A Low-Cost Distributed Denial-of-Service Attack Architecture

KAIFAN HUANG1, LU-XING YANG2, (Member, IEEE), XIAOFAN YANG1, (Member, IEEE), YONG XIANG2, (Senior Member, IEEE), AND YUAN YAN TANG3, (Life Fellow, IEEE)

1School of Big Data and Software Engineering, Chongqing University, Chongqing 400044, China
2School of Information Technology, Deakin University, Burwood, VIC 3125, Australia
3Department of Computer and Information Science, University of Macau, Macau 999078, China

Corresponding authors: Lu-Xing Yang (ylx910920@gmail.com) and Xiaofan Yang (xfyang1964@gmail.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61572006, and in part by the Chongqing Basic Research and Front Exploration Project under Grant cstc2018jcyjA3093.

ABSTRACT With the advent of Internet-of-Things (IoT) age, IoT-based distributed denial-of-service (DDoS) attacks have become the mainstream of DDoS attacks. This paper is devoted to exploring the possibility of launching an IoT-based DDoS attack at an extremely low cost. First, a new DDoS attack architecture is proposed. Since the proposed architecture enjoys the advantages of zero management cost, good undetectability, and strong robustness, it is especially suited to resource-limited DDoS attackers. In this architecture and based on a novel botnet growth model, the optimal design of attack strategy is reduced to a variational problem, where the objective functional stands for the estimated expected impact of the DDoS attack associated with a DDoS attack strategy. Finally, the variational problem is resolved for three different types of DDoS defense strategies. This work deepens our understanding of IoT-based DDoS attacks.

INDEX TERMS Cybersecurity, distributed denial-of-service (DDoS) attack, Internet-of-Things (IoT), DDoS attack architecture, botnet growth model, attack strategy, variational problem.

I. INTRODUCTION

Generally speaking, a distributed denial-of-service (DDoS) attack is a cyber attack in which the malefactor attempts to paralyze a web server by flooding it from a botnet [1]. Traditional botnets are created by compromising home PCs. With the enhancement of PC built-in security, building a traditional botnet becomes increasingly difficult.

Internet-of-Things (IoT) devices are a blanket term for various gadgets that are not PCs but have processing power and an Internet connection. These devices, ranging from home routers and security cameras to baby monitors, are often deployed in remote and inaccessible locations. With the advent of IoT age, the number of IoT devices is growing explosively. According to a report of IoT Analytics Company, the total number of active IoT devices worldwide exceeded 7 billions in 2018, and the number is expected to grow to 10 billion by 2020 and 22 billion by 2025 [2]. Owing to lack of built-in ability to be patched remotely, IoT devices are much more vulnerable to cyber attacks than PCs [3].

As a result, IoT-based DDoS attacks have become the mainstream of DDoS attacks. As an instance, it was estimated by BitSight that in the aftermath of the 2016 Mirai cyber attack, which is an IoT-based DDoS attack, roughly 8% of Dyn’s customer base stopped using their services [4]. Consequently, gaining a deep insight into IoT-based DDoS attacks has recently become a research hotspot in the domain of cybersecurity [5], [6].

A. BACKGROUND

In order to launch an IoT-based DDoS attack, the attacker has to own an IoT botnet temporarily or permanently. Traditionally, there are two different ways to own an IoT botnet, which are briefly reviewed below.

• Manage an IoT botnet [7]–[9]. However, the management of an IoT botnet is costly. First, in order to protect the communication channel between the botnet and the attacker’s command-and-control (C&C) system from detection or hijacking, a set of channel protection techniques, ranging from domain generation algorithms and encryption techniques to covert channel techniques, must be employed, incurring an added cost.
in order to avoid single point failure, the C&C system should be deployed in a distributed or clustered way, increasing the cost for constructing the infrastructure and deploying the collaborative/cooperative protocol. Thirdly, in order to guarantee the effectiveness of a DDoS attack, the status of the botnet must be checked periodically. When an anomaly happens, the malware deployed in the botnet must be updated in a timely manner, which adds the management cost. Therefore, IoT botnets are usually managed by well-resourced criminal organizations.

- Pay for using a ready-made IoT botnet [10]. In this situation, there is no cost for managing the botnet. However, the long-term rental of an IoT botnet is still very expensive.

In the real world, most DDoS attackers have only very limited resources. Therefore, they can neither manage nor rent an IoT botnet. A question arises naturally: can an IoT-based DDoS attack be launched at extremely low cost? In this paper, we answer the question in a positive way.

### B. MAIN CONTRIBUTIONS

This paper is dedicated to exploring the possibility of launching an IoT-based DDoS attack at a lower cost. Our main contributions are sketched as follows.

- A new DDoS attack architecture is proposed. Different from traditional DDoS attack architectures, in this architecture the attack strategy is embedded into the botnet malware once and for all, and there is no botnet management at all. As a result, the cost for launching a DDoS attack is extremely low. Consequently, the new architecture is expected to be adopted by DDoS attackers with limited resources.

- In the new architecture and based on a novel botnet growth model, the optimal design of attack strategy is studied. First, the problem is modeled as a variational problem. Second, the variational problem is resolved for three different types of DDoS defense strategies (i.e., hard-threshold defense strategies, soft-threshold defense strategies, and smooth defense strategies), respectively.

The remainder of this paper is organized as follows. Section II reviews the related work. Section III describes the new architecture. Sections IV reduces the design of an optimal attack strategy as a variational problem, and Section V deals with the variational problem. This paper is closed by Section VI.

### II. RELATED WORK

In this section, we review the previous work that is closely related to the present paper, with the goal of highlighting the novelty of our work.

### A. DDoS ATTACK ARCHITECTURE

In the existing DDoS attack architectures, the botnet management is indispensable. According as the difference in the management mode of botnet, these architectures can be roughly classified into two different types: centralized and decentralized [7]–[9]. Additionally, the two architectures may be mixed to form various hybrid DDoS attack architectures.

In a centralized DDoS attack architecture, there is no communication between zombie machines in the botnet. Instead, all the machines are connected to a system of command-and-control (C&C) servers (C&C system, for short), and the botnet is managed by issuing commands directly to these zombies. The development of the centralized DDoS attack architecture undergoes three phases: Internet Relay Chat (IRC)-based, web-based, and agent-handler. Below let us make a brief review.

Botnet originates from the Internet Relay Chat (IRC) protocol released in 1993 [11]. The protocol was originally designed for realizing instant online chatting function. In the same year, Eggdrop as the first known botnet malware that exploits the IRC protocol to communicate with zombies was published [12]. Due to ease in realization, IRC-based DDoS attack architectures became very popular in the following decade. GTbot [13], SDbot [14], Spybot [15], and Agobot [16] are all examples of this architecture.

Since IRC-based botnets are easily detectable, DDoS attackers turned to exploit hypertext transport protocol (HTTP) to communicate with zombie machines. Since the messages used for managing the botnet are blended into HTTP traffic streams, the detection of web-based botnet becomes very difficult. In the past decade, web-based DDoS attack architectures have been configured on multiple botnets, including Pushdo [17], Blackenergy [18], Zeus [19], and Srizbi [20].

In a web-based architecture, the management of large botnet is complex. Therefore, DDoS attackers developed a hierarchical structure of botnet management, which is named the agent-handler model. In recent years, many botnets, ranging from Luobot [21] to Mirai [4], were built based on agent-handler DDoS attack architecture.

All the above centralized DDoS attack architectures have a common defect: the botnet is vulnerable to single-point failure. Specifically, once the C&C system is blocked by an Internet Service Provider (ISP) or taken over by a hacker, the botnet would no longer exist. To enhance the robustness of the botnet, decentralized DDoS attack architectures were proposed [7]–[9].

In a decentralized DDoS attack architecture, the machines in the botnet form a peer-to-peer (P2P) network, and the botnet is managed by issuing commands to one or a few machines, which in turn forward the commands to other machines through the P2P network. Due to strong robustness, the P2P architecture have become very popular, especially for very large botnets. Notable examples include TDL-4 [22], Conficker [23], Strom [24], and MegaD [25]. To reduce the response latency in these architectures, [26] proposed a hybrid P2P structure.

Since the botnet management in all the above DDoS attack architectures is costly, they are only suited to well-resourced...
DDoS attackers. For DDoS attackers with limited resources, none of these architectures is applicable.

In the present paper, we propose a new DDoS attack architecture. Since there is no botnet management cost, this architecture is especially suited to DDoS attackers with limited resources. Consequently, we expect that the architecture will be used in most IoT-based DDoS attacks.

**B. DDOS ATTACK STRATEGY**

A DDoS attack strategy is a specification of the common attack traffic of all zombies at each time in the attack course. According to [27], [28], all the DDoS attack strategies can be classified into three categories: constant-rate, increasing-rate, and varying-rate. For a constant-rate attack strategy, all zombies deliver flooding packets to the target server at a constant rate. With regard to an increasing-rate attack strategy, the attack traffic is increasing over time until the bandwidth of the target server is used up. When it comes to a varying-rate attack strategy, the attack traffic varies over time according to a specified mode. For example, in a pulse DDoS attack, the attack traffic bursts periodically.

To our knowledge, all the existing DDoS attack strategies are constant-rate. Based on the assumption that there are only three-level attack rates (i.e., high, medium, and low), a number of optimal constant-rate DDoS attack strategies have been presented [29]–[32]. On the other hand, the effect of continuous attack rates on the attack benefit has been studied through game-theoretic approach [33]–[38].

In this paper, we study the optimal varying-rate attack strategy in the new DDoS attack architecture. First, we reduce the design of optimal attack strategy to a variational problem. Second, we solve the variational problem. Unexpectedly, the resulting attack strategy has a constant attack traffic.

**III. A NEW DDOS ATTACK ARCHITECTURE**

This section is devoted to developing a new DDoS attack architecture. First, we recall centralized DDoS attack architectures. Second, we review decentralized DDoS attack architectures. Finally, we present our DDoS attack architecture.

**A. CENTRALIZED DDOS ATTACK ARCHITECTURE**

A typical centralized DDoS attack architecture comprises four components: an attacker, a target server, a botnet, and a C&C system. See Figure 1. In the architecture, the attacker uses the C&C system to manage the botnet in a real-time manner. As a result, there is no communication between zombies.

The advantages of this architecture are obvious. First, the botnet is undetectable by observing communications between zombies. Second, the real-time management of the botnet enables the attacker to flexibly adjust his attack strategy. However, managing or renting a botnet is costly. What is worse, the cost is increasing very rapidly with the botnet size. Additionally, the robustness of the botnet is weak, because the failure of the C&C system would lead to the breakdown of the whole botnet.

**B. DECENTRALIZED DDOS ATTACK ARCHITECTURE**

In order to enhance the robustness of the botnet, a variety of decentralized DDoS attack architectures have been suggested. A typical decentralized DDoS attack architecture comprises three components: a DDoS attacker, a target server, and a botnet. See Figure 2. In the architecture, all the machines in the botnet constitute a peer-to-peer (P2P) communication network, and the attacker can indirectly manage the botnet by means of the P2P network. Specifically, a query or attack instruction is issued to a specific machine and is forwarded to all other machines through the P2P network.

Obviously, the botnet in this architecture is much more robust than that in a centralized DDoS attack architecture. However, the botnet in this architecture is easily detectable by analyzing the communication pattern of the P2P zombie network. Additionally, the botnet management is still costly,
TABLE 1. A comparison of the botnets in the three DDoS attack architectures.

| Architecture    | Centralized | Decentralized | New |
|-----------------|-------------|---------------|-----|
| Management cost | High        | High          | Null|
| Rental fee      | High        | High          | Null|
| Undetectability | Good        | Poor          | Good|
| Robustness      | Weak        | Strong        | Strong|
| Flexibility     | Good        | Good          | Poor|

and there is a non-negligible latency from the time an instruction is issued to the time the instruction takes effect.

C. THE NEW DDoS ATTACK ARCHITECTURE

A low-cost DDoS attack architecture should have the following properties simultaneously: low management cost, undetectability, and strong robustness. With this in mind, we present a new DDoS attack architecture as follows.

The new architecture comprises three components: a DDoS attacker, a target server, and a botnet. See Figure 3. In this architecture, the attacker gives up botnet management. Instead, he needs to write a bot malware with an attack module once and for all, in which a predetermined attack strategy is realized. See the subsequent two subsections for optimal design of attack strategy.

This architecture enjoys three remarkable advantages. First, the management cost is zero. Second, the undetectability is as good as a centralized DDoS attack architecture, because there is no communication between zombies. Thirdly, the robustness is as strong as a decentralized DDoS attack architecture, because there is no C&C system. Consequently, this architecture is suited to resource-limited DDoS attackers. For a comprehensive comparison of the botnets in these three DDoS attack architectures, see Table 1.

IV. THE OPTIMAL DDoS ATTACK STRATEGY

In the previous section, we proposed a new DDoS attack architecture. In this architecture, an attack strategy has to be specified prior to the attack. In this context, we face the following problem.

**DDoS attack strategy (DAS) problem:** In the new architecture, develop a DDoS attack strategy that achieves the best attack effect.

This section is devoted to the modeling of this problem. First, we characterize the expected growing process of the botnet. Second, we estimate the effect of an attack strategy. On this basis, we model the DAS problem as a variational problem.

A. THE GROWTH OF THE BOTNET

Consider a network of $N$ IoT devices labelled $v_1$ through $v_N$. Let $G = (V, E)$ denote the topological structure of the network, i.e., $V = \{v_1, \cdots, v_N\}, \{v_i, v_j\} \in E$ if and only if there is a communication link between the device $v_i$ and the device $v_j$. Let $A = (a_{ij})_{N \times N}$ denote the adjacency matrix of $G$, i.e., $a_{ij} = 1$ or 0 according as $\{v_i, v_j\} \in E$ or not.

Suppose a DDoS attacker intends to exploit the network to launch a DDoS attack on a target server in the time horizon $[0, T]$. To achieve the goal, he needs only to write a bot malware with a preloaded attack module and inject it into a small subset $U$ of devices. The malware will propagate automatically from device to device through the network, forming a growing botnet.

At any time $t \in [0, T]$, each device in the network is either uncompromised or compromised. Let $X_i(t) = 0$ and 1 denote that the device $v_i$ is uncompromised and compromised at time $t$, respectively. Then the botnet at time $t$ can be characterized by the vector

$$X(t) = (X_1(t), X_2(t), \ldots, X_N(t)).$$

Obviously, $X_i(0) = 1$ or 0 according as $v_i \in U$ or not.

Let $U_i(t)$ and $C_i(t)$ denote the probabilities of the device $v_i$ being uncompromised and compromised at time $t$, respectively.

$$U_i(t) = \Pr[X_i(t) = 0], \quad C_i(t) = \Pr[X_i(t) = 1].$$

Since $U_i(t) = 1 - C_i(t)$, the expected botnet at time $t$ can be characterized by the vector

$$C(t) = (C_1(t), \ldots, C_N(t))$$

Let

$$C^* = (C^*_1, \ldots, C^*_N),$$

where $C^*_i = 1$ or 0 according as $v_i \in U$ or not. Then $C(0) = C^*$ stands for the initial botnet.

Let $\beta$ denote the average rate at which the bot malware propagates from a compromised device to a neighboring uncompromised device. For an IoT, this propagation rate is very high. Inspired by malware propagation theory [39]–[42], we characterize the expected growth process of the botnet as follows.
The function $x$ the prespecified attack traffic of all zombies at time $t$. Let $x$ attack module preloaded in the malware. Let $x$ that is not blocked by the target server is $x$ is detailed discussion of the defense strategy. And observing the attack effect. See the next section for a defense strategy used by the defender of the target server at time $t$. Specifically, the impact is negligible if $x$ denote the communication bandwidth of the target server at time $t$. Denote this increasing function. On this basis, the expected impact of the DDoS attack strategy is estimated to be $A(t)$. Specifically, the impact is negligible if $A(t)$ relative to $B$. Specifically, the impact is negligible if $A(t)$ far less than $B$, is increasing rapidly when $A(t)$ approaches $B$, and is tremendous if $A(t)$ exceeds $B$. Let $f_B$ denote this increasing impact function. See Figure 4 for a diagram of the impact function. Based on the above discussions, we model the DAS problem as a variational problem as follows.

$$\max_{x \in X} I(x) = \int_0^T f_B \left( x(t) \left[ 1 - p(x(t)) \right] \sum_{i=1}^N C_i(t) \right) dt, \quad (10)$$

where $C_i(t)$ ($i = 1, \cdots, N, 0 \leq t \leq T$) are calculated by using the botnet growth model (5). We refer to this problem as the DAS model.

**V. SOLVING THE DAS MODEL**

In the previous section, we proposed the DAS problem and modeled the problem as a variational problem, i.e., the DAS model. In this section, we devote ourself to solving the DAS model.

Obviously, the DAS model (10) boils down to the following series of optimization problems:

$$\max_{0 \leq z \leq z_{max}} f_B \left( z \left[ 1 - p(z) \right] \sum_{i=1}^N C_i(t) \right), \quad t \in [0, T]. \quad (11)$$

Since $f_B$ is increasing and $\sum_{i=1}^N C_i(t) > 0$ for all $t \in [0, T]$, this series of optimization problems is reduced to the following optimization problem:

$$\max_{0 \leq z \leq z_{max}} g(z) = z \left[ 1 - p(z) \right]. \quad (12)$$

The optimal solution to the problem is dependent on the function $p$. In practice, this function stands for a defense strategy used by the defender of the target server. Next, we consider three different types of defense strategies.

**A. HARD-THRESHOLD TRAFFIC-BLOCKING STRATEGY**

First, consider the jump function

$$p(z) = \begin{cases} 0 & \text{if } 0 \leq z \leq \theta, \\ 1 & \text{if } z > \theta, \end{cases} \quad (13)$$

where $\theta > 0$. See Figure 5. This function stands for a hard-threshold traffic-blocking strategy in which the traffic of a device is blocked or not according as the traffic exceeds the threshold $\theta$ or not. In this setting, we have

$$g(z) = \begin{cases} z & \text{if } 0 \leq z \leq \theta, \\ 0 & \text{if } z > \theta. \end{cases} \quad (14)$$
Theorem 2: For the hard-threshold traffic-blocking strategy (13), the optimization problem (12) admits
\[ z^{opt} = \begin{cases} 
  x_{\max} & \text{if } x_{\max} \leq \theta, \\
  \theta & \text{if } x_{\max} > \theta,
\end{cases} \tag{15} \]
as the unique optimal solution.

Proof: We distinguish between two possibilities.

Case 1: \( x_{\max} \leq \theta \). It follows from Eq. (14) that the optimization problem (12) is equivalent to the optimization problem \( \max_{0 \leq z \leq \theta} z \), which admits \( x_{\max} \) as the unique optimal solution.

Case 2: \( x_{\max} > \theta \). It follows from Eq. (14) that the optimization problem (12) is equivalent to the optimization problem \( \max_{0 \leq z \leq \theta} z \), which admits \( \theta \) as the unique optimal solution.

Combining the above discussions, we get Eq. (15).

Example 1: Suppose all the devices in the IoT network under consideration have a common bandwidth of \( x_{\max} = 2 \) Mbps [44]. Suppose the defender of the target server uses the hard-threshold traffic-blocking strategy (13).

(a) Suppose \( \theta = 3 \) Mbps. Since \( x_{\max} \leq \theta \), it follows from Theorem 2 that the optimal attack strategy is \( z^{opt} = x_{\max} = 2 \) Mbps.

(b) Suppose \( \theta = 1 \) Mbps. Since \( x_{\max} > \theta \), it follows from Theorem 2 that the optimal attack strategy is \( z^{opt} = \theta = 1 \) Mbps.

B. SOFT-THRESHOLD TRAFFIC-BLOCKING STRATEGY

Consider the piecewise linear, continuous function
\[ p(z) = \begin{cases} 
  0 & \text{if } 0 \leq z \leq \theta - \tau_1, \\
  \frac{z - (\theta - \tau_1)}{\tau_1 + \tau_2} & \text{if } \theta - \tau_1 \leq z \leq \theta + \tau_2, \\
  1 & \text{if } z \geq \theta + \tau_2,
\end{cases} \tag{16} \]
where \( \theta > 0, 0 < \tau_1 < \theta, \tau_2 > 0 \). See Figure 6. This function stands for a soft-threshold traffic-blocking strategy in which the traffic of a device is blocked if the traffic exceeds \( \theta + \tau_2 \), is not blocked if the traffic does not exceed \( \theta - \tau_1 \), and is blocked with a probability that is increasing linearly from 0 to 1 if the traffic is between \( \theta - \tau_1 \) and \( \theta + \tau_2 \). In this setting, we have
\[ g(z) = \begin{cases} 
  z & \text{if } 0 \leq z \leq \theta - \tau_1, \\
  h(z) & \text{if } \theta - \tau_1 \leq z \leq \theta + \tau_2, \\
  0 & \text{if } z \geq \theta + \tau_2,
\end{cases} \tag{17} \]
where
\[ h(z) = \frac{1}{\tau_1 + \tau_2} z[(\theta + \tau_2) - z], \quad z \in (-\infty, \infty), \tag{18} \]
which stands for a downward parabola that is strictly increasing in the interval \( (-\infty, \frac{\theta + \tau_2}{2}) \) and strictly decreasing in the interval \( \left( \frac{\theta + \tau_2}{2}, \infty \right) \).

Theorem 3: For the soft-threshold traffic-blocking strategy (16), the optimization problem (12) admits
\[ z^{opt} = \begin{cases} 
  x_{\max} & \text{if } x_{\max} \leq \frac{\theta + \tau_2}{2}, \\
  \frac{\theta + \tau_2}{2} & \text{if } x_{\max} > \frac{\theta + \tau_2}{2} \geq \theta - \tau_1, \\
  \theta - \tau_1 & \text{if } x_{\max} > \theta - \tau_1 \geq \frac{\theta + \tau_2}{2},
\end{cases} \tag{19} \]
as the unique optimal solution.

Proof: We distinguish among three possibilities.

Case 1: \( x_{\max} \leq \theta - \tau_1 \). It follows from Eq. (17) that the optimization problem (12) is equivalent to the optimization problem \( \max_{0 \leq z \leq \theta - \tau_1} h(z) \), which admits \( x_{\max} \) as the unique optimal solution.

Case 2: \( \theta - \tau_1 < x_{\max} \leq \theta + \tau_2 \). Since the optimization problem \( \max_{0 \leq z \leq \theta - \tau_1} z \) admits \( z_1 = \theta - \tau_1 \) as the unique optimal solution, it follows from Eq. (17) that the optimization problem (12) is equivalent to the optimization problem
\[ \max_{\theta - \tau_1 \leq z \leq x_{\max}} h(z). \tag{20} \]
We proceed by treating three subcases, respectively.

Subcase 2.1: \( x_{\max} \leq \theta - \tau_1 \). Then the optimization problem (20) admits \( z_2 = x_{\max} \) as the unique optimal solution. Since
\[ g(z_2) = h(z_2) > h(z_1) = g(z_1), \tag{21} \]
the optimization problem (12) admits \( z_2 = x_{\max} \) as the unique optimal solution.

Subcase 2.2: \( x_{\max} > \frac{\theta + \tau_2}{2} \geq \theta - \tau_1 \). Then the optimization problem (20) admits \( z_2 = \frac{\theta + \tau_2}{2} \) as the unique optimal solution. Since
\[ g(z_2) = h(z_2) > h(z_1) = g(z_1), \tag{22} \]
the optimization problem (12) admits \( z_2 = \frac{\theta + \tau_2}{2} \) as the unique optimal solution.

Subcase 2.3: \( \theta - \tau_1 > x_{\max} > \frac{\theta + \tau_2}{2} \). Then the optimization problem (20) admits \( z_2 = \theta - \tau_1 \) as the unique
optimal solution. Hence, the optimization problem (12) admits \( z_2 = \theta - t_1 \) as the unique optimal solution.

Case 3: \( x_{\text{max}} > \theta + t_2 \). Since the optimization problem
\[
\max_{0 \leq z \leq \theta - t_1} h(z) = \frac{\theta + t_1}{2} \text{ as the unique optimal solution. Since } g(z_2) = h(z_2) \geq h(z_1) = g(z_1),
\]
the optimization problem (12) admits \( z_2 = \frac{\theta + t_2}{2} \) as the unique optimal solution.

Subcase 3.1: \( \frac{\theta + t_2}{2} \geq \theta - t_1 \). Then the optimization problem
\[
\max_{0 \leq z \leq \theta - t_1} h(z) = \frac{\theta + t_1}{2} \text{ as the unique optimal solution.
\]
So, the optimization problem (12) admits \( z_2 = \theta - t_1 \) as the unique optimal solution.

By combining the above discussions, we get Eq. (19).

Example 2: Suppose all the devices in the IoT network under consideration have a common bandwidth of \( x_{\text{max}} = 2 \) Mbps [44]. Suppose the defender of the target server used the soft-threshold traffic-blocking strategy (16).

(a) Suppose \( \theta = 4 \) Mbps, \( t_1 = 2 \) Mbps, and \( t_2 = 1 \) Mbps. Since \( x_{\text{max}} = \frac{\theta + t_2}{2} \), it follows from Theorem 3 that the optimal attack strategy is \( z^{\text{opt}} = x_{\text{max}} = 2 \) Mbps.

(b) Suppose \( \theta = 3 \) Mbps, \( t_1 = 2 \) Mbps, and \( t_2 = 0.5 \) Mbps. Since \( x_{\text{max}} > \frac{\theta + t_2}{2} \), it follows from Theorem 3 that the optimal attack strategy is \( z^{\text{opt}} = \theta - t_1 = 1.75 \) Mbps.

(c) Suppose \( \theta = 2 \) Mbps, \( t_1 = 0.5 \) Mbps, and \( t_2 = 1 \) Mbps. Since \( x_{\text{max}} > \theta - t_1 \), it follows from Theorem 3 that the optimal attack strategy is \( z^{\text{opt}} = \theta - t_1 = 1.5 \) Mbps.

C. SMOOTH TRAFFIC-BLOCKING STRATEGY

Assume the function \( p \) is strictly increasing and differential. In this setting, the function \( g \) defined by Eq. (12) is unimodal, i.e., it is first increasing then decreasing. See Figure 7.

Theorem 4: The optimization problem (12) admits the unique root of the equation
\[
p(z) + zp'(z) = 1
\]
as the unique optimal solution.

Proof: Since \( g \) is unimodal, it attains the maximum at the unique root of the equation
\[
g'(z) = 1 - p(z) - zp'(z) = 0.
\]

The claim follows.

Example 3: Suppose all the devices in the IoT under consideration have a common bandwidth of \( x_{\text{max}} = 2 \) Mbps [44]. Suppose the defender of the target server used a smooth traffic-blocking strategy. Suppose
\[
p(z) = \frac{1}{1 + e^{-20(z-1)}}.
\]
Since Eq. (25) admits \( z^* = 0.8608 \) as the unique root, it follows from Theorem 4 that the optimal DDoS attack strategy is \( z^{\text{opt}} = z^* = 0.8608 \) Mbps.

VI. CONCLUSIONS

In this paper, a DDoS attack architecture that is suited to resource-limited IoT-based DDoS attackers. In this architecture, the optimal design of attack strategy is modeled as a variational problem, which is resolved for three types of DDoS defense strategies. This work helps us to understand IoT-based DDoS attacks.

In the new architecture, the optimal design of DDoS defense strategy is challenging, because the effect of a defense strategy is dependent on the attack strategy used by the attacker, which is unknown to the defender. According to our experience, the problem might be studied in the framework of game theory [45]–[49]. Additionally, it is worthwhile to inspect conventional DDoS defense techniques and frameworks [50]–[53] in the proposed architecture.

ACKNOWLEDGMENT

The authors are grateful to the three anonymous reviewers and the editor for their valuable suggestions that have greatly improved the quality of this paper.

REFERENCES

[1] D. K. Bhattacharyya and J. K. Kalita, DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. London, U.K.: Chapman & Hall, 2016.

[2] K. L. Lueth, State of the IoT 2018: Number of IoT devices now at 7B - Market accelerating IoT Analytics, Accessed: Aug. 2018. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-2018-number-of-iot-devices-now-7b/

[3] E. Bertino and N. Islam, “Botnets and Internet of Things security,” Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[4] F. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, “Understanding the mirai botnet,” in Proc. 26th Usenix Secur. Symp., 2017, pp. 1093–1110.

[5] M. E. Ahmed and H. Kim, “DDoS attack mitigation in Internet of Things using software defined networking,” in Proc. IEEE 3rd Int. Conf. Big Data Comput. Service Appl., Apr. 2017, pp. 271–276.

[6] H. Mustapha and A. M. Alghamdi, “DDoS attacks on the Internet of Things and their prevention methods,” in Proc. 2nd Int. Conf. Future Netw. Distrib. Syst. (ICFNDS), 2018, pp. 1–5.

[7] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, “Botnets: A survey,” Comput. Netw., vol. 57, no. 2, pp. 378–403, Feb. 2013.

[8] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, “Botnet in DDoS attacks: Trends and challenges,” IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2242–2270, Jul. 2015.
LU-XING YANG (Member, IEEE) received the B.Sc. degree from the School of Mathematics and Statistics, Chongqing University, in 2012, and the Ph.D. degree from the College of Computer Science, Chongqing University, in 2015. He visited Imperial College London, from 2014 to 2015. From 2016 to 2017, he was a Postdoctoral Research Fellow with the Delft University of Technology. From 2018 to 2019, he was an Alfred Postdoctoral Research Fellow with Deakin University, Australia, where he is currently a Lecturer in cybersecurity with the School of Information Technology. He has published more than 50 academic articles in peer-reviewed international journals. His research interests include epidemic dynamics and cybersecurity.

XIAOFAN YANG (Member, IEEE) received the B.Sc. degree from the Department of Mathematics, Sichuan University, in 1985, the M.Sc. degree from the Department of Applied Mathematics, Chongqing University, in 1988, and the Ph.D. degree from the Department of Computer Science, Chongqing University, in 1994. From 1998 to 1999, he visited the University of Reading. He is currently a Professor of computer science with Chongqing University. He has published more than 160 academic articles in peer-reviewed international journals and more than 20 students received the Ph.D. degree under his supervision. His research interests include fault-tolerant computing, epidemic dynamics, and cybersecurity.

YONG XIANG (Senior Member, IEEE) received the Ph.D. degree in electrical and electronic engineering from The University of Melbourne, Australia. He is currently a Professor with the School of Information Technology, Deakin University, Australia. He has published five monographs, over 130 refereed journal articles, and numerous conference papers in these areas. His research interests include information security and privacy, signal and image processing, data analytics and machine intelligence, the Internet of Things, and blockchain. He is a Senior Area Editor of the IEEE Signal Processing Letters and an Associate Editor of IEEE Access. He served as the Honorary Chair, the Program Chair, a TPC Chair, the Symposium Chair, and the Track Chair for a number of international conferences.

YUAN YAN TANG (Life Fellow, IEEE) is currently a Chair Professor with the Faculty of Science and Technology, University of Macau, and a Professor/Adjunct Professor/Honorary Professor with several institutes, including Chongqing University, Concordia University, and Hong Kong Baptist University. He has published over 400 academic articles. He has authored/coauthored over 25 monographs/books/book chapters. His current research interests include wavelets, pattern recognition, image processing, and cybersecurity. He is a Fellow of IAPR. He is the Founder and the Chair of Pattern Recognition Committee in the IEEE SMC. He is the Founder and the Editor-in-Chief of the International Journal on Wavelets, Multiresolution, and Information Processing and an Associate Editor of several international journals.