Game based DDoS Attack Strategies in Cloud of Things

Yichuan Wang[1, a], Yefei Zhang[1,b] ,Liumei Zhang[2,c],
Lei Zhu[1,d] and Yanxiao Liu[1,e]

[1]Faculty of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[2]School of Computer Science, Xi'an Shiyou University, Xi'an, 710065, China
[a]ctechsky@xaut.edu.cn, [b]xiaxuena1@163.com, [c]zhangliumei@xsyu.edu.cn,
[d]leizhu@xaut.edu.cn, [e] yanxiao_liu@hotmail.com

Keywords: Cloud of Things, Network Security, DDoS Attack, Smart Gateway.

Abstract. Integration of Internet of Things (IoT) with Cloud Computing, termed as Cloud of Things (CoT). In typical CoT infrastructure, the data collected from wireless sensor networks and IoTs will be transmitted through smart gateway (SG) to cloud. The bandwidth between IoT access point and SG becomes a bottleneck for information transmission. In this paper, we propose a novel game-theory model to describe the CoT attacker, who expects to use minimum set of IoT attack devices to occupy as much bandwidth resources as possible in a given time. By analyzing the model, we have found that the game model is a non-cooperative and repeated games of incomplete information. The best strategy for the attacker is that if over the half of attack connections are effective, decreasing number of attack nodes; contrary, increasing number of attack nodes. The simulation result shows that our strategy can decrease the number of exposed attack devices for the Distributed Denial of Service(DDoS) attack significantly.

Introduction

The core idea of Internet of Things(IoT) is A worldwide network of interconnected entities[1]. Cloud computing is a model for enabling ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources. Cloud computing can provide significant convenience to its customers, and improvement in performance via resources sharing[2].

Cloud can even benefit from Internet of Things(IoT) that it can extend its limits with real world things in more dynamic and distributed manner, and deliver massive number of services in real time. Cloud will act as intermediate layer between the applications and the things conceal all the functionalities and complexities required for processing later[3]. The framework affects future application development, where information gathering process and transmission will deliver new challenges to be addressed in a multi-Cloud environment[4]. The following are the advantages gained in adopting the Cloud IoT paradigm, termed as Cloud of Things(CoT) [3][5][6].

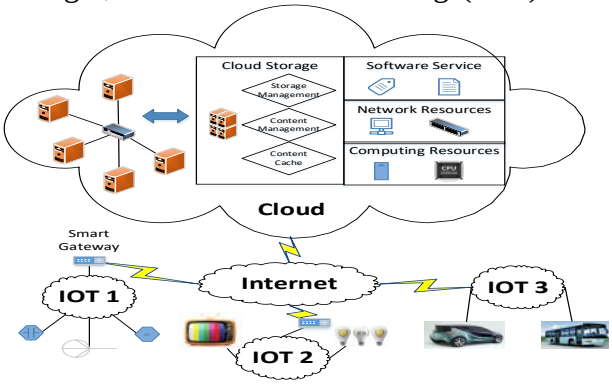

Fig. 1. Cloud of Things

Fig. 1 presents an overall communication pattern of CoT. It helps manage IoT resources and provide more cost effective and efficient means to produce services.

Smart gateway(SG) would help in better utilization of network and cloud resources. The data collected from wireless sensor networks and IoTs will be transmitted through gateways to cloud. The received data is then stored in the cloud and from there, it is provided as a service to the users. There is a possibility that the data gathered from IoT is transmitted directly to the Smart Gateway, or multiple IoTs are connected with base station(s), which in turn transmits the data to the smart gateway. The bandwidth between IoT access point and SG becomes a bottleneck for information transmission.

In this paper, we propose a novel game-theory model to describe the CoT attacker strategies. By analyzing the model, we have found that the game model is a non-cooperative and repeated games of incomplete information. The simulation result shows that our strategy can decrease the number of exposed attack devices for the DDoS attack significantly.

Game Model and Analysis

An DDoS attack towards the smart gateway is regarded as effective if the adversary can consume the network resources between AP and SG so sharply and massly. We present our game models for CoT DDoS attacks and their possible countermeasures. We consider the interaction between DDoS attacking devices master (AM) and defense mechanism (DM) in smart gateway as a two-player game. It is a non-cooperative game of incomplete information.

The DM knows the network connection numbers and loads. It can determine whether stay connected or disconnect the link depends on the suspicious value for each connection α using IDS. Such strategy according to a threshold value which represented by β and Neyman-Pearson criterion for hypothesis testing.

When $\alpha > \beta$, the DM consider the device in IOT as an attacker and disconnect the link from it to free bandwidth resources. The DM tries to avoid the bandwidth overload, then avoid disconnect the legal things links. It then need to improve the attacking recognition rate γ. This degree is only a theoretical value that DM is able to improve it. Then the DM to evaluate such value from the known attacks. Thus the DM attempts to find out an optimal strategy for the threshold value β of disconnection request to improve the detection rate and cuts false alarm rate of current knowledge base.

The AM knows all attack nodes status, which includes the total number of attack nodes and link numbers, network infrastructure and whether the attack link has been disconnected. He is able to gather information via varies ways(e.g. network detection). Such information includes the bandwidth resources consumption of normal and attack nodes as well as the current load. The AM is able to prepare an attack strategy such as how many attack nodes are needed at one time and the attack mode (represented by function N_A). He needs to avoid the DM to detect all attack nodes which represented by N_B, since for each attraction N_B is a constant. The strategy must ensures an efficient DDOS attack and hide attack nodes proportion of the AM to the highest degree in the meantime.

The AM is unsure with if the DM been equipped sandbox or honeypot for series detection and measurement toward himself. The decision criteria of the AM is dedicated by the probability of denied attack of each attack nodes. Assuming N_A is the current total active attack nodes that retain connected with the smart gateway. N_T represents the total active attack nodes in time T. It is a non-decreasing function related to time t and has a minimum value 0, maximum value N_B denotes the total attack nodes. While, the function itself is depend on the strategy that AM decided. $\frac{N_A}{N_T}$ depicts the ratio of the DM that forwarding attack flows from attack nodes. We use $1-\frac{N_A}{N_T}$ to denote the denying probability of next attack.

The AM can apply strategies, launching attack or hide among all attack nodes. Obviously, the attack nodes, which already attacked, and its connections shall be considered as exposure regardless of whether AM continues the attack strategy. Meanwhile, we assume that the AM decides whether to

start an attack flow based on the current time t if it bigger than T. Where \$ T \$ is the actual time of current launching attack nodes for starting attack. That is to say, if $t > T$ then the attack link starts, if $t \le T$ then hide and not to start attacks.

Then for each connection of every attack nodes, we get the strategies distribution for the AM, which is shown in Table 1.

Table 1. Strategies Distribution of the AM

Judge\ Strategies	Attack	Hide	Probability
Detected	P_{DA}	P_{DH}	$1-N_A/N_T$
Not Detected	P_{NA}	P_{NH}	N_A/N_T
Probability	$P\{t>T\}$	$P\{t\le T\}$	

Because variables N_A and T are independent of each other, we assume the joint distribution is independent. Thus, we get

$$\begin{cases} P_{DA} = P\{t>T\}(1-N_A/N_T) \\ P_{DH} = P\{t\le T\}N_A/N_T \\ P_{NA} = P\{t>T\}(1-N_A/N_T) \\ P_{NH} = P\{t\le T\}N_A/N_T \end{cases}$$

We get the strategies expectation of AM for connection i,

$$E_A^i = P_{DA}^i W_{DA} + P_{DH}^i W_{DH} + P_{NA}^i W_{NA} + P_{NH}^i W_{NH}$$

The utility function of AM is $U_A = \frac{N_T}{N_B}W_E + (1-\frac{N_T}{N_B})W_A\sum_{i=1}^{N_A}E_A^i + \frac{N_C}{N_R}W_S, (N_T \le N_B)$

W_E denotes the weight of costs if AM expose all attack nodes. W_A denotes the weight if AM is not exposure. W_S denotes the income if AM finish the DDoS attack to crash the smart gateway successfully.

For the AM, we consider the scenario $W_{DA} = W_{NH} = -1$ and $W_{DH} = W_{NA} = 1$. We find that the best strategy for AM is hiding the some attack nodes to avoid from detection and counterattack, if over the half of attack connections are effective, that is $\varepsilon = N_A/N_T > 1/2$. Contrary, if AM has less than half of attack connections are effective, that is $\varepsilon = N_A/N_T \le 1/2$, the best strategy is to increase the number of current launching attack nodes.

Simulation

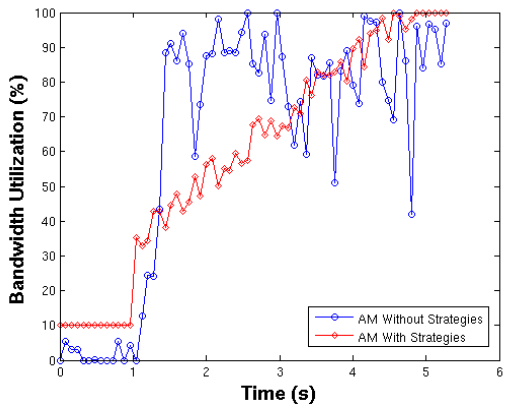

Fig. 2. Bandwidth Utilization under Attack

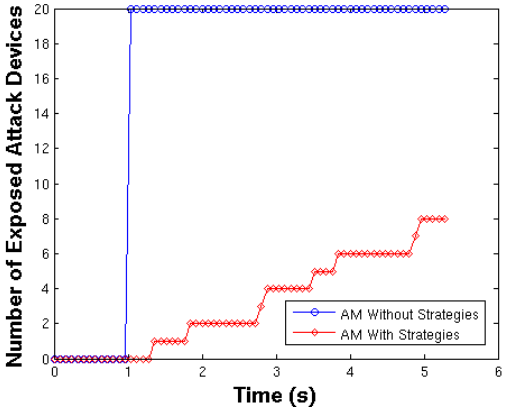

Fig. 3. Number of Exposed Attack Devices

We use NS-3 network simulation tool as the platform to validate our model. There are some normal IoT nodes and attack IoT nodes in the AP radio coverage. The data collected from wireless sensor networks and IoTs will be transmitted through SG to cloud. The simulation configurations are:

NS-3 Version: V 3.25; Server CPU: INTEL XEON X5650 12M Cache, 2.66 GHz, 6.40 GT/s; Server OS: Fedora 21 Linux System; Bandwidth: 10Mbps IoT node to AP, 100Mbps AP to SG; Delay: 2ms IoT Nodes to AP, 1ms AP to SG; Wifi Channel Model: YANS; Traffic Type: TCP Socket; Port: 8080; Interarrival Time(ms): Normal ~ uniform[15,45], Attack ~ uniform[0,40]; IoT Nodes Number: Normal: 30, Attack: 20; Access Start Time: Normal: 0th second, Attack: 1th second; Simulation End Time: 5.5th second.

Fig. 2 shows the comparison between the two cases: (i) AM launch DDoS attack without adopt our strategies; (ii) AM launch DDoS attack with adopt our strategies. The X-axis is the time of simulation, and the Y-axis is the bandwidth utilization rate of the line between AP and SG. We can see that in two cases, the bandwidth utilization increasing sharply. Fig. 3 shows that the number of exposed attack devices comparison. It is clear that if the AM adopt our strategies, the number of exposed is much less than not adopt, and the DDoS attack still successful.

Conclusion

In this paper, we propose a novel game-theory model to describe the CoT attacker, who expects to use minimum set of IoT attack devices to occupy as much bandwidth resources as possible in a given time. By analyzing the model, we have found that the game model is a non-cooperative and repeated games of incomplete information. The simulation result shows that our strategy can decrease the number of exposed attack devices for the DDoS attack significantly.

Acknowledgements

This work is supported by Ph.D. Research Startup Funds of Xi'an University of Technology (112-256081504), College Research Funds of Xi'an University of Technology (112-451016007).

References

[1] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer Networks. 57(10). p.2266-79. (2013)

[2] Wang Y, Chandrasekhar S, Singhal M, Ma J. A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing. Cluster Computing. 19(2):p. 647-62. (2016)

[3] Botta A, De Donato W, Persico V, Pescapé A. On the integration of cloud computing and internet of things. InFuture Internet of Things and Cloud (FiCloud), 2014 International Conference. IEEE. p. 23-30. (2014)

[4] Aguzzi S, Bradshaw D, Canning M, Cansfield M, Carter P, Cattaneo G, Gusmeroli S, Micheletti G, Rotondi D, Stevens R. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. European Commission, Directorate-General of Communications Networks, Content & Technology, Brussels, Belgium, Rep. SMART. p.37. (2014).

[5] Aazam M, Khan I, Alsaffar AA, Huh EN. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. InProceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, IEEE. p. 414-419. (2014)

[6] Aazam M, Hung PP, Huh EN. Smart gateway based communication for cloud of things. InIntelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference IEEE . p. 1-6. (2014)