IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Defending Against DDoS Attacks Using Ant Colony Optimization

Dr. R. M. Mallika1,M.Tech, Ph.D., P Lavanya2 M Peddaiah3 K Lohith4 P Lokeswari5
[1]Associate Professor, [2345]UG Student [12345]Department of Computer Science and Engineering
[12345]Siddharth Institute Of Engineering &Technology, Tirupathi, Andhra Pradesh, India

ABSTRACT

The importance of the DDoS issue and the rise in the frequency, sophistication, and power of assaults have prompted the development of several prevention techniques. Each suggested preventive measure differs from the others in certain specific benefits and drawbacks. In this study, we categorise the many defences against potential DDoS assaults that have been put forth in the literature and evaluate the advantages and disadvantages of each defence. It is preferred to consider that the number of maximum continuous DoS attacks in both the S-C and the C-A channels is bounded because of the cost effect of attacks. In this project on Distributed denial of service (DoS) attacks in cyber-systems, DoS attacks exist in between the sensor and controller communications and the controller-to-actuator communications. Then, a successful security control technique is developed to counter two-channel DoS attacks, fully utilising the hardware to guarantee that control inputs are periodically captured during each time slot. A security controller that includes both the present and future control inputs is designed at the same time. The addressed CPS can be stable under 2-channel DoS attacks while maintaining control effectiveness under an appropriate security control strategy and security controller. Last but not least, simulations and tests are provided to show the viability of the suggested active security control approach.

Index Terms—*DoS attacks, Security transmission policy, Actively defend, Security control, Experiments, Cyber-physical systems.*

INTRODUCTION

Cyber-physical systems (CPSs) have found widespread use in a number of engineering sectors, including intelligent transportation, the smart grid, chemical process control, and process automation systems. CPSs are integrations of computing, communication, and control that help physical processes behave as planned. These CPSs are, however, susceptible to malicious assaults including denial-of-service (DoS) attacks and deception attacks because they rely on communication networks. These malevolent attackers pose a threat to physical systems as well as communication networks. In order to ensure the security of CPSs in the face of malicious attacks, it is required to build an effective control approach. With the introduction of the Internet, the field of computers and communication underwent a transformation. The Internet has grown in importance in today's culture. Technology is transforming how we communicate, conduct business, and even live our daily lives [1]. Almost all traditional services, including banking, power, healthcare, education, and military, are now available online. Fig. 1, which depicts the exponential rise in the number of hosts connected to the Internet [2], illustrates the effects of the Internet on society. As businesses, governments, and people continue to rely more and more on this technology, internet usage is increasing exponentially.

A coordinated DOS assault is launched against one or more targets by a DDoS attacker using a large number of devices [5]. It is indirectly launched by sending a flood of pointless aggregate traffic intended to explode victim resources over numerous infected computing systems. They frequently cause network congestion as a side effect while travelling from a source to a target, disturbing regular Internet activity. For the past few years, DDoS attacks have been dangerously on the rise [6]. Organized crime groups target online retailers, gambling websites, financial institutions, and other targets with many of today's DDoS attacks.

LITERATURE SURVEY

Denial of service attack definition (DoS)

A Denial-of-Service (DoS) attack aims to bring down a computer system or network so that its intended users are unable to access it. DoS attacks achieve this by providing the victim an excessive amount of traffic or information that causes a crash. Both times, the DoS attack denies the service or resource that legitimate users (such as employees, members, or account holders) expected.

DoS assaults frequently target the web servers of well-known corporations, including media, financial, and commercial companies, as well as governmental and commercial organisations. DoS attacks can cost the victim a lot of time and money to deal with, even while they normally do not lead to the theft or loss of important information or other assets.

DoS attacks typically use one of two approaches: flooding services or crashing services. Flood assaults happen when the server cannot handle the amount of traffic coming into the system, which causes it to sluggishly and eventually cease. A common flood assault is:

The most frequent DoS attack is a buffer overflow: The idea is to transmit more traffic to a network address than the system's design allows for. It consists of the following attacks in addition to others that are intended to take advantage of flaws unique to particular programmes or networks.

Flood ICMP: pings every computer on the targeted network instead of just one particular machine by sending fake packets that take advantage of incorrectly configured network devices. The traffic is subsequently amplified by the network. The smurf attack and the ping of death are some names for this attack.

Sends a request to connect to a server using the SYN flood technique, but never completes the handshake. continues until there are no open ports left for reputable users to connect to due to demand overload on all open ports. Some DoS attacks merely take use of flaws that result in the target system or service crashing. In these attacks, input is received that exploits flaws in the target and causes the system to crash or become very unstable, making it impossible to access or utilise the system.

The Distributed Denial of Service (DDoS) assault is a type of DoS attack.

When several systems coordinate a synchronised DoS attack on a single target, the result is a DDoS attack.

The main distinction is that the target is attacked simultaneously from multiple locations rather than just one. The attacker gains a number of benefits from the spread of hosts that characterises a DDoS, including:

It is more challenging to shut down multiple machines than one because of the following factors:

- He can use the larger number of machines to carry out a seriously disruptive attack;

- The location of the attack is difficult to determine because of the randomly distributed attacking systems (often worldwide);

- It is more difficult to shut down multiple machines than one;

- The true attacking party is very difficult to identify because they are concealed behind many (mostly compromised) systems.

Current security technologies have created defences against the majority of DoS assaults, but because DDoS attacks have particular features, Organizations who worry about becoming the target of such an assault are more worried about it since it is still considered as an elevated threat.

Priyanka Kamboj[11] proposed Detection techniques of DDOS attacks, Security is the main confront of internet, Distributed Denial of Service (DDOS) is the major cause of threat. DDOS reduces the network resources, and results in bandwidth depletion. The main aim of

DDOS is to prevent legitimate users from assessing the services. There also exists a difficulty to differentiate between flash crowd and DDOS attack traffic. The various existing solutions which are given in order to detect DDOS has been discussed. The goal of the paper is to review how the different methods are helping in downsizing the effect of DDOS and also how that are being used to detect a DDOSattack.

Vanitha.K.S. Dr.S.S.K [12], published Distributed Denial of Service: Attack techniques and mitigation, A Distributed Denial of Service (DDOS) attack is an attempt to make a service unavailable by overwhelming the server with malicious traffic. DDOS attacks have become the most tedious and cumbersome issue in recent past. The number and magnitude of attacks have increased from few megabytes of data to 100s of terabytes of data these days. Due to the differences in the attack patterns or new types of attack, it is hard to detect these attacks effectively.

Suman Nandi,SantanuPhadikar [13] proposed Detection of DDOS Attack and Classification Using a Hybrid Approach, our hybrid approach for detecting the DDOS attack gives the best detection rate compared to some existing methods.Distributed denial of service (DDOS) attack is one of the major security issues in the cloud where the resources being unavailable for legitimate users. So, the detection of DDOS attack is a challenging work such that actual users are not suffering from the unavailability of resources. To detect the DDOS attack from a dataset, the most important thing is to select the appropriate features such that the attacking packets are correctly classified by any classifiers. So, the effective feature selection plays a significant role to make an efficient DDOS detector.

Ruiguo,Guiranchan [14] suggested DG-Based Active Defense Strategy to Defend against DDOS, It is advocated that defenders should take active action to stop DDOS attacks. They Propose a new model based on differential games theory. The defense mechanism of DDOS attacks, particularly the multi-based, multi-approached and diversified flow method of offensive artifice, simulating the competition of legal users, inhabits a keystone and difficulty in the internet security arena, especially for the attacker using lots of Bots. The method is cost-effective, while resulting in a high performance. Furthermore, it is easy to deploy. The impact of the model on the network is only minor, while the survival of the server during a DDOS attack is greatly improved. Our future work will focus on other issues in our DGM implementation. One challenging issue for us is to reduce a large number of Bots controlled by Botnet

RECENT WORKS

An incident in which a genuine individual or organisation is denied access to services like web, email, or network connectivity that they would ordinarily expect to have is known as a distributed denial of service attack. DDoS is essentially a problem with resource overload. The resource may be memory, CPU time, bandwidth, file descriptors, buffers, etc. The attackers flood the resource with packets or activate several processes with a single logic packet to deplete the finite supply [20]. A simplified distributed DoS attack scenario is shown in Fig. The diagram depicts how the attacker employs three zombies to flood the victim's website with large amounts of fraudulent traffic, preventing legitimate users from using the service. outside network. As a result, the client's network bandwidth may be completely consumed by traffic coming from the Internet. As a result, the targeted network will be unable to fulfil a valid request. The vast majority of traffic aimed at the target network during a DoS attack is malicious and was either intentionally or unintentionally created by an attacker. These attacks on January 25, 2003, halted major ISPs like Freetel, SK Telecom, and KoreaTelecom and prevented 13,000 Bank of America ATMs from providing the withdrew services.

Router-based packet filtering: Developed by Park and Lee [35], route-based filtering expands on ingress filtering by utilising route information to weed out fake IP packets. It is predicated on the idea that there are only a finite number of source addresses from which traffic on each link in the Internet's core could have come. An IP packet can be censored if an unexpected source address appears in the packet; this indicates that the source address has been fake. RPF filters traffic with fake source addresses using knowledge of the BGP routing topology.

According to simulation data, if RPF is implemented in at least 18% of ASs on the Internet, a sizable portion of spoof IP addresses can be filtered. This plan does have a few drawbacks, though. The first drawback has to do with how RPF is really put into use. Given that there are over 10,000 ASs on the Internet, RPF. The DoS attack is a more feasible assault pattern in a communication network and will result in the most financially costly security issues because it doesn't require any system information.

When an open-loop vital industrial control process is unstable, it is noted that communication networks cannot successfully update data packets if DoS attacks last for a prolonged period of time Hence, such networks cannot be controlled by closed-loop feedback. This presents fresh theoretical difficulties for control system analysis and synthesis. The secure control problem for CPSs under DoS attacks has been explored in some previous publications, and it can be roughly solved by simultaneously considering the best DoS attack and defence strategies. where the frequency and length of the attacker action affected the DoS model.

DoS attacks may cause environmental harm.

• Will result in the most costly security events in terms of money

• Communication networks are unable to successfully update data packets.

PROPOSED METHOD

CPSs concentrate on two key areas: 1) how to create a control strategy that fully utilises unattacked intervals to achieve closed loop feedback control under two-channel DoS attacks, and 2) how to design an effective controller to improve system performance in comparison to sample-and-hold or zero-input control strategy techniques. This proposal will take into account the basic scenario where DoS assaults happen in the SC channel and the C-A channel either concurrently or independently in order to address these issues. Attackers typically face economic restrictions (such as restricted energy sources) that make it impossible for them to continuously mount DoS attacks. Thus, it makes sense to assume that the highest continuous DoS attack rate in both the S-C channel and the Then, a unique security control strategy is designed to actively counter DoS assaults on the basis of the event-triggered concept and predictive control theory.

BENIFITS

• Fully utilises the times between attacks to make sure the control inputs are updated on time during each session of the two-channel DoS attacks.

• Security controller with both present and upcoming control inputs.

• DoS attacks are asymptotically stable while maintaining control performance.

• The constraint is satisfied by the control inputs.

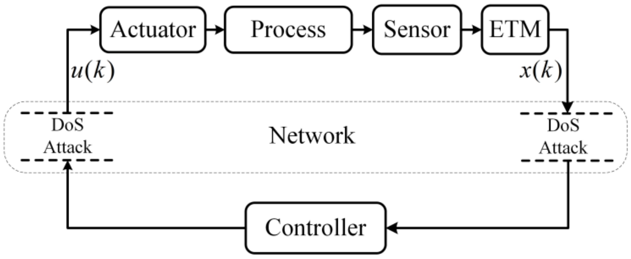
ALGORITHM:

Procedure Active security control strategy Algorithm

- *Step 1: the actuator receives the control sequence* $U_{\omega(k_d)}(k_d)$ *at time* k_d,
- *Step 2: the actuator executes the control inputs* $u_{\omega(k_d)}(k_d), \ldots, u_{\omega(k_d)}(k_d + i), \ldots, u_{\omega(k_d)}(k_d + N_C - 1)$
- *Step 3: sensor executes event triggered condition to determine the event-triggered at time* k_t.
- *Step 4: At time* k_t, *the sensor sends the state vector to the controller* $N_{sc} + 1$ *times continuously from* k_t *to* $k_t + N_{sc}$.
- *Step 5: Controller receives the state* $x(k_{s+1})$ *at time* k_{s+1},
- *Step 6: Controller constructs the control sequence* $U_{\omega(k_{d+1})}(k_{d+1})$ *and then sends it to the actuator* $N_{ca} + 1$ *times continuously from* k_{s+1} *to* $k_{s+1} + N_{ca}$.
- *Step 7: Actuator receives the control sequence* $U_{\omega(k_{d+1})}(k_{d+1})$
- *Step 8:* $k_d \rightarrow k_{d+1}$ *and* $k_s \rightarrow k_{s+1}$. *Return to the Step*

End procedure

ARCHITECTURE DIAGRAM



Network Simulation Module

In order to demonstrate the effectiveness of the suggested approaches through simulations and experiments, a networked inverted pendulum control system is taken into consideration in this section. The corresponding structure diagram can be illustrated by the location of the data packets being transmitted over communication networks using the User Datagram Protocol (UDP).

Control of active security

An active security control approach that fully utilises the unattacked intervals is created to make sure that there are adequate control inputs to be updated in each period in order to actively defend against the two-channel DoS attacks. Also, the closed-loop system produced by the active security control technique is analogous to the situation in which DoS attacks are not present.

Security Transmission Policy based on Events

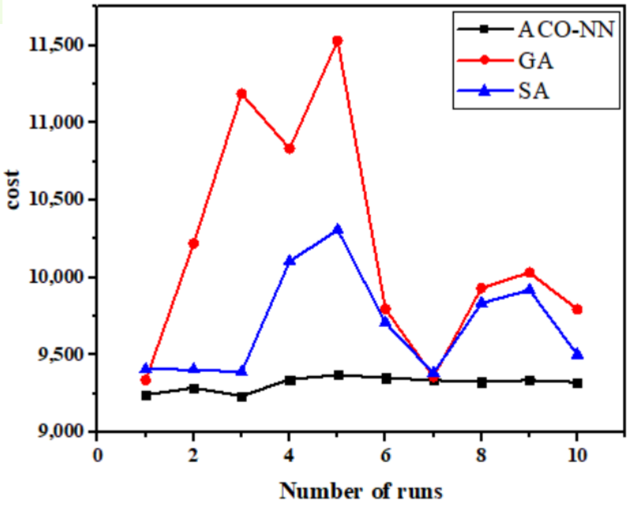
In this paragraph, an event-based security transmission policy is proposed. Event-triggered conditions are taken into consideration.

Module for Message Packet Transmission

By offering end-to-end communications that specify how data should be divided into packets, addressed, transferred, routed, and received at the destination, UDP/IP defines how data is shared over the internet. UDP/IP is made to enable networks to automatically recover from the failure of any device on the network and requires little central supervision.

The IP suite's two primary protocols each have a distinct purpose. UDP outlines how programmes can establish networks-wide communication channels. Also, it controls how a message is divided up into smaller packets before being sent over the internet. then reassembled in the appropriate order at the final location.

EXPERIMENTS



The experiment findings are displayed using the identical network environment and parameter settings as in the simulations and the active security control methodology suggested in this paper. Figure 8 illustrates the feedback control timing diagram of the first 50 periods during the two-channel DoS attacks in the experiment, demonstrating the stability of the networked inverted pendulum control system and the satisfaction of the constraint by the control inputs. This diagram demonstrates that the control sequence U(kd)(kd), which includes both the present and future control inputs, is Pos (m) -0.2 0 0.2 Time(s) 0 2 4 6 8 10 Angle Time(s) 0 2 4 6 8 10 (rad) -0.2 0 0.2 Time(s) 0 2 4 6 8 10 Control input: -20 0 20 (m/s 2) Figure 8 shows the system outputs and inputs for the experiments. Periods of Control: 0 10 20 30 40 50 DoS attacks with 1 trigger time per S-C channel Periods of Control: 0 10 20 30 40 50 U(kd) DoS attacks on the C-A channel: Update time. Over the first 50 periods, the feedback control timing diagram in Experiments that was subject to two-channel DoS attacks was successfully updated ten times. The control inputs u(kd)(kd), u(kd)(kd+1),..., u(kd)(kd+ j 1) will be implemented consecutively in the situation of kd+1 = kd + j when the actuator gets the control sequence U(kd)(kd). (j ∈ {1, 2, . . . , 9}). As a result, shows that the active security control approach must be used to implement the proper control inputs to be updated in each period under the two-channel DoS attacks. The active security control strategy suggested in this research is effective in the actual system, as shown.

CONCLUSION

The number of maximum continuous DoS attacks in both the SC and the C-A channels is thought to be constrained due to the cost restrictions of attacks, and an active security control technique has been developed for CPSs under the two-channel DoS attacks. The active security control technique in Algorithm 1 has been devised to actively counter two-channel DoS assaults. This can guarantee that the correct control inputs are available for updating each time.

The closed loop system produced by the active security control technique is comparable to the situation without DoS attacks, it can be deduced from Theorem 1a. Algorithm 2 has since provided the security controller design process. Theorem 2 states that the active security control strategy suggested in this research can ensure that the addressed CPS is asymptotically stable under two-channel DoS attacks without sacrificing control performance. Lastly, simulations and tests were used to demonstrate the value of the active security control strategy that was suggested. Yet, a lot of the physical processes in CPSs are noisy and nonlinear. So, one of our next studies will be the creation of the active security control approach for nonlinear CPSs with noises. One of our upcoming projects is the design of active defences against deception assaults.

REFERENCES

[1] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, “A survey on security control and attack detection for industrial cyber-physical systems,” Neurocomputing, vol. 275, pp. 1674-1683, Jan. 2018.

[2] A. Cetinkaya, H. Ishii, and T. Hayakawa, “An overview on denialof-service attacks in control systems: Attack models and security analyses,” Entropy, vol. 21, no. 2, pp. 210, Feb. 2019.

[3] P. Leitao, S. Karnouskos, L. Ribeiro, J. Lee, T. Strasser, amd A.W. Colombo, “Smart agents in industrial cyber-physical systems,” Proc. IEEE, vol. 104, no. 5, pp. 1086-1101, May. 2016.

[4] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, “Recursive Filtering of Distributed Cyber-Physical Systems With Attack Detection,” IEEE Trans. Syst., Man, Cybern., Syst., to be published, doi: 10.1109/TSMC.2019.2960541.

[5] G. Wu, J. Sun, and J. Chen, “A survey on the security of cyber-physical systems,” Control Theory Technol., vol. 14, no. 1, pp. 2-10, Feb. 2016.

[6] X. Cao et al., “Cognitive radio based state estimation in cyber-physical systems,” IEEE J. Sel. Areas Commun., vol. 32, no. 3, pp. 489-502, Mar. 2014.

[7] M.S. Mahmoud, M.M. Hamdan, and U.A. Baroudi, “Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges,” Neurocomputing, vol. 338, pp. 101-115, Apr. 2019.

[8] B. Chen, D.W. Ho, W.-A. Zhang, and L. Yu, “Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks.” IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 2, pp. 455-468, Feb. 2019.

[9] N. Hou, Z. Wang, D.W.C. Ho, and H. Dong, “Robust PartialNodes-Based State Estimation for Complex Networks Under Deception Attacks.” IEEE Trans. Cybern., 2019. to be published, doi: 10.1109/TCYB.2019.2918760.

[10] L. Hu, Z. Wang, Q.-L. Han, and X. Liu, “State estimation under false data injection attacks: security analysis and system protection.” Automatica, vol. 87, pp. 176-183, Jan. 2018.

[11] Priyanka Kamboj1,Munesh Chandra Trivedi1, Virendra Kumar Yadav1, Dr. Vikash Kumar Singh2, “Detection techniques of DDOS attacks”, vol. 87, pp. 176-183, Jan. 2017.

[12] Vanitha.K.S. Dr.S.S.K, “Distributed Denial of Service: Attack techniques and mitigation.”, vol. 87, pp. 176-183, Jan. 2017.

[13] Suman Nandi,SantanuPhadikar , Koushik, Detection of DDOS Attack and Classification Using a Hybrid Approach”, vol. 87, pp. 176-183, Jan. 2018.

[14] Ruiguo,Guiranchan, Yuhaiqin, Baojingsun , An Liu, Bencheng Zhang , Dan peng, “DG-Based Active Defense Strategy to Defend against DDOS”, vol. 87, pp. 176-183, Jan. 2008.