ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

ATTACKER AGAINST NETWORK INTERDICTION IN UNKNOWN PRIORI

A.Vijayalakshmi[1] , T.Akila[2] and S.Bargunan[3]

[1]Assistant Professor, [2]Assistant Professor, [3]PG Scholar

Department of Computer Science and Engineering[1], Department of Information Technology[2]

Mahendra College of Engineering, Salem

[1] vijayalakshmia@mahendracollege.com, [2] akilat@mahendracollege.com, [3] sbargunan@gmail.com

Abstract:
Network interdiction refers to disrupting a network in an attempt to either analyze the network's vulnerabilities or to undermine a network's communication capabilities. A vast majority of the works that have studied network interdiction assume *a priori* knowledge of the network topology. However, such knowledge may not be available in real-time settings. Traditional method developed several learning techniques that enabled the attacker to learn the best network interdiction strategies (in terms of the best nodes to attack to maximally disrupt communication in the network) and also discussed the potential limitations that the attacker faces in such blind scenarios. We considered settings where 1) only one node can be attacked and 2) where multiple nodes can be attacked in the network. Several different network topologies are considered in this study and this also not suitable for secure nodes from attacks. So we propose a method for selecting route node automatically, from that the sender node automatically select route node for transferring file to receiver or destination node, so the attackers difficult to attack that node.

.

1. INTRODUCTION

Network centric architectures are increasingly gaining prominence, be it social networks or wireless networks, as they allow for decentralized operation among various nodes without the need for a central entity to control their communication. With the widespread deployment of such architectures, the security aspects of the underlying net-works are now a major concern. Security-related studies not only enable us to understand the vulnerabilities of the underlying network architecture, but also shed light on how to best attack that network. The ability to undermine a malicious network's communication capabilities is crucial for ensuring security in sensitive environments. In this paper, we particularly focus on attacks against networks when their topology is unknown a priori. Most studies that are related to attacking communicating nodes only consider the presence of a single node (source-destination pair) and develop optimal strategies, either at the physical layer or the MAC layer or the network layer (denial of service, or spoofing) in order to disrupt the communication capabilities of this node. Various formu-lations, ranging from optimization, game theory, information theory and machine learning, see, have been used to attack this node depending on the amount of knowledge that is available to the attacker. However, as mentioned earlier, with the rapid deployment of network centric architectures, it is now crucial to understand attacks against networks.

Network interdiction, as it is popularly known, has predominantly been studied by assuming that the network topology is known a priori. Optimization-based network interdiction formulations were presented in and game theoretic formulations were considered in . In the context of wireless networks, a flow-based formulation for jamming (the popular term used for attacks in the wireless communications literature) was discussed in where an optimization problem was formulated to identify the best jammer-to-flow association that will maximally

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

disrupt the network. In and references therein, the behavior and robustness of various network topologies were studied by attacking different nodes or edges-based on several graph-theoretic metrics (i.e., the network is modeled as a graph). For instance, some of the commonly used graph-theoretic metrics are degree centrality, between-ness centrality, min-cut etc. However, these metrics can only be exploited when the attacker has a prioriknowledge of the network topology. Further, attack strategies that are developed for one type of a network topology such as random Erdös-Rényinetworks may not always be capable of efficiently attacking other network topologies such as scale-free networks. Hence, in order to blindly attack net-works, online learning strategies that determine the best nodes to attack and disrupt communication in these networks are necessary.We assume that a) the attacker is aware of the total number of nodes in the network and b) is capable of identifying the total number of successful and unsuccessful flows in this network by observing the network traffic. By flow, we refer to a mes-sage that is exchanged between different nodes in the network. For instance, in the case of communication networks, acknowledgement (ACK) and no-acknowledgement (NACK) packets that are exchanged between the various nodes in this network indicate the total number of successful and unsuccessful message exchanges. Using such information, we present MAB algorithms with provable regret1 guarantees that indicate the learning performance of the attacker in comparison with the omniscient (optimal) attacker (i.e., one that has complete knowledge about the flows and topology of the network.). [5] discussed about a Secure system to Anonymous Blacklisting. The secure system adds a layer of accountability to any publicly known anonymizing network is proposed. Servers can blacklist misbehaving users while maintaining their privacy and this system shows that how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services.

2 EXISTING SYSTEM

Most Existing studies that are related to attacking communicating nodes only consider the presence of a single node (source-destination pair) and develop optimal strategies. Network interdiction, as it is popularly known, has predominantly been studied by assuming that the network topology is known *a priori*. Optimization-based network interdiction formulations were presented and game theoretic formulations were considered. In the context of wireless networks, a flow-based formulation for jamming (the popular term used for attacks in the wireless communications literature) was discussed where an optimization problem was formulated to identify the best jammer-to-flow association that will maximally disrupt the network. The behavior and robustness of various network topologies were studied by attacking different nodes or edges-based on several graph-theoretic metrics (i.e., the network is modeled as a graph). For instance, some of the commonly used graph-theoretic metrics are degree centrality, betweenness centrality, min-cut etc. However, these metrics can only be exploited when the attacker has *a priori* knowledge of the network topology.

Disadvantage:

- No unknown priori possible
- Attacker can easily attack a node

3.PROPOSED SYSTEM

In this Proposed we develop several multi-armed bandit (MAB) algorithms that provide finite-time guarantees for the attackers performance when attacking a network blindly. We assume that a) the attacker is aware of the total number of nodes in the network and b) is capable of identifying the total number of successful and unsuccessful flows in this network by observing the network traffic. By flow, we refer to a message that is exchanged between different nodes in the network. For instance, in the case of communication networks, acknowledgement (ACK) and no-acknowledgement (NACK) packets that are exchanged between the various nodes in this network indicate the total number of successful and unsuccessful message exchanges. Using such information, we present MAB algorithms with provable regretguarantees that indicate the learning performance of the attacker in comparison with the omniscient (optimal) attacker (i.e., one that has complete knowledge about the flows and topology of the network).

Architecture Diagram

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

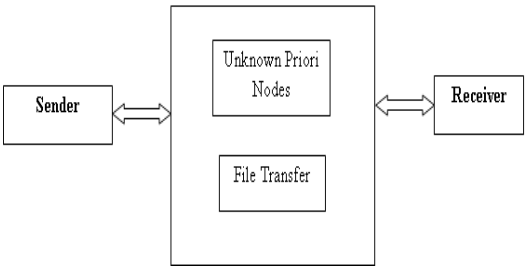

Fig.3 Architecture Diagram

Advantage

- It's capable of identifying the total number of successful and unsuccessful flows in this network.
- Efficient Unknown priori node
- Difficult to attack node

4.MODULE'S DESCRIPTION

4.1 Client-Server File Transfer

File transfer is a generic term for the act of transmitting files over a computer network like the internet. There are numerous ways and protocols to transfer files over a network. Computers which provide a file transfer service are often called file servers. Depending on the client's perspective the data transfer is called uploading or downloading. File transfer for the enterprise now increasingly is done with managed file transfer. In this paper, we develop several learning techniques that enable the attacker to learn the best network interdiction strategies (in terms of the best nodes to attack to maximally disrupt communication in the network) and also discuss the potential limitations that the attacker faces in such blind scenarios

4.2 Single-Node Attack

We first intend to find the single best node that can be attacked in order to disrupt the flows in the network. In this paper, we only focus on finding the node that enables the attacker to stop the maximum number of flows and the specific details regarding the attack procedures (either at the physical layer or MAC layer) can be found. For example similar details about attacks in social networks can be found. We first focus on the case where flows (the number as well as the source-destination pairs) are fixed over the time period of interest T and later we will consider cases where the flows change randomly.

We discuss a) existing attack strategies (which are not blind) that are used for benchmarking the attacker performance and b) performance metrics that enable for net-work interdiction performance comparison and to compare the gap in the learning performance of the attacker under blind scenarios.

4.3 Random Attacks

In this module, we discuss network interdiction strategies that the attacker can use under blind settings i.e., when the network topology is unknown *a priori*. These attack strategies will be comparedwith the benchmark non-blind attack strategies discussed in the previous section.

In this strategy, the attacker randomly attacks a node during every epoch. As expected this strategy performs worse than the other strategies discussed in this paper. This is the best it can do in completely blind settings when there is no feedback regarding its attack performance and serves as a lower bound to compare the various network attack strategies.

.

4.4 Learning Strategies against Fixed Flow Scenarios

We present multi-armed-bandit-based learning strategies where the attacker can learn the best node to attack in a real-time manner without knowledge of the network topology. For reasons that will be explained soon, except for some specific network topologies (such as tree, star), these learning algorithms cannot achieve performance close to the omniscient attack. It turns out that this is an inherent limitation in blind settings i.e., when the network topology is unknown. All learning algorithms are presented for the case when the network flows remain fixed for T epochs. Later, we discuss the performance of these algorithms when the flows change randomly at every epoch.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

4.5 The Route Discovery

The route discovery module is responsible for the discovery of trustworthy paths from a source to a destination. This module is invoked by the source whenever there is no cached path to the destination. To quantify the trustworthiness of a path, we define the following path reputation metric.

CONCLUSION

We studied blind network interdiction strategies i.e., attacking networks when their topology is unknown. Several learning algorithms have been proposed that attempt to learn the best node to attack in order to disrupt the network. We considered cases where a single attacker or multiple attackers can attack either a single node or multiple nodes in the network. We showed that (a) relying on well-known graph metrics, such as betweenness centrality, to attack a network works only in the case of star networks and does not necessarily work for all network topologies unless the flows are random, (b) under blind scenarios, the learning rates cannot be improved beyond $O(|V|)$ where $|V|$ is the number of nodes in the network, (c) in fixed-flow scenarios, the proposed slotted explore-exploit learning algorithm learns the optimal node to attack and in random flow scenarios it learns the node with the maximum betweenness.

REFERENCES

[1] S. Amuru and R. M. Buehrer, "Optimal jamming in digital communication—Impact of modulation," in *Proc. Global Commun.Conf.*,Austin, TX, USA, Dec. 2014, pp. 1619–1624.

[2] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modula-tion," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2212–2224, Oct. 2015.

[3] S. Amuru*et al.*, "Jamming bandits—A novel learning method for optimal jamming," *IEEE Trans. Wireless Commun.*, 2016, to be published.

[4] S. Amuru and R. M. Buehrer, "Optimal jamming using delayed learning," in *Proc. Mil.Commun.Conf.*, Baltimore, MD, USA, Oct. 2014, pp. 1528– 1533.

[5] Christo Ananth, A.Regina Mary, V.Poornima, M.Mariammal, N.Persis Saro Bell, "Secure system to Anonymous Blacklisting", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015,pp:6-9

[6] A. Proano and L. Lazos, "Selective jamming attacks in wireless net-works," in *Proc. Int. Conf. Commun. (ICC)*, Cape Town, South Africa, May 2010, pp. 1–6.

[7] R. K. Wood, "Deterministic network interdiction," *Math. Comput.Modell.*, vol. 17, no. 2, pp. 1–18, 1993.

[8] E. Israeli and R. K. Wood, "Shortest-path network interdiction," *Networks*, vol. 40, no. 2, pp. 97–111, 2002.