WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Fault Detection and Controller Co-Design for Unmanned Surface Vehicles Under DoS Attacks

Giftson Baruch A

Dr.MGR Educational and Research Institute,Maduravoyal,chennai-600095.

A B S T R A C T

My paper addresses the problem of a fault detectionand controller for a networked-based nodes to nodes system subject to communication delays, external disturbance, faults, and aperiodic denial-ofservice (DoS) jamming attacks. An event-triggering communication scheme is proposed to enhance the efficiency of network resource utilization while counteracting the impact of aperiodic DoS attacks on the server control system performance. An event-based switched server control system is presented to account for the simultaneous presence of communication delays, disturbance, faults, and DoS jamming attacks. Criteria for exponential stability analysis and of a desired observerbased fault detection filter and an event-triggered controller are derived and expressed in terms of linear matrix inequalities. The results show that this method not only ensures the safe and stable operation of the server but also reduces the amount of data transmissions.

1. INTRODUCTION:

Ensuring the availability and security of project data, services and resources is still a crucial and challenging issue. The DOS attacks are the most prevalent cybercrime attacks. DDoS TCP flood attacks can exhaust the cloud resources, consume many of its bandwidth, and destroy an entire project within a small period. The detection and prevention of such attacks in cloud projects, especially for eHealth clouds. In my paper, we present a new classifier system for detecting and preventing DDoS syn flooding attacks in public clouds. It secured records by classifying the incoming packets and making a decision based on the results. During the detection time, the DOS identifies and whether a packet is normal from an attacker. During the prevention time, packets which are classified as malicious will be denied access to the service and the source IP will be blacklisted. It can detect DDoS syn flood attacks with about 97% accuracy.

2. SCOPE:

To exponential stability analysis and co-design of a desired observer-based fault detection filter and an event-triggered controller are derived and expressed in terms of linear matrix inequalities.To server to can handle the multiple clients on all the available access points on which the server is started up.To make request to the server and can receive response for the requested service. Initially the RAP detection system is trained with observables and the hidden states. Secondly, RAP detection system is started monitoring the network traffic for detecting malicious network activities such as probing and compromising the access points.

3. EXISTING SYSTEM:

- The exponential growth of computer/network attacks are becoming more and more difficult to identify the need for better and more efficient intrusion detection systems increases in step.

- The main problem with current intrusion detection systems is high rate of false alarms.

* *Corresponding author.* Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: author@institute.xxx

- The design and implementation of traffic coming from clients and the traffic originated from the attackers is not implemented.

4. PROPOSED SYSTEM:

- If the attacker identifies the port, he can intrude or interfere in the communication and flood DOS attack and can hack communicating data.

- Clock drifts method is not reliable because, DDOS attacks are flooding of large number of requests by the attacker, which leads to decrease in bandwidth, and low latency time.

4.1 PROPOSED SYSTEM ADVANTAGES:

- More reliable communication between server and clients
- Active communications remains unaffected even in the presence of DDOS attacks.
- Difficult to intrude into communications
- Less probability of hacking
- Effective and efficient response processing for incoming requests.

5. INPUT DESIGN:

Input design is one of the most important part of the system design. Input design is the process where the input received in the system are planned, so as to get necessary information from the user, the information that is not required. The aim of the input design is to ensure the most possible levels of accuracy and also ensures that the input is accessible that acceptance by the user.

The input design is the system design. If the data going into the system is incorrect then the processing and output will the errors.

During input design are :

- Creation of input processing.
- Flexibility and thoroughness of validation rules.
- Handling of properties within the input documents.
- Design to ensure correct and efficiency of the input relationship.
- Design of the input also involves to error handling, controls, batching and validation procedures.

Input design features can ensure the reliability of the system and create result from correct data.

6. OUTPUT DESIGN:

Computer output is the must important and source of information to the user. Efficient, intelligible output design should improve the system's connection with the user and help in decision creating. A major form of output is the hard copy from the printer.The time requirements, expected print and number of copies needed. . All nodes in the network may depart or failure.

The continuously generated measurement data by time, where a source block refers to the amount of data is created by one time . How many time slots of data can be cached depends on the size of the node cache database.

A packet occurs immediately before the first active sample on every line, and immediately after the last active sample.A systems flowchart specifies bigger files, transaction files and computer programs. Input Data are collected and organized into similar data. Once identified, input media are processing. The output devices to depend on factors such as compatibility of the device with the machine, response time requirements, expected print and number of copies needed. All nodes in the network may depart or failure.

7. CONCLUSION:

The existing mechanism eliminates the want for a centralized trusted authority which is not practical in network due to their self organizing creation. The results demo that the presence of a DOS increases the packet loss in the network. The proposed mechanism protects the network, fully distributed and localized procedure. The additional certificate publishing happens only for a small duration of time during which almost all nodes in the network get certified by their neighbor. After a time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a

excellent network performance. In terms of security as compare with attack case. The attack prevented has a much bigger impact on the performance of the protocol. The existing mechanism can also be applied.

REFERANCE:

[1]Nieto-Hidalgo M., Gallego A.-J., Gil P., and Pertusa A., "Two-stage convolutional neural network for ship and spill detection using SLAR images," IEEE Trans. Geosci. Remote Sens., vol. 56, no. 9, pp. 5217–5230, Sep. 2018.
[2]Fossen T. I., Handbook Marine Craft Hydrodynamics Motion Control. Hoboken, NJ, USA: Wiley, 2011.
[3]Bertram V., "Unmanned surface vehicles—A survey," SkibstekniskSelskab, vol. 1, pp. 1–14, Mar. 2008.
[4]Peng Z., Wang J., and Wang D., "Distributed maneuvering of autonomous surface vehicles based on neurodynamic optimization and fuzzy approximation," IEEE Trans. Control Syst. Technol., vol. 26, no. 3, pp. 1083–1090, May 2018.
[5]Ma Y., Hu M., and Yan X., "Multi-objective path planning for unmanned surface vehicle with currents effects," ISA Trans., vol. 75, pp. 137–156, Apr. 2018.
[6]Ma Y., Zhu G., and Li Z., "Error-driven-based nonlinear feedback recursive design for adaptive NN trajectory tracking control of surface ships with input saturation," IEEE Intell. Transp. Syst. Mag., vol. 11, no. 2, pp. 17–28, Mar. 2019.