© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

A Novel Method for Resilient Networked Industrial Control System Security

M. Umashankar
Department of MCA, Sona College of Technology, Salem, Tamilnadu, India

ABSTRACT

Current Industry processing is using the digital data which are coming from different geographical location and different environmental resources with the help of internet. Here no one can be trusted and it is possible more than a few kind threads come from different directions. Multidimensional approach to the network security is the only way able to crash these challenges. Diffusion methods or canned attacks which are recommended by the conventional network security system are outdated and impractical. It is essential to create a new resilient architecture that can survive the different types of attack and then need the speedy recovery if a breach does occur. Resilient Industrial networked control system is very important for every organization which is using a number of decisive infrastructures. Proposed method provide a framework of the control system application to build effective security mechanism that integrate all aspects of cyber security, incorporating desktop and business computing systems with industrial automation and control systems through a novel attack resilient algorithm. This paper to recommend the path to reduce the complexity of the control system and provide the safety mechanism for reliable system which is decreased the threads and increase the data integrity with privacy in all kind of organizational processing.

Keywords: Wireless security, resilient control system, cyber security, data fusion, integrated system.

I. INTRODUCTION

Today's competitive industry marketplace, the companies have demand to improve their process efficiency. Using the low cost industrial automation system with intelligent is to improve the productivity. Here the collaborative integrated system acts a very big role with the functions of self-organization, rapid deployment, flexibility, and inherent intelligent-processing. Resilience is the ability to maintain acceptable levels of operation in the presence of abnormal conditions. A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. The foundation of resilient design needs the determination of proper operation requires for contemplation of all threats and measures. Measures can be categorized as cyber and physical security, process efficiency and stability, and process compliancy. Recent research in resilient has focused in two different areas such as organizational and information technology. Organizational resilient is the ability to survive in the face of threats, Information technology resilient is defined the stability and quality of service to face the threats in the computing and networking. The Primary things of a resilient control system is feedback control loop, it may be hosted on different communicating environment includes displays, transformers, transmitters, logical processors. These are the elements are used to build the optimized interactions of the various resources present in the architecture which is specially designed by the organization. Data fusion is a promising technology, concerning the problem of how to fuse data from multiple sensors in order to make a more accurate estimation of the environment. It plays a vital role in the fields of environment monitoring, automatic target detection and tracking, battlefield surveillance, remote sensing, global awareness, equipment maintenance, energy management, etc. With the help of the automatic fusion and interpretation of the information generated by large-scale sensor networks, resilient control systems do to their job fruitfully. In data aggregation we limit the processing of raw data to reduce the amount of communication and improve the communication efficiency and also minimize the traffic load.

Developing a Wireless sensor Networks for industrial applications required a combination of expertise from different disciplines. While designing a resilient controlled system for an industry to see the trust control, authentication, privacy, robustness, secure routing, group management, secure data aggregation and intrusion detection. Securing the communication is the main focus of academia and industry so they design and develop new kind of security mechanism frequently. With the help of IT- security methods literatures and their features new applications are enhanced their security. The security goal of the industrial control system is to protect the transactions from intentional assaults. Here we need to preserve the data integrity is more important because the data comes from deferent devices which are having operationally different characteristics and process in real time. Sometimes the required data is invalid if it arrived too late so we must keep timeliness and stale data should be detected. Most of the operational data received from the sensors through the communication channels; here the possibility of the compromising sensor data and forge messages is high. In this research we give the importance to the protocol specification which is used to avoid the integrity attacks. During the DoS attack on a sensor a controller stops getting new measurements. As an outcome, the controller will be generating control commands based on the last received reading. Multiple strategies can be applied here to identify the falsify sensor data. Based on our analysis we found that the sensitivity control loops to integrity attacks are varies so the different type of safety mechanisms can be recommended for different type of resources. Our analysis helps do discover the possibilities of cyber attacks also. The design of any resilient control system is a single control structure it capable of accommodate all operational and communicational objectives and should be find the expected operational and communicational disturbances.

A Resilient control systems is a Networked control system used for critical infrastructure systems which is very much required to detect the component failures, human errors and capable to face the problems from natural disasters, malicious attacks and environmental changes. With help of several design considerations resilient control system can predict incipient failures and take preventive actions to prevent the situation from getting worse. System should be designed to take the right action at the right time. Using the feature of networked control system any fault or accident happened in any one subsystem immediately another subsystem to take needful action and the information of measurements and decision making is passed between subsystems. A sensible and significant design deliberation associated to the networked control system is taking apart of communication links of control systems and the communication links of protect systems. As the safety systems have to be extremely reliable that do not allow packet loss and long time delays. Universal security issues with wireless communications is the attackers revealed wireless communications points can control the wireless networks and take advantage for broadcasting, restricted access controls, lack of encryption, and limited network segmentation. These kind of unauthorized access into the control domain can afford an attacker can bypassing security components and do anything in the network. So it is necessary to make the architecture more robust and improve the security in such environments.

II. RELATED WORKS

A resilient control system is a new standard that encompasses control design for cyber security, physical security, process competence and strength, and process fulfillment in the complex systems. RCS is defined as a control system that maintains status responsiveness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. The resilient system design is primarily dependable on computing with fault tolerant control, it has been argued in [1] that dependable computing views malicious faults as a source of failure, but does not consider the effect of these faults on the underlying physical processes in a large-scale complex system. Emphasizes a holistic cross-layer philosophy for developing security solutions and provides a game-theoretical approach to model cross-layer security problems in cyber physical systems [3]. Different types of disturbances at different layers of the system to be designed with game theoretic frame work [4].

Cyber security is an essential component of resilience of control systems a hybrid system model is created by[5]. [29] Proposed a state estimation with a bank of observers combined through median operations and the estimated states asymptotically converge to the true state despite attacks on sensors. The cyber security of control systems has received increasing attention. The research effort has been devoted to studying two aspects: attack detection and attack-resilient control. Regarding attack detection, a particular class of cyber attacks, namely false data injection, against state estimation is studied in [19], [20], [21].

In [9], a network level configuration of security devices has been addressed by considering the interdependence of devices in the network. As control systems become more decentralized, the ability to characterize interactions, performance and security becomes more critical to ensuring resilience [12].Multiple heterogeneous devices are able to communicate and interact with each other to achieve common goals[14] where cyber and physical components are tightly coupled and intertwined. In [15] application-specific models may provide structural properties that can be leveraged to develop efficient algorithms, as was recently shown for electric power systems. Health care security with resilient system discussed in [18]. Cyber-attacks on control systems compromising measurement and actuator data integrity and availability have been considered in [16]. The paper [23] studies the detection of the replay attacks, which maliciously repeat transmitted data. In the context of multi-agent systems, the papers of [24], [25] determine conditions under which consensus multi-agent systems can detect misbehaving agents. As for attack-resilient control, the papers [26], [27] are devoted to studying deception attacks, where attackers intentionally modify measurements and control commands. Energy efficient data fusion voting scheme developed efficiently for wireless sensor network security [30].

III. PROBLEM IDENTIFICATION

Recent digital era give more advantage to the industrial process, at the same time give added complexity. Operations could be fully or partially automated, sure it will give efficiency. Due to the lot of digital information generates by the organizational process make the confusion to the human operator who are responsible for the particular processing element. Integrated Control systems could be received the input data might be coming from different resources, different geographically locations and different networks. In this scenario the attackers having a chance to discover any one of the communication point, can influence the internal architecture of the network and take this advantage to do their misbehaving activities. Therefore it is necessary to increase the security in such a environments. Nature of the resilient control system becomes more decentralized. Have the ability to characterize the intercommunications, produce the high performance secure results. Help this capability the system very reliable to implicit redundancy and diversity. Key feature of a resilient control system is able to maintain state awareness and acceptable performance under unexpected events. Using of standard communication technologies, to enable access to remote devices and to facilitate a smooth interface between devices from different vendors as a result the number of possible attack points for malicious fake agents to exploit has significantly increased. Resilient networked control system design complement conventional contemplation of reliability and trustworthy computing, which are well established research domain. However while reliable design must be consider the attributes that are particular to networked control system with no meticulous focus on the use of the specific platform operations and communications.

IV. PROPOSED SYSTEM

This research focused on the security and efficiency of the control system which is required by the different kind of organizations recently. This Paper proposed a new integrated system should be able to understand the consequences of an attack and to build effective security mechanism that integrate all aspects of cyber security, desktop and business computing systems incorporating with industrial automation and control systems. New system to provide guidance for securing control systems, including acquisition which is used to collect the control information through different data resources, it is focused to provide more resilient to the friendly human. System design having distributed controlled environment to perform different control functions. It provides topologies and architectures to identify known threads and vulnerabilities and recommended security measures to mitigate the associated risks.

Architecture of the system includes a control server which is placed at a control center, communication components, remote terminal units which are controls and monitors the sensors. Here the control server is the centralized processing element to store and process the data which are received from different data resources of the organization. Processed the information and data are transfer between the control server and the different Input /output units with the help of communication lines. With the help of the Intelligent electronic device and proactive rely the system may communicate directly to the control server. Specialized software used to intimate what kind of process monitoring required and when it is needed and where it is required and informed the level of acceptable values and parameters. Different assessment approach has been designed to monitor the process with the disparity privacy requirements needed by the centralized control system. As an integrated control architecture to control multiple and integrated sub-systems used to control the information of a localized process. System can focused on the automated control of a process within an organization and geographically isolated systems or processes. The technology that used in this system to permit the user to collect data from one or more remote facilities and/or send limited control instructions to those facilities. To make use of MAC address filtering on the access points that permits only those stations with Ethernet MAC sub layer addresses on a list contained within the access point to communicate with the access point. According to the input data and the MAC, the control server releases the error free and authenticated aggregation outputs, which can protect the privacy from malicious adversaries

Required cyber security should be well planned and communicated with the subsystems it prevent and resolved the potential faults. The estimations and control algorithm are used to visible the attacker, intrusion detection algorithm can used to detect malicious components and send these details to the resilient control algorithm , to provide the verification and validation tools to check the potential vulnerability. Proposed system implements efficient control strategies with real time data on production operations, combined with communication protocols and increased connectivity to outside of the organizations improve the safety, and reduce the cost of the operation.

V. CONCLUSION

This paper discuss the problem of resilient control system security, it provide a framework of the control system application. Here it is recommended the way to reduce the complexity of the control system and provide the safety mechanism for reliable system which is decreased the threads and increase the data integrity in cyber world. Proposed method requires the system acquired the data from every sensor and wireless devices which are supply the data for organizational operations. Proposed method gained the computational efficiency; it is used to secure not only the data and also the operations which are processed by the organizational processing elements. Proposed a novel measurement residual and secured algorithm which can be investigated and calculated the effect in real time used to protect manipulation and distributed attack. In addition the control algorithm is relevant to maintain the privacy for private information system should provide adequate levels of controlling mechanism to handle different attacks.

VI. REFERENCES

[1]. C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: Next generation design research," 2nd Conference on Human System Interactions, Catania, Italy, pp. 632 636, May 2009.

[2]. C. G. Rieger, "Notional examples and benchmark aspects of a resilient control system," 3rd International Symposium on Resilient Control Systems, August, 2010.

[3]. Q. Zhu, C. Rieger and T. Bas¸ar, "A hierarchical security architecture for cyber-physical systems," in Proc. of the 4th Intl. Symposium on Resilient Control Systems (ISRCS), Boise, ID, Aug. 9 - 11, 2011.

[4]. Q. Zhu and T. Bas¸ar, "Robust and resilient control design for cyberphysical systems with an application to power systems," in Proc. Of 50th IEEE Conference on Decision and Control and European Control Conference (CDC/ECC), Orlando, Florida, Dec. 12 - 15, 2011.

[5]. Q. Zhu and T. Bas¸ar, "A dynamic game-theoretic approach to resilient control system design for cascading failures," in Proc. of International Conference on High Confidence Networked Systems (HiCoNS) at CPSWeek 2012, in Beijing, China.

[6]. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bas¸ar, J.-P. Hubaux, "Game theory meets network security and privacy," Accepted and to appear in ACM Survey, 2012.

[7]. Q. Zhu and T. Bas¸ar, "Indices of power in optimal IDS default configuration: theory and examples," in Proc. of 2nd Conference on Decision and Game Theory (GameSec 2011), College Park, MD, USA. Nov. 14 - 15, 2011.

[8]. Q. Zhu and T. Bas¸ar, "Dynamic policy-based IDS configuration," in Proc. of 48th IEEE Conference on Decision and Control (CDC), Shanghai, China, Dec. 2009.

[9]. Q. Zhu, H. Tembine and T. Bas¸ar, "Network security configuration: a nonzero-sum stochastic game approach," in IEEE Proc. of 2010 American Control Conference (ACC), Baltimore, MD, 2010.

[10]. Craig G. Rieger†, Senior Member, IEEE, David I. Gertman†, Miles. A. McQueen†, Member, IEEE †Idaho National Laboratory, Idaho Falls, Idaho, USA, Next Generation Design Research

[11]. H. B. Mitchell, Multi-Sensor Data Fusion, Springer-Verlag, Berlin, 2007.

[12]. S.P. Meyn, Control Techniques for Complex Networks, Cambridge University Press, New York, NY, 2008.

[13]. E. Hollnagel, D. D. Woods, and N. Leveson, Resilience Engineering: Concepts and Precepts, Ashgate Publishing, Aldershot Hampshire, UK, 2006.

[14]. Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The internet of things:A survey. Computer Networks, 54(15):2787–2805.

[15]. K. C. Sou, H. Sandberg, and K.H. Johansson. 2013b. On the exact solution to a smart grid cyber-security analysis problem. IEEE Transactions on Smart Grid, 4(2):856–865.

[16]. A.A. Cardenas, S. Amin, and S.S. Sastry. 2008b. Research challenges for the security of control systems. In Proceedings of the 3rd USENIX Workshop on Hot Topics in Security.

[17]. A. A. Cardenas, S. Amin, Z. Lin, Y. Huang, C. Huang, and S. S. Sastry. 2011. Attacks against process control systems: risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS.

[18]. M.Umashankar, "Privacy Preserving Healthcare System using secured cloud environment ", International Journal Of Engineering And Computer Science ISSN:2319-7242,Volume 6 Issue 6 June 2017, Page No. 21814-21817

[19]. F. Pasqualetti, R. Carli, and F. Bullo, "A distributed method for state estimation and false data detection in power networks," in Proc. IEEE Int. Conf. Smart Grid Communications, Oct. 2011, pp. 469–474.

[20]. A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in Proc. IEEE Int. Conf. Decision and Control, Atlanta, GA, Dec. 2010, pp. 5991–5998.

[21]. L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in Proc. IEEE Int. Conf. on Smart Grid Communications, Gaithersburg, MD, Oct. 2010, pp. 226–231.

[22]. Y. Mo and B. Sinopoli, "Secure control against replay attacks," in Allerton Conf. on Communications, Control and Computing, UrbanaChampaign, IL, Sep. 2009.

[23]. F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," IEEE Trans. Autom. Control, vol. 57, no. 1, pp. 90–104, Jan. 2012

[24]. S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," IEEE Trans. Autom. Control, vol. 56, no. 7, pp. 1731–1742, Jul. 2011.

[25]. M. Zhu and S. Martínez, "Attack-resilient distributed formation control via online adaptation," in IEEE Int. Conf. on Decision and Control, Orlando, FL, Dec. 2011, pp. 6624–6629.

[26]. M. Zhu and S. Martínez, "Stackelberg game analysis of correlated attacks in cyber-physical system," in Proc. American Control Conf., Jun. 2011, pp. 4063–4068.

[27]. M. Zhu and S. Martínez, "On distributed resilient consensus against replay attacks in adversarial networks," in Proc. American Control Conf., Montreal, QC, Canada, Jun. 2012, pp. 3553–3558

[28]. M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attack," 2013. [Online]. Available: http://arxiv.org/abs/1307.2790

[29]. Heegyun Jeon,1 Sungmin Aum,1 Hyungbo Shim,2 and Yongsoon Eun1 'Resilient State Estimation for Control Systems Using Multiple Observers and Median Operation " Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2016, Article ID 3750264, 9 pages http://dx.doi.org/10.1155/2016/3750264

[30]. Umashankar M and Chandrasekar C., "Energy Efficient Secured Data Fusion Assurance Mechanism For Wireless Sensor Networks", European Journal Of Scientific Research, Vol.49, No.3, pp. 455-463, February – 2011. ISSN : 1450-216X/1450-202X