International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S, October 2019

Intrusion Detection System for Detecting Cyber Attacks

A.Annamalai Giri , P Yogananda, Nithya.M

Abstract- The proposed topology for a wireless networked control system is learnt under several cyber-attack situations, and a distributed intrusion detection system (IDS) is created to see the presence of attacks. More particularly, the paper shows a modeling structure for the closed-loop control system with the IDS, and a computational method to create and compute the IDS. The computational procedure delivers a stable closed-loop control system with the IDS being sensitive to cyber-attacks. Also, a simulation example is used to demonstrate the application of the proposed procedure as well as its effectiveness.

Keywords: IDS, cyber physical system, WCN, FDI.

I. INRTODUCTION

The use of both wired and wireless communication networks in a closed-loop control system has been learnt in various horizons. Compared to wired communication networks, the use of wireless communication networks provides many benefits.

Several affiliated challenges also exist and need further research. One of the challenges is to avoid attackers and have increased security of the closed loop control system. Thus IDS is very efficient in keeping the attackers out. More specifically, in the existence of an intruder (or attacker), the components and the communicated information in the control system are subject to eavesdropping and manipulation which can affect its stability and performance. Many different types of attacks are described in, where the associated goals of the attacker are specified. For example, in a denial of service (DoS) attack, the attacker has an impact on communication channels such that communicated information between devices are blocked (i.e., a receiving device can no longer receive information from a transmitting device); in a replay attack, the attacker eavesdrops as well as influences communication channels such that transmitted information are retransmitted later and in a bias injection attack, the attacker influences communication channels such that other information is injected and transmitted to a receiving device. The security of control systems has also been learnt in different horizons.

Manuscript published on 30 October 2019.
***** Correspondence Author (s)
Dr. A.Annamalai giri, Professor in the Department of Computer Science and Engineering at Marri Laxman Reddy Institute of Technology And Management, Dundigal, Hyderabad, Telungana, India.
Mr. Yogananda.p, Lecturer in the Department of computer science & Applications, RJS First Grade College, Koramangala, Bengaluru, Karnataka, India.
M.Nithya, Assistant Professor in Sri Sairam Engineering College.

For example, the estimation and control of linear systems when an attacker corrupts sensors and actuators are addressed; the growth of model-based methodology for the detection of integrity attacks on the sensors of a control system is inquired and the problem of network control system resiliency under the presence of replay attacks is studied. Further, for a networked control system using wireless communication networks, the modeling and design and plan of a topology comprises of plant, controller and midway network systems were studied, where the topology builds on the idea of the Wireless Control Network (WCN) architecture (for more details on the WCN, see for example and associated references listed. However, the security of the topology was not considered. In this paper, the topology is addressed under the existence of cyber attacks on the communicated information in the topology.

II. LITRATURE SURVEY

Robert Mitchell et.al. analyzed the outcome of intrusion detection and response on the reliability of a cyber physical system (CPS) consisting of sensors, actuators, control units, and physical objects for controlling and shielding a physical infrastructure. We build up a probability model based on stochastic Petri nets to explain the behavior of the CPS in the presence of both malicious nodes exhibiting a range of attacker behaviors, and an intrusion detection and response system (IDRS) for detecting and responding to malicious events at runtime. Our results point out that adjusting detection and response power in response to attacker strength and behavior detected can considerably increase the reliability of the CPS. We report numerical data for a CPS subject to determined, random and insidious attacks with physical interpretations given.

Yilin Mo et.al ensured the security of systems based on supervisory control and data acquisition is a major challenge. The goal of this paper is to develop the model-based methodologies capable of detecting integrity attacks on the sensors of a control system. The effect of integrity attacks on the control systems is analyzed and countermeasures capable of exposing such attacks are proposed.

The main contributions of this paper, beyond the originality of the problem formulation, lies in enumerating the conditions of the possibility of the replay attack, and suggesting countermeasures that increase the probability of detection by conceding control performance. The techniques are shown and the theoretical results are affirmed using several sets of simulations.

Peng He et.al identified Intrusion detection is one of the most demanding tasks and of main concern in the cyber security field; however, traditional intrusion detection methodologies often are not successful to handle the difficult and vague network attack correlation tasks. We suggest the usage of semantic networks that build relationships among network attacks and help in automatically identifying and predicting related attacks.

Also, our technique can increase the accuracy in detecting probable attacks. Experimental results show that our Semantic Network using the Ander berg similarity measure performs better in terms of accuracy and recall compared to current correlation approaches in the cyber security domain.

III. PROBLEM OF STATEMENT

The IDS consists of distributed detectors that are located with the nodes of the network system, the actuator nodes of the plant system, and the input nodes of the controller system.

In future study, the design of an ID Swill is investigated for the closed-loop control system with its complete communication links as well as the design of the network and controller system along with the IDS.

IV. EXISTING SYTEM

We first present the reduction of the active duration of the Intrusion Detection System (IDSs) in the nodes of a MANET as an optimization problem.

The primary aim of the Intrusion Detection System (IDSs) is to observe the nodes in its neighborhood at a desired security level so as to detect any abnormal behavior.

Intrusion Detection System conserves as much energy, not distributed to neighboring nodes.

V. PROPOSED SYSTEM

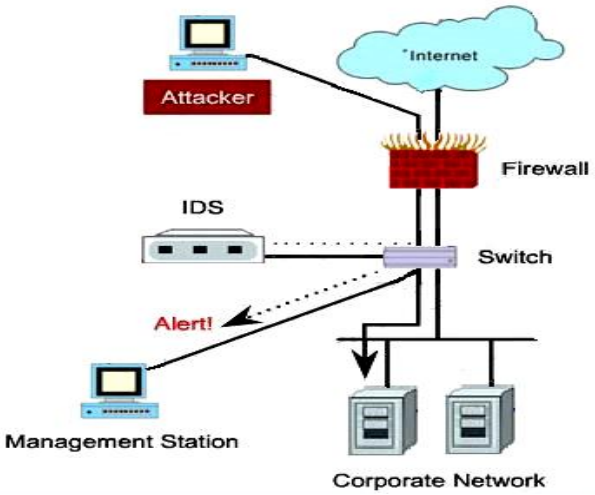
A distributed IDS is suggested for the topology discussed in and it is executed by inserting IDS in each node of the network system actuator node of the plant system and input node of the controller system.

This is sensible since each node has the ability of performing computations. Also it allows for distributing the detection tasks such that each node can only detect an attack on the transmitted information from the neighboring nodes and hence, an attack on the neighboring node. The plan of a detector for the presence of cyber-attacks can be associated to the design of a detector for fault detection and isolation (FDI).

Secure control systems Distributed detection the proposed procedure as well as its effectiveness.

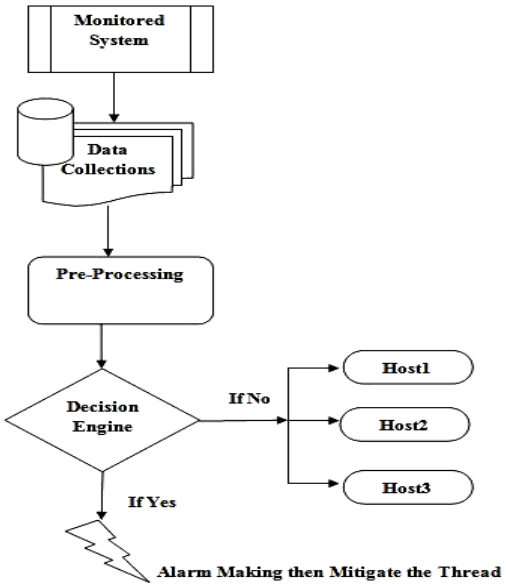
VI. PROPOSED SYSTEM TECHNIQUE

Intrusion Detection System (IDS) is intended to be a software application which observes the network or system behavior and discovers if any malicious operations occur. Tremendous increase and usage of internet raises concerns about how to safe guard and communicate the digital information in a safe and secure manner. Nowadays, hackers use various types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms aid to detect these attacks.



Intrusion Detection System Architecture

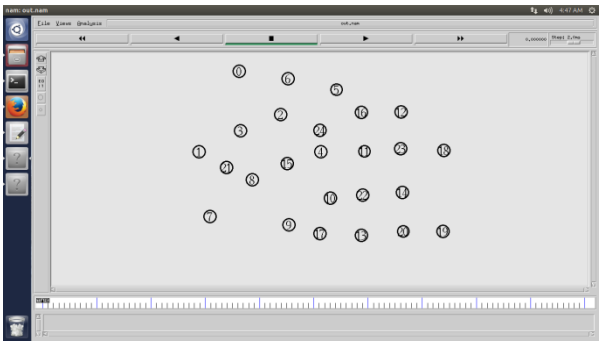
The contributions of the paper are summarized as follows: a distributed IDS to detect cyber attacks in the closed loop control system is proposed; a modeling framework for the closed-loop control system with the IDS is presented; and a design process for the computation of the IDS under a maximum number of cyber attacks on the communicated information is discussed. Further, a simulation example is illustrated to demonstrate the effectiveness of the IDS in detecting cyber attacks.



MODULES

Node Initialization:

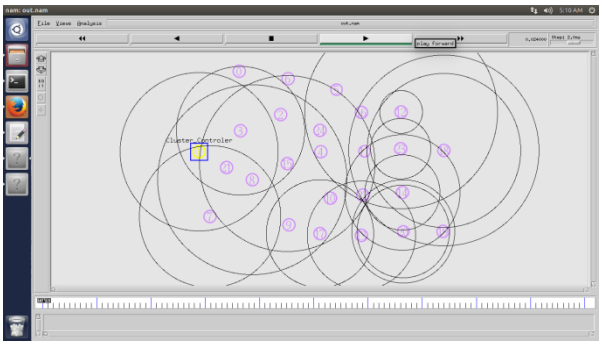
The below diagram is the NAM (Network Animator). Which is the output obtained from the graph . The output is obtained by calling command ‘ns’.



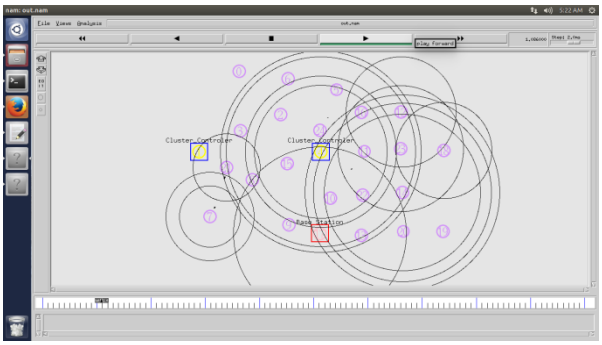
Here the nodes are just declared and positioned in accordance with x and y coordinates.

Node Communication:

Here the pink nodes are normal nodes and the yellow node is the controller.



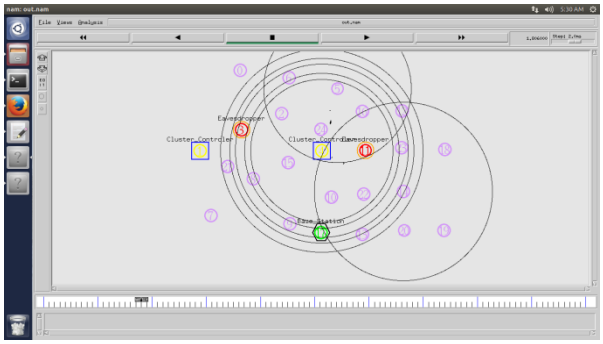
Basic node communication happens in this stage. Node communication is denoted by the circles.



Here the yellow nodes denote that they are controller and the red node is the base station. The collective information is sent to the base station.

Eavesdroppers:

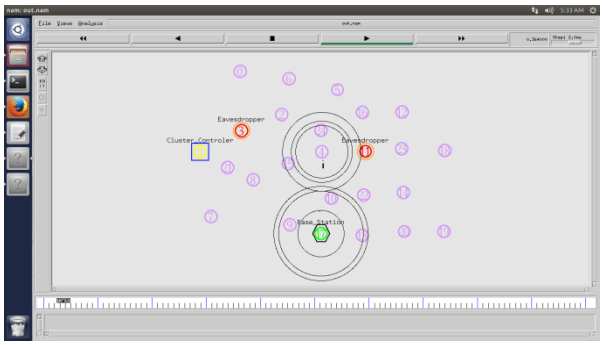
Here the communication is intercepted secretly by an attacker node, this is eavesdropping.



DoS attack, where the attacker blocks the transmission of information between the transmitting and receiving nodes; a replay attack, where the attacker eavesdrops and records transmitted information, and replays the information at a later time; and a bias injection attack, where the attacker injects values into the transmitted information to manipulate the information.

IDS Alarming:

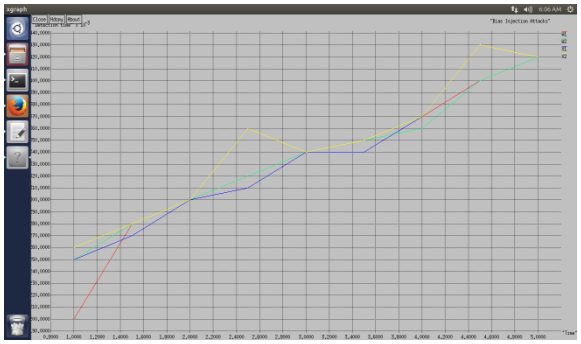
This step happens after monitoring data collection and pre processing. The decision raises an alarm if the decision engineer is a yes and sends messages to host if it’s a no.



Therefore the system is secure and there are no threats or cyber attacks that can harm our system.

Bias Injection:

A bias injection attack is where the attacker injects values into the transmitted information to manipulate the information.



Time Samples:

Closed loop control system uses IDS methodologies and shows us how many attacks occur in our system in a particular given time period.

VII.FUTURE ENHANCEMENTS

The investigation of using more advanced techniques, such as state estimation and filtering, into the functionality of the nodes and detectors; considering noise and disturbance, and frequency specifications of the attacks; and the design of the detectors while accounting for performance actions in addition to the stability of the closed-loop control system are topics for future research for interesting methods for possible application.

VIII. CONCLUSIONS

The paper discusses the aim of a distributed intrusion detection classification for a proposed topology for a wireless networked control system. The IDS consists of distributed detectors that are placed with the nodes of the network system, the actuator nodes of the plant system, and the input nodes of the controller system. In future study, the design of IDS will be investigated for the closed-loop control system with its entire communication links as well as the design of the network and controller system along with the IDS.

REFRENCES

1. Alvaro A. Cárdenas, Saurabh Amin , Zong-Syun Lin , Yu-Lun Huang , Chi-Yen Huang† and Shankar Sastry, Fujitsu Laboratories of America , University of California, Berkeley , National Chiao Tung University, Taiwan" Attacks Against Process Control Systems: Risk Assessment, Detection, and Response"-2011.
2. Yichi Zhang The University of Toledo."Distributed intrusion detection system in a multilayer network architecture of smart grids" 2011
3. International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 DOI: 10.5121/ijnsa.2012.4208 109 "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM" Lecturer, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh.
4. "Mutual information-based feature selection for intrusion detection systems" Fatemeh Amiri a,n , Mohammad Mahdi Rezaei Yousefi a , Caro Lucas a , Azadeh Shakery b , Nasser Yazdani b a Center of Excellence, Control and Intelligent Processing, School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran b School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran-2011.
5. IEEE TRANSACTIONS ON RELIABILITY, VOL. 62, NO. 1, MARCH 2013 "Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems Robert Mitchell and Ing-Ray Chen", Member, IEEE.

AUTHORS PROFILE

Dr. A.Annamalai giri received the Masterr of Technology degree from the Sathyabama University Chennai, India in 2007 and the Ph.D. degree from Mononmanium Sundaranar University, Thirunelveli,Tamilnadu, India. He worked as assistant professor in Sapthagiri college of engineering and various colleges in Bangalore. He is currently working as a Professor in the Department of Computer Science and Engineering at Marri Laxman Reddy Institute of Technology And Management,Dundigal,Hyderabad,Telungana, India. His research interests are in Image Processing, Software Engineering, Mobile Computing and Cloud Computing. Dr. A.Annamalai Giri has published more than 30 papers in the Journals and conferences of repute. He serves as IQAC Director, Selection panel, Academic committee member and resource person in various conferences. He is a life time member of IEANG, ISTE.

Mr. Yogananda.p received Masters of Computer Applications degree in 1998 from Osmania University,Hyderabad. He is currently working as Lecturer in the Department of computer science & Applications, RJS First Grade College, Koramangala, Bengaluru,Karnataka,India. He is pursuing PhD From Annamalai university ,Tamilnadu. His research interests include Data Mining,AI, Machine learning. He has published more than 5 papers in the Journals and conferences of repute.

M.Nithya is currently working as Assistant Professor in Sri Sairam Engineering College. She completed B.Tech Information Technology in Bharathidasan University in 2005. Completed M.E in Computer science in Sathyabama University in 2008 and completed Ph.D (" Medical data Extraction akin to privacy") In Sathyabama Institute of science and technology in 2019. Nithya.cse@sairam.edu.in