Analysis of the Impact of Denial of Service Attacks on Centralized Control in Smart Cities

Evariste Logota, Georgios Mantas, Jonathan Rodriguez and Hugo Marques

Instituto de Telecomunicações, Aveiro, Portugal
{logota,gimantas,jonathan,hugo.marques}@av.it.pt

Abstract. The increasing threat of Denial of Service (DoS) attacks targeting Smart City systems impose unprecedented challenges in terms of service availability, especially against centralized control platforms due to their single point of failure issue. The European ARTEMIS co-funded project ACCUS (Adaptive Cooperative Control in Urban (sub)Systems) is focused on a centralized Integration and Coordination Platform (ICP) for urban subsystems to enable real-time collaborative applications across them and optimize their combined performance in Smart Cities. Hence, any outage of the ACCUS ICP, due to DoS attacks, can severely affect not only the interconnected subsystems but also the citizens. Consequently, it is of utmost importance for ACCUS ICP to be protected with the appropriate defense mechanisms against these attacks. Towards this direction, the measurement of the performance degradation of the attacked ICP server can be used for the selection of the most appropriate defense mechanisms. However, the suitable metrics are required to be defined. Therefore, this paper models and analyzes the impact of DoS attacks on the queue management temporal performance of the ACCUS ICP server in terms of system delay by using queueing theory.

Keywords: Smart City Security, Denial of Service Attacks, Security Modeling, Queueing Theory.

1 Introduction

Denial of Service (DoS) attacks are one of the oldest and most serious threats on the Internet. The main objective of DoS attacks is to prevent legitimate access to services of a target machine by overwhelming its resources (e.g., CPU, memory, network bandwidth). Essentially, DoS attacks are a type of attacks against availability of the targeted machine, which is an important security property for modern Internet-based systems. There are two main categories of DoS attacks: network layer DoS attacks and application layer DoS attacks [1], [2]. Network layer DoS attacks are carried out at the network layer and they attempt to overwhelm the network resources of the targeted victim with bandwidth-consuming assaults such as TCP SYN, ICMP or UDP flooding attacks. On the other hand, application layer DoS attacks are more sophisticated attacks that exploit specific characteristics and vulnerabilities of application layer protocols (e.g., HTTP, DNS, VoIP or SMTP) and applications running on the victim system in order to deplete its resources [1].

Specifically in the case of Smart Cities, the effect of both categories of DoS attacks on any platform providing centralized control in these environments can be catastrophic since any unavailability of the platform (single point of failure) would plunge the cities into chaos. For example, the ongoing European research project ACCUS (Adaptive Cooperative Control in Urban (sub) Systems) [3] aims to provide a centralized Integration and Coordination Platform (ICP) for urban systems to leverage real-time collaborative applications across them. Furthermore, ACCUS is defining an adaptive and cooperative control architecture and the corresponding algorithms for urban subsystems in order to optimize their combined performance in Smart Cities. Thus, it becomes clear that DoS attacks on the ACCUS ICP server can jeopardize the safety and well-being of the ACCUS citizens. Additionally, there are huge incentives for cyber-criminals to launch DoS attacks against Smart Cities, like ACCUS City, ranging from financial gain to cyberwarfare.

Taking into consideration all the above mentioned, it is of utmost importance for ACCUS ICP to be protected with the appropriate defense mechanisms against these types of attacks in order to provide reliable and secure services to citizens. Towards this direction, the study and analysis of the impact of DoS attacks on the performance of the ICP server can play a critical role. Due to the fact that the impact of DoS attacks on the victim's performance is a key characteristic of them, the measurement of the performance degradation of the ACCUS ICP server imposed by these attacks can be used by the ACCUS ICP city planners to evaluate existing defense mechanisms. Then, it will enable them to select the most appropriate ones. However, the appropriate metrics are required to be defined firstly. Therefore, in this paper, as an initial step towards the definition of the appropriate metrics, we model and analyze the impact of DoS attacks on the queue management temporal performance within the ACCUS ICP server in terms of system delay by using queueing theory.

The rest of this paper is organized as follows. Section 2 demonstrates a scenario of ACCUS ICP server under a DoS attack. In Section 3, the model for analyzing the impact of DoS attacks on the ACCUS ICP server is presented. In Section 4 the performance evaluation takes place in order to assess the impact of DoS attacks on the ACCUS ICP server. Finally, Section 5 concludes the paper.

2 DoS Attack Threat against ACCUS Smart City

The ACCUS ICP targets at interconnecting many communicating entities geographically distributed over a heterogeneous communication network and handling different types of data derived from many different sources. These entities include urban subsystems (e.g., traffic and energy subsystems) and end-users' devices (e.g., smartphones) supporting appropriate applications in the ACCUS Smart City, as in Fig. 1. As everything is interconnected through the ICP, any damage of it, due to DoS attacks, can severely affect not only the subsystems but also the end-users.

Especially, the level of their severity can grow dramatically as attackers take advantage of the botnet technology. A botnet is a network of compromised machines (e.g., legitimate PCs, laptops), commonly referred to as bots, which are under the control of an attacker through central Command & Control (C&C) servers.

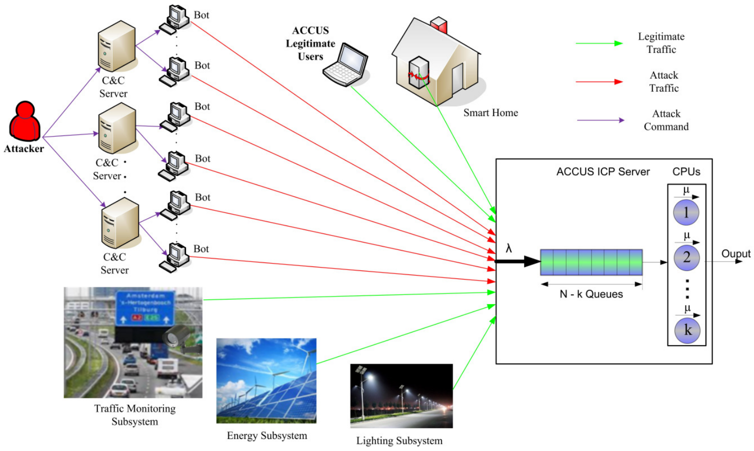

Fig. 1. ACCUS ICP server under DDoS Attack.

Hence, the attacker is able to access and manage the botnet remotely via the central C&C servers. A depiction of a typical botnet architecture is included in Fig. 1. Botnets usually consist of several thousand bots and enable the attacker to launch Distributed Denial of Service (DDoS) attacks causing serious performance degradation on the victim's side (e.g., web server). DDoS attacks are a variation of the typical DoS attacks, where a single attacking host targets a single victim. Particularly, in contrast to DoS attacks, DDoS attacks deploy multiple attacking entities (e.g., bots), often located in disparate locations, in order to achieve their goal. The multiple attacking entities and the fact that they can be located in different locations are two factors that make the detection and mitigation of these attacks more challenging. Besides, it is worthwhile to mention that the legitimate user of a bot has no knowledge that his/her machine has been compromised and is taking part in a DDoS attack [4], [5]. It turns out that the ACCUS ICP server's protection is of paramount importance to guarantee reliability and security for ACCUS users.

Due to the fact that the impact of DoS attacks on the victim's performance is a key characteristic of them, it can be used as a feature for evaluation and accurate selection of existing defense mechanisms by the ACCUS ICP city planners. In this sense, the following section provides our analysis of the impact of this threat on the ACCUS ICP server.

3 A Model for Analyzing DoS Attack Impact on ACCUS ICP

The main objective of this section is to provide a model for analyzing the impact of DoS attacks on the queue management temporal performance of the ACCUS ICP server in terms of the system response time. To facilitate the understanding of the description of this work, we use queueing theory and emulate the ACCUS ICP server depicted in Fig. 1. For simplicity, we assume that the ACCUS ICP server is made up of k Central Processing Units (CPUs), a corresponding queue of size Q, and the Input/Output interfaces. This means that the ACCUS ICP server can accommodate a total number of $N = Q + k$ queries, where k, N and Q are integers. In addition, λ_i denotes a Poisson process-based request arrival rate for an incoming traffic i, which may originate from ACCUS subsystems (e.g., traffic monitoring subsystem), legitimate users (e.g. Smart Home) and a botnet commanded by an attacker (see Fig. 1). Hence, the sum of λ_i, denoted λ (see Fig. 1), is also a Poisson process. Besides, we assume that each CPU has the same service rate μ.

Basically, in this ACCUS ICP server model, a request arriving at the system is submitted to a CPU for processing. In case all the CPUs are busy, the request is placed in the queue and waits for its turn to be processed. When a higher priority request arrives in the ICP server, then a lower priority request currently getting service is pre-empted and the higher priority request gets service from the CPU. In the same way, an incoming lower priority request waits in the queue for service. Such birth-death processes of the ACCUS ICP server's operations described herein above can be studied by using the M/M/k/N queueing model [6]. Hence, let P_n be the probability that exactly n requests are in the ACCUS ICP server. Thus, as described in [7], we express the steady-state distribution of requests into the ICP server as:

$$P_n = \left\{ \begin{array}{lll} \dfrac{\lambda^n}{n! \times \mu^n} \times P_0 & , & for \quad 0 \le n \le k \\ \dfrac{\lambda^n}{k^{n-k} \times \mu^n \times k!} \times P_0 & , & for \quad k < n \le N \end{array} \right\} . \qquad \textbf{(1)}$$

To obtain the mean response time denoted $E[D]$, we first deduce the mean queue length denoted $E[Q]$ by using the equation (1) and the work in [7] as follows:

$$E[Q] = \sum_{n=k+1}^{N} (n-k) \times P_n = \sum_{n=k+1}^{N} (n-k) \times \frac{\lambda^n}{k^{n-k} \times \mu^n \times k!} \times P_0 = \frac{P_0 A^k \rho}{k!} \sum_{i=1}^{N-k} i \rho^{i-1} \ . \qquad \textbf{(2)}$$

where, $A = \dfrac{\lambda}{\mu}$ and $\rho = \dfrac{A}{k}$.

In addition, let's simplify the equation (2) further by considering the two cases of $\rho = 1$ and $\rho \neq 1$ as follows:

$$\sum_{i=1}^{N-k} i \rho^{i-1} = \left\{ \begin{array}{ll} 1 + 2 + \ldots + N - k = \dfrac{(1+N-k)(N-k)}{2} & , \quad for\, \rho = 1 \\ \dfrac{d}{d\rho}\left(\displaystyle\sum_{i=0}^{N-k} \rho^i \right) = \dfrac{d}{d\rho}\left(\dfrac{1-\rho^{N-k+1}}{1-\rho} \right) & , \quad for\, \rho \neq 1 \end{array} \right. . \qquad \textbf{(3)}$$

From the equations (2) and (3), we have:

$$E[Q] = \left\{ \begin{array}{ll} \dfrac{P_0 A^k \rho (1+N-k)(N-k)}{2k!} & , \quad for\, \rho = 1 \\ \dfrac{P_0 A^k \rho \left[1 - \rho^{N-k+1} - (1-\rho)(N-k+1)\rho^{N-k} \right]}{k!(1-\rho)^2} & , \quad for\, \rho \neq 1 \end{array} \right. . \qquad \textbf{(4)}$$

By applying the equation (4) to Little's formula, we obtain the mean response time *E[D]* imposed by the ICP server on incoming requests as:

$$E\left[D\right]=\frac{E\left[Q\right]}{\lambda}=\begin{cases}\dfrac{P_0A^k\rho\left(1+N-k\right)\left(N-k\right)}{2\lambda k!} & , \quad for\,\rho=1\\ \dfrac{P_0A^k\rho\left[1-\rho^{N-k+1}-\left(1-\rho\right)\left(N-k+1\right)\rho^{N-k}\right]}{\lambda k!\left(1-\rho\right)^2} & , \quad for\,\rho\neq 1\end{cases} \qquad \textbf{(5)}$$

.

4 Performance Evaluation

In order to assess the impact of DoS attacks on the ACCUS ICP server we implemented the ICP model described earlier in this work (M/M/k/N model) in Matlab by configuring each CPU service rate μ = 30 requests/(time unit) and the ICP server's queue size Q = 400 requests. We simulated a DoS attack scenario (i.e., Distributed DoS attack) by increasing the overall request arrival rate, λ, from light traffic load perspective until the ICP is completely overloaded. The overloading occurs when $\lambda = \mu * k$. In addition, we run the simulation for different number of CPUs (for k = 2, 3 and 4) so as to evaluate how increasing the processing capacity of the ICP server could alleviate the impact of DDoS attacks on the ACCUS service delivery performance. In this way, we are able to study the degradation of the ACCUS queue management temporal performance under DoS attacks.
Thus, Fig. 2(a) shows that the mean response time increases with the increase of the request arrival rate, as we expected. Also, one can observe in Fig. 2(a) that, the response time improves with the increase of the number of CPUs in the ACCUS ICP. However, Fig. 2(b) warns that the queue utilization increases rapidly and reaches full utilization of 100%, regardless of the number of CPUs running in the ACCUS ICP server. This effectively demonstrates the negative impact that DoS attacks can impose on the ICP server even if one can keep increasing its capacity in an attempt to improve its performance.

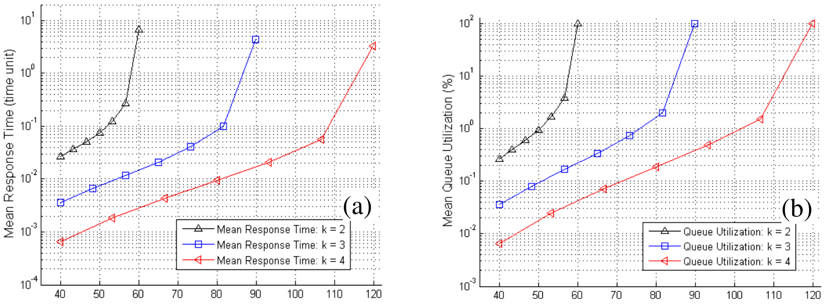

Fig. 2 . Mean Response Time (a) and Mean Queue Utilization (b).

5 Conclusion and Future Work

In this paper, we have focused our attention on the measurement of the performance degradation of the ACCUS ICP server imposed by DoS attacks, since it can be used by the ACCUS ICP city planners to evaluate existing defense mechanisms and select the most appropriate ones. Therefore, we modeled and analyzed the impact of DoS attacks on the queue management temporal performance of the ACCUS ICP server in terms of system delay by using queueing theory. As a result of this work, the mean response time and the mean queue utilization can be used as metrics for measuring the negative impact that DoS attacks can impose on the ACCUS ICP server's performance.

As future work, we plan to evaluate further, through a series of experiments, the mean response time and the mean queue utilization as metrics for accurate measurement of the performance degradation of the ACCUS ICP server due to DoS attacks. We also plan to use these metrics as parameters for the evaluation of existing defense mechanisms against DoS attacks.

Acknowledgments. The research leading to these results has received funding from the ARTEMIS Joint Undertaking Project ACCUS (ACCUS–ARTEMIS-005-2012/GA number 333020).

References

1. McGregory, S.: Preparing for the next DDoS attack. Network Security. 2013, 5, 5--6 (2013)
2. Zargar, S.T., Joshi, J., Tipper, D.: A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials. 15, 4, 2046--2069 (2013).
3. ACCUS (Adaptive Cooperative Control in Urban (sub) Systems), http://projectaccus.eu
4. Freiling, F., Holz, T., Wicherski, G.: Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-service Attacks. In: 10th European Symposium on Research in Computer Security, pp. 319—335. Milan, Italy (2005)
5. Specht, S.M., Lee, R. B.: Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures. In: 17th International Conference on Parallel and Distributed Computing Systems, pp. 543-550. San Francisco, California, USA (2004)
6. Zukerman, M.: Introduction to Queueing Theory and Stochastic Teletraffic Models. (2014). [Online]. Available: http://arxiv.org/pdf/1307.2968.pdf
7. Sztrik, J.: Basic Queueing Theory. (2012). [Online]. Available: http://irh.inf.unideb.hu/~jsztrik/education/16/SOR_Main_Angol.pdf