# Assessment of Group Dynamics During Cyber Crime Through Temporal Network Topology

Nima Asadi[1(✉)], Aunshul Rege[2], and Zoran Obradovic[1]

[1] Computer and Information Sciences Department, Temple University, Philadelphia, USA
nima.asadi@temple.edu

[2] Department of Criminal Justice, Temple University, Philadelphia, USA

**Abstract.** Understanding group dynamics can provide valuable insight into how the adversaries progress through cyberattacks and adapt to any disruptions they encounter. However, capturing the characteristics of such dynamics is a difficult task due to complexities in the formation and focus of the adversarial team throughout the attack. In this study, we propose an approach based on concepts and measures of social network theory. The results of experiments performed on observations at the US Industrial Control Systems Computer Emergency Response Team's (ICS-CERT) Red Team-Blue Team cybersecurity training exercise held at Idaho National Laboratory (INL) show that the team dynamics can be captured and characterized using the proposed approach. Moreover, we provide an analysis of the shifts in such dynamics due to the adversarial team's adaptation to disruptions caused by the defenders.

**Keywords:** Network theory · Group dynamics · Machine learning

## 1 Introduction

Governments and organizations worldwide are experiencing a continuously evolving threat landscape, where cyberadversaries are highly organized, sophisticated, and persistent. Defenders can only be effective if they understand how adversaries organize, make decisions, carry out attacks, and adapt to disruptions. Earlier research has examined adversarial attack paths also known as intrusion chains, time spent on the various stages of cyberattacks, and which stages adversaries focus on more when they are disrupted by defenders span [1–4].

However, little is known in the open literature about adversarial group dynamics. It is imperative to study how adversaries interact, structure themselves, change over the duration of the attack, manage disruptions by defenders, recover from their mistakes, and make decisions as they progress through cyberattacks in real-time.


R. Thomson et al. (Eds.): SBP-BRiMS 2018, LNCS 10899, pp. 401–407, 2018.
https://doi.org/10.1007/978-3-319-93372-6_44

## 2 Methodology

### 2.1 Case Studies

The dataset for our first case study was collected at a five day cybersecurity training organized by the United States Industrial Control Systems Computer Emergency Response Team (ICS-CERT) and hosted by Idaho National Laboratory (INL) in September/October 2014. The training included a Red Team/Blue Team exercise (RTBTE), where the Red team operated as the adversarial team. The Red Team consisted of ten members who had a mixed set of skills. The data for the second case study was collected at a one-day student cybersecurity competition where a team including 7 members was observed and interviewed. The data used for the case studies in this paper included time stamped observations of the Red Teams in both of the mentioned exercises.

### 2.2 Construction of the Temporal Network

Capturing the characteristics and patterns in the adversarial team's formation during the cyber intrusion can helps us gain important knowledge about the decision making, task scheduling and planning its process. Here we propose a methodology for capturing and analyzing such information by using concepts and measurements of network science. In order to perform such analysis, we first create the temporal network of the adversarial team based on the commonalities in activities of the team members during each time point. In other words, if, team members A and B perform the same intrusion chain stage during the time point t, a link is drawn between them in the network. For this purpose, we use the intrusion chain model proposed by [3]. Therefore, at each time point, the team members are the nodes of the network, and the links (edges) between them indicates that the nodes have been performing similar intrusion stage during that specific time point. Each time point for our case study spans for 15 min. Therefore, this criteria generates T different networks where T is the number of time points.

After creating the team network for each time point, we are able to take advantage of several informative measures for capturing and analysis of team dynamics. In the next section, we discuss our proposed measures for the analysis of team dynamics using the constructed temporal networks.

### 2.3 Analytical Measures

**Number of Connected Components.** Number of connected components is an important topological invariant of a graph [6]. In this study, a high number of connected components in a graph shows that a majority of team members work individually on non-similar intrusion stages, while a lower number of connected components shows that more members work together on similar intrusion stages. In other words, the number of connected components is an indicator of the level of connectivity and cooperation.

**Edge Density.** Density of the edges in the network shows the level of overall connection in the network. This measure is defined as the number of connections a node has, divided by the total possible connections a node can have [6].

**Transitivity.** Transitivity is the overall probability of the existence of tightly connected communities or cliques. This measure is calculated as the transitivity is the ratio of triangles to triplets in the network.

**Average Shortest Path Length.** Average shortest path length in a graph is calculated as the average number of stops needed to reach two distant nodes in the graph. The smaller the result, the more efficient the network in information circulation.

**Average Node Degree.** Average node degree is simply calculated by averaging the degrees of all of the nodes in the graph.

**Modularity.** Modularity quantifies the degree to which the network may be subdivided into clearly delineated groups.

After deriving the listed network characteristics, they are used to form the feature vector for detection of possible anomalies in the adversarial movement. In order to make such prediction, we train an algorithm for binary classification where the labels indicate if the condition is normal, or an anomaly is taking place, i.e. a disruption is happening. Sources of disruptions can be the Blue team or the Red team's own failures. We used support vector machine (SVM) and logistic regression as the classifiers for this study.

## 3 Results

### 3.1 Team Dynamics Characteristics

The team dynamics networks were created for each time point according to the descriptions provided in the previous section. The duration of the first and second RTBTE sessions were 9 and 6 hours, respectively. An example of the network created at four different time points for the first case study is provided in Fig. 1. In that figure, the top left figure indicates the graph at the very beginning of the exercise where we can observe a complete graph (each node is connected to every other node). This is due to the fact that in the team spent the very early phase of the exercise discussing the plans, meaning that the entire team was involved in one task. The three other plots display the Red Team's formation during three different periods of the exercise. For instance, in the top right figure, we can observe that team members 2 and 8 were working individually on separate intrusion chain stages while two other groups, each including four members, were involved in different intrusion chain stages.

### 3.2 Network Analysis Results

A plot of number of connected components and edge density for the first case study are provided in Fig. 2. An observation one can make based on that figure is

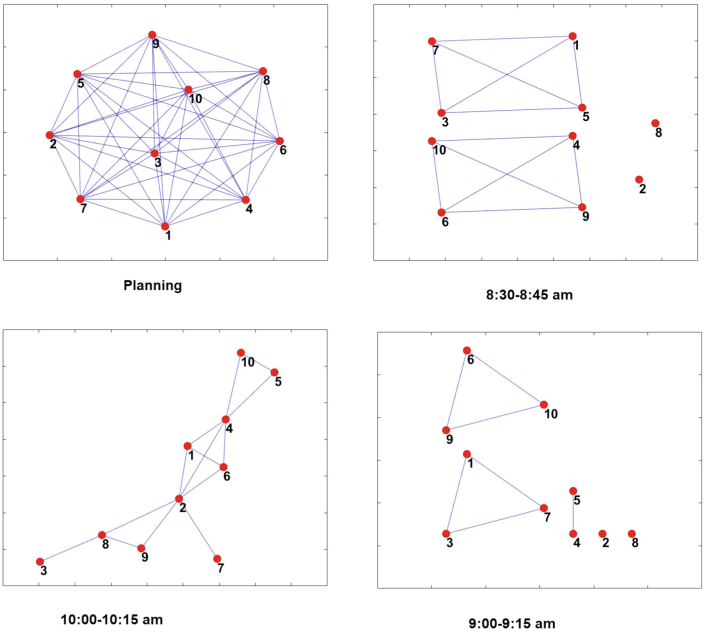


**Fig. 1.** Example graphs constructed from the case study data at four different points of the exercise.

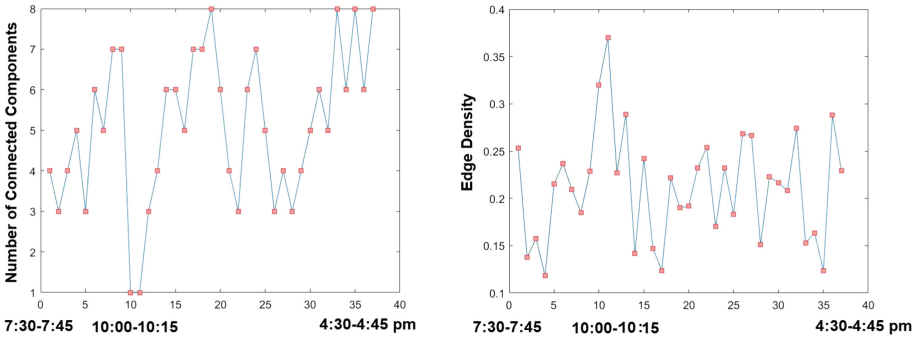


**Fig. 2.** Analytical results of team dynamics based on constructed temporal networks. Left: the number of connected components at each time point. Right: the edge density of the networks at each time point.

the existing anomaly in both number of connected components and edge density plots during the time point 10:00 am to 10:15 am. This can be associated to the fact that two disruptions were observed at the case study one at that time. As we can observe in Fig. 2, during and after occurrence of a disruption, the number of connected components decreased to one while the edge density was increased to above 0.3. One can interpret this decrease of the number of connected components and increase in edge density as the immediate increase in the entire Red team's focus on a few certain intrusion stages. This observation can be expanded to other network network measures as well. For anomaly detection We used the data from case study one as the training sample, and case study two as the test sample. The reason for using different case studies as the train and test datasets is to ensure the generalizability of the model. Note that each data point in our prediction is a time point at the cyber security training. The prediction results are provided as the area under the curve (AUC) in Fig. 3. We can observe that AUC of 0.782 and 0.735 were achieved using logistic regression and SVM, respectively.

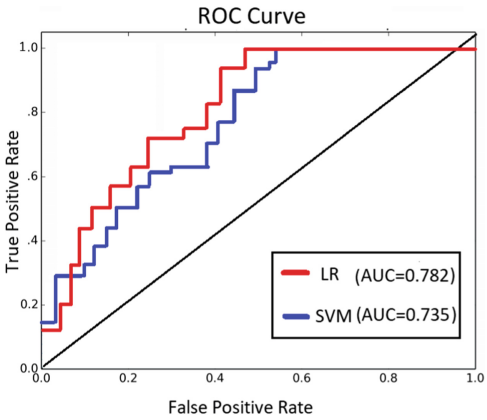


**Fig. 3.** Area under the curve (AUC) for anomaly prediction through characteristics of team dynamic network. LR stands for logistic regression, and SVM denotes support vector machine.

## 4 Conclusion

Certain limitations with this study, such as lack of generalizability are inevitable. However, the authors argue that this work intends to lay the framework for further research in the area. Moreover, the case study in this paper is based on two case studies including one of the most reputable force on force ("paintball") exercises in the United States.

The proposed network analysis offers some interesting findings about the adversarial team dynamics:

**The Team Dynamics Networks Usually Contains More than One Connected Component**

Except from the two time periods after the disruptions occurred, the number of connected components remained above two. This indicates that usually the adversarial subgroups perform multiple intrusion stages in parallel.

**The Edge Density is Usually Low Throughout the Exercise**

Except the time span when the disruptions took place, the edge density of the constructed networks was below 0.3. This further indicates the sparse and parallel performance of the subgroups of the Red Teams rather than being highly connected and focused on few intrusion stages together.

**Disruptions Can Affect Team Dynamics**

Topological characteristics of the team dynamic networks show deviation during disruptions. For instance, the decrease in connected components and the increase in edge density can be interpreted as a change in team dynamics towards more focus on certain intrusion stages with higher connection among team members. The results of anomaly detection using the machine learning algorithms further prove the effect of disruptions on team dynamics.

This paper offered a preliminary analysis of adversarial group dynamics during a real-time cybersecurity exercise. Future research, however, should delve deeper into other aspects of groups, such as the influence and interaction in groups, performance and functionality, divisions of labor, and subgroup decision-making and autonomy.

**Acknowledgements.** This material is based upon work supported by the National Science Foundation CAREER Award, Grant No. CNS1453040 and partially by National Science Foundation CPS Award, Grant No. 1446574. The authors thank the Industrial Control Systems Computer Emergency Response Team (ICSCERT) and Idaho National Laboratory (INL) for allowing data collection at their September/October 2014 Red Team/Blue Team Cybersecurity Training Exercise.

## References

1. Rege, A., Obradovic, Z., Asadi, N., Singer, B., Masceri, N.: A temporal assessment of cyber intrusion chains using multidisciplinary frameworks and methodologies. In: 2017 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp. 1–7. IEEE, June 2017
2. Rege, A., Obradovic, Z., Asadi, N., Parker, E., Masceri, N., Singer, B., Pandit, R.: Using a real-time cybersecurity exercise case study to understand temporal characteristics of cyberattacks. In: Lee, D., Lin, Y.-R., Osgood, N., Thomson, R. (eds.) SBP-BRiMS 2017. LNCS, vol. 10354, pp. 127–132. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60240-0_16
3. Cloppert, M.: Security Intelligence: Attacking the Cyber Kill Chain (2009). http://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain. Accessed 2 Feb 2014
4. Colbaugh, R., Glass, K.: Proactive Defense for Evolving Cyber Threats. Sandia National Laboratories [SAND2012-10177] (2012). https://fas.org/irp/eprint/proactive.pdf. Accessed 15 Feb 2017

5. Leclerc, B.: Crime scripts. In: Wortley, R., Townsley, M. (eds.) Environmental Criminology and Crime Analysis. Routledge, Abingdon (2016)
6. Krause, J., Croft, D.P., James, R.: Social network theory in the behavioural sciences: potential applications. Behav. Ecol. Sociobiol. **62**(1), 15–27 (2007)
7. Rokach, L., Maimon, O.: Clustering methods. In: Maimon, O., Rokach, L. (eds.) Data Mining and Knowledge Discovery Handbook, pp. 321–352. Springer, Boston (2005). https://doi.org/10.1007/0-387-25465-X_15
8. Schneider, R.: Survey of peaks/valleys identification in time series. Department of Informatics, University of Zurich, Switzerland (2011)
9. Ellens, W., Kooij, R.E.: Graph measures and network robustness. arXiv preprint arXiv:1311.5064 (2013)