MINT program helps pinpoint threats contained in intelligence data

May 22 2014, by Rick Robinson

The GTRI MINT team – (left to right standing) Alan Nussbaum, Shane Carleton, Chris Kennedy, (sitting) Brian Mulvaney, Dana Fitzgerald and Ben Davis – reviews a graph network of nodes on-screen showing the amount of support for hypothesized relationships among users of multiple location-based social media networks. Credit: Gary Meek

Every day U.S. military and security units receive vast amounts of data collected by intelligence, surveillance and reconnaissance (ISR) sensors. Human analysts constantly review this data, searching for possible

threats.

To aid this effort, researchers from the Georgia Tech Research Institute (GTRI) are helping to improve the capabilities of the nation's Multi-Disciplinary Intelligence (Multi-INT) system, which monitors incoming data.

A key to improving the U.S. Multi-INT system involves bringing "actionable intelligence" – information that could require immediate response – to the attention of human analysts as quickly as possible, explained Chris Kennedy, a research program analyst who leads the MINT effort in GTRI. But finding actionable intelligence is a challenge; it must be identified from myriad raw data gathered by intelligence sources, which include optical and radar sensors, communications sensors, measurements and signatures intelligence (MASINT) and others.

"The number of analysts is limited, and they can only perform a certain number of actions," said Kennedy. "So out of a huge set of information – which could involve millions of data points – you need to find the most valuable pieces to prioritize for investigation and possible action."

Accelerating the System

GTRI's work addresses two related Multi-INT challenges:

- Network bandwidth and workstation processing power sometimes can't keep up with incoming data sets that contain terabytes or even petabytes of raw information.
- Human analysts need to stay on top of incoming data by concentrating on the most significant information.

Metadata are small amounts of information that contain the key elements

of a data point, which is an individual piece of data. For example, in the case of a car moving down a road, its metadata might consist of the make/model/color, location, speed and number of passengers. Those attributes are highly informative, yet much easier to transmit and process than, say, a video of the car, which would involve large amounts of data.

The GTRI approach creates metadata fields, or utilizes existing ones, thereby characterizing each data point with minimal overhead. Then only the metadata is transmitted to the main system for immediate processing; the rest of the raw data is retained in an archive in case it's needed later.

The metadata technique results in much smaller amounts of information being relayed from ISR sources to computers. That reduces processing loads, helping computers and networks keep up with incoming data. The raw data is also stored and can be examined if necessary.

"Obviously under this data-reduction approach there are information losses that could affect how our program makes decisions, which is why our system is only a tool for – and not a replacement for – the human analyst," Kennedy said.

Informing the Analyst

The second challenge – supporting human analysts – is addressed by methods that improve the system's ability to identify, compare and prioritize different types of information.

First, the gathered metadata is converted into a single uniform format. By creating one format for all incoming metadata, data points from many different sources can be more readily identified and manipulated. This uniform format is independent of the data source, so different types of ISR data can be processed together.

Then, utilizing the identity-bearing metadata tags, GTRI researchers use complex machine-learning algorithms to find and compare related pieces of information. Powerful concurrent-computing techniques allow problems to be divided up and computed on multiple processors. That helps the system perform the complex task of determining which data points have been previously associated with other data points.

Metadata approaches have been used in the past, Kennedy explained, but only for a single intelligence technology – such as a text-recognition program that identifies keywords in voice-to-text data. The GTRI approach differs because it integrates metadata from a variety of intelligence disciplines into a single technology that prioritizes corroborative relationships from multiple sources.

Under GTRI's integrated approach, one set of potentially significant signals could be quickly compared to others in the same vicinity to form an in-depth picture. For example, in a disaster relief scenario, one aircraft-mounted ISR sensor might detect information indicating abandoned vehicles. But if another sensor detected a functioning communications device in one of the vehicles, that would indicate a higher likelihood of finding a survivor, prompting a rescue reconnaissance.

The relationship found between the communications device's signal information and the vehicle's imagery information would be prioritized against other found relationships and displayed to the analyst on mapping software, such as GTRI's FalconView program.

Ongoing Improvement

Recently, the MINT team began working with a GTRI group that's involved in the ongoing development of Stinger, a Georgia Tech-produced graph-analysis software. Stinger's capabilities could aid MINT

in recording and analyzing information about long-term patterns of observed relationships – that, for instance, a type of vehicle and a specific communications device are frequently observed together by independent sensors.

This information would then be sent to an analyst through a web-based portal, giving the analyst access to alerts regarding specific kinds of relationships identified by MINT.

The MINT team is presently focused on improving the program's capacity to process many data points quickly. They're using three primary sets of testing data involving thousands or millions of data points over lengthy time spans. The researchers' goal is to achieve real-time or near-real-time processing capability, so analysts can be alerted to abnormal information almost instantly.

"We want to get to the point where, as the latest data is coming in, it's being correlated against the data we already have," Kennedy said. "We need to able to say to the analyst, 'OK you've got a million data points, but look at these 10 first.' "

Provided by Georgia Institute of Technology

Citation: MINT program helps pinpoint threats contained in intelligence data (2014, May 22) retrieved 18 July 2024 from https://phys.org/news/2014-05-mint-threats-intelligence.html