TOP SECRET STRAP1

Graph theory in the operational environment

[redacted] - GCHQ

Information & Communications Technology Research (ICTR)

What I will cover

- Finding operational closed loops:
  - The reality of target behaviour
  - The process of looking for closed loops
  - Some statistics on a large graphs components
  - A real life example
  - Cheap and disposable handsets
  - Catching targets for real
  - What Donald Rumsfeld taught me about closed loops
- Using graphs to visualise and characterise timing relationships in a contact graph

What is a closed loop?

- A set of (for example) phones that communicate only amongst themselves as a means of communications security
- This is generally speaking too loose a definition for practical purposes

Tightening up the definition of a closed loop

- A component on three or more nodes that is neither the giant component nor a tree

Work on this topic since 2005

- GCHQ initially interested in topic following use of a closed loop by the July 7, 2005 bombers
- Analysis of anonymised meta-data for bulk UK-UK mobile call records indicated that this was a rare phenomenon and pointed to possible target discovery opportunities
- Closed loop analysis of VOICESAIL showed promise but work was truncated
- SANAR-08 presentation demonstrated that operational closed loops could in theory be discovered

The reality of target behaviour

- Targets from different IPT's regularly purchase groups of cheap mobile phones and use them operationally for a short period (possibly as long as three months) before getting a new set
- Two critical features:
  - Most of the phones start life at about the same time
  - Most of the phones are cheap handsets
- Sometimes the targets make a mistake and make a call to a phone outside the closed loop

The process of looking for closed loops

- Choose a time window (e.g. 10 days)
- Clean up the data for that period
- Componentize the graph
- Extract the components that fit the closed loop definition

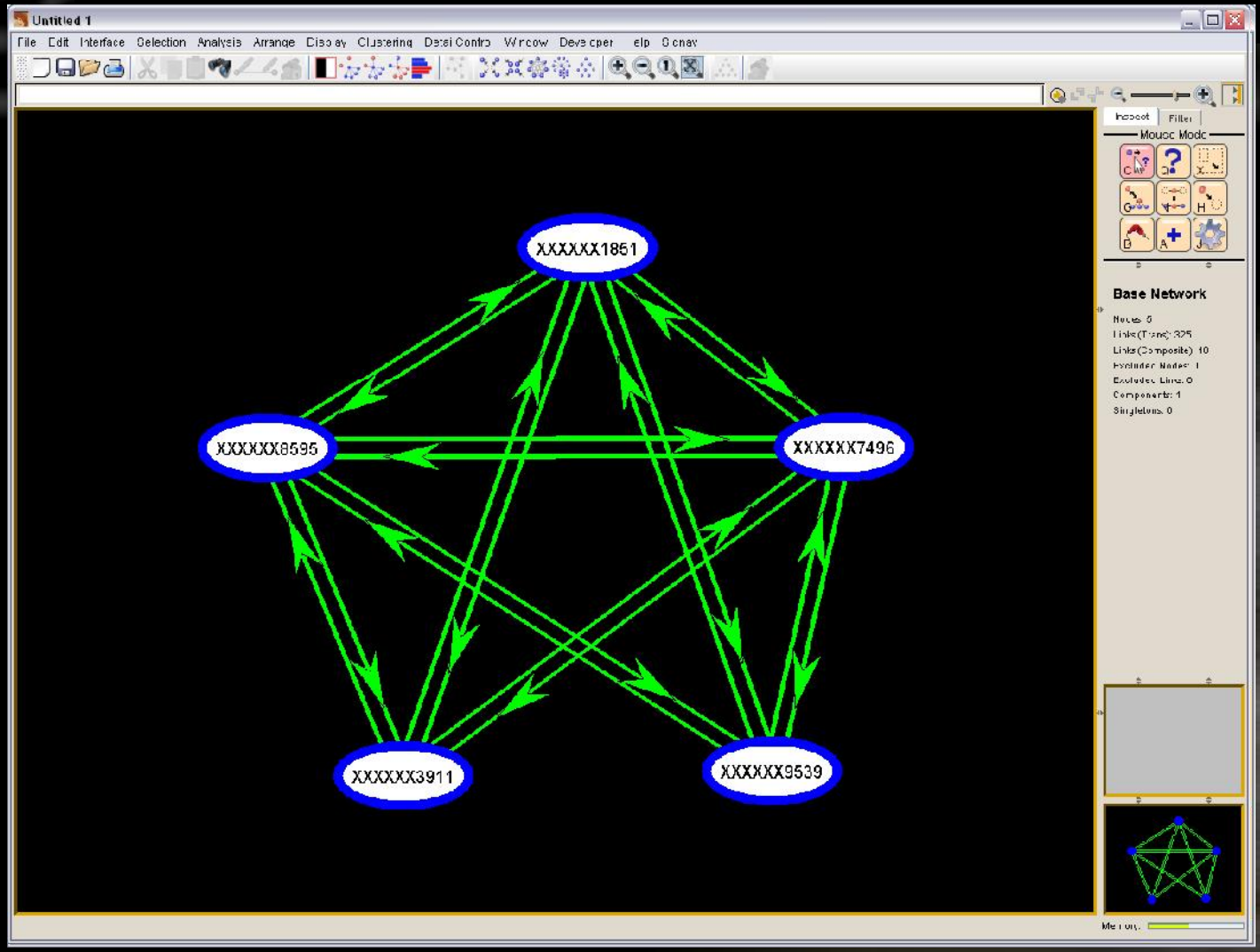
The effect of windowing

- We need to window the data or else slip ups by the closed loop members will render the group invisible
- Need to choose a window that is large enough to allow the giant component to form but not so large that we never see targets who periodically goof up.

Some statistics about components

- 1507405 edges and 1606330 nodes
- 922135 nodes in the giant component (57%)
- 222477 components, of which 218327 (98.1%) are trees
- 4149 non-tree, non-giant components, involving 39927 nodes (2.5% of total)
- 17 of these components had at least 70% of the nodes illuminating within a 3 week period.

A closed loop is born...



When geolocation is not enough...

- Targets love cheap handsets, bless ‘em
- Nokia occupy the largest segment of the cheap phone market. Nokia 1* phones are nasty.

Nokia 1616

"Unashamedly aimed at the bottom end of the mobile phone spectrum... under the bonnet things remain distinctly unimpressive"

TOP SECRET STRAP1

Vodafone 252

"A very affordable handset that comes with basic voice call and message services"

Samsung 1150

"This cut-price phone offers bare-bones functionality and lacks what many mobile users would deem to be essential features"

TOP SECRET STRAP1

Testing the cheap phone hypothesis

- What type of handset did the July 7, 2005 London bombers use?
- At least three of the four phones used on that day were a Nokia 1100