Honeypot Game Strategy for Distributed Denial of Service in Advanced Metering Infrastructure

[1]Priyanka B, [2]Alaguroja R, [3] R.Kalpana, [4] Kapila Vani R.K.
[2]Student, [2]Student, [3]Assistant Professor, [4]Assistant Professor
[1]Department of Computer Science and Engineering,
[1]Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India

Abstract : Attacks remains major issue, the alleviation is hard especially in highly distributed systems. Since the size of the Network overload increases, the intrusion detection rate also increases for the reduction of conjunction. In this, we discuss about distributed denial of service (DDos) attack and by how it is overcomed in Advanced Metering Infrastructure. The interaction between the customer and AMI network make AMI vulnerable to Threats. We introduce honeypot to detect and store the information about the attacker. Finally the result show that our proposed system improves the detection rate and energy consumption. Also ensures security to the AMI networks in Smart grid.

IndexTerms **- Distributed Denial of Service attack, Advanced Metering Infrastructure, Honeypot algorithm.**

1. INTRODUCTION

ADVANCED Metering infrastructure is the improved version of existing automatic meter reading(AMR) systems which is implemented in recent times. AMI is the main component in the smart grid which is used to obtain real time price information for customers[1] and help them to optimize the power usage. It is the bi-direction communication between AMI headend and smart meters. AMI system makes the smart grid to receive information about the home energy management appeal. AMI technology improves the key feature in grid system including: System Reliability, Energy Cost, Electricity Theft. It consist of smart meters, data aggregators, central system, meter information management system, communication network, and communication technologies.
An AMI network communicates between home area network(HAN), local area network(LAN), neighbour area network(NAN),and wide area network(WAN). The various communication technologies used in AMI network are optical fiber, Zigbee, and power line carrier[2]. The network protocols used here are Internet Protocol Suite(IPS), Open smart grid protocol which enhances the feature scalability[3].

The drawback of implementing AMI Infrastructure is, it is vulnerable to Threats. The security standards of AMI system are integrity, availability, and accountability. The cyberthreats is based on connection and device [2]. The connection based attacks are wireless scrambling, eaves dropping, message modification and injection whereas device based vulnerabilities are man-in- the-middle, metering storage tampering, denial of service abuse. In this, we concentrate mainly on the distributed denial of service attack which is been initiated by the attacker who targets at mainly on a smart meter, an aggregator, or headend. An attacker can insert the malicious code through an smart meter and tampers the data in the storage[4]. Attacks in smart meter are meter spoofing, denial of service, and power disconnection[5]. This weaken the real time metering, and it cannot report the updated energy usage[6], which leads to financial loss.

Honeypot strategy is one of the approach to counter the distributed denial of service attack in an AMI network and pretends to be a normal server which can attract, detect, and gather information about the attackers by consuming the hackers time and resources. It is mainly contrivance to recognize the goal of the attackers and stores the attacker information by consuming less resources. The main system monitors the intrusion of the attacker to the honeypot which is present in between them by protecting the central server from the hackers.

A Dynamic attack on the main system will damage or destroy defense system. The honeypot system is identified using the Anti-honeypot feature by transmitting the initiative package to the system. If the hacker identified the honeypot server, they can able to access the defense network before which the main system gets to realize about the hacker.In this work, we study various ways of DDos abuse occuring in AMI network. As a result we install honeypots in the network to improve the detection rate and to reduce the energy consumption. To this end, our contribution is to collect and gather information about the attacker by using the attack classifier and fircol which provide secure communication between the consumers and AMI operators.

The remainder of this paper has the details as follows. We review the background and the related work in section 2 We narrate the performance evaluation results and the discussions in section 3 followed by conclusion in section.

2. BACKGROUND AND RELATED WORKS

The distributed dos attacks creates an interest to many people, including the researchers, since it is a serious security and privacy danger.

2.1 Brief Antiquity:

Distributed dos attacks arise around 1996. In about 20 years, it had pilot critical threats in websites, online services, and applications. In the cyber records the foremost time it was used in september 1996. It first attacked the ISP PANIX which affected the business as ISP and started to evolve which ultimately reached its peak during 2015. But still the techniques for ddos attack are growing more further such that the detection of ddos abuse has become a complex task.

2.2 DDos attack propagation methods:

The attacker propagate the malicious code into the hardware and identifies the software security weakness on meter, and use them as a communication module. The hacker must select a proper propagation medium to spread the malware. There are 3 popular approaches for propagation, they are:

Central repository The agents are hidden from the assailant using IP spoofing which leads to extend the difficulty level of determining the starting point of the attack, especially in the large network.

a. approach: In this approach, the attacker places the poisonous program in the file repository and is propagated to other meters from this repository.

b. Back-chaining approach: In this, the agent is compromised by the assailant to download the poisonous cipher from the malware guest.

c. Autonomous approach: it is identical to back-chaining but it is differs by combining the malicious code with the agent instead of downloading the malware.

2.3 DDos attack mechanisms:

There are many ways where ddos attack can happen, such as:

a. *Abuse on protocol*: Here, the assailant target on the concord to deplete the resources. For Example, IP based AMI network make use of transmission control protocol(TCP). The attacker use TCP SYN flooding attack to degrade the performance.

b. *Abuse on infrastructure*: It pivot on infrastructure, and routers plays an important role in AMI system. The attacker will destroy the routing tables which leads to packet loss.

c. *Abuse on bandwidth*: The assailant transmit excessive communication packets to the node which leads to traffic and force to drop the legitimate packets.

2.4 AMI structure:

AMI is an advanced model of automated meter reading(AMR). It enables two-way communication between the customer and the AMI administrator. It sends price information to the customer by which they can be able to optimize their power usage, also they are awake to their home appliances energy consumption. AMI structure consist of smart meters, central system, meter data management system, and communication networks. The headend is used as the interaction between the AMI network and the utility applications.

Smart meter is the main component in the AMI network which is used to analyse, monitor, store, and report power consumption details to the client. Every smart meter connected to the aggregators, from which the data is transmitted to the AMI network. The meter can also be connected via another meter. All aggregators are connected to the headend.

Many firewalls are placed between the energy providing network and the AMI. These components are connected in a hierarical manner, where the top one is the headend, followed by aggregators and then smart meters.

Attacks can be happened in any agent such as smart meter, aggregators or headend but most probably it occurs in the smart meters. Attackers attack the agents by propagating the malicious code and start spreading these malware[7] to different abuse in the lattice to deteriote the accomplishment of the network. DDos abuse happens when the legitimate user did not get service such as resources, network by Internet Service provider. The attacker mostly target the critical server by transmitting

the flooding request or messages. First, the nodes along the path are exhausted, then the nodes fail to communicate with the base station which leads to the network paralysis, power shortage, and power overhead in smart grid[12].

2.5 Honeypot Game Strategy:

Honeypots act as a normal servers to absorb the attacker inorder to analyse the intention of the hacker by collecting evidence about the hacker to hide real servers from them, and to utilize the collected information about the hacker for future retrievement[13].

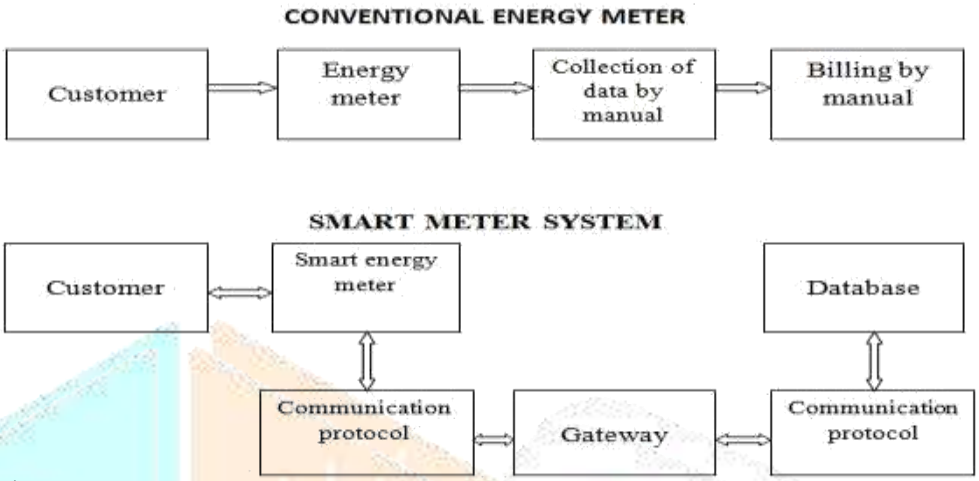

Fig1: architecture diagram

The attack classifier is used to store the attackers information based on their motive and the output generates a dynamic list of attacks which are then queued in the firecol logic which is build with neural network to interpret the various approaches of deportment and design of the attacker. In AMI network, there are more possible ways to attack the servers and for this purpose Honeypot is implemented to make attacker to hack the honeypot server and resulting in waste of time and resourses of the attacker by which the real servers are concealed. The Honeypot are embedded with the real servers which can serve as an internal network on honeypot, that increases the detection date. Even if the attacker attack the server, they will not get any information because the honeypot server is been hacked instead.

The network sniffer tool is used in the network to analyse from where the attack is launched and from which path the attacker direct excessive communication package in order to brick that path. The attacker profile is built based on their attacks in order to identify their preferred attack methods similar to criminal profiles used by law enforcement agencies. The new vulnerabilities and risk of various operating system, environment and programs are not thoroughly recognize at the moment.

In the dynamic rule construction mechanism, a suspicious violator and intrusions can be detected[14] easily based on the deportment and context boycott of the resource, host, and the IP network can be done without much overhead. These rules are used to differentiate normal network connection from anomalous relationship by referring to the probability of intrusions. The Network Intrusion Detection System monitors the packet on the network and discover an intruder by matching the attack pattern to a database of known attack patterns. In the process, boycott is the list of disprove access members. Every organization may keep a blacklist of software or websites in the computer system. These mechanisms are monitored by the real servers by the information assemble from the honeypot server[12].

3. PERFORMANCE EVALUATION

3.1 Experiment Settings

In this section, we build the AMI testbed[15] and deploy honeypot. AMI testbed is used to judge the performance of the honeypot design(as shown in fig.2,) and the honeypot treated as real server which is used to attract the hackers and to address the ddos attacks in AMI network. The constructed tree consists of honeypots, anti-honeypots, routers, smart meters, and normal servers. Here the normal servers are the victims which is hacked by the attackers.

In fig 2, a small-scale testbed is constructed with 4 servers, 10 honeypots and 2 anti-honeypots. The simulation settings for the AMI network testbed was shown in the Table 1. We consider two honeypot services which includes:

- Honeypot service: It is deployed to protect the real servers. Adding more honeypots will improve the performance and increase the detection rate.
- Anti-honeypot service: It is deployed to help the attackers to identify the honeypot in the apology system, apparatus in AMI

testbed.
The performance is judged based on the collation between the endure Cluster Head(CH) model[17], All Monitor(AM) model[18] and our Honeypot game(HG) model.

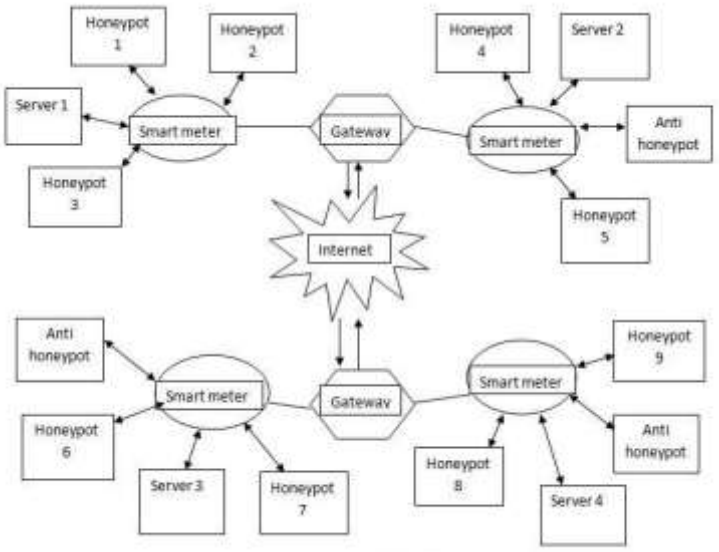

Fig 2. AMI network testbed

3.2 Experimental Results

The performance is judged based on the comparison between the existing Cluster Head(CH) model, All Monitor(AM) model and our Honeypot game(HG) model.

The comparisons between different probabilities show the proof in the improvement of detection rate and the energy consumption which help us to find the reason for the deployment of honeypot and anti-honeypot in the AMI network. In Fig. 3, it shows the change in the slope of the energy consumption curve of the HG model which is relatively glossy and energy consumed is loggy. Honeypot and anti-honeypot deployed represented in fig.3 shows different energy consumption in HG model.

TABLE I: Simulation Network Settings

PARAMETERS	PARAMETER VALUES
Scalability	500m*500m
Number of nodes	600
Simulation duration	8 min
Smart meter to router	0.65 Mbps
Router to smart meter	0.3 Mbps
Server to router	4 Mbps
Router to gateway	75 Mbps
Length of demand	1000 bytes
Demand time	7 s
Period time	11 s
Response time	4 ms
Compared model	CH monitor model, All Monitor model

As shown in Fig. 4, the existing model shows the detection rate of CH model between 40%-60%, on average of 50%. In the honeypot game model, the detection rate is between 80%-90%, on average 85%. Thus it shows that increasing the number of honeypot and significantly reducing the number of anti-honeypot in the AMI network will improve the performance of the detection rate. As a result, the normal servers get rid of the attacking zone.

In Fig 3(b), the energy consumption of HG model is more than the CH model and the detection rate is also more. Then the fig 3(c), the

energy consumption is adjacent to AM model but the detection rate is higher than the AM model. So when we continue to increase the number of honeypots and decrease the anti-honeypots, then the detection rate is improved and energy consumption is low. As a result we conclude that:

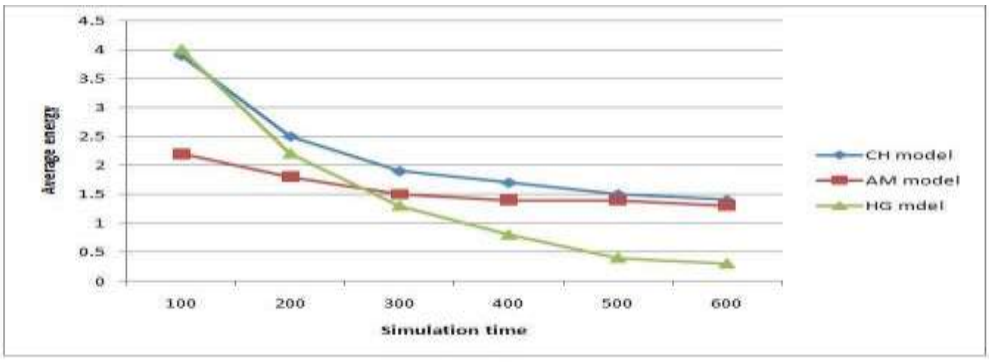

Fig 3. Performance of Energy Consumption

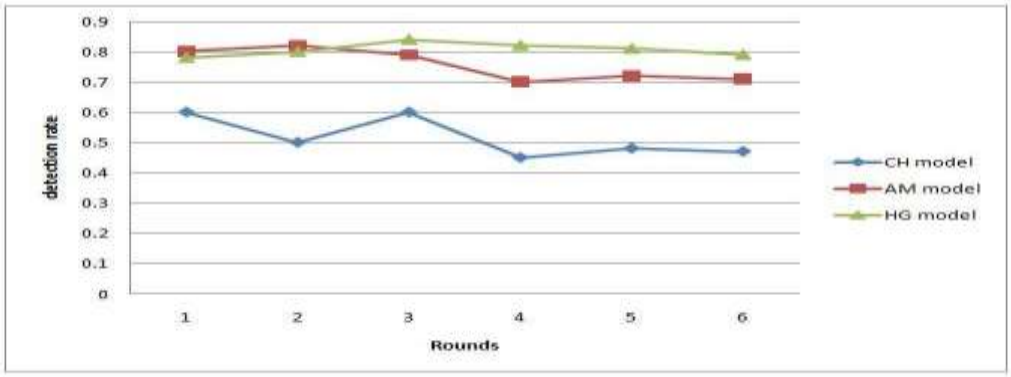

Fig 4. Performance of Detection rate

1. In the testbed {0.6,0.2}, we achieve optimal production and we can deploy about 10 honeypot and 3 anti-honeypots.
2. In the AMI network, more number of honeypots do not effectively increase the performance of the defense system
3. When the performance reaches the dynamic balance {0.55,0.25}, then the HG model reach the optimal
4. Solution between the attacker and the defender.

4. CONCLUSION AND FUTURE WORK

In this paper,the model of the ddos attack is discussed and honeypot is introduced in the AMI network of smart grid to resolve the problem arised by the DDos attack. Honeypot is also used to analyse, monitor, and gather the information about the attacker. The simulation results shows the performance improvement in the energy consumption and the detection rate by using the honeypot game strategy to safeguard the data and ensure security to the AMI network in the smart grid. Future work will focus on the anti-honeypot problem from the perspective of the attacker and developing effective defense approach against DDos attack in smart grid.

REFERENCES

1. "A real-time information based demand-side management system in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 329-339, 2016
2. "Communication security for smart grid distribution networks," IEEE Commun. Mag., vol. 51, no. 1, pp. 42–49, 2013.
3. "Architecture and Protocols," Dec. 2009. [Online]. Available: http://dlms.com/documents/Excerpt GB7.pdf
4. "Energy theft in the advanced metering infrastructure" in Proc. 4th Int. Workshop Crit. Inf. Infrastruct Security, Sep. 2009, pp. 176-187.
5. "Multi-vendor penetration testing in the advanced metering infrastructure", in Proc. Annual Computer Security Applications Conference, pp. 107-116.
6. "Security and privacy challenges in the smart grid", IEEE Security Privacy, vol.7,pp.75-77,2009.
7. "Technical Report for Denial Of Service Attack Technology, "CERT Coordination Center, October 2001. Available: http://www.cert.org/archive/pdf/Dos_trends.pdf
8. TCP SYN Flooding and IP Spoofing Attacks. Available: http://www.cert.org/historical/advisories/CA-1996-21.cfm

9. Security Risk Assessment. Available: http://www.cymru.com/Documents/barry2.pdf
10. Internet Denial of Service: Attack andDefense Mechanisms, 1st ed. Prntice Hall, 2005
11. "Demand response management in the smart grid in a large population regime" IEEE Trans. Smart Grid, vol. 7, no.1, pp. 189-199, 2016.
12. "Mobile big data fault tolerant processing for eHealth networks" IEEE Netw., vol. 30, no. 1, pp. 1-7, 2016
13. "Tracking smart grid hackers", UPEC, PP.1-5, 2014.
14. "Data-stream based intrusion detection system for advanced metering Infrastructure in smart grid: a feasibility study", IEEE syst.J., vol.9, no.1, pp. 31-44, 2015
15. "Collapsar: A vm-based architecture for network attack detection center", in Proc 13th USENIX Security Sym., 2004.
16. "Scalability , fidelity and containment in the Potemkin virtual honeyfarm",in Proc, ACM Sym. SOSP., 2005.
17. "Game theory based active defense for intrusion detection in cyber-physical embedded systems" ACM Trans. Embedded Comp Syst., vol. 16, no. 1, Article 18, 2016.
18. "A game theoretic framework for robust optimal intrusion detection in wireless sensor networks", IEEE Trans. Inf. Forensics Security, vol. 9, no.9, pp.1367-1379, 2014.

BIOGRAPHY

Priyanka.B is a student doing B.E degree in computer science and engineering in Prince shri venkateshwara padmavathy Engineering college, Chennai. Her research interest includes Cryptography, network security, cyber security.

Alaguroja.R is a student doing B.E degree in computer science and engineering in Prince shri venkateshwara padmavathy Engineering college, Chennai. Her research interest includes visual cryptography, information security.

Kalpana. R is an assistant professor in computer science department at Prince Shri Venkateshwara padmavathy Engineering college, Chennai. She is a M.E graduate. Her research interest includes computer graphics, internet programming, mobile computing
.

Kapila Vani. R. K. as Assistant Professor in computer science department at Prince Dr.K vasudevan College of Engineering and Technology, Chennai. She is a M.E graduate. Her research interest includes compiler design, Theory of computation and Software project management.