Event-based Model Simulating the Change in DDoS Attack Trends after P/DIME Events

Adam Tse and Kathleen M. Carley

Institute for Software Research
Carnegie Mellon University, Pittsburgh, PA 15213
atse1@andrew.cmu.edu,kathleen.carley@cs.cmu.edu

Abstract. This paper describes the methods for creating an event-based simulation used to predict DDoS attacks against countries following international events. The model uses various parameters for an event and generates time series DDoS attack data for the two countries over one week. The simulation uses a weighted, tit-for-tat approach in determining retaliation. The model was evaluated using attack data of actual events provided by Arbor Networks consisting of a two-week interval plus a day, centered around the start of the events. The model was sufficient in predicting the change in frequency of DDoS attacks following hostile diplomatic events, but it was unsuccessful at simulating attacks following friendly, military, and economic events. Overall, the resulting simulation was a successful baseline for future work in the field.

Keywords: DDoS, simulation, modeling, cyberwarfare, cyber-policy, cyber-attacks, international relations

1 Introduction

Cyberwarfare has become a difficult issue in international relations. Nations are suspected of facilitating cyber-attacks to steal intellectual property and attack urban infrastructure to improve their own economic status and there has been little success in holding countries responsible for cyber-attacks[9][1]. One prominent tactic of cyberwarfare is distributed denial of service (DDoS) attacks against infrastructure and state resources. DDoS attacks are a type of attack where a victim machine is made unavailable due to flooding of bandwidth or resources from a network of compromised machines. Few examples of state-sponsored attacks include a Russian attack on major Estonian webservers in 2007 and a series of Iranian DDoS attacks against banks in the United States (U.S.) in 2013[2].

Previous research indicated that cyber-attacks are associated with social, political, and cultural conflicts[3]. Thus, a simulation was created using P/DIME (political/diplomatic, informational, military, and economic), a reputed methodology defined by the National Defense University for managing operations to attain the effect required to complete an objective, to classify international events and predict their effect on DDoS attack trends[8].

The paper is organized into the following sections: the relevant works, the methods of the simulation, the virtual experiment using five real events, the results and discussion, and limitations of the model, and a conclusion along with possible directions to expand the research.

2 Relevant Work

Though there has been a large amount of research on cyber-attacks, DDoS attacks, and attribution, most of those works have focused on the technical defenses and processes of DDoS attacks[6][5]. This paper is novel because it focuses on a "sociology of nations" perspective of DDoS attacks rather than a technical perspective. The most similar research includes a focus on game theory between institutions and other analysis on motivations of cyber-attacks[3][8][1][7].

3 Method

Users have the ability to control the P/DIME Category, whether an event was hostile or friendly (1 or 0), the severity of an event (1 to 3), the source and target country of the event, and a random noise coefficient represented as number between 0 and 10. Events tested in the simulation are defined by the previously mentioned properties minus the random noise coefficient. The schema was represented as E(Type, Hostility, Severity, Source, Target). The dependent variables for the simulation include the total number of DDoS attacks and the attacks per hour targeting both the source country of the event and the target country of the event.

The static variables were the ally matrix (matrix specifying ally countries; 0 or 1), the enemy matrix (matrix specifying enemy countries; 0 or 1), countries (U.S., China, and Russia), and country attributes (aggression, GDP[4], percentage of internet users[10], and average attacks per hour).

A high level diagram of each simulation iteration is shown on Figure 1 and a more detailed description of the algorithm is provided in additional works in the Springer Journal.

4 Virtual Experiment

In order to test the simulation, the results of the simulation were compared with real DDoS attack data taken around the timeframe of the events. The data was provided by Arbor Networks from the Digital Attack Map website at `http://www.digitalattackmap.com/`.

The real DDoS attack data was compared with the simulated data for similarities using the Google CausalImpact R library. In each comparison, the pre period started a week before the event and the post period started 24 hours after the event. If the scenario models exhibited behavior closer to the real data than the None scenario, then it was concluded that adding event-driven cyber-attacks improved the realism of the model. The events chosen included the following:

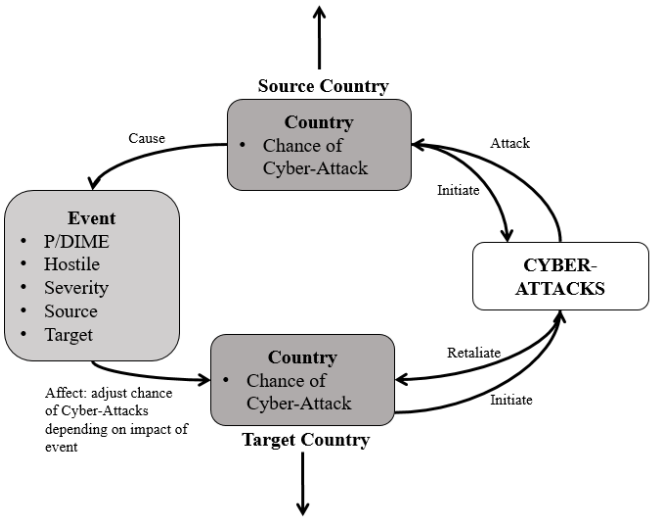

Fig. 1. System diagram of simulation algorithm

- China ignores court decision South China Sea 07/12/2016; E(D, 1, 2, China, U.S.)
- U.S. China Cybersecurity talk 06/14/2016; E(D, 0, 1, U.S., China)
- U.S. claims Russia hacked Democratic National Committee (DNC) and Hilary Clinton 10/14/2016; E(D, 1, 3, U.S., Russia)
- Vladimir Putin exits nuclear security pact 10/03/2016; E(M, 1, 3, U.S., Russia)
- Chen Fengs HNA Group bus $6.5 billion stake in Hilton 10/28/2016; E(E, 0, 2, China, U.S.)

These events were chosen because of their variance in P/DIME categories, hostility, and severity. Only events between U.S., China, and Russia were chosen because of the high number of cyber-attacks happening between the three countries. Additionally, in current events, the U.S., China, and Russia are currently the three strongest cyber powers in the world.

5 Results and Discussion

5.1 Overview

The complete results are presented in Table 1. A detailed analysis of each event and possible explanation of the results is below. Time series plots showing the impact of events over the week are in additional works in the Springer Journal. Overall, the event cases exhibited better performance than the no event case for all five events.

The simulated effect of the South China Sea Dispute Court Decision and Hacking of the DNC were very accurate. Both countries suffered an increase in

Table 1. Comparison of results of simulation with real world data

Event	Schema	Arbor	Simulation
South China Sea Dispute 07/12/2016	E(D, 1, 2, CN, US)	CN 6.3%, [-37%, 50%] P=.371	CN 1.8%, [0.76%, 2.7%] P=.001
		US 66%, [32%, 97%] P=.001	US 0.55%, [-0.28%, 1.3%] P=.084
China Cybersecurity Talk 06/14/2016	E(D, -1, 1, US, CN)	US 50%, [-0.51%, 103%] P=.027	US -4.4%, [-5.3%, -3.5%] P=.001
		CN -32%, [-77%, 14%] P=0.082	CN 0.13%, [-0.82%, 1.1%] P=.404
Hacked DNC 10/14/2016	E(D, 1, 3, US, RU)	US 50%, [9.8%, 90%] P=.007	US 3.3%, [2.5%, 4.1%] P=.001
		RU 150%, [6.7%, 293%] P=.018	RU 0.18%, [-0.77%, 1.1%] P=.365
Nuclear Security Pact 10/03/2016	E(M, 1, 3, US, RU)	US -32%, [-74%, 7.7%] P=.059	US 61%, [60%, 62%] P=.001
		RU -57%, [-144%, 29%] P=.121	RU 148%, [147%, 149%] P=.001
HNA Group Stake Hilton 10/28/2016	E(E, -1, 2, CN, US)	CN -70%, [-166%, 23%] P=.067	CN 77%, [77%, 78%] P=.001
		US -20%, [-56%, 12%] P=.127	US 145%, [144%, 146%] P=.001

DDoS attacks. Additionally, the effect of the Hacking of the DNC had a higher degree than the effect of the South China Sea Dispute which was consistent with the higher severity score of the Hacking of the DNC. The only inconsistency was the degree of increase in DDoS attacks. The inconsistencies with the South China Sea Dispute Court may be attributed to interference from a previous event where the U.S. had sent the U.S. Navy to hinder Chinese claims on the sea.

Though DDoS attacks against China after the U.S./China Cybersecurity Talk dropped, the assumption that friendly events cause a decrease in all DDoS attack trends was false as indicated by the increase in DDoS attacks against the U.S. This can be explained by the hidden agendas and intents behind events. Though China was stating publicly that they would try to stop cyber-attacks, sanctioned attacks could have still been going on as a result of the event.

In regards to the Failed Nuclear Security Pact and the Group Stake on Hilton, the simulation predicted a significant increase in DDoS attacks, however the Arbor data showed a significant, large decrease in DDoS attacks. The decline in DDoS attacks after the Failed Nuclear Security Pact can be a result of limitations in data or it may indicate that both parties wanted to maintain relations after the argument. The decrease in DDoS attacks after the HNA Group Stake might be because economic events between the private industry may not have an effect on DDoS attacks and other events may be influencing the decrease. Additional study on these types of events may be needed to see if the correlations are consistent.

Overall, the results were very good considering the little amount of study done in the field. Diplomatic events were predicted fairly accurately and only little adjustments will be needed to improve the model. However, friendly, military, and economic events exhibited the opposite effect of what was predicted. More analysis of these events may be needed to create a more accurate model.

5.2 Limitations

The first issue with the methods mentioned above was the Causal Impact analysis. At the start of the experiment, it was assumed that an international event would have an effect lasting one week. Google's Causal Impact Library takes a pre-period and a post-period as parameters where the change between pre-period and post-period determines whether a significant event happened between the two periods. Because of the low significance in effect for some of the real data, the experiment indicated that events may have shorter effect times. As a result, further studies must be made on different post-periods to determine how long would an event impact the frequency of DDoS attacks.

Additionally, the virtual experiment was limited in depth. The experiment only consisted of one event of each type category which was not a significant enough sample given the many input parameters for the simulation. As a result, it is difficult to prove if these results can be generalized for all events. This can be seen by the outcome of friendly, military, and economic events. The results were different from the model. However, it was not clear if this was a result of an incorrect assumption in the model or an anomaly event. On the contrary, diplomatic events seemed accurate because it had a consistent effect between the two events. Future study must be made specifically on each event type and input variable to see if the results are accurate.

However, even without the validation and virtual experiment issues, the model has quite a few limitations because of the simple assumptions it makes. First, the simulation assumes events are isolated. In the real world, events take place concurrently affecting each other and it is difficult to determine causation because of the sheer amount of noise. Additionally, the simulation does not take into account groups within nations. It assumes events affect whole nations when they may only affect groups within the nation such as civilians, companies, non-profits, or governments. Lastly, it assumes events have a visible effect on DDoS attack trends one day after the event. This is probably dependent on the event itself and the experiment may need to be repeated where effects begin in different periods after the event occurred.

6 Conclusion

Overall, the simulation is on the right track to predicting the impact of DDoS attacks. Though it may need tuning on the degree of increase, it correctly predicted the increase of DDoS attacks for both hostile diplomatic events. It also

predicted that there would be an increase in DDoS attacks against one country and a decrease in DDoS attacks for another country on diplomatic, friendly events. Some features of the simulation that require tuning are its estimation of friendly, military, and economic events, the time it takes for the effect to occur and the duration of the effect, and the degree of effect for hostile diplomatic events.

For future work, an in-depth analysis should be done on each parameter of the simulation to determine the exact correlation of the parameter if one is found. The most logical one to examine is hostile diplomatic events which seemed to have fairly accurate results. Afterwards, events with unknown effects such as Military and Economic events should be analyzed to determine how they can be modelled. Overall, this study has proved that modelling and simulating the impact of international events on DDoS attacks is feasible.

If the model was tuned accurately, the research should be pushed to being able to predict cyber-incidents rather than just DDoS attacks. Other possible directions would be to be able to simulate a sequence of events on cyber-attack trends and predict the effect of events on multiple countries over time. These additions would make it possible to recreate cyber-attacks worldwide and judge the vulnerability of countries and help attribute state-sponsored attacks.

References

1. Chaturvedi, A.R., Gupta, M., Mehta, S.R., Yue, W.T.: Agent-based simulation approach to information warfare in the seas environment. In: System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on. pp. 10–pp. IEEE (2000)
2. Clarke, R.A., Knake, R.K.: Cyber war. HarperCollins (2011)
3. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine 30(1), 28–38 (2011)
4. Group, W.B.: World bank group. (n.d.). gdp (current us$) (2016), `http://data.worldbank.org/indicator/NY.GDP.MKTP.CD`
5. Kotenko, I., Alexeev, A., Man'kov, E.: Formal framework for modeling and simulation of ddos attacks based on teamwork of hackers-agents. In: Intelligent Agent Technology, 2003. IAT 2003. IEEE/WIC International Conference on. pp. 507–510. IEEE (2003)
6. Kotenko, I., Ulanov, A.: Simulation of internet ddos attacks and defense. In: International Conference on Information Security. pp. 327–342. Springer (2006)
7. Kumar, S., Benigni, M., Carley, K.M.: The impact of us cyber policies on cyber-attacks trend. In: Intelligence and Security Informatics (ISI), 2016 IEEE Conference on. pp. 181–186. IEEE (2016)
8. Starr, S.H.: Toward a preliminary theory of cyberpower. Cyberpower and national security pp. 43–88 (2009)
9. Tereshchenko, N.: Us foreign policy challenges: cyber terrorism and critical infrastructure, e. International Relations 12 (2013)
10. Union, I.T.: "individuals using the internet 2005 to 2014", key ict indicators for developed and developing countries and the world (totals and percentage rates) (2015), `http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls`