Protecting Elections with Minimal Resource Consumption (Extended Abstract)

Yunpeng Li
School of Computer Science and Engineering
Southeast University
Nanjing, Jiangsu, China
yunpengli.seu@gmail.com

Yichuan Jiang*
School of Computer Science and Engineering
Southeast University
Nanjing, Jiangsu, China
yjiang@seu.edu.cn

Weiwei Wu
School of Computer Science and Engineering
Southeast University
Nanjing, Jiangsu, China
weiweiwu@seu.edu.cn

ABSTRACT
In democratic elections, malicious agents may attempt to control elections to achieve their own goals. To guarantee impartiality, it is necessary to protect the election outcomes from control. In this paper, we consider how to protect election outcome from control using minimal resources. We assume malicious agents attempt to prevent a specific candidate from winning a democratic election with plurality rule through denial-of-service (deletion) attacks on voter groups (e.g., polling places). First, we show that the problem is NP-hard. Second, we propose a ($|C|$-1)-approximation algorithm for the problem, where $|C|$ is the number of candidates. Finally, we validate the efficiency of our approximation algorithm based on simulation experiments.

Keywords
Election protection, Minimal Resources, Approximation algorithm

1. INTRODUCTION
Democratic elections are an important part of modern society. Malicious agents may attempt to control elections to achieve their own goals. For example, the 2013 election in Pakistan was marred by a series of election-day bombings, resulting in over 30 dead and 200 injured, in an attempt to subvert the voting process [17], and the 2010 Sri Lanka election exhibited 84 major and 202 minor incidents of poll-related violence [4]. Incidents of this sort seriously threaten impartiality. To guarantee impartiality, it is necessary to protect the election outcomes from control.

Computational complexity of election control has been intensely studied. In the seminal work of Bartholdi, Tovey, and Trick [2], the authors state that a voting rule is resistant if it is NP-hard to control (i.e., it is NP-hard to find a feasible strategy to manipulate the election outcome), and vulnerable otherwise. Since then, researchers extended the study of election control to many other models and voting rules [3, 5, 6, 7, 9, 10, 11, 13, 14, 16]. In [8, 12], voting rules that are NP-Hard to control have been designed to protect elections. However, NP-Hardness of control does not provide complete protection because it is possible to solve large-scale instances of NP-Hard problems in practice (e.g., Xu et al. [19] in the case of SAT) [20]. Therefore, Yin et al. [20] propose to protect the election by preventing election control attacks from influencing the election outcome. Nevertheless, it is still an unanswered question that how many resources are sufficient to protect election outcome from control.

In this paper, we assume that malicious agents attempt to prevent a specific candidate from winning a democratic election with plurality rule through denial-of-service (deletion) attacks on voter groups (which may represent polling places). We consider how to protect the election outcome from control using minimal resources (e.g., physical security resources for polling places). First, we show that the problem is NP-hard. Second, we propose a ($|C|$-1)-approximation algorithm for the problem, where $|C|$ is the number of candidates and is usually small in real democratic elections, e.g., presidential (or prime minister) election [1, 18]. In the algorithm, we divide the problem into sub-problems with two candidates and construct the protection strategy based on solving the sub-problems. Finally, we validate the efficiency of our approximation algorithm based on simulation experiments. To the best of our knowledge, this is the first work studying the optimal protection strategy for plurality voting that can ensure the election outcome is not manipulated by group-deletion-attacks and minimal resources are consumed.

2. FORMAL MODEL
We consider the destructive control problem where malicious agents attempt to prevent a specific candidate from winning through denial-of-service (deletion) attacks on voter groups (which may represent polling places). Based on the model of [20], we present our model: Let $V=\{v_1,\ldots,v_n\}$ represent the set of n non-overlapping groups of voters and let $C=\{c_1,\ldots,c_m\}$ represent the set of candidates that voters prefer. We use $v_i(c_j)$ to represent the number of votes that candidate $c_j \in C$ can obtain in group $v_i \in V$ and use $v(c_j)=\sum_{v_i \in V} v_i(c_j)$ to represent the total votes that $c_j \in C$ can obtain from group set V. We consider plurality voting where each voter only votes for one candidate and the candidate with the most votes wins (we assume that a tie-breaking rule is adopted in the election). Let $w \in C$ represent the candidate who would have won the election with the original set of voters. We assume that malicious agents attempt to prevent w from winning by deleting a subset of V. The idea is to give a candidate $c \in C^{-w}$ (C^{-w} represents the candidate subset $C \backslash \{w\}$) a vote advantage over w and make it impossible for w to win the election. Conversely, the election defender hopes to ensure that w can win the election even if malicious agents implement attacks. The defender is willing to provide enough resources (e.g., physical security resources) to protect the election. However, it needs a certain cost to deploy each resource. Therefore, we consider how to protect the election outcome from control using minimal resources. We assume that the malicious agents and defender have the same knowledge about the vote distribution in each voter group (which can be obtained from the pre-election poll) and can predict the election outcome

* Corresponding author

Appears in: *Proc. of the 16th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2017), S. Das, E. Durfee, K. Larson, M. Winikoff (eds.) May 8–12, 2017, São Paulo, Brazil.*

based on the knowledge. If a group is protected, it cannot be deleted.

Let $\boldsymbol{d}(c_j)=\langle d_i(c_j) : v_i \in V\rangle$ denote a vector with $d_i(c_j)=v_i(c_j)-v_i(w)$ that is the vote advantage of candidate $c_j \in C^{\neg w}$ over w in group $v_i \in V$. Use $tb(c_j, w)$ to represent the advantage of candidate c_j over w in the tie-breaking rule. If c_j precedes w in the tie-breaking rule, we set $tb(c_j, w)=1$ and $tb(w, c_j)=0$, otherwise set $tb(c_j, w)=0$ and $tb(w, c_j)=1$. We assume that malicious agents adopt attack strategy AS, namely, deleting group subset $AS \subseteq V$ and the defender adopts protection strategy DS, namely, protecting group subset $DS \subseteq V$. Then, for a candidate $c_j \in C^{\neg w}$, its total vote advantage over w during the election can be defined as follows:

$$\begin{aligned} sup(c_j, DS, AS) &= \sum_{v_i \in V \setminus (AS \setminus DS)} v_i(c_j) - \sum_{v_i \in V \setminus (AS \setminus DS)} v_i(w) + tb(c_j, w) \\ &= \sum_{v_i \in S_>(c_j) \setminus (AS \setminus DS)} d_i(c_j) - \sum_{v_i \in S_<(c_j) \setminus (AS \setminus DS)} |d_i(c_j)| + tb(c_j, w) \\ &\le \sum_{v_i \in S_>(c_j)} d_i(c_j) - \sum_{v_i \in S_<(c_j) \cap DS} |d_i(c_j)| + tb(c_j, w) \qquad (1) \\ &= UB(c_j, DS) \end{aligned}$$

where $S_>(c_j)=\{v_i \in V \mid d_i(c_j)>0\}$ and $S_<(c_j)=\{v_i \in V \mid d_i(c_j)<0\}$.

Proposition 1. $sup(c_j, DS, AS)>0 \Leftrightarrow$ Candidate c_j can prevent w from winning the election.

Proposition 2. $sup(c_j, DS, AS) \le 0 \Leftrightarrow$ Candidate c_j cannot prevent w from winning the election.

Without loss of generality, we assume that one protection resource is required to protect one voter group. Then, the problem can be formulated as follows:

$$\begin{aligned} \min \quad & |DS| \\ s.t. \quad & sup(c_j, DS, AS) \le 0, \forall c_j \in C^{\neg w}, \forall AS \in VS \end{aligned} \qquad (2)$$

where $|DS|$ represents the cardinality of DS and VS represents the power set of V. Due to the limitation of space, we omit the proof.

Theorem 1. Finding a minimal resource-consumption strategy that can protect the election outcome from control is NP-hard.

Theorem 2. Protection strategy $DS \subseteq V$ can protect the election outcome from control implemented by group-deletion-attacks $\Leftrightarrow$ $UB(c_j,DS) \le 0$ for each $c_j \in C^{\neg w}$.

Theorem 3. For a candidate $c_j \in C^{\neg w}$, if $DS \subseteq DS'$ and $UB(c_j,DS) \le 0$, we have $UB(c_j,DS') \le 0$.

3. APPROXIMATION ALGORITHM

Based on Theorem 3, we propose the approximation algorithm that is described in Algorithm 1.

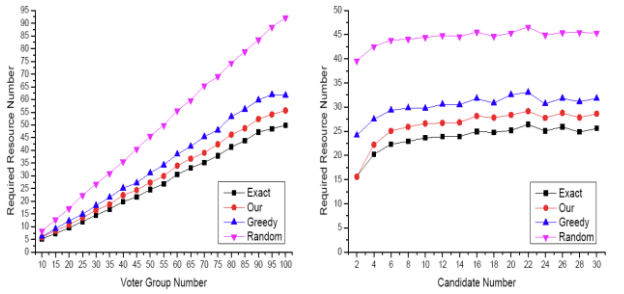
Algorithm 1: The Approximation Algorithm

```
1: input: d* = {d(c_j) | c_j ∈ C^¬w}
2: output: the protection strategy DS
3: DS ← ∅
4: for each c_j ∈ C^¬w do
5:     DSC_j ← ∅
6:     V' = <v^o, ρ ∈ 1,…,n> ← sort v_i ∈ V by increasing d_i(c_j)
7:     for ρ in 1…n do
8:         UB ← tb(c_j, w) /* Compute UB(c_j, DSC_j ∪ DS)*/
9:         for each v_i ∈ V do
10:            if d_i(c_j)>0 or v_i ∈ DSC_j ∪ DS then
11:                UB ← UB + d_i(c_j)
12:            end if
13:        end for
14:        if UB ≤ 0 then break /*UB(c_j, DSC_j ∪ DS) ≤ 0*/
15:        DSC_j ← DSC_j ∪ {v^o}
16:    end for
17:    DS ← DS ∪ DSC_j
18: end for
19: return DS
```

Theorem 4. Algorithm 1 is a ($|C|$-1)-approximation algorithm for the election protection problem.

4. EXPERIMENTAL EVALUATIOM

Based on the theoretical analyses, we have demonstrated that the proposed algorithm can output feasible protection strategies. Therefore, we mainly evaluate the solution quality of the proposed algorithm in the simulation experiments. We compare the proposed algorithm with three baselines. The first, termed *Exact*, returns a optimal protection strategy for the problem. The second, termed *Random*, randomly selects voter groups to add to the protection strategy until it can protect the election outcome from control. The third, termed *Greedy*, continually selects the voter group that holds the maximum $v_i(w)$ among the unprotected groups to add to the protection strategy until it can protect the election outcome from control. In the experiments, we randomly generated a vote tally for each candidate within each group uniformly in [0, 100] [20]. Each data point is an average over 50 such samples.



(a) Changing voter groups (b) Changing candidate number

Figure 1: Comparison of resource consumption

Figure 1 shows the comparison of resource consumption. In Figure 1(a), there are 15 candidates and in Figure 1(b), the number of voter groups is 50. From Figure 1(a), we find that more protection resources are needed to protect the election as the number of voter group increases. Besides, we find that our approximation algorithm outperforms other non-optimal approaches and its resource consumption is close to that of the exact (optimal) algorithm. From Figure 1(b), we find that resource consumption increases slowly as the candidate number increases and our approximation algorithm also has the best performance among non-optimal approaches. Besides, we find that the difference between the resource consumption of our approximation algorithm and that of the exact (optimal) algorithm is relatively stable as the candidate number increases. It illustrates that our approximation algorithm can offer relatively stable performance as the candidate number increases.

5. COCLUSION

In this paper, we investigate how to protect the election outcome of plurality voting from group-deletion-control using minimal resources. First, we show that the problem is NP-hard. Second, we propose a ($|C|$-1)-approximation algorithm for the problem, where $|C|$ is the number of candidates. Experimental results show that the proposed approximation algorithm produces near-optimal solutions.

6. ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (No. 61472079, No. 61170164, No. 71201077 and No. 61672154).

7. REFERENCES

[1] Bakst, B. 2012. Electoral College vote affirms Obama re-election. U.S. News & World Report. http://www.usnews.com/news/politics/articles/2012/12/17/electoral-college-set-to-affirm-obama-re-election

[2] Bartholdi, J. J., Tovey C. A., and Trick, M. A. 1992. How hard is it to control an election? *Mathematical and Computer Modelling*, 16(8):27–40.

[3] Betzler, N. and Uhlmann, J. 2009. Parameterized complexity of candidate control in elections and related digraph problems. *Theoretical Computer Science*, 410(52):5425–5442.

[4] Bhattacharjya S. 2010. Low turnout and invalid votes mark first post war general polls. http://www.sunday times.lk/100411/News/nws_16.html.

[5] Chen, J., Faliszewski, P., Nie-dermeier, R., and Talmon, N. 2014. Combinatorial voter control in elections. In *Proceedings of the 39th International Symposium on Mathematical Foundations of Computer Science* (Budapest, Hungary, August 25-29, 2014). MFCS'14. Springer Berlin Heidelberg, 153–164.

[6] Chen, J., Faliszewski, P., Nie-dermeier, R., and Talmon, N. 2015. Elections with few voters: Candidate control can be easy. In *Proceedings of the 29th AAAI Conference on Artificial Intelligence* (Austin, Texas, US, January 25-30, 2015). AAAI'15. AAAI, 2045–2051.

[7] Erdélyi, G., Hemaspaandra, E., and Hemaspaandra, L. A. 2015. More natural models of electoral control by partition. In *Algorithmic Decision Theory*, 396–413.

[8] Erdélyi, G., Nowak, M., and Rothe, J. 2009. Sincere-strategy preference-based approval voting fully resists constructive control and broadly resists destructive control. *Mathematical Logic Quarterly*, 55(4):425–443.

[9] Faliszewski, P., Hemaspaandra, E., and Hemaspaandra, L. A. 2011. Multimode control attacks on elections. *Journal of Artificial Intelligence Research*, 40(1):305–351.

[10] Faliszewski, P., Hemaspaandra, E., and Hemaspaandra, L. A. 2013. Weighted electoral control. In *Proceedings of the 12th international conference on Autonomous agents and multi-agent systems* (Saint Paul, MN, USA, May 6-10, 2013). AAMAS'13. IFAAMAS, 367–374.

[11] Hemaspaandra, E., Hemaspaandra, L. A., and Rothe, J. 2007. Anyone but him: The complexity of precluding an alternative. *Artificial Intelligence*, 171(5):255–285.

[12] Hemaspaandra, E., Hemaspaandra, L. A., and Rothe, J. 2009. Hybrid elections broaden complexity-theoretic resistance to control. *Mathematical Logic Quarterly*, 55(4):397–424.

[13] Liu, H., Feng, H., Zhu, D., and Luan, J. 2009. Parameterized computational complexity of control problems in voting systems. *Theoretical Computer Science*, 410(27):2746–2753.

[14] Liu, H. and Zhu, D. 2010. Parameterized complexity of control problems in maximin election. *Information Processing Letters*, 110(10):383–388.

[15] McCormick, G. P. 1976. Computability of global solutions to factorable nonconvex programs: Part I-convex underestimating problems. *Mathematical Programming*, 10:147–175.

[16] Menton, C. 2013. Normalized range voting broadly resists control. *Theory of Computing Systems*, 53(4):507–531.

[17] RT 2013. Election day bombings sweep Pakistan: Over 30 killed, more than 200 injured. https://www.rt.com/news/pakistan-election-day-bombing-136/.

[18] TW 2015. Election results live 2015: David Cameron wins UK general election. http://www.theweek.co.uk/election-2015-4

[19] Xu, L., Hutter, F., Hoos, H. H., and Leyton-Brown, K. 2008. SATzilla: Portfolio-based algorithm selection for sat. *Journal of Artificial Intelligence Research*, 32(1):565–606.

[20] Yin, Y., Vorobeychik, Y., An, B., and Hazon, N. 2016. Optimally Protecting Elections. In *Proceedings of the 25th International Joint Conference on Artificial Intelligence* (New York, NY, USA, 9-15 July 2016). IJCAI'16. IJCAI/AAAI, 538-545.