Distributed Tracking for Fake Safety Management of Complex Dynamical Networks

[1]Tanveer Amena, [2]Mr. G. Praveen Babu

[1]PG Scholar, Dept of Computer Science, School of Information Technology JNTUH, Kukatpally, Hyderabad, Telangana, India

[2]Associate Professor, Dept of CSE, School of Information Technology JNTUH, Kukatpally, Hyderabad, Telangana, India.

Abstract : Complex dynamical networks are the main area of research at present. Complex networks have attracted increasing attention from various fields of science and engineering. Dynamical networks target the actual data that flows between endpoints, and the confidentiality and integrity of the data itself. Distributed tracking problem for complex Dynamical Networks are investigated using cyber-physical systems. Cyber-physical system refers to the integration of physical components as well as cyber-communication and computation processes. The two main aspects of complex dynamical networks are: Firstly, it focuses on exploring a network’s intrinsic statical characteristics and forming mechanisms. Secondly, the emergence of collective behaviours of complex networks has wide applications in the fields of military, aerospace, wireless communication, etc. In this project, the dynamical networks attacks are analysed by the resistance control system it performs uniquely throughout the system. It will cross check not only the key of the file but also the IP address of the user who is retrieving that file. Finally, a simulation example validating the main results is presented. Distributed intrusion detection is the interesting topic for complex cyber-physical networks to be done in future.

***IndexTerms*-**Complex Dynamical Networks,Cyber-Physical Systems,Resistance Control System, Distributed Intrusion Detection.

I. INTRODUCTION

Modern control systems are usually composed of observers, controllers, actuators, etc. These components exchange their obtained information to achieve specific control objectives, for instance, observers first observe the output information of the original system and transmit it to the controllers' side, then control inputs will be computed and transmitted to the actuators' side in order to be physically implemented. Noting that nowadays, wireless networks are becoming more popular and applicable than wired networks for such communicating purpose among these components. However, the involvement of wireless networks will make the entire control system becoming vulnerable to the cyber attacks, which may disrupt the normal information exchanges, degrade the systems' performance and even cause instability of the physical system. Thus, comprehensive thinking of physical infrastructures and cyber communication process should be emphasized. Complex cyber-physical network refers to a new generation of complex networks whose normal functioning significantly relies on tight interactions between its physical and cyber components. Many modern critical infrastructures can be appropriately modelled as complex cyber-physical networks. Typical examples of such infrastructures are electrical power grids, WWW, public transportation systems, state financial networks, and the Internet. These critical facilities play important roles in ensuring the stability of society as well as the development of economy. Advances in information and communication technology open opportunities for malicious attackers to launch coordinated attacks on cyber-physical critical facilities in networked infrastructures from any Internet-accessible place. Cybersecurity of complex cyber-physical networks has emerged as a hot topic within this context. Physical components affect communication and computation, while embedded computers in networks monitor and control the physical elements. The social and economic significance of complex cyber-physical networks is becoming increasingly prominent, so more and more investigations from various fields have been made on this attractive subject. For example, safety and efficiency of transportation systems will be largely improved when cyber- intelligence is incorporated into vehicles; networked control systems for buildings and factory equipments can contribute to energy saving by dynamically implementing the demand requirements. High reliability is one of the first issues to be considered and also one great challenging task in configurating complex cyber-physical networks in practice. The introduction of cyber-communication part also brings about an opportunity for malicious attacks invading into the cyber channels.

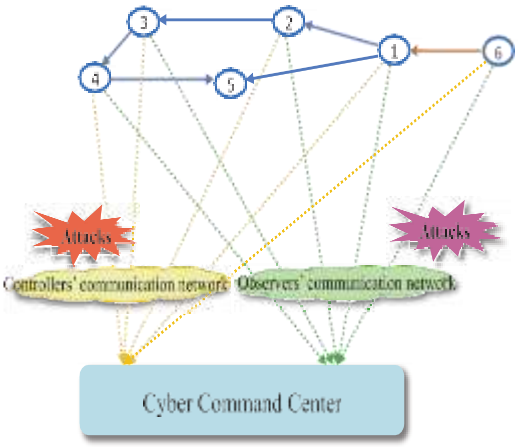
3
2
1
6
4
5
Attacks
Attacks
Controllers' communication network
Observers' communication network
Cyber Command Center

Fig. 1. complex cyber-physical network

Fig.1.is the Illustration of a complex cyber-physical network with 5 followers and one leader labeled as 6, where agent 1 is pinned by the leader. The agents are in the physical space while control and observation commands are generated from the cyber command center though two communication channels, which may be disrupted by malicious attacks. Differing from other studies of observer-based control problems for complex dynamical net- works and multi-agent systems, it considers here the scenario that the communication channels for controllers and observers may be subjected to frequently malicious attacks, which will destroy the communication links and result in disconnected topologies of the communication networks.

The main contributions of this paper can be summarized as follows:

- Consensus tracking problem of complex dynamical networks is investigated from the perspective of cyber-physical systems under a cyber attack scenario. There exists two spaces with physical components of agents in the physical space and a cyber command center in the cyber space. The information of these nodes are transmitted through communication channels to the cyber command center, and real-time control inputs will act on these agents. The complex dynamical network and cyber-physical network are synthesized under the framework proposed in this paper, which is quite different from most if not all existing works.
- The attacks are assumed to impact the communication channels for the controllers and the observers in an independent way. When an attack comes, it will destroy at least one link in a communication channel, which results in disconnectedness of the network.
- A Resistance Control System(RCS) algorithm is used to detect the IP address of the attacker.

II. RELATED WORK

Distributed control and optimization of multiagent systems (MASs) has attracted substantial attention in the past few years. Research of MASs has been partly motivated by the engineering benefits such as strong robustness, large flexibility, high efficiency, and low cost. However, there are still many challenging issues that need to be addressed. One interesting yet important issue in MASs is to devise communication protocols based only on the local relative information making states of all the agents converge to the same, which is known as the consensus problem. . To achieve consensus tracking in the considered MASs, a new class of observer-based protocols is proposed. More recently, a new kind of monitoring-based "reconstruction+repairing" resilient strategy was proposed for achieving pinning synchronization in complex cyber-physical networks against malicious attacks on nodes.Discrete-time multi-agent systems with lossy sensors was studied against cyber-attacks, where observer-based event-triggering consensus control was designed. The information received by observers is subjected to packet dropouts and cyber-attacks. Specifically, the control objective of the complex networks considered, focuses on consensus tracking for reference signals. Consensus problem is originated from automata theory and distributed computing with quite a long history. Due to their extensive applications, such as formation control of satellites and distributed sensor networks , consensus problems with cooperative control have attracted wide attentions ranging from physics to engineering in the past two decades. Consensus means that some specified states of individuals in a network reach an agreement, on which lots of interesting works have been reported. In real applications, since state information of nodes are unattainable or too costly to be obtained due to practical limitations, observers are often used to reconstruct the agent's states for the subsequent controller's design. The consensus control problem for linear multi-agent systems with discontinuous observations is investigated.

III. ALGORITHM

Input: Evolution of a network subject to attacks. Take Time =t ,*t*0 is the initial time and is set to be 0 .(T=t1, t2, t3,………. t_i).

Pi represents the system plant of agent *i*, $F_i$and C_i are the observer andcontroller for agent *i*, respectively. The output of agent *i* and those of itsneighbors are transmitted though observers' communication

Output: This equipment deals with the Dynamical Networks vulnerability of mobile applications by taking on the security checks required to establish a proper secure connection.

1. *t*0 is the initial time and is set to be 0. At time $\bar{\tau}_i$, the *i*-th malicious attack occurs. Agent i is attacked by some attacker.

2. Controller (Server) C_i get the attacker ip address and key, then he can easily block the attacker.

3. At time $\tilde{\tau}_i$, the attack is detected and the repair system is activated. Controller C_i and observer F_i are recognizes the network flow and block the particular attacker from the network.

4.$\bar{\tau}_i$is the time instant when the *i*-th attack has been cleared and the communication of nodes has been recovered. When the attacker is removed from the network the flow will be normal in the network.

IV. SYSTEM ARCHITECTURE

In the registration page, the user first creates an account with the PC name, IP address and the local port number. After login by the user with his/her correct credentials, a welcome page is visible where number of users who are in communication with each other by sending and receiving files is clearly indicated. A secret key is generated to encrypt the text message which is unique.

Attacker uses his/her port number and also the hacking port number and subsequently enters the secret key. The attacker demands for the original text. wherein, the secret key doesn’t match with the actual key,hence it is an unauthorized access.

To view the status for any hacker/attacker activities, we need to login to the server with the relevant credentials. A notification is shown that the attack has occurred. The server identifies the attackers port number and blocks it. As a result. the attackers account will be deactivated from the network. All such activities are stored in the server’s database for any post verification.

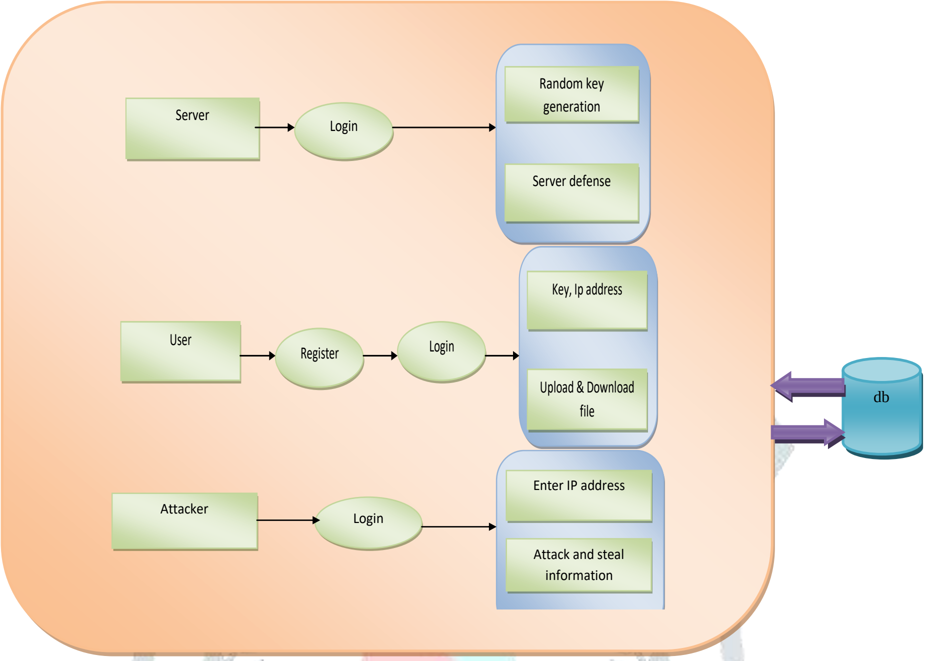

Fig.4. System Architecture.

V. EXPERIMENTAL RESULTS

Communication takes place in the network by sending and receiving packets with the help of generated secret key. Several experiments were conducted to identify threats by registering different users in a network. Wherein we observe man in the middle attacks, the attacker hacks the information by retrieving those packets. The server tracks the information and blocks the attacker/hacker’s port number and it is deactivated from the network. The Fig.5 shows the total number of users and the hackers detected in the network.

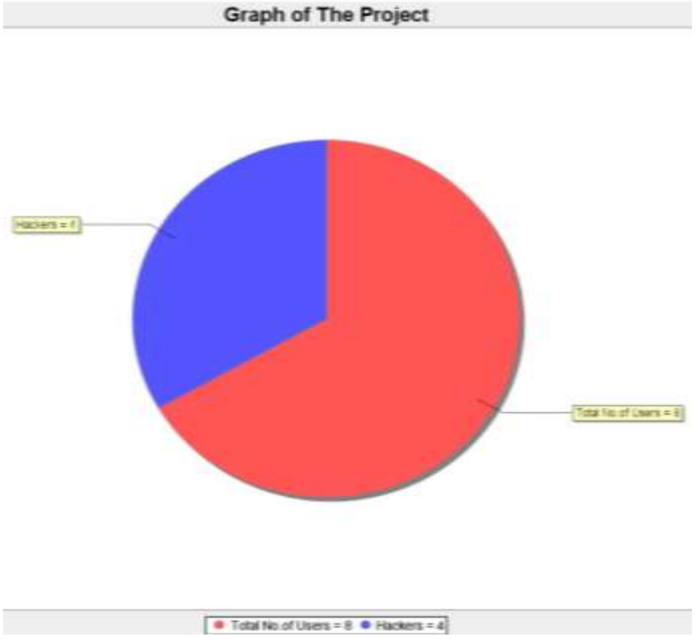

Fig.5. A graph shows the total number of users in the network and the hackers who tried to steal the information within the network.

VI. CONCLUSION

In this paper, a distributed observer-based cyber-security control problem for consensus tracking on complex dynamical networks is studied. The channels for transmitting control input signals and observation signals are assumed to be independent of each other and both can be destroyed by frequently occurred attacks. After the attacks have been detected by the network, a repairing mechanism will be activated until the communication topology is recovered. Assuming that only the relative observation information of the agents can be utilized, distributed observers are designed such that the states of the followers can be reconstructed. Combining the information of the distributed observers, a control protocol for regulating the followers to track the leader is then designed. Future works include investigations of cyber-security control for systems with state and input delays. In real applications, due to different environmental influences or implemented equipments, it is also important and practical to consider the heterogeneous case where A, B, C and function f are different for the followers. Furthermore, since input saturation nonlinearities are ubiquitous in physical and engineering systems, it is necessary to explore the consequences of input saturation in these systems in presence of cyber-attacks on their communication channels. Distributed intrusion detection and resilient distributed estimation are also interesting topics for complex cyber-physical networks.

VII. REFERENCES

[1] Z. Duan, J. Wang, G. Chen, and L. Huang, “Stability analysis and decentralized control of a class of complex dynamical networks,” Automatica, vol. 44, no. 4, pp. 1028–1035, Apr. 2008.

[2] S. H. Strogatz, “Exploring complex networks,” Nature, vol. 410, pp. 268–276, Mar. 2001.

[3] M. E. J. Newman, “The structure and function of complex networks,” SIAM Rev., vol. 45, no. 2, pp. 167–256, May 2003.

[4] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, “Complex networks: Structure and dynamics,” Phys. Rep., vol. 424, no. 4, pp. 175–308, Feb. 2006.

[5] R. Albert and A. Barabási, “Statistical mechanics of complex networks,” Rev. Mod. Phys., vol. 74, no. 1, pp. 47–97, Jan. 2002.

[6] X. F. Wang and G. Chen, “Complex networks: Small-world, scalefree and beyond,” IEEE Circuits Syst. Mag., vol. 3, no. 1, pp. 6–20, Sep. 2003.

[7] J. Lü, X. Yu, and G. Chen, “Chaos synchronization of general complex dynamical networks,” Phys.A, Statist. Mech. Appl., vol. 334, nos. 1–2, pp. 281–302, Mar. 2004.

[8] J. Liang, Z. Wang, and X. Liu, “Exponential synchronization of stochastic delayed discrete-time complex networks,” Nonlinear Dyn., vol. 53, no. 1, pp. 153–165, Oct. 2008.

[9] W. Yu, G. Chen, and J. Lü, “On pinning synchronization of complex dynamical networks,” Automatica, vol. 45, no. 2, pp. 429–435, Feb. 2009.

[10] J. Lu, D. W. C. Ho, and J. Cao, “A unified synchronization criterion for impulsive dynamical networks,” Automatica, vol. 46, no. 7, pp. 1215–1221, Jul. 2010.

[11] E. A. Lee, “Cyber physical systems: Design challenges,” in Proc. 11th IEEE Int. Symp. Object Oriented Real-Time Distrib. Comput. (ISORC), Orlando, FL, USA, May 2008, pp. 363–369.

[12] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, “Cyber-physical systems: A new frontier,” in Machine Learning in Cyber Trust. New York, NY, USA: Springer, 2009, pp. 3–13.

[13] S. K. Das, K. Kant, and N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure: Foundation and Challenges. Burlington, MA, USA: Morgan Kaufmann, 2012.

[14] G. Wen, W. Yu, X. Yu, and J. Lü, “Complex cyber-physical networks: From cybersecurity to security control,” J. Syst. Sci. Complex, vol. 30, no. 1, pp. 46–67, Feb. 2017.

[15] R. Mitchell and I.-R. Chen, “A survey of intrusion detection techniques for cyber-physical systems,” ACM Comput.Surv., vol. 46, no. 4, Apr. 2014, Art. no. 55.