Applying algorithm to social networks can reveal hidden connections criminals use to commit fraud

September 6 2012

Fraudsters beware: the more your social networks connect you and your accomplices to the crime, the easier it will be to shake you from the tree.

The Steiner tree, that is.

In an article recently published in the journal Computer Fraud *and Security*, University of Alberta researcher Ray Patterson and colleagues from the University of Connecticut and University of California – Merced outlined the connection linking fraud cases and the algorithm designed by Swiss mathematician Jakob Steiner. Fraud is a problem that costs Canadians billions of dollars annually and countless hours of police investigations. Patterson says that building the algorithm into fraud investigation software may provide important strategic advantages.

The criminal path of least resistance

To quote a television gumshoe, everything's connected. Figuring out who knows who and who has access to the money is like playing a game of connect-the-dots. Patterson says that for crimes like fraud, the fewer players in the scheme, the more likely it will be accomplished. Maintaining a small group of players is also what links it to the Steiner tree. He says that by analyzing various connecting social networks—email, Facebook or the like—finding out the who, what and how of the crime can be boiled down to numbers.

"You're really trying to find the minimum set of connectors that connect these people to the various [network] resources," he said. "The minimum number of people required is what's most likely to be the smoking gun. You can do it with math, once you know what the networks are."

Fraud and the Steiner tree, by the numbers

In their article, Patterson and his colleagues explored how networks such as phone calls, business partnerships and family relationships are used to form essential relationships in a fraud investigation. When these same relationships are layered, a pattern of connection becomes obvious. Once unnecessary links are removed and false leads are extracted, the remaining connections are most likely the best suspects. Patterson says that finding the shortest connection between the criminals and the crime is the crux of the Steiner tree.

"All of these things that we see in life, behind them is a mathematical representation," said Patterson. "There are many, many different algorithms that we can pull off a shelf and apply to real-life problems."

A potential tool for the long arm of the law?

Patterson says that with the amount of work that could potentially go into investigating a fraud case, such as obtaining warrants for phone or email records, and identifying and interviewing potential suspects, developing a program that uses a Steiner tree algorithm may save a significant portion of investigators' time—time that, he says, could likely be reallocated to backlog or cold case files. "If you can reduce your legwork by even 20 per cent, that has massive manpower implications. I think algorithms like this one could help you reduce your legwork a lot more than that," he said.

Although there is software that police and other law enforcement agencies can use to solve fraud, Patterson sees no evidence that those programs use a Steiner tree algorithm, something he says would bring some structure to an unstructured area. He hopes programmers and investigators will take note of the findings and make changes to their practices.

"It might take several years or many years before anyone picks it up," said Patterson. "But it's a good thing if we can point people towards what's useful."

Provided by University of Alberta