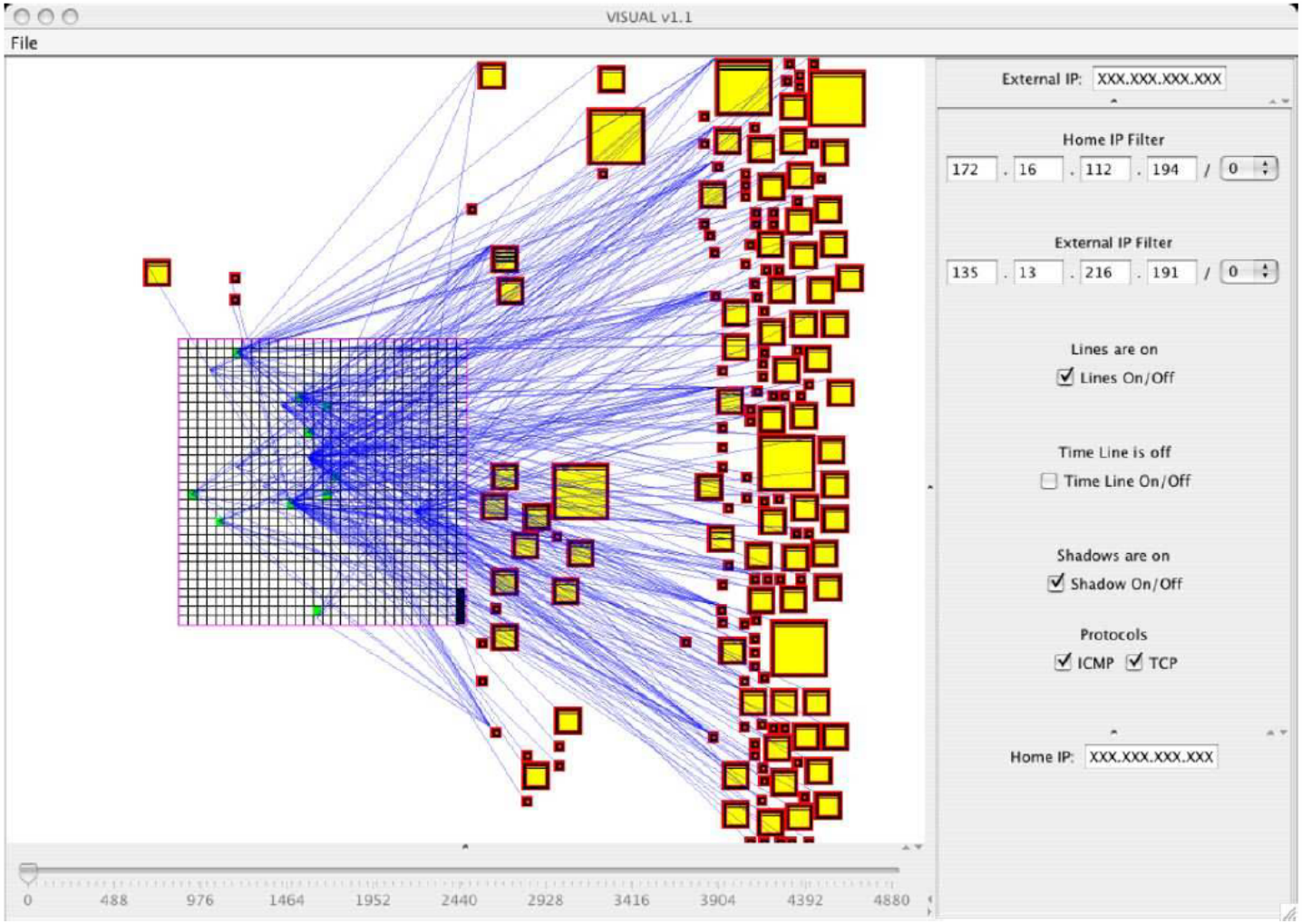


Figure : VISUAL (Ball et al., 2004)

Visual analytics for network security

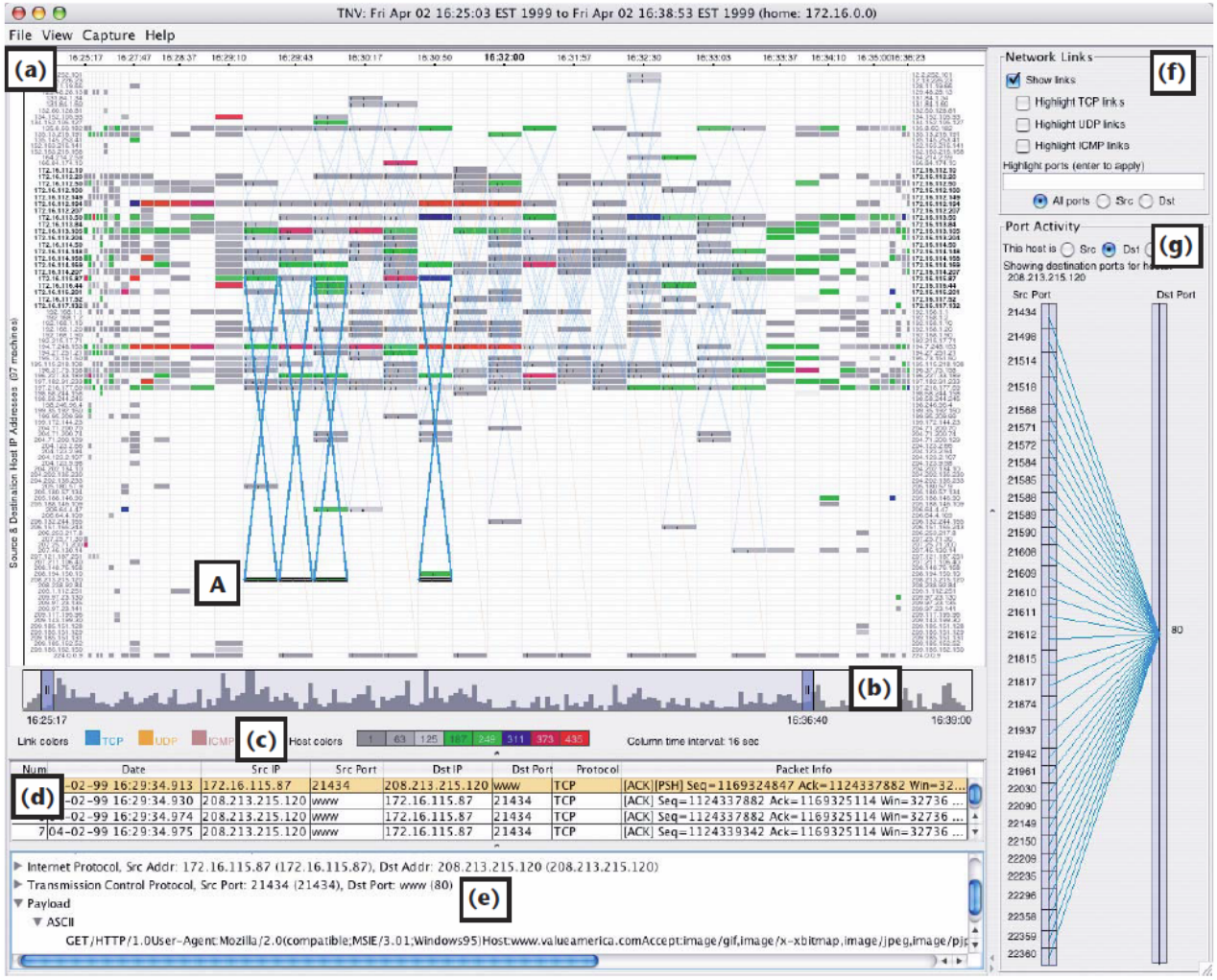


Figure : TNV (Goodall et al., 2006)

Visual analytics for network security

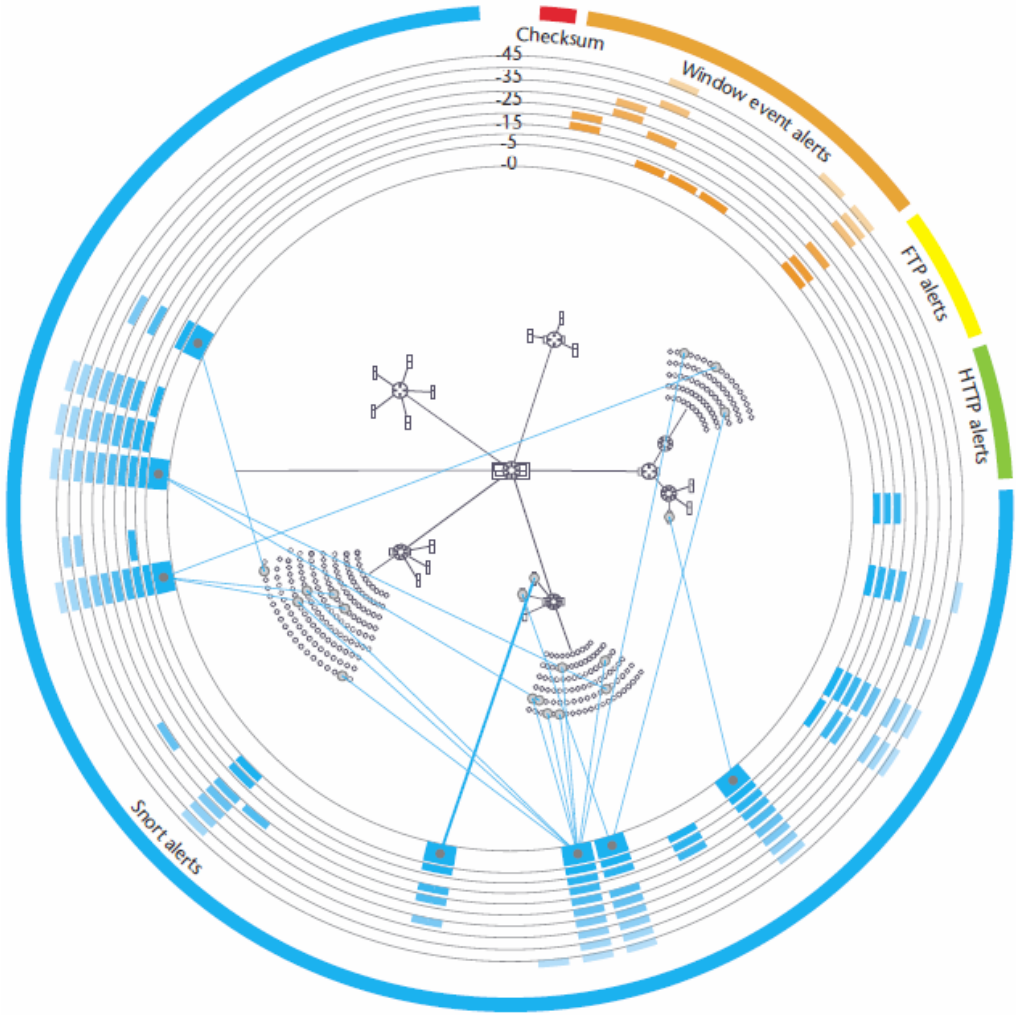


Figure : VisAlert (Foresti et al., 2006)

Visual analytics for network security

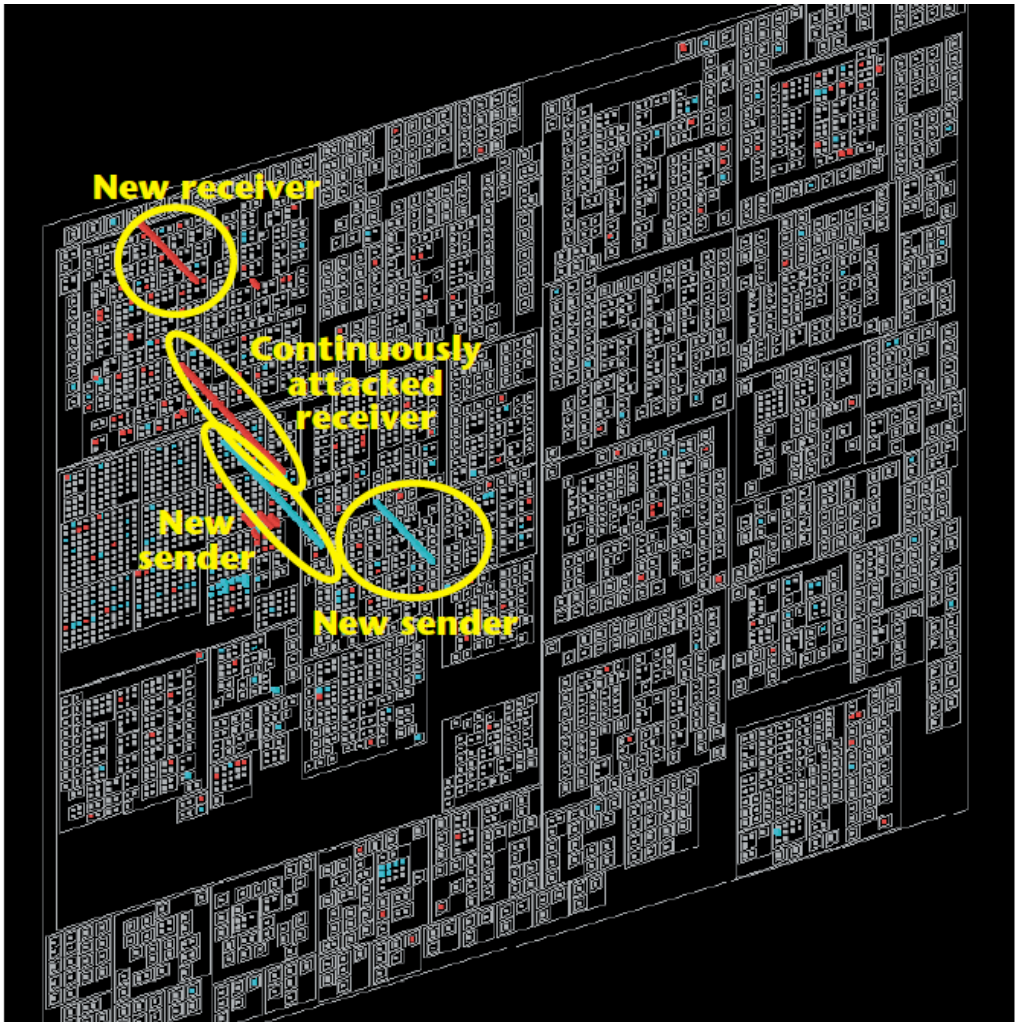


Figure : Itoh et al., (2006)

Visual analytics for network security

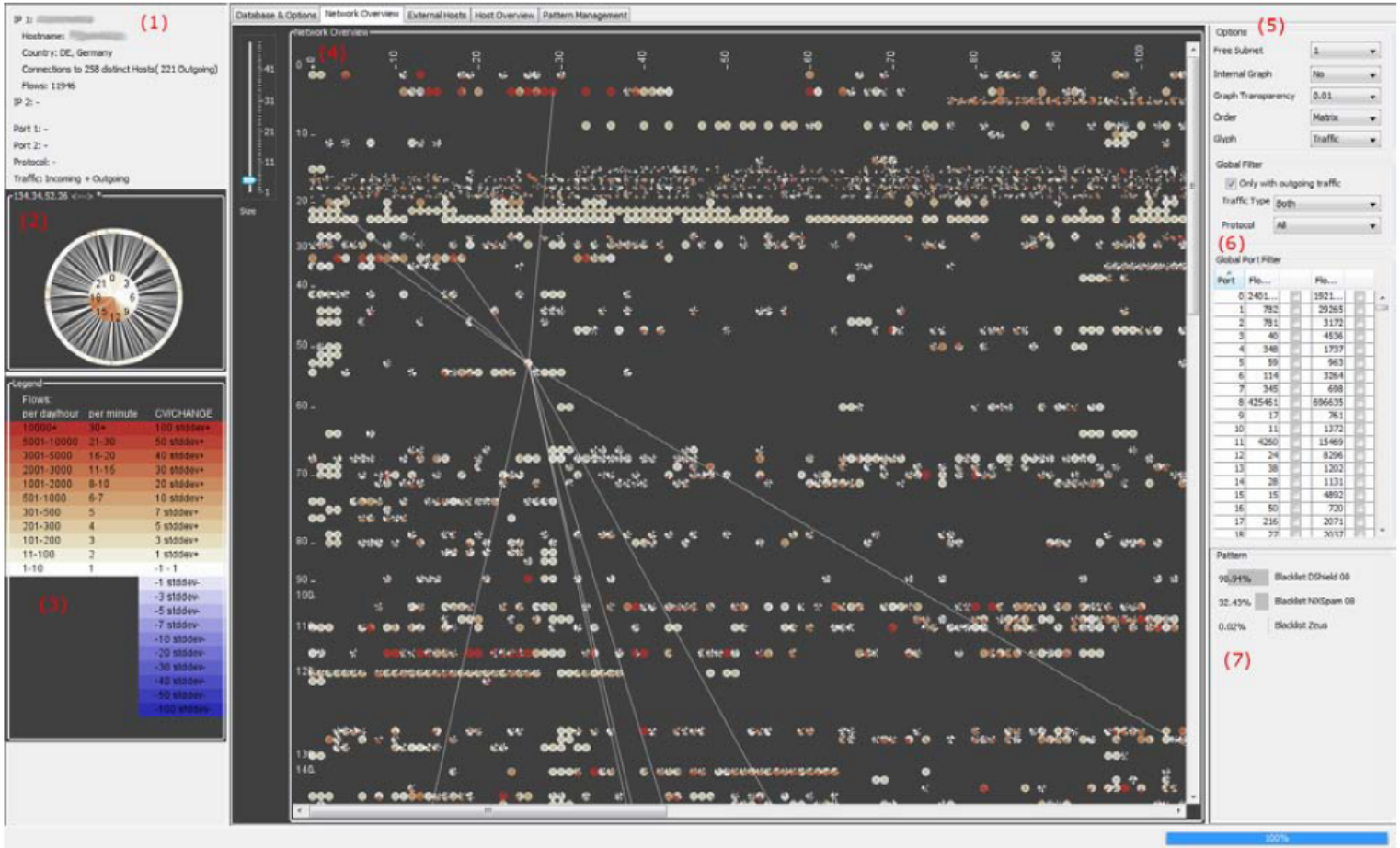


Figure : ClockView (Kintzel et al., 2011)

Visual analytics for network security

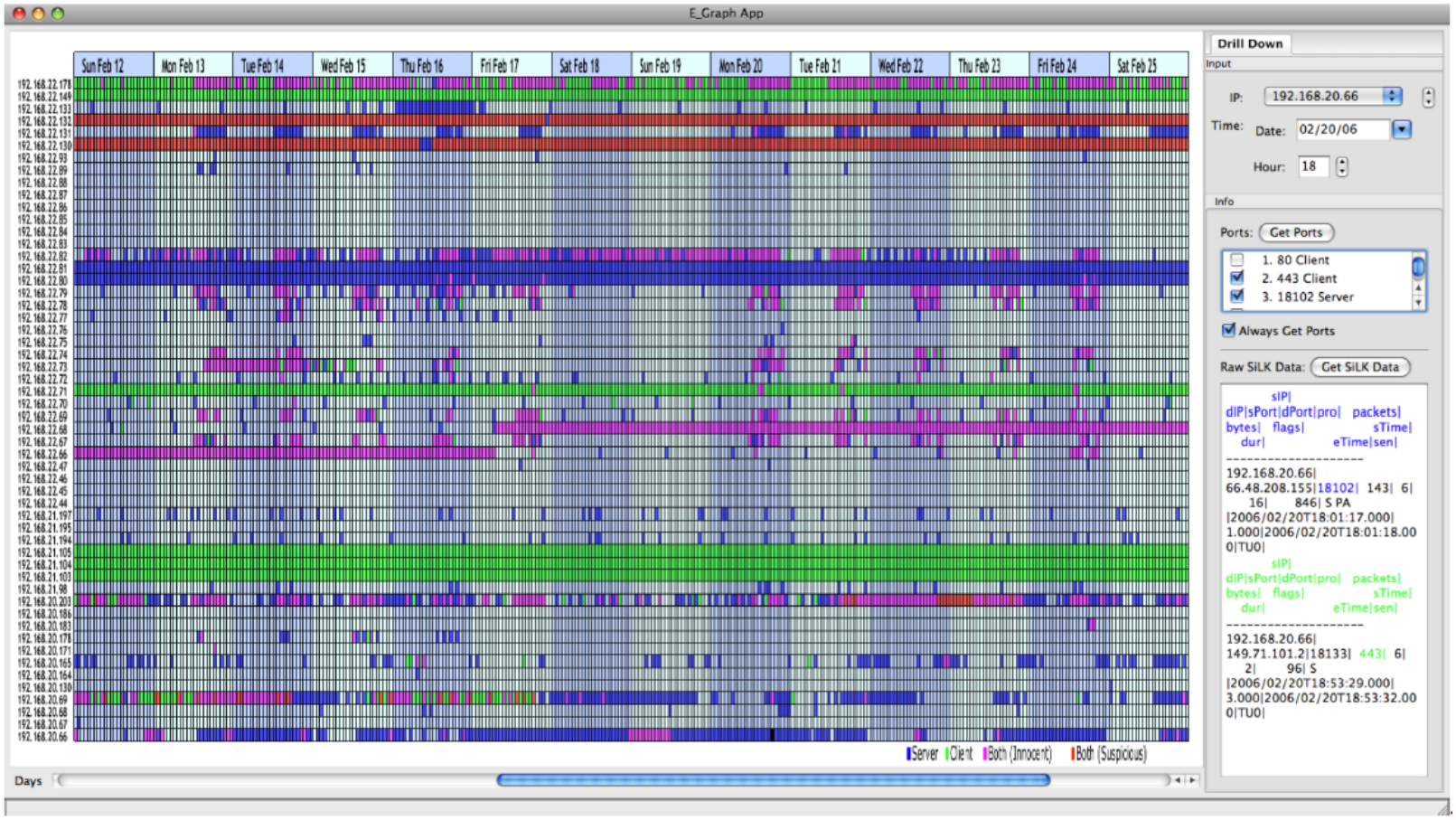


Figure : FloVis (Taylor et al., 2009)

Visual analytics for network security

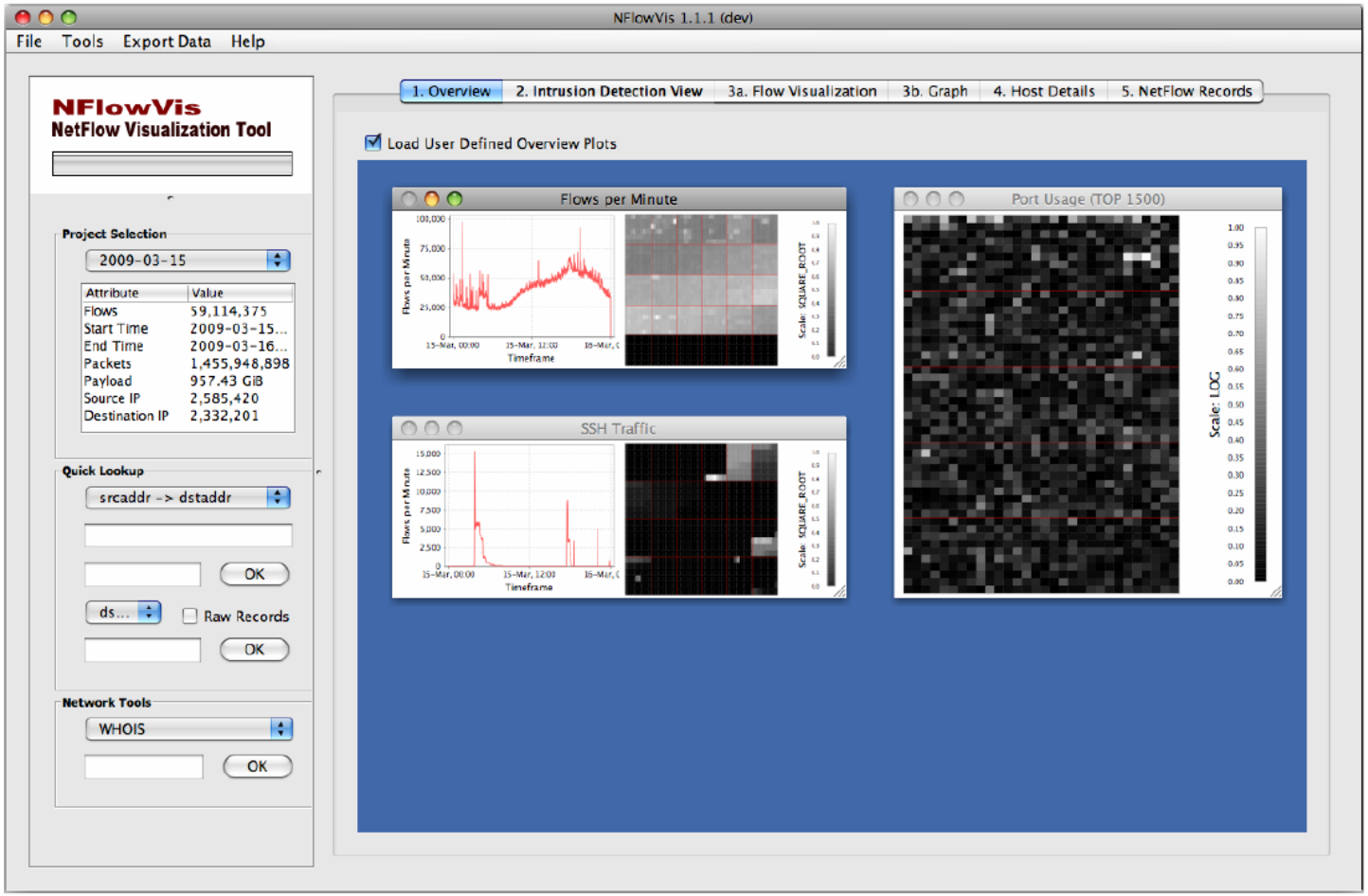


Figure : NFlowVis (Mansmann et al., 2009)

Visual analytics for network security

- Several common issues
  - Target fairly broad use cases
  - Lack design justifications
  - Don't necessarily meet user needs (match their work practices)

  "researchers come to us and say, here's a visualization tool, let's fit your problem to this tool. But what we need is a tool built to fit our problem" (Hao, VizSec 2013)
- Closest to our design are FlowVis and NFlowVis

Our approach

- Use case: detecting potential bandwidth depletion DDoS attacks
- Approach
  1. Started with a **low-fidelity design** of the proposed visual analytics tool based on existing design guidelines
  2. Selection of appropriate **time series visualisations** for tool by performing a quantitative graphical perception study
  3. Evaluation of the **proposed tool** by designing and conducting a mixed-method user study.

Our goal was to not only design a tool, but to do so via an effective user-centred design process

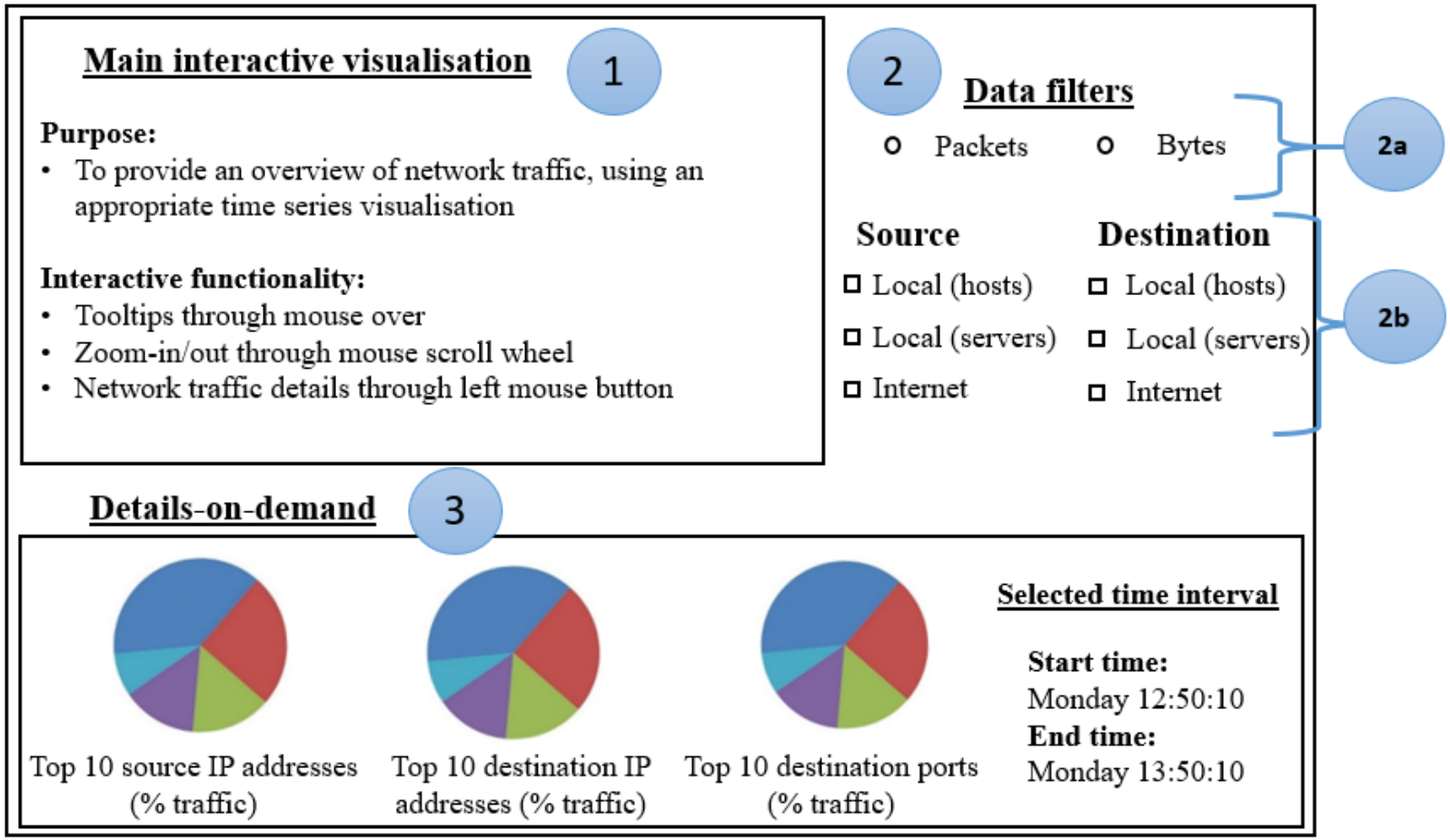
Talk Outline

1. Low-fidelity design
2. Time series visualisations
3. Proposed tool evaluation

Talk Outline

1. **Low-fidelity design**
2. Time series visualisations
3. Proposed tool evaluation

Initial low-fidelity design



1. Network traffic overview
2. Data filters (a) packets & bytes (b) source & destination
3. Network traffic details

Initial LF design approach

- Use case: detection of bandwidth depletion DDoS attacks from network flow data
- Pre-design domain analysis of use case identified following characteristics
  - Causes a considerable increase in the amount network traffic
  - Originates from multiple source IP addresses
  - Usually targets servers within a network
  - Usually targets well-known services/ports within a network (e.g., web and e-mail services)
- Shneiderman design: "Overview first, zoom and filter, then details-on-demand"
  - Hence, included options for tooltips and zoom

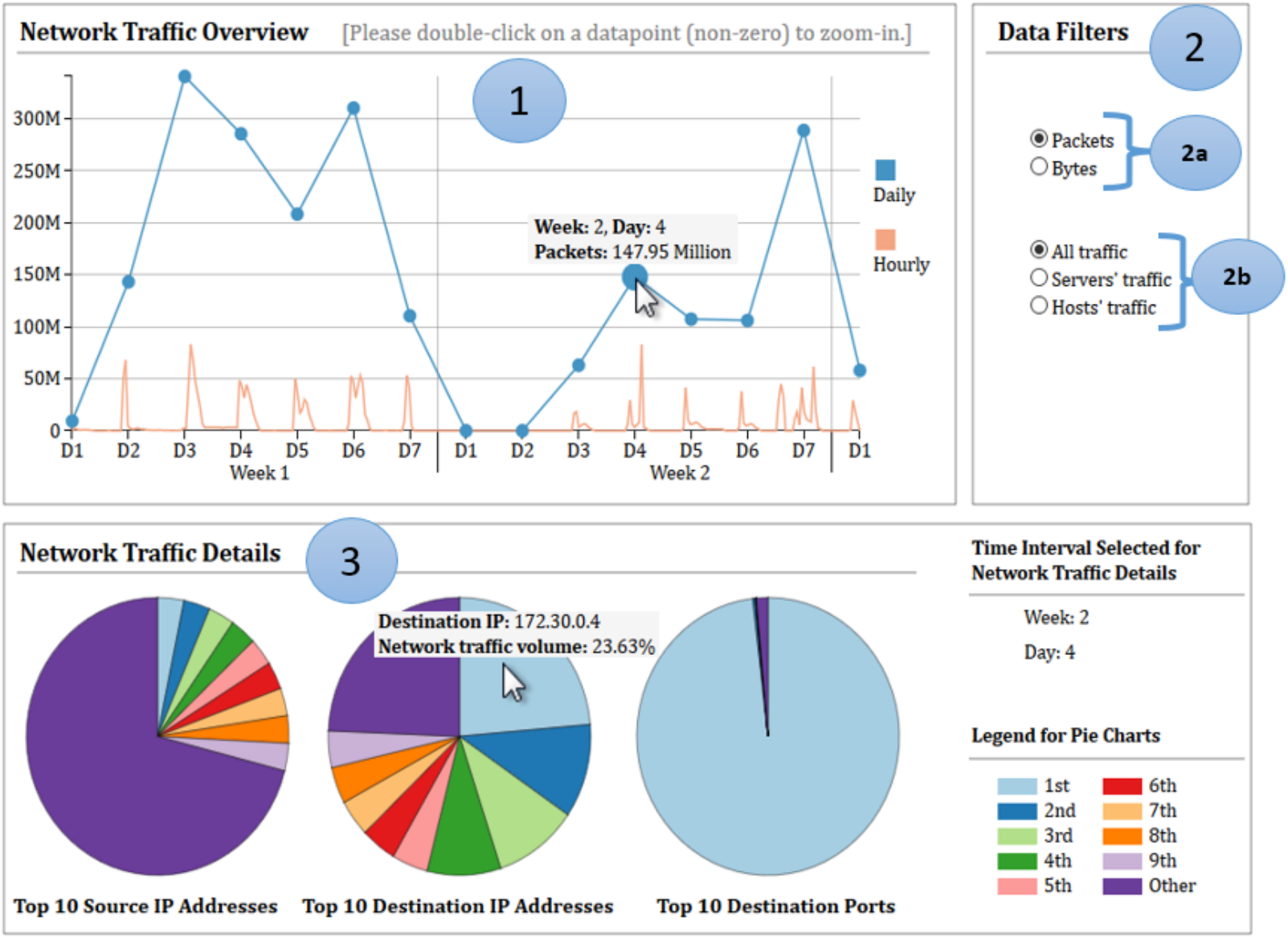
LF design validation

- Semi-structured design interviews with network security professsionals
- Asked about suitability of different components of proposed tool
- Interviews coded and analysed using the constant comparative method (CCM)
  - Part of grounded theory
- Categories
  - Core design elements
  - Interaction techniques
  - Titles and legends
  - Placement of interface components
  - Network traffic details
  - Network traffic overview

LF design validation (some results)

- Interaction techniques
  - Simplification of data filters
  - Endorsement of interaction techniques (e.g., tooltips, zoom)
- Increased specificity for titles
  - From ‘main interactive visualisation’ to ‘network traffic overview’
  - From ‘details on demand’ to ‘network traffic details’
- Inclusion of baseline historical data for network traffic overview

Proposed tool – A sneak peek



Talk Outline

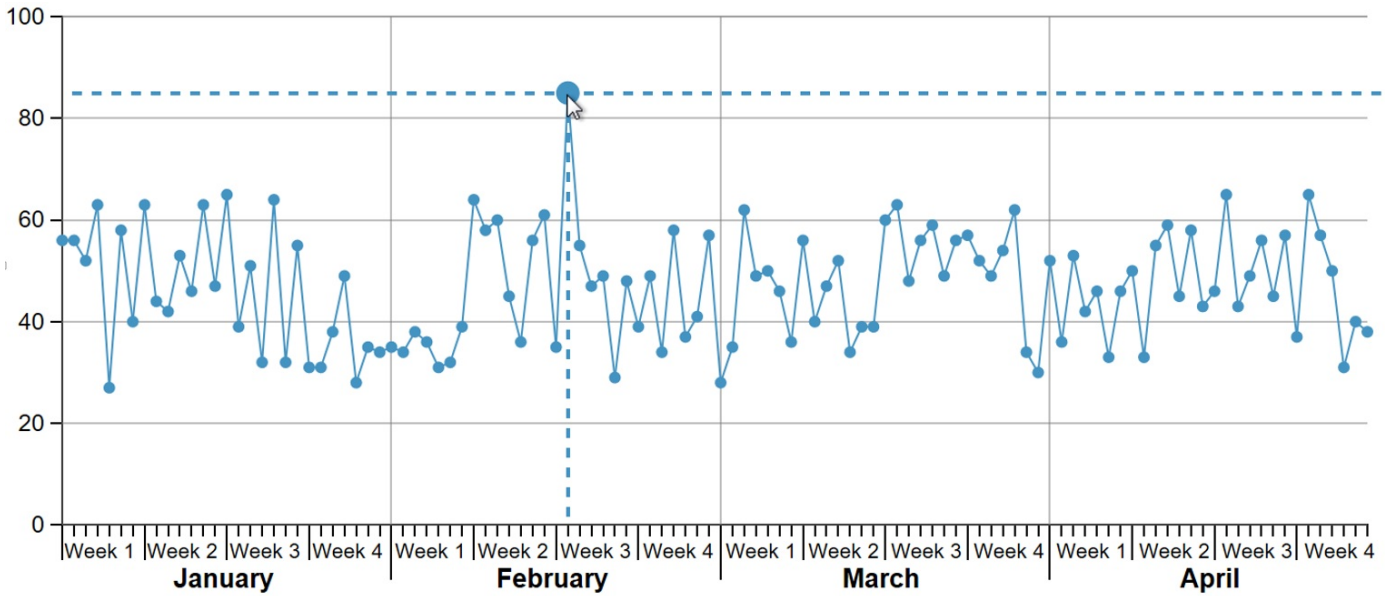
1. Low-fidelity design
2. **Time series visualisations**
3. Proposed tool evaluation

Time series visualisation component

- Initial plan: Determine appropriate time series visualisation based on feedback from LF designs
- In fact, we introduced 10 visualisations as part of our LF validation
  - Scatter plot, line chart, silhouette/area chart, bar chart, horizon graph, radar chart, rectangular heatmap, circular heatmap, treemap and sunburst visualisation
- However, feedback was not conclusive
- Further research uncovered gaps in the study of time series visualisations

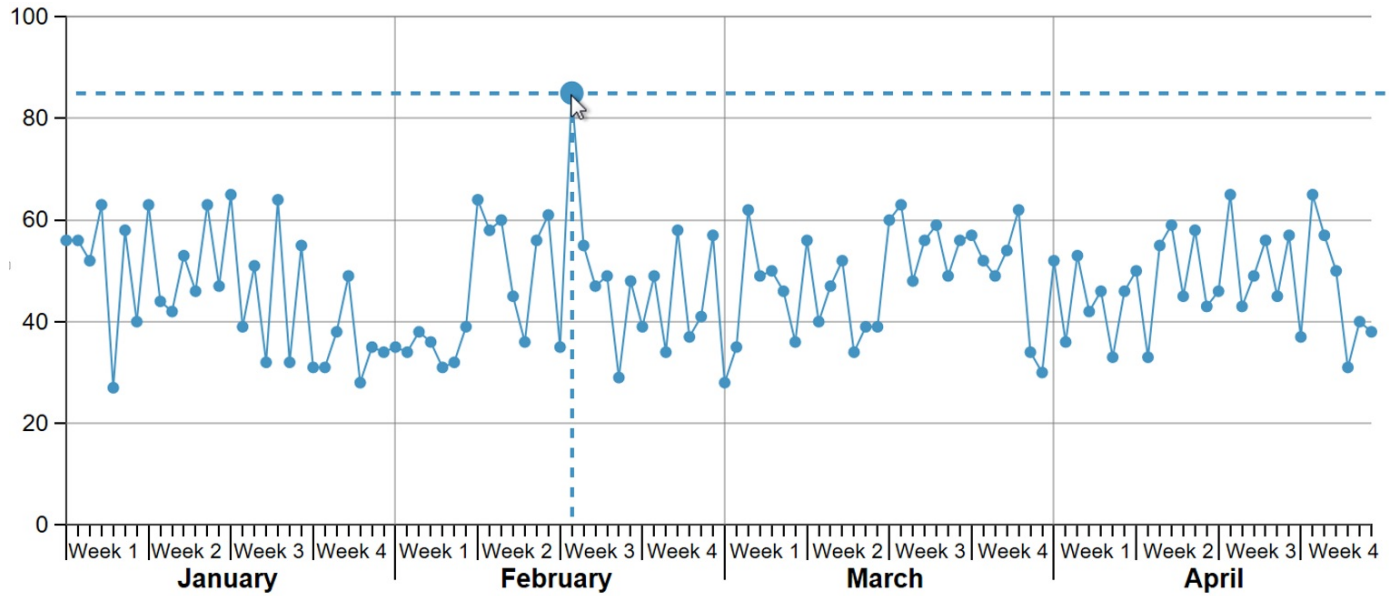
Time series visualisations

- Time series visualisations widely used
- Example: Network security analysis
  - Time (horizontal), number of packets (vertical)



Time series visualisations

- Time series visualisations widely used
- Example: Network security analysis
  - Time (horizontal), number of packets (vertical)



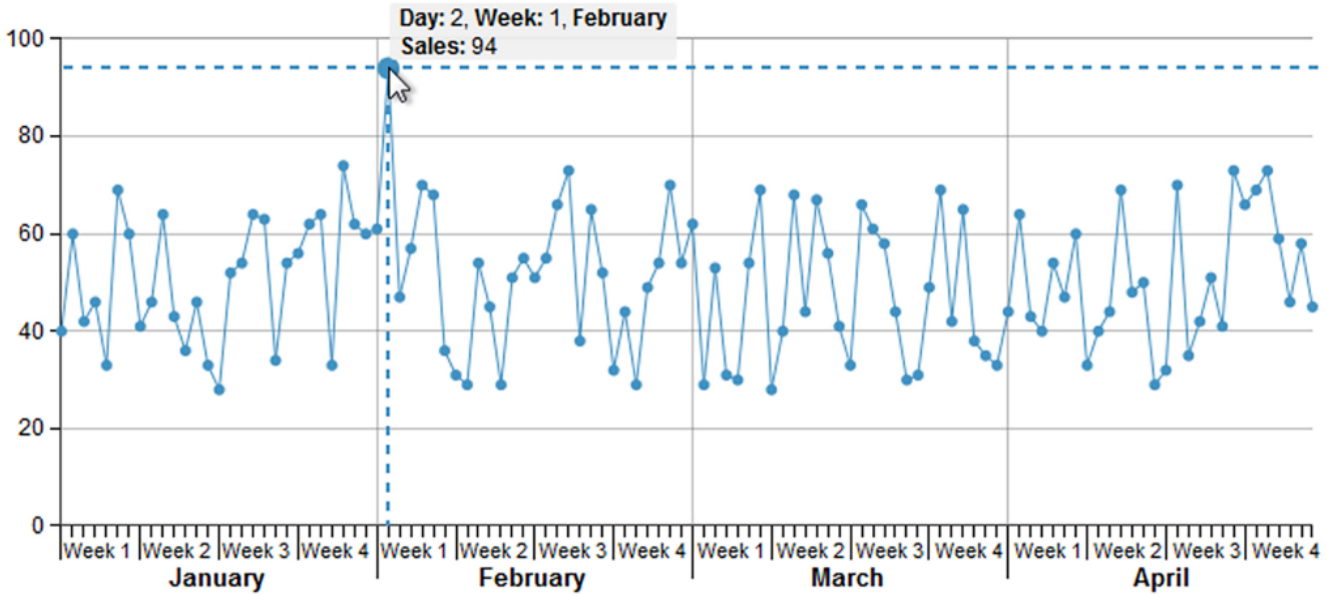
- Tasks such as maxima and comparison used to identify possible Denial of Service attacks

Time series visualisations

- Several possible visual representations to use

Time series visualisations

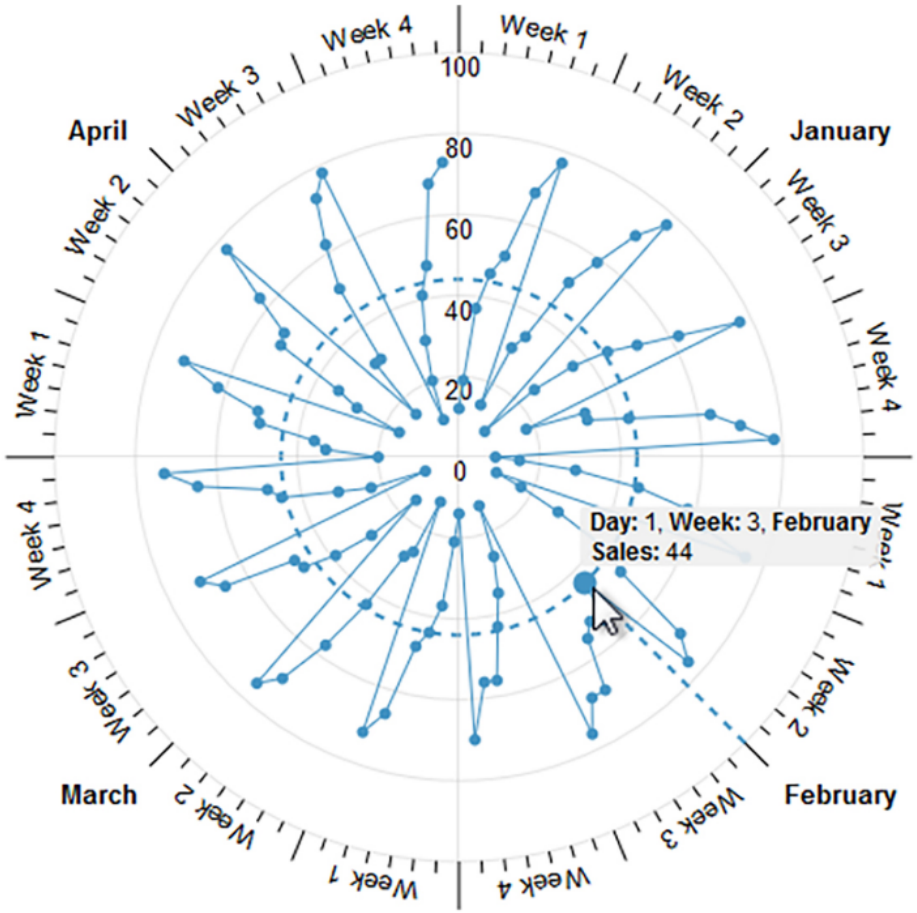
- Several possible visual representations to use



(a) Line chart

Time series visualisations

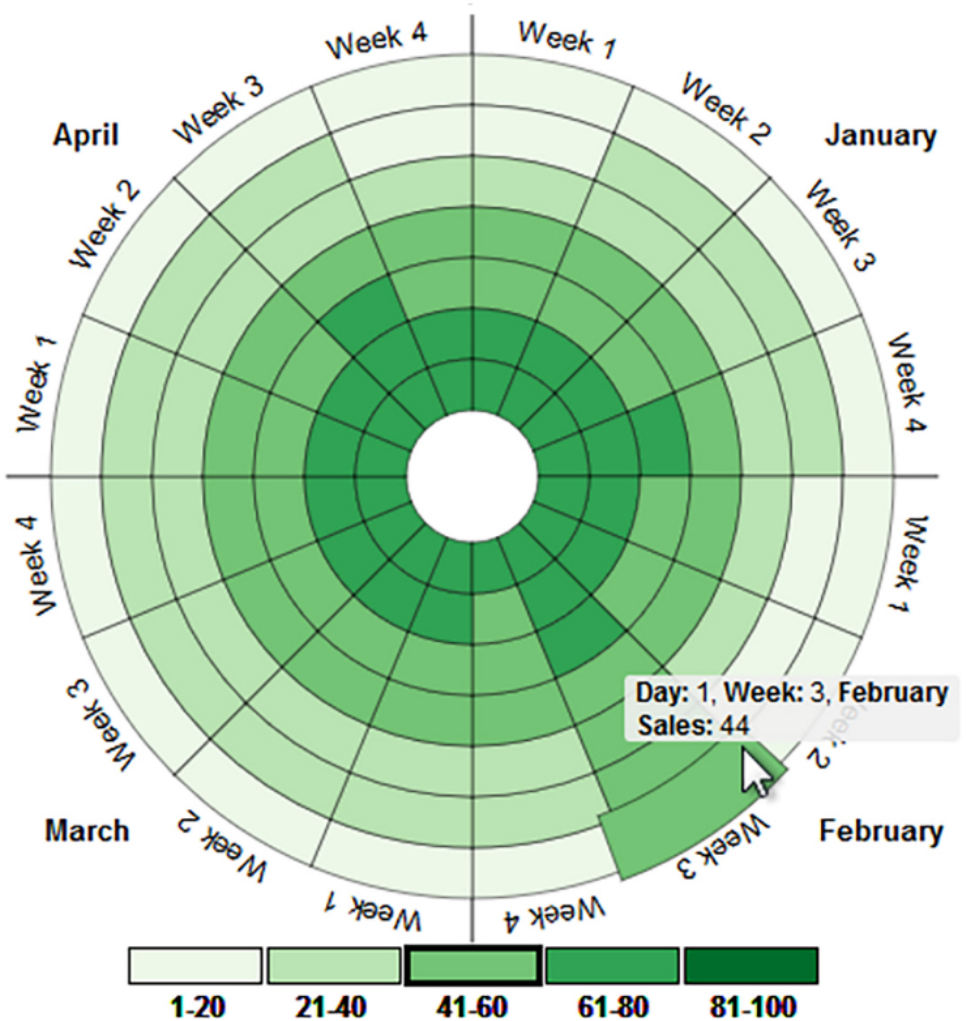
- Several possible visual representations to use



(b) Radar chart

Time series visualisations

- Several possible visual representations to use



(d) Circular heatmap

Time series visualisations

- Which visual representation to use?

Time series visualisations

- Which visual representation to use?
- What about user interaction?

Time series visualisations

- Which visual representation to use?
- What about user interaction?
- Dozens of research papers since early 80s on visual representation and graphical perception
- Gaps re: some fundamental factors
  - Interaction techniques
  - Visual encodings
  - Coordinate systems

Gaps

Interaction techniques

Graphical perception studies commonly in **static setting**, limiting knowledge of **user experience**.

Gaps

Interaction techniques

Graphical perception studies commonly in **static setting**, limiting knowledge of **user experience**.

Visual encodings

Effectiveness within and across position and colour visual encodings, but **not area**.

Gaps

Interaction techniques

Graphical perception studies commonly in **static setting**, limiting knowledge of **user experience**.

Visual encodings

Effectiveness within and across position and colour visual encodings, but **not area**.

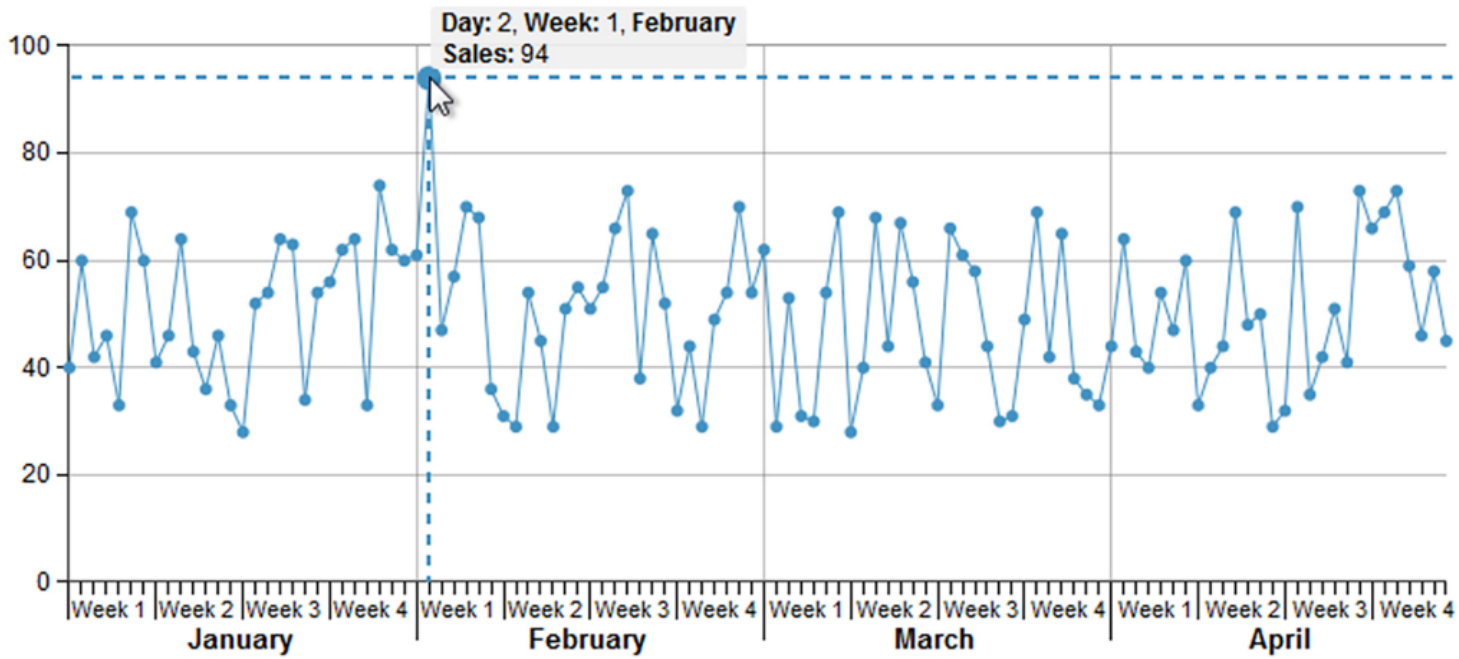
Coordinate systems

Limited empirical evidence on **Cartesian vs. Polar** coordinate systems for time series visualisations using different visual encodings.

Visual Representations

- Visual encodings: Position, colour, and area
- For each, a Cartesian and polar coord. system
- Interaction techniques: highlighting & tooltips

Position encoding: Cartesian (line chart)

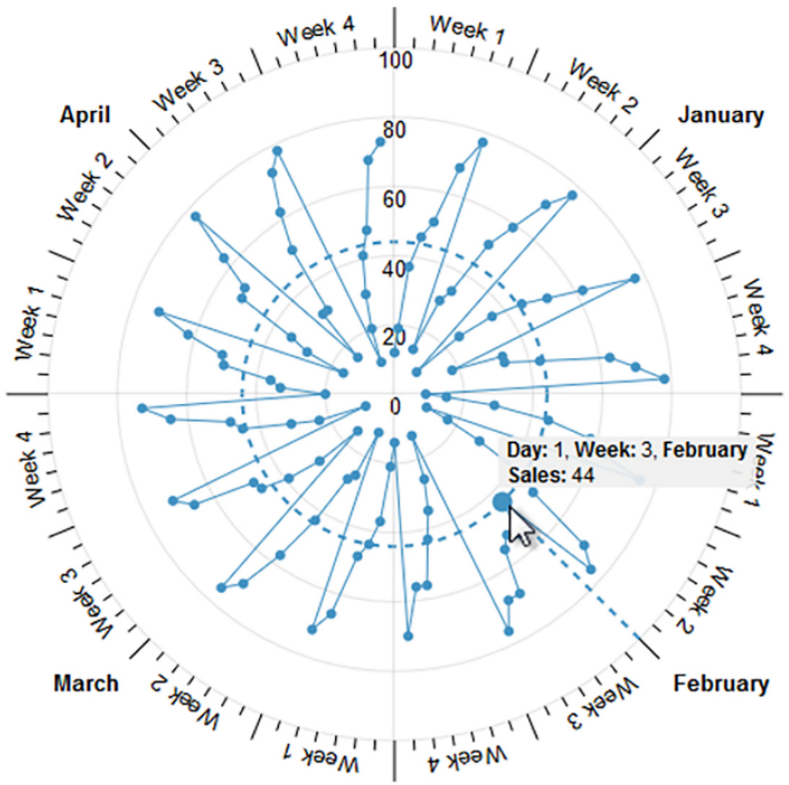


(a) Line chart

Visual Representations

- Visual encodings: Position, colour, and area
- For each, a Cartesian and polar coord. system
- Interaction techniques: highlighting & tooltips

Position encoding: Polar (radar chart)

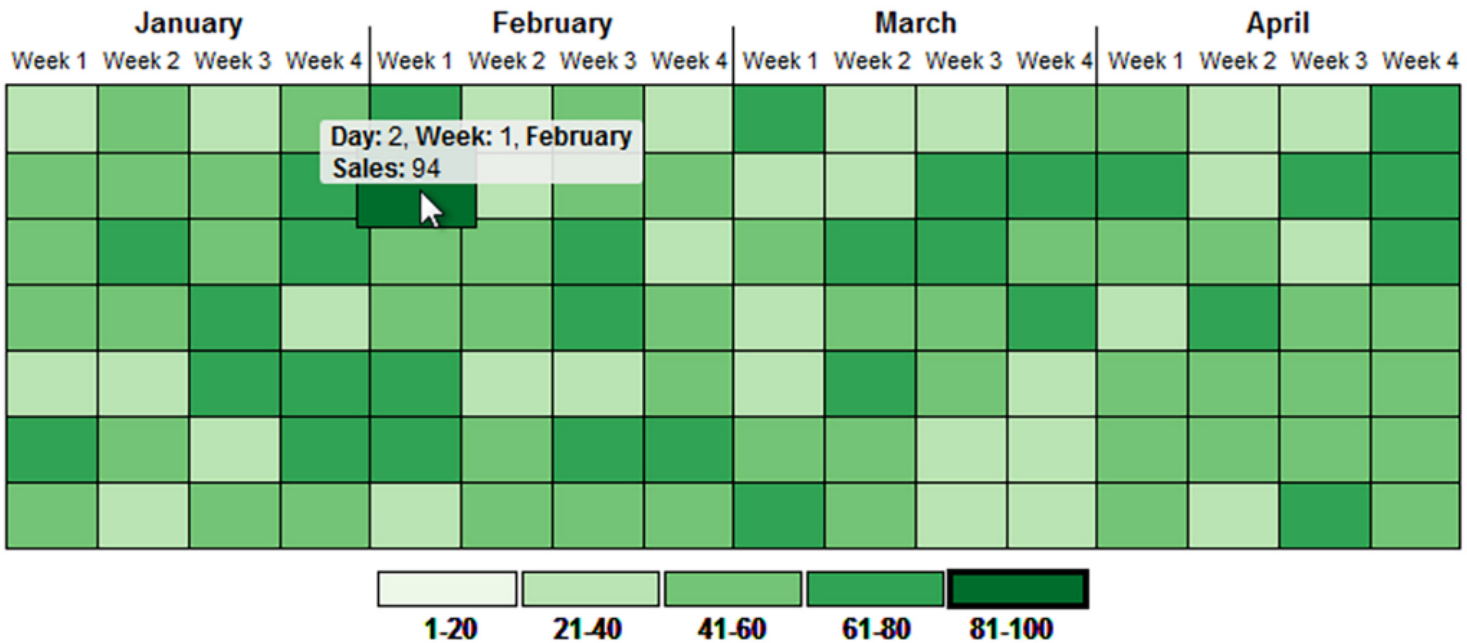


(b) Radar chart

Visual Representations

- Visual encodings: Position, colour, and area
- For each, a Cartesian and polar coord. system
- Interaction techniques: highlighting & tooltips

Colour encoding: Cartesian (rectangular heatmap)

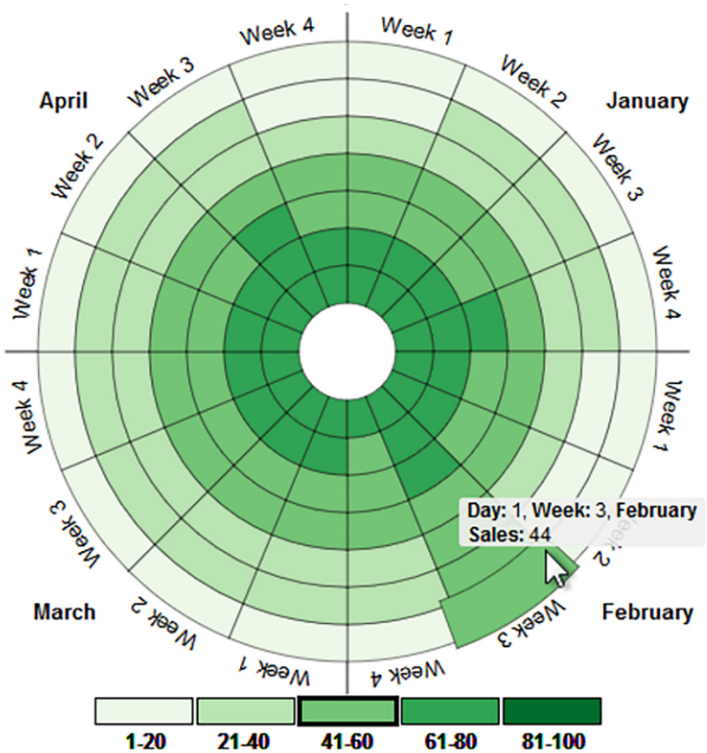


(c) Rectangular heatmap

Visual Representations

- Visual encodings: Position, colour, and area
- For each, a Cartesian and polar coord. system
- Interaction techniques: highlighting & tooltips

Colour encoding: Polar (circular heatmap)

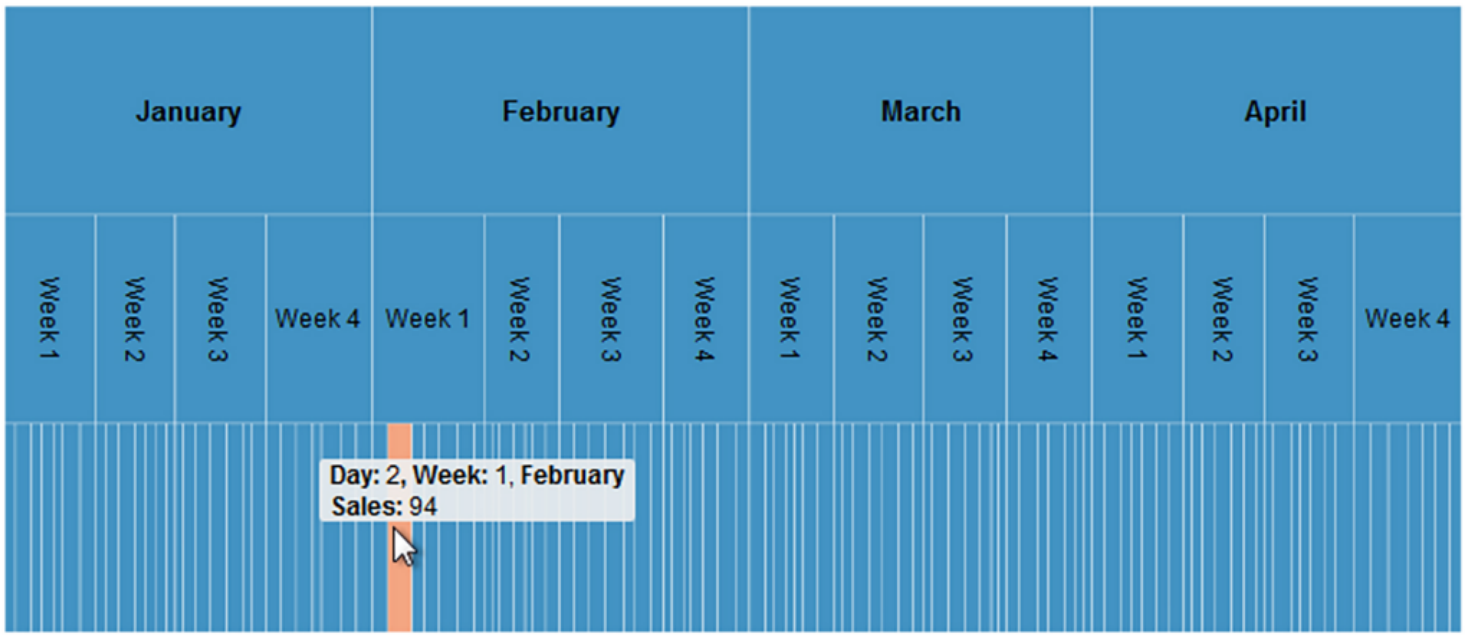


(d) Circular heatmap

Visual Representations

- Visual encodings: Position, colour, and area
- For each, a Cartesian and polar coord. system
- Interaction techniques: highlighting & tooltips

Area encoding: Cartesian (icicle plot)

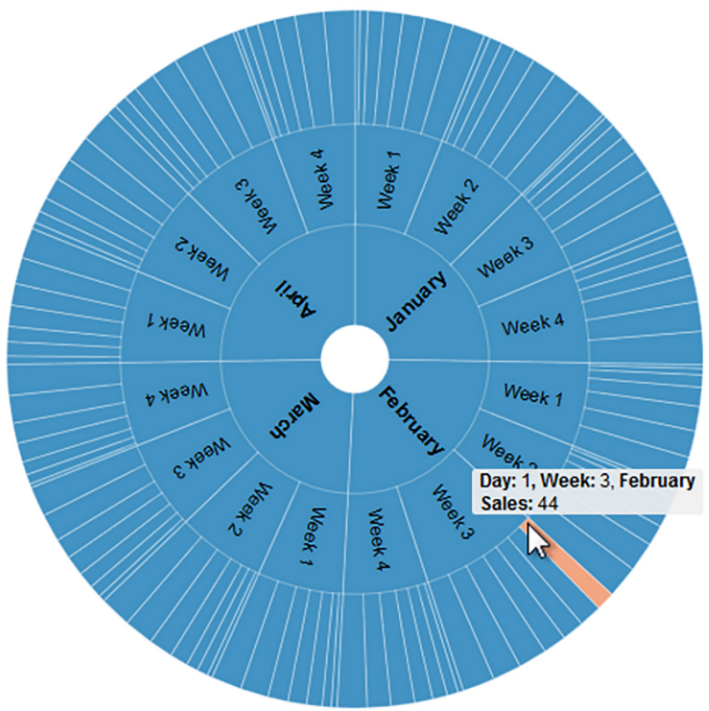


(e) Icicle plot

Visual Representations

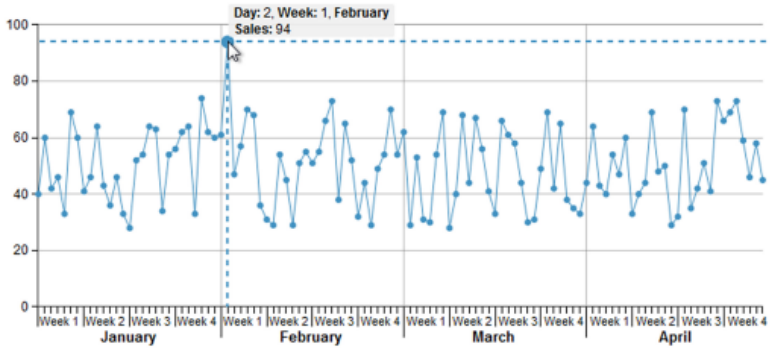
- Visual encodings: Position, colour, and area
- For each, a Cartesian and polar coord. system
- Interaction techniques: highlighting & tooltips

Area encoding: Polar (sunburst plot)

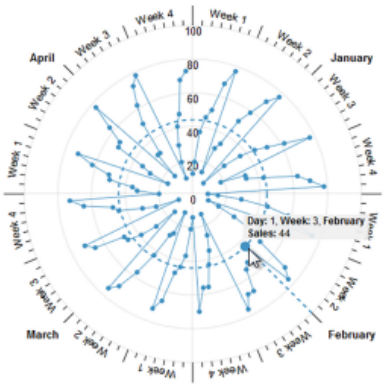


(f) Sunburst visualisation

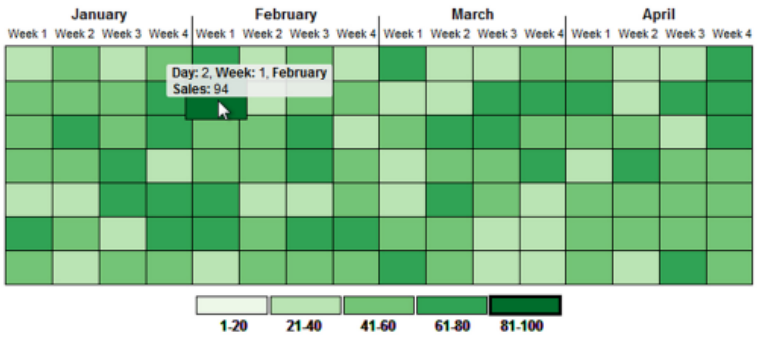
Visual Representation Summary



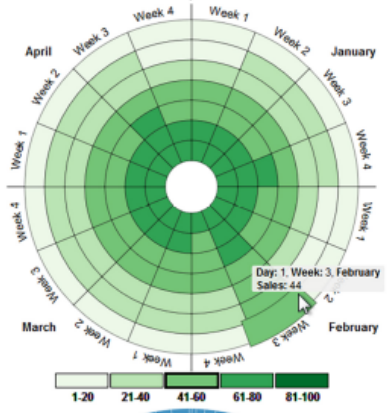
(a) Line chart



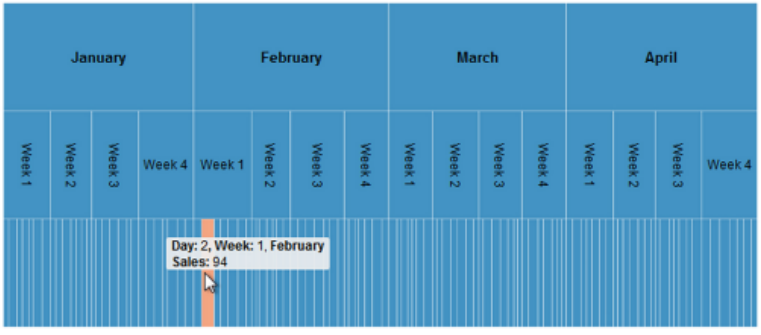
(b) Radar chart



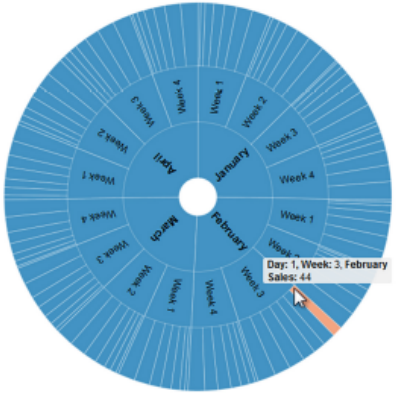
(c) Rectangular heatmap



(d) Circular heatmap



(e) Icicle plot



(f) Sunburst visualisation

Graphical perception study

- Graphical perception study

Graphical perception study

- Graphical perception study
  - 4 arrangements of two **interaction techniques**:

    No interaction Only tooltips
    Only highlighting Both highlighting & tooltips

  - 3 **visual encodings**:

    Position Colour Area

  - 2 **coordinate systems**:

    Cartesian Polar

  - 4 **study tasks**:

    Maxima Comparison
    Minima Trend detection

- 96 (4x3x2x4) experimental conditions

Study Tasks

- Maxima
  - To identify the highest absolute value in a dataset
- Minima
  - To identify the lowest absolute value in a dataset
- Comparison
  - To compare two sets of data points to find out which set has the highest aggregated value
- Trend detection
  - To identify subset of data (i.e., a week) with lowest value increase (upward trend) within dataset

Study Tasks

- Maxima
  - To identify the highest absolute value in a dataset
- Minima
  - To identify the lowest absolute value in a dataset
- Comparison
  - To compare two sets of data points to find out which set has the highest aggregated value
- Trend detection
  - To identify subset of data (i.e., a week) with lowest value increase (upward trend) within dataset

Task scenario

Presented as sales data of a fictitious company

Study Design

- Study design
  - 24 study participants
    (14 male, 10 female; 18-44 years old)
  - Within-subject factorial design with 96 (4x3x2x4) experimental conditions for each participant
- Experimental conditions
  - Counterbalanced visualisations and interactions
  - Tasks ordered simple to complex
    (Javed et al., 2010)
- Data for visual representations
  - 96 distinct, synthetic time series datasets (one for each condition) following Fuchs et al. (2013)
  - Each dataset had 112 data points (1 per day) over 16 week period

Study Procedure

Stage	**Description**
Introduction	Greetings, consent, demographic questionnaire, study explanation
Maxima	Task training, 24 conditions
Minima	Task training, 24 conditions
Comparison	Task training, 24 conditions
Trend detect.	Task training, 24 conditions

Study Procedure

Stage	**Description**
Introduction	Greetings, consent, demographic questionnaire, study explanation
Maxima	Task training, 24 conditions
Minima	Task training, 24 conditions
Comparison	Task training, 24 conditions
Trend detect.	Task training, 24 conditions

24 experimental conditions for each task
(3 visual encodings x 2 coord. systems x 4 interact.)

Study data collected

Effectiveness measured with four components, collected after each experimental condition

Study data collected

Effectiveness measured with four components, collected after each experimental condition

- Completion of an experimental condition (sec)
- Accuracy of the given answer (binary)
- Confidence of the given answer (5-point Likert)
- Ease of use of a visualisation (5-point Likert)

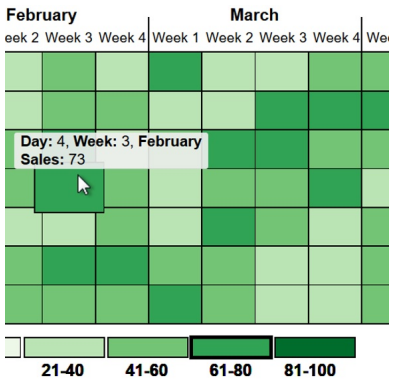
Final two collected via questionnaire per condition

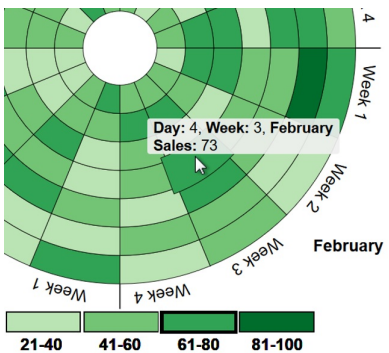
Results: Interaction Techniques

- Interactivity enhanced user experience
  - Interaction significantly better than no interaction
  - Confidence and ease-of-use
  - No affect on completion time or accuracy

Results: Interaction Techniques

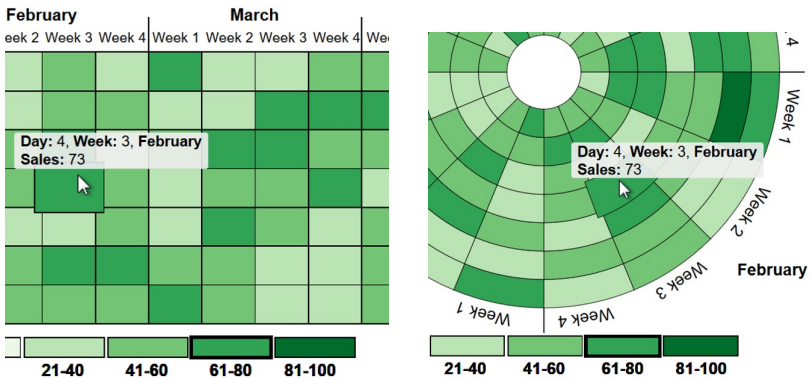
- Interactivity enhanced user experience
  - Interaction significantly better than no interaction
  - Confidence and ease-of-use
  - No affect on completion time or accuracy
- Exception: Minima, and colour encoding





Results: Interaction Techniques

- Interactivity enhanced user experience
  - Interaction significantly better than no interaction
  - Confidence and ease-of-use
  - No affect on completion time or accuracy
- Exception: Minima, and colour encoding



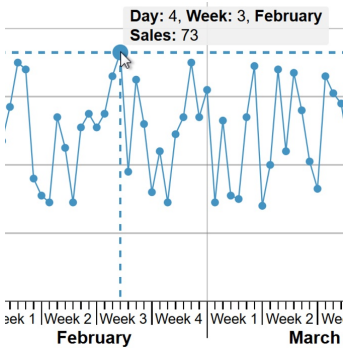
- Textual (tooltips) better than highlighting

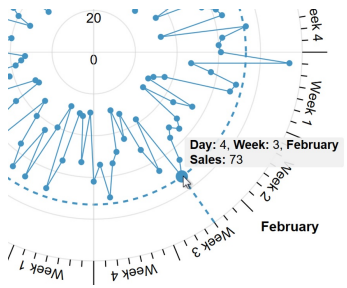
Results: Visual Encodings

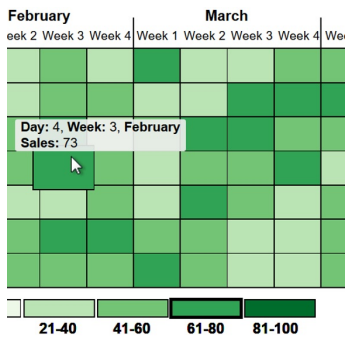
- Completion, accuracy, confidence, & ease

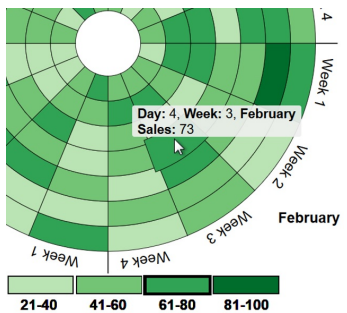
Results: Visual Encodings

- Completion, accuracy, confidence, & ease
- Position & colour better: max, min, trend det.
  - Colour more accurate for minima



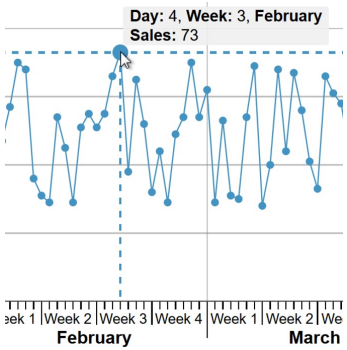


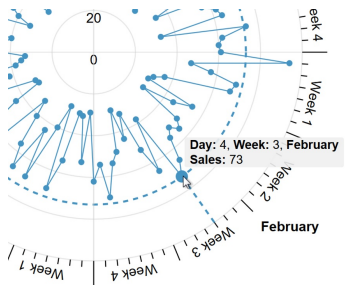


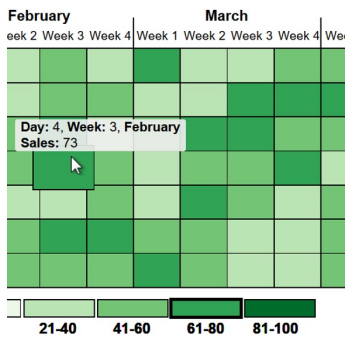


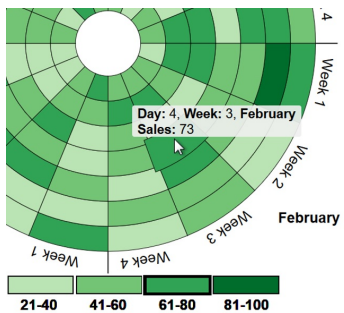
Results: Visual Encodings

- Completion, accuracy, confidence, & ease
- Position & colour better: max, min, trend det.
  - Colour more accurate for minima

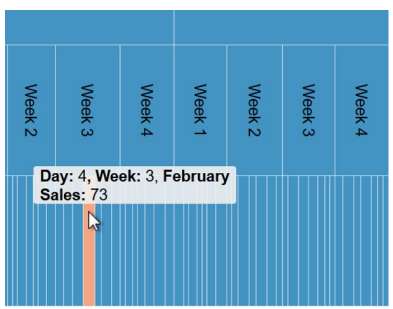


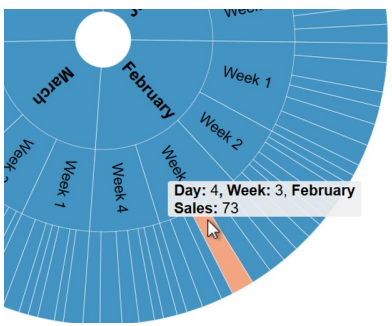






- Area more effective for comparison task





Results: Coordinate Systems

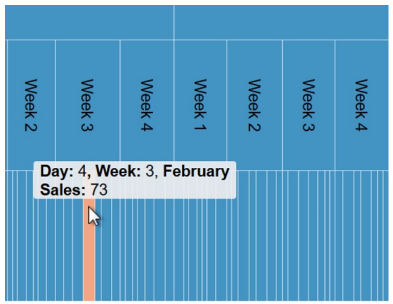
- Completion, accuracy, confidence, & ease

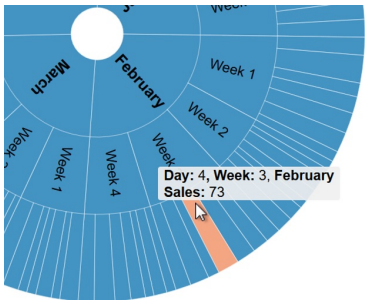
Results: Coordinate Systems

- Completion, accuracy, confidence, & ease
- Cartesian generally better than polar

Results: Coordinate Systems

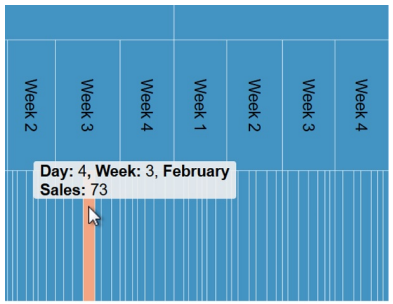
- Completion, accuracy, confidence, & ease
- Cartesian generally better than polar
- Polar better for minima task with area

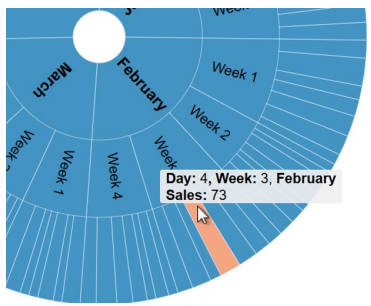




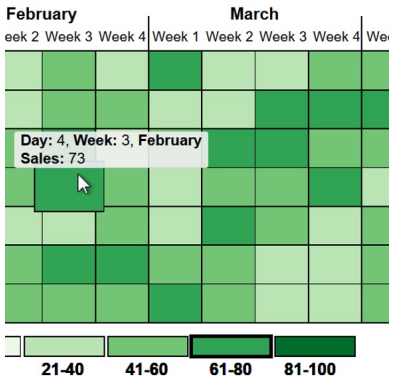
Results: Coordinate Systems

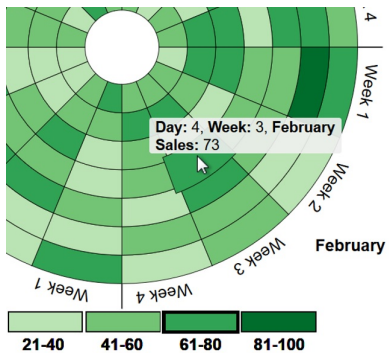
- Completion, accuracy, confidence, & ease
- Cartesian generally better than polar
- Polar better for minima task with area





- Neglible effect of coordinate system for colour





Key Findings

- Interactivity improved user experience
  - Improved confidence and ease of use, without a significant decrease in completion time or accuracy.

Key Findings

- Interactivity improved user experience
  - Improved confidence and ease of use, without a significant decrease in completion time or accuracy.
- No “one-size-fits-all”
  - The choice of a visual representation should be based on the type of tasks

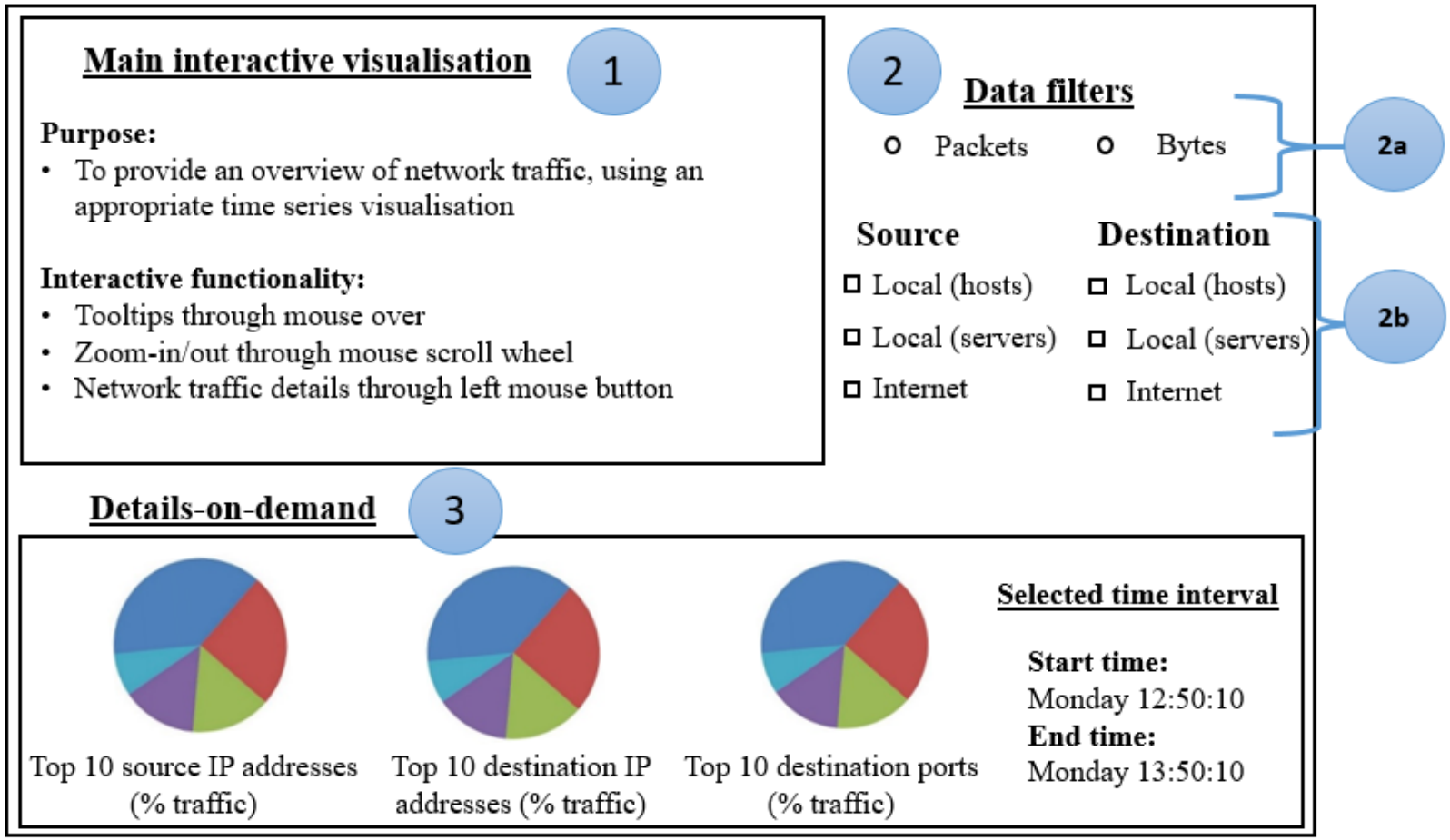
Key Findings

- Interactivity improved user experience
  - Improved confidence and ease of use, without a significant decrease in completion time or accuracy.
- No “one-size-fits-all”
  - The choice of a visual representation should be based on the type of tasks
- Generally, Cartesian is better
  - Cartesian coordinate systems are generally comparable or more effective than Polar, except for visualisations that use area for minima.

Talk Outline

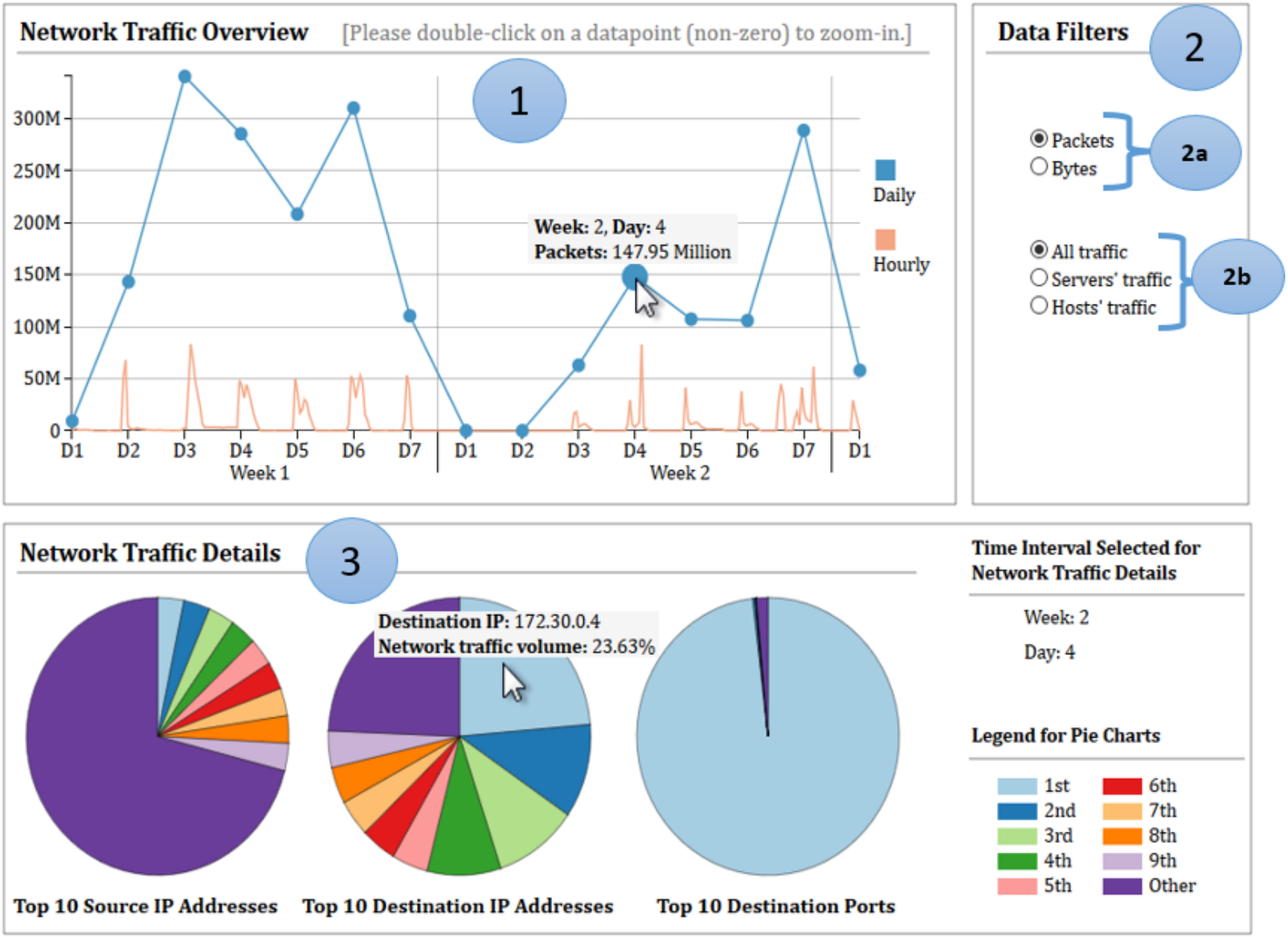
1. Low-fidelity design
2. Time series visualisations
3. **Proposed tool evaluation**

Initial low-fidelity design (reminder)

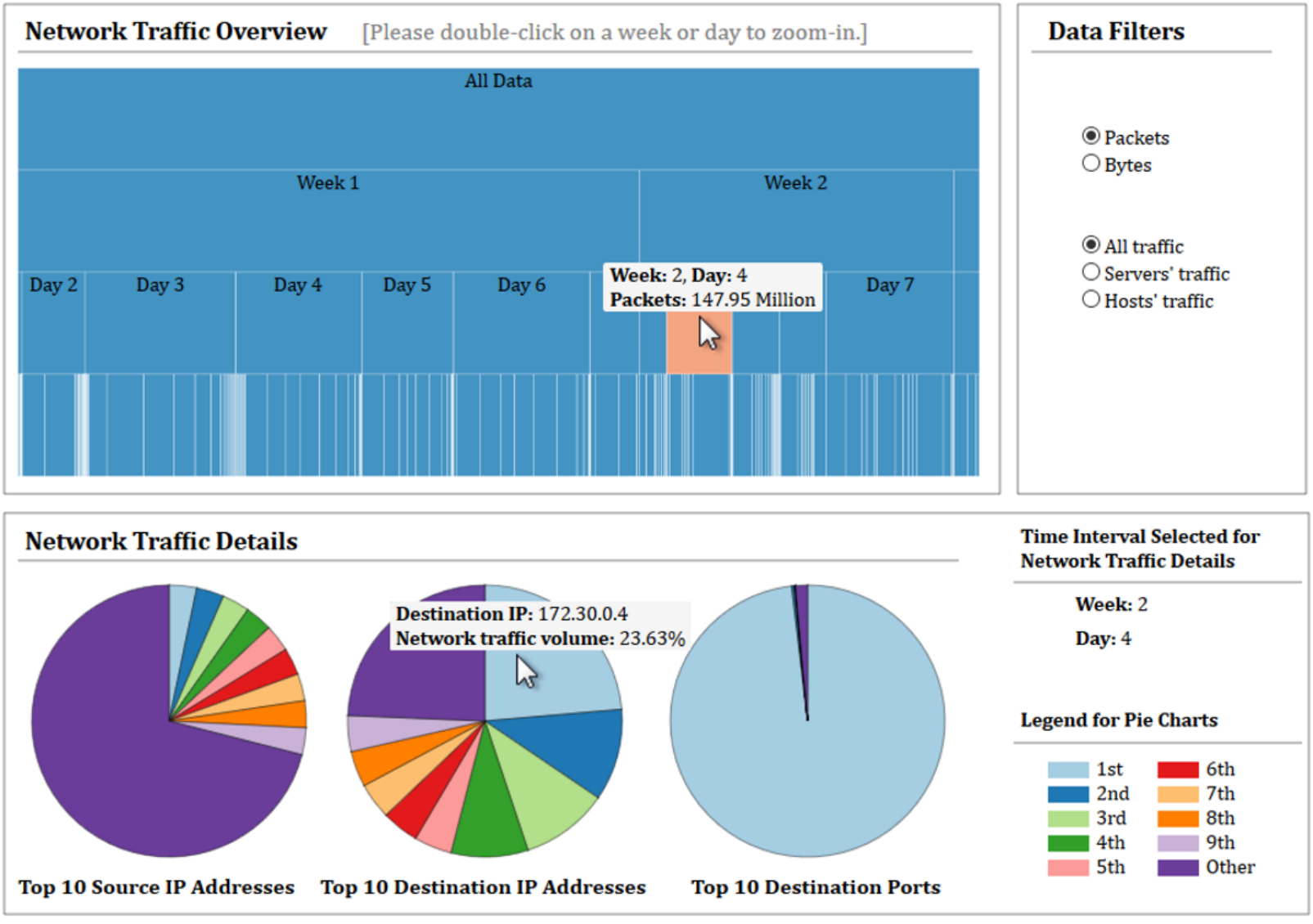


1. Network traffic overview
2. Data filters (a) packets & bytes (b) source & destination
3. Network traffic details

Proposed tool – Line chart



Proposed tool – Icicle plot



Proposed tool – Updates

- Streamline of source and destination filters
  - And radio buttons, rather than checkboxes
- Updates to some titles
- Inclusion of zoom interaction
- Visualsation choices
  - Line chart: Effectiveness for maxima, minima, and trend detection
    (could have also selected rectangular heatmap)
  - Icicle plot: Effectiveness for data comparison
    (could have also selected sunburst visualisation)

Tool Development and Dataset

- Developed as a web application
  - HTML5, CSS, Javascript, and D3.js
  - MySQL to store network flow data, via PHP
- Network flow dataset from the VAST 2013 challenge
  - 8GB of data with about 70mil network flow records
  - 15 days of network traffic collected from a simulated network
  - Includes four potential bandwidth depletion DDoS attacks
- We created three different variations of the dataset for our three experimental conditions
  - Original & increased/decreased traffic volume
  - Temporal position of DDoS attacks randomly positioned

User Study

- We recruited 12 participants for a lab study to measure the tool's effectiveness
- A within-subjects design with participants exposed to three conditions (counterbalanced)
  1. Tool with line chart only
  2. Tool with icicle plot only
  3. Tool with both visualisations available (radio button)
- Participants asked to find three possible network attacks
- Measures
  - Completion time and accuracy
  - Usability measure using SUS and NASA-TLX
  - Also conducted a post-evaluation design interview

Quantitative Results

Conditions	Time(s)	Acc.(%)	SUS	NASA-TLX
Line	153	89	77	31
Icicle	129	89	76	31
Both	164	97	80	31
Average	149	92	78	31

- No statistically significant difference between the conditions

Qualitative Results

- Post-evaluation semi-structured design interview
- Interviews recorded and analysed similar to LF design
- Network traffic overview
  - Preference for line chart vs. icicle
  - Desire for ability to better compare data, e.g., view zoomed chart simultaneously with original
- Network traffic details
  - Desire for more detail and interaction
- Interactive functionality
  - Desire for more detail with tooltips

Looking Ahead

- Future work on time series visualisations
  - Increased study of interactivity
  - Offset, interaction effects, different tasks and interactions
  - Use in different domains
- Visualisations for network security
  - Challenge to meet needs/desires of network security professionals
  - Challenge to convey information in visualisations. Max/min are "easy". Comparison and trend detection more challenging.
  - Approaches need to start with clear use case, and requirements (e.g., involvement of end-user professionals)

Further reading

Work on time series visualisations was published at CHI'16. Paper available from my website.

Contact

Interactive & Trustworthy Technologies (ITT)

Web	http://www.ittgroup.org/
Twitter	@ITT_Research

Mike Just

Web	http://www.justmikejust.co.uk/
Email	m.just@hw.ac.uk