Print

Social Networks and their Applications: Fraud

Social networks can also be used for fraud detection. Fraudsters tend to cluster together to exchange knowledge about how to commit fraud, use the same resources, and collaborate on fraudulent activities. Different profiles sometimes turn out to belong to a single person, such as in identity theft. Common types of fraud are credit-card transaction fraud, tax evasion or Social Security fraud, and identity theft. Let's discuss these in more detail.

Here you can see a subset of a real-life credit card transaction network, which we analyzed in previous research. The yellow nodes represent stolen credit cards. The blue nodes represent the stores or merchants. Red edges represent fraudulent transactions, whereas green edges represent legitimate transactions. From this network, it can be seen that stolen credit cards are often used in the same stores. Typically, each of these stores will also process legitimate transactions to cover up fraudulent activities.

In tax evasion or Social Security fraud, we study links between companies. These companies set up fraud rings to evade taxes or Social Security payments. Here you can see a network of companies in which the green nodes represent legitimate companies and the red nodes represent fraudulent companies. A key issue here is the definition of the edges. How can we define a connection between two companies? A connection can be based on shared infrastructure, shared employees, or a shared physical address, for example. A popular fraud construction in tax evasion or Social Security fraud is the concept of a spider construction. The black central node is the key perpetrator and coordinator of the fraud ring. The fraudster starts up a company or white node, which does not pay taxes or Social Security payments, and intentionally goes bankrupt. The resources such as personnel, equipment, and so on, are then shifted to another legitimate company or white node, which does the same thing. This process creates a web or spider construction. Using the concept of social networks, these spider constructions can be detected.

Social networks can also be used to detect identity theft. In this form of fraud, a fraudster adopts another person's profile. Examples of identity theft can be found in telecommunications fraud, where fraudsters steal an account from a legitimate customer. In the network on the left, the legitimate customer (customer 1) calls his or her frequent contacts. The network on the right shows what happens after the fraudster (customer 2) steals the identity of customer 1. Each customer's legitimate calls are shown in green. Because the fraudster continues to call his or her own contacts, the network starts linking customer 1's account with the fraudster's own account. As the red lines indicate, you can now see customer 1 making fraudulent calls to customers H through O, who were previously part of customer 2's network. This is a clear sign of identity theft.

Close