A new game theory algorithm could one day help detect election tampering

March 2 2017, by Heidi Hall

America's president isn't the only one considering the possibility of rigged elections.

Vanderbilt University's Yevgeniy Vorobeychik, assistant professor of computer science and computer engineering, spent much of last year researching how and why someone would want to tamper with an election and then developing an algorithm to protect against those efforts. He and his international colleagues are improving that algorithm through a number of extensions and testing it on 2016 U.S. election data.

Vorobeychik said he ultimately wants to translate the best version into software available to public agencies.

His first inspiration came from Pakistan in 2013, where bombings by terrorists subverted the electoral process. Other nations may more likely face the cyberattack version of that violence—bloodless, but no less damaging to the democratic process.

Vorobeychik is a game theory expert who has applied that branch of mathematics to genomic data privacy, homeland security and emergency response, but he quickly saw connections between these fields and attacks on the voting process. He began reading the work of J. Alex Halderman, a computer science professor at the University of Michigan, on electronic voting machine flaws that attackers could use to compromise elections.

"With increased use of electronic voting machines, it's more important to consider why someone would attack them, what it would accomplish and how to address that," Vorobeychik said.

He explains how game theory applies to this field by using the example of two diamonds in two vaults, one considerably more valuable than the other. Do guards protect the most expensive one? Or is it the cheaper one, since the thief assumes the other is being watched? Game theory randomizes the process and increases the guards' chances of duplicating the criminal mind and protecting the correct diamond.

The algorithm can be used for monitoring machines in certain polling places during elections or for auditing polling places or districts after voting ends but before elections are certified. People committing election fraud obviously don't want to be detected, so their interference will be subtle, Vorobeychik said, likely targeting individual machines or districts so that they're effectively removed from the total votes – making the outcomes close to a tie in districts that are likely to support the candidate they want to fail.

"The new extension more realistically models the attacks on voting systems that would actually happen," Vorobeychik said. "It's easy enough for humans to just work with a list of districts in order of importance to, say, a presidential election. It's harder to figure out how to randomize that list to best determine which districts would be targeted. Turns out it helps a tremendous deal to have a computer."

His team tested the algorithm on both randomly generated data and results from the French presidential election of 2002 because it was readily available. (That test found nothing alarming.) Now, they're using recently available 2016 presidential election results from Michigan because it was a state with a suspicious swing.

The problem of randomizing decisions for both the defender protecting elections and the attacker seeking to infiltrate them is NP-hard, which means it's computationally intractable. The team used a double-oracle framework and mixed-integer linear programming techniques to write an algorithm that can be scaled up for large elections.

It will allow the computer to pull random districts likely to be targeted and let auditors check for discrepancies in vote totals. Doing that by hand would be labor-intensive, and those tampering with machines could find out the selection system. The algorithm makes that process completely unpredictable. The new extension to the algorithm makes it better reflect whatever system election attackers are using to make their decisions.

"Would they have an algorithm like this? Our work assumes the worst case scenario—that they do," Vorobeychik said. "We're designing protection around that. If they design something not as intelligent, we only do better.

"With game theory, you can systematically address attacks and their consequences. If there are a million people who voted illegally, you want to know that and mitigate it. How you deal with that is going to be up to the authorities, but they need to detect it first."

His original paper, "Optimally Protecting Elections," was published July 2016 at the International Joint Conference in Artificial Intelligence. His collaborators are in Beijing, Singapore and Israel.

Provided by Vanderbilt University

election.html