Analysis of Wireless Intrusion Detection and Prevention System against Cyber Attacks

P. Adlene Ebenezer, Asha Shajee, Dhruv Patel, Himangshu Shekhar Saikia, Rahul Mishra

Abstract--- This is a proposed topology for a wireless networked control system. It is implemented under several cyber attack scenarios and a distributed intrusion detection system (IDS) is designed to identify the existence of attacks. More specifically, it presents a modelling framework for the closed-loop control system with the IDS. It ensures a computational procedure to design and compute the IDS. After successful detection, IPS will be implemented.IPS analyzes packets for harmful protocols and stops these packets from reaching their destination based on the results of IDS.

Keywords--- IDS, IPS, Cyber Security, Cyber Attack, Intrusion Detection and Prevention, Analysis System.

I. INTRODUCTION

This is a proposed topology for a wireless networked control system. It is implemented under several cyber attack scenarios and a distributed intrusion detection system (IDS) is designed to identify the attacks in existence. More specifically, it presents a modelling framework for the closed-loop control system with the IDS. It ensures a computational procedure to design and compute the IDS. After successful detection, IPS will be implemented. IPS analyzes packets of harmful protocols and stops these packets from reaching their destination based on the results of IDS. In the literature, the use of both wired and wireless communication networks in a closed-loop control system has been studied in different horizons. Compared to wired communication networks, the use of wireless communication networks provides many advantages. However, several associated challenges also exist and require further research. One of the challenges is the security of the closed-loop control system. More specifically, in the presence of an attacker or force intrusion, the components and the communicated information in the control system are subject to eavesdropping and manipulation which can affect its stability and performance. The theory of convention with many ideal assumptions such as synchronized control and non delayed sensing and actuation, must be revaluated before they can be given into the system. There are some issues that needed to be addressed which are raised because of this theory. These issues are addressed so that research can be done in order to overcome any failure and so that no malicious activity or illegal entry can take place. IDS/IPS system is coated with algorithm that is designed to overcome any failed activity and protect the system from outside unwanted entry. Some issues needed to be addressed are:-

1) The network-induced delay that occurs while exchanging data among devices connected to the shared network can degrade the performance of control systems designed without taking in the delay and can also destabilize the system.

2) The network can be specified as a web of untrusted transmission paths. Some packets can be lost during transmission.

3) The plant outputs may be transmitted using multiple network packets due to the bandwidth and packet size constraints of the network.

These are some issues to overcome in order to increase the stability and performance of the IDS/IPS system. A complete balance between both IDS and IPS can be obtained only with overcoming these statements and researching it for finding solution. A perfect balance and stability can be obtained that will result in increasing of performance and reliability.

II. LITERATURE SURVEY

We did literature survey from 6 papers, including 1 base paper, and its corresponding papers.

1) We analyzed the process of distributing IDS to detect the existence of attacks for a wired and wireless communication network in a closed loop system. [1]

2) The stability for interconnected network control system was analyzed by determining the tradeoffs between MATI and MAD in Network Control System. [2]

3) Study of Predictive Controller Design of Networked System with communication delays and Data Loss using NCS feedback control system in closed loop was done. [3]

4) The control of a linear plant when plant state information is transmitted from a sensor and received by the controller over a wireless fading channel is analyzed. The power consumption with respect to transmitted data is analyzed. [4]

5) The process of monitoring, coordination and controlling a network infrastructure is studied. [5]

6) The process of detecting maximum number of attacks. [6].

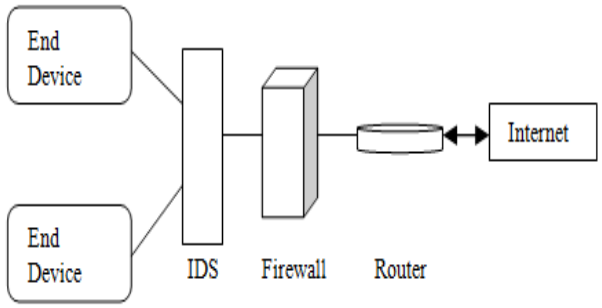
Revised Version Manuscript Received on 22 February, 2019

P. Adlene Ebenezer, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India.
(e-mail : adlenepackiadoss@gmail.com)
Asha Shajee, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India.
(e-mail : ashashajee@hotmail.com)
Dhruv Patel, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India.
(e-mail : dhruvp3012@gmail.com)
Himangshu Shekhar Saikia, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India.
(e-mail : dimpusaikia6@gmail.com)
Rahul Mishra, Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, India.
(e-mail : rahulbhai2496@gmail.com)

III. SYSTEM DESCRIPTION

IDS

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Intrusion Detection Systems take action when they detect any malicious activity or unwanted protocols in input packets. IDS checks for malicious and unwanted activities and are also sensitive to false alarms. Organizations need to fine-tune their IDS products when they first install them by properly configuring their intrusion detection systems to recognize malicious activity.

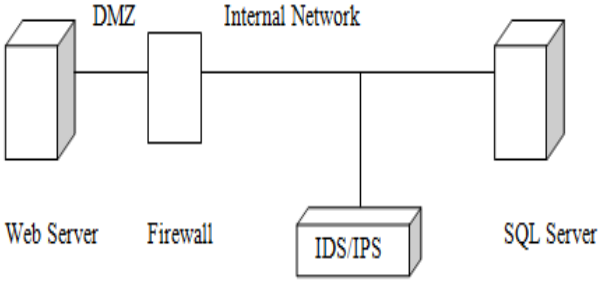


Intrusion Detection System is typically passive. It detects and alarms on suspicious protocols and entries. It has a reputation for false positive. The end devices while accessing the internet comes across a router, a firewall and IDS. When the requested data reaches IDS, it checks for any corrupted request or unwanted string of data that is not requested but is sent from the server. The IDS looks for any malicious protocol that might be embedded with the response string that can cause any harm or might result in entry of an attacker. Intrusion is detected by IDS server and is made sure that all data received is up to mark. If any suspicious activity is detected, it gives out a warning and alarms an error.

IPS

The IPS often sits directly behind the firewall and provides a complementary layer of analysis that prevents dangerous content. The IPS is placed in line, actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include:

- Sending an alarm to the administrator
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection



IPS is used for intrusion prevention. It can be used either alongside IDS or has IDS capabilities embedded into it. It is installed inline. It drops any malicious or suspicious activities preventing intrusion. After IDS detects the malicious or suspicious protocol, IPS uses the data provided by IDS to stop the malicious protocol from coming inside the system. The harmful protocol that might result in malicious activity is completely dropped by IPS.

Difference between IDS and IPS

The difference between IDS and IPS can be determined and given in the following way:

1) IDS don't take actions by itself. It detects any harmful activities. IPS, on the other hand, drops these activities based on the result produced by IDS.

2) IDS require a support to make a report and gather information on any activity while IPS can work on its own after receiving reports from IDS.

3) IDS provide a full report analysis of the coming packets of data to use as asecurity measure to prevent any unwanted activities. IPS catches these harmful packets of data and drops them before these packets gets to their destination.

4) IPS is more passive than IDS.

Criticality of IDS/IPS in Cyber Security

IDS/IPS provides some specific and important jobs of a cyber security strategy:

- Automation: Limited recourses are used to protect the network from known threats.
- Compliance: Implementing an IDS/IPS gives solution to a number of security measures.
- Policy enforcement: IDS/IPS provides security policies internally at the network level that helps in policy control of the system.

Challenges for IDS and IPS

IDS

IPS is used more and more as a replacement for IDSs or to make a distinction between them. IPS is more widely recommended because they not only detect any intrusion but also has the capabilities to remove any harmful or malicious packets that come as input.

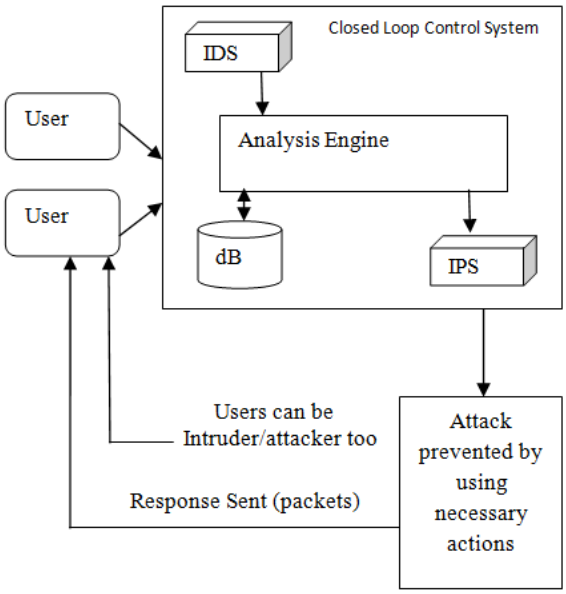
IPS

IPSs prolonged on the functionality make available by IDS by enabling to stop attack next two of network.By means of admiration from suggestion, they present real-time disturbance avoidance and indiscretion system. Major difficulty IPS is notice only attack they know from name.

According to Schultz, IPS future technology should vary, such as improving underlying interruption detection; progression in application-level psychoanalysis; more complicated reply capabilities; addition of interruption avoidance into other security devices.

Moreover, the forecast about interruption avoidance technology is very optimistic in market.

IV. SYSTEM ARCHITECTURE DESIGN



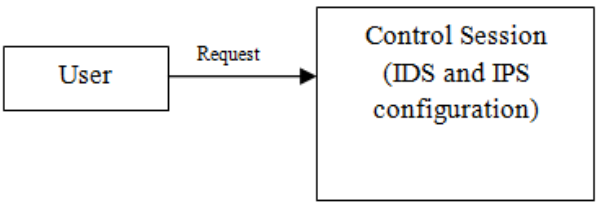
When a request is made by the user, it goes to a closed loop control system. The closed loop control system consists of 4 components: IDS, IPS, Analytical Engine and Database (dB). The IDS at first detects any malicious protocols or harmful and suspicious packets. After that it makes a report and is sent along with the request. The request is then received by Analytical engine that analyzes the request and makes a response along with the type of attack (if any). The database holds knowledge/information. The analytical engine with the help of database produces a response to an attack and is sent to IPS. The IPS checks on the report and analyses any harmful protocols and suspicious packets. If everything is all right, then response is sent back otherwise malicious activity is prevented by IPS. IPS normally sends an alarm or error message when intrusion takes place. In serious cases the IPS drops these requests and prevents intrusion.

NOTE: It's not always the case that an attacker has to be an outsider. A user that normally accesses the system can be an intruder too that may sent harmful packets and breach the security.

This architecture brings stability and increases performance in preventing intrusion. The following will be the modules that show the step wise working of the system. The modules include the process of how input is taken and the way detection, prevention and action on the harmful inputs takes place. The action is taken according to the threat warning of the packets.

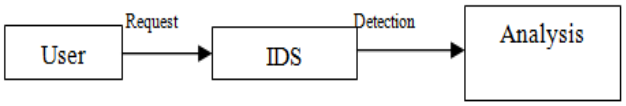
V. MODULE DESCRIPTION

1) Request Module



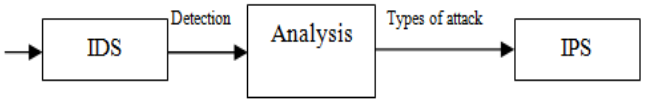
User request packets and the request go to the control session which is a closed loop control system.

2) Detection Module



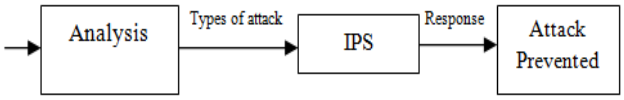
The request goes to IDS that detects any malicious activity or intrusion and then sends the request to the Analytical Engine.

3) Analysis (detection) Module



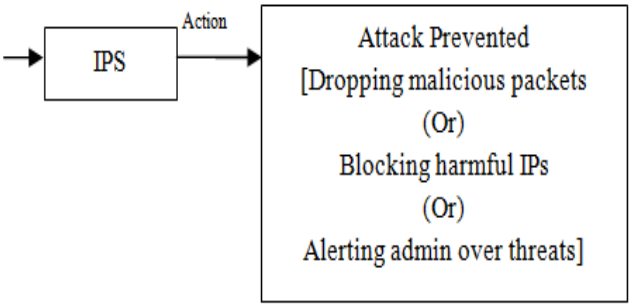
The IDS sends the detection report and sends it to analytical engine that analyses the type of attack along with the response and sends it to IPS.

4) Prevention Module



The type of attack detail report is provided to IPS. The IPS takes the report and prevents any malicious activity by dropping them. The attack is prevented and response is sent.

5) Action Module

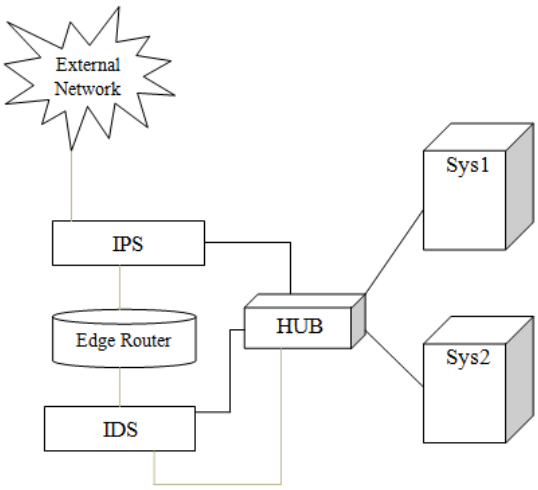


The IPS does the necessary actions and prevents the attack. The attack can be prevented by dropping malicious packets or blocking harmful IPs or alerting admin over threats.

Thus, these are the main modules that are used for the execution of the system that leads to efficient and stable implementation of IDS and IPS system for Intrusion Detection and Prevention. These modules are serially followed for the purpose of detecting, analysing and preventing of intrusion and also providing reports on the type of attack taking place. These modules are used for the system's working and bring out the best output as expected from the system.

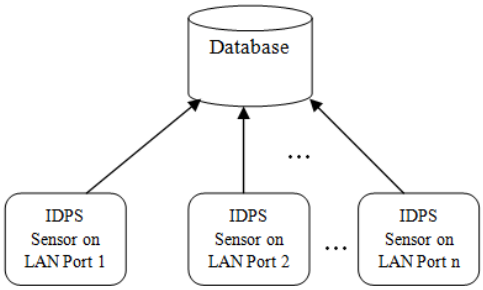
VI. IMPLEMENTATION

There are several ways to connect an IDPS to capture and monitor traffic. However, our project is based on inline configuration in order to bring out the best and efficient performance of the whole system.



Edge router is placed between two routers, IPS and IDS which makes the system called IDPS. This whole system is deployed here for Wireless Networks. Now acknowledge that the router is defined as a trust zone edge or network edge between LAN and WAN that connects the edge of the network. IPS is in the connection to provide admin privileges for internal networks. IDS are there with Out-Of-Bound connection. Which is in internal network and highlighted connection are used to gather the data to analyze. In the another variation of connection the Edge Router is directly connected to the Hub / Switch which makes IDS in Inline Connection and IPS in Spanning Port Connection.

Expected Outcome



The data fetched by the number of the sensors is fed to the database to maintain the logs. The logs are then used to define the new generation definition of the anomalies that can define next time. Due to the usage of signature based identification the signatures are stored in the database and those signatures are monitored by the administration and can be analyzed and new reports are generated to prevent the malicious traffic if the same traffic takes place again then administration can define the definitions to filter the packets and decide whether to stop the packets or to forward the packets to the server or to the next hop to fulfill the asked requirements of the sender or previous hop. Here the database is centralized.

VII. PERFORMANCE ANALYSIS

The performance of the system is analyzed. A stable configuration is needed between the IDS and IPS for better and efficient performance.

IDS is configured in such a way that it detects any minor suspicious activity entering the system and make report of it. IDS scan all packets that come through and harmless packets are sent normally, however, any packets with minor suspicious protocol are marked as warning and an alert is sent to the admin. Packets that have high threats are dropped and blocked then and there.

The Analysis Engine analyses the type of attack (if any) and uses the Knowledge Database (dB) to create a response. This response along with a report of the input packet is sent to the IPS that does the prevention work.

IPS gets these reports and response and if threat is detected it does one out of the following:

- It drops the malicious packets that it obtained by analyzing the given report.
- It blocks the IPs that is sending these malicious and suspicious packets and spammer are taken into full consideration.
- It alerts the admin over the threat if detected. This is mainly done when the harmful level is at a minimum.

The IPS then prevents the attack from taking place and a response of the respective request is sent back to the user. Thus, IDS and IPS should be properly configured for efficient performance.

VIII. FUTURE WORK

For future work, the recommended tasks that can be analyzed are the configurations that can bring more stability to IDS and IPS, hence, increasing the performance of the system.

IDS discard all highly harmful packets that it receives. Sometimes, some of these packets might not be harmful and might be treated as a malicious packet due to some configuration. IDS can be improved by configuring in such a way that it actually giving a warning and then discard because if that packet was a useful one then it can be requested again.

IPS can be improved by improving underlying interruption detection. The progression in application-level psychoanalysis should be more stabilized. It should stop giving more complicated reply and an addition of interruption avoidance into other security devices.

The whole system can be upgraded as a whole in order to bring more efficiency and increase performance as a whole. In now a day's world, attackers find various ways for intrusion. So the system should be upgraded as required, adding more and more types of attack and their respective solution on how to find and prevent it. In this way the whole system will remain efficient with time and will bring out the best performance it can. This will result in the most stable system for detecting and preventing any intrusion.

IX. CONCLUSION

Thus, we conclude our paper by stating that our project will not only bring more security, but, also provide protection from any type of intrusion. IDS and IPS together can become a very powerful tool when it comes to cyber security.

It will guard one's system from security breaches by detecting and preventing any malicious packets and suspicious protocols and protect the security of one's system. If the system is updated along with time and new types of attacks, then this system can become one of the most powerful tools in cyber security and help in stopping serious cyber crime. Thus, implementing IDS and IPS system will bring security, stability and act as a firewall and defender for a system by detecting and dropping any suspicious and malicious intrusions.

REFERENCES

1. Ahmad W. Al-Dabbagh, Yuzhe Li and Togwen Chen, "An Intrusion Detection System for Cyber Attacks in Wireless Networked Control System," IEEE, 2016.
2. Kun Zhi Liu, Rui Wang and Guo Ping Liu, "Tradeoffs between transmission intervals and delays for decentralized networked control systems based on a gain assignment approach", IEEE, 2015.
3. G.P Liu, "Predictive Controller Design of Networked Systems With Communication Delays and Data Loss", IEEE, 2010.
4. Konstantinos Gatis and Alejandro Riberio, "Optimal Power Management in Wireless Control Systems", IEEE, 2013.
5. Andre Teixiera, Iman Shames, Henrik Sandbag and Karl Hendrik Johnnason, "A secure control framework for resources limited adversaries," IEEE, 2015.
6. Hamza Fauzi, Paulo Tabuada and Suhas Diggavi, "Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks," IEEE, 2013
7. M. Pajic, S. Sundaram, G. J. Pappas, and R. Mangharam, "The wireless control network: a new approach for control over networks," IEEE Transactions on Automatic Control, vol. 56, no. 10, pp. 2305–2318, 2011.
8. R. Mangharam and M. Pajic, "Distributed control for cyber-physical systems," Journal of the Indian Institute of Science, vol. 93, no. 3, pp. 353–388, 2013.
9. I. Hwang, S. Kim, Y. Kim, and C. E. Seah, "A survey of fault detection, isolation, and reconfiguration methods," IEEE Transactions on Control Systems Technology, vol. 18, no. 3, pp. 636–653, 2010.
10. M. R. Davoodi, K. Khorasani, H. A. Talebi, and H. R. Momeni, "Distributed fault detection and isolation filter design for a network of heterogeneous multiagent systems," IEEE Transactions on Control Systems Technology, vol. 22, no. 3, pp. 1061–1069, 2014.
11. R. E. Skelton, T. Iwasaki, and K. M. Grigoriadis, A Unified Algebraic Approach to Linear Control Design. Taylor & Francis, 1998.
12. J. Han and R. E. Skelton, "An LMI optimization approach for structured linear controllers," in 42nd IEEE Conference on Decision and Control, vol. 5, Maui, Hawaii, USA, 2003, pp. 5143–5148.