International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1119-1125 www.ijaem.net ISSN: 2395-5252

# Control-Theoretic Stabilization Framework for Wormhole Attack on Network Control System

[1]A. Avina, [2]Dr.M.R.Geetha,
*Associate Software Engineer, Infoview Technologies, Chennai,*
*Professor, Department of ECE, Ponjesly College of Engineering, Nagercoil,*

Submitted: 15-10-2021 Revised: 26-10-2021 Accepted: 28-10-2021

**ABSTRACT—** A novel delay-distribution approach is proposed for continuous-time networked control systems (NCS) with time-varying transmission delays and transmission intervals based on an input-delay approach. The real-time distribution of input delays is modeled as a continuous dependent and non-identically distributed (d.n.d.) process. By introducing multiple indicator functions, the NCS is represented as a hybrid system with multiple input-delay subsystems. An improved Lyapunov-Krasovskii method is pro- posed and it additionally exploits the real-time distribution of input delays by means of estimating the cross-product integral terms in the infinitesimal of the Lyapunov functional using a new bounding technique. Delay-distribution-dependent sufficient con-ditions are derived for the deterministic exponential stability and stabilizability of the NCS, which leads to tighter bounds of input delays than existing results. The resulting controller design me- thod is formulated as an iterative linear optimization algorithm subject to linear matrix inequality constraints. Finally, numerical examples are presented to substantiate the effectiveness and ad-vantage of the results.

**Keywords—** Delay-distribution approach, networked control systems, transmission delays, transmission intervals.

## I. INTRODUCTION

Networking is the interfacing of two or more computing device with each other for the purpose of sharing data. Network control system has distributed sensors and actuators. Distributed embedded devices such as sensors and actuators that exchange sensed data and control signals via a wireless network and it forms a networked control system. By introducing and modifying delays in the communication network, the adversary can cause violations of the timing constraints that are critical in maintaining safe operation of real-time cyber-physical systems. The suggested framework models of wormholes have three interdependent components namely flow allocation by network nodes, delay characteristics introduced by wormholes, and mitigation algorithms employed by the network.

Adversary creates link between two regions of the network by using antennas. An adversary records message, observed in one region of the network and replays message in another region. To avoid the difficulty of estimating the probability density, under certain conditions, according to the similarity of the sample set sample space is divided into several subsets, indicating the quality of the clustering criterion function is maximized. Distributed network fault diagnosis model based on Bayes classifier suggested a distributed network fault diagnosis system model framework based Agent, the model for Bayesian classification theory of promotion. Model prior knowledge and observation data greatly improve the diagnostic performance of the system.

The centralized nodes nearest nodes are affected by byzantine attack. Computer network technology, making the function of network increase, promoting research on computer network reliability issues continue to depth direction of development. With the acceleration of information society, not only the user of the computer network on the increase, and the connection of regional and network connection of the computer network scale is rapidly expanding. As an important field of computer network is widely used in enterprises and institutions, bank, traffic, communication, industry, national defense, the complexity of the computer network of powerful or not and its structure proportion. The user dependence on computer network bigger, to the requirements of computer network becomes high, namely: the accurate, rapid, safe, convenient and reliable. Thus, we can see the importance of research questions the reliability of computer network and the urgency to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1119-1125 www.ijaem.net ISSN: 2395-5252

study the reliability of computer network has very important theoretical significance and practical value.

The wormhole attack, first introduced in the context of wireless routing, is one such attack that exploits the time delays and violates the timing constraints of the targeted system. In the wormhole attack, an adversary records messages observed in one region of the network and replays them in a different region. By doing so, the adversary creates a communication link between two end points in otherwise disjoint geographic areas. This can be accomplished by either compromised or colluding network nodes, known as the in-band wormhole or via a side channel such as high-gain directional antennas, known as the out-of-band wormhole. Unsuspecting network nodes will route network traffic through the wormhole. Once significant traffic starts flowing through the wormhole, the adversary can selectively drop or delay time critical packets in order to destabilize or degrade the system performance.

The formulation of dynamical system represents the network flow allocation, delays and packet drops at the wormhole link, and the mitigation strategies of the system, for out-of-band, in-band, and joint in- and out-of-band wormhole attacks. The overall flow allocation and delay are characterized by the interconnection.

- The delay characteristics of out-of-band wormhole links based on the rate at which the adversary drops packets traversing the wormhole link.
- The dynamical model integrates timing based mitigation mechanisms, such as the packet leash into our framework.

The control-theoretic framework is used for modeling and mitigating the wormhole attack on networked control systems. The suggested framework models the impact of wormholes, as well as the integration of existing mitigation strategies, on the allocation of network flows and resulting delays.

The rest of this paper is structured as follows: section II describes the related works and the existing systems. Section III describes the proposed system and discusses its different components in detail. Implementation and results are provided in section IV. Section V deals with the performance evaluation and conclusion is drawn in section VI.

## II. RELATED WORKS

This section deals with analyzing the existing system. It is the process of gathering information and diagnosing the problems in the existing system, then suggesting an idea for the improvement of the existing system.

In [5] P. Lee, A. Clark, L. Bushnell (2013) had Introduce control-theoretic framework for modeling and mitigating the wormhole attack on networked control system. Wormhole allows the adversary to violate the timing constraints of real-time control systems by delaying or dropping packets. In [10] J. T. Wen,M. Arcak (2013) describes the traffic between sources and links based on congestion. By using a passivity approach, the current nodes of stable flow controllers by the source and link update laws with passive dynamic systems. In [6] P. Kruus, D. Sterne, R. Gopaul (2014) Description of in-band wormholes, connect the neighbor via covert, multi-hop tunnels through the primary link layer. Identify the self-contained and extended forms of in-band wormhole. The in-band wormhole contains colluding nodes that can modify the time stamps using valid cryptographic keys, the out-of-band wormhole mitigation is ineffective and hence adds no delay to in-band wormhole links. The stability of the in-band wormhole enables us to characterize the average delay due to the wormhole in steady state. Stability of the network in the presence of the in-band wormhole is a result of the following proposition, which establishes the passivity of the wormhole link price. In [4] P. Lee, A. Clark, L. Bushnell (2014) A passivity-based control-theoretic framework for modeling and mitigating the wormhole attack. Under framework, the flow allocation of the valid nodes, the delays experienced on the wormholes, and the wormhole mitigation algorithms were modeled as distinct, interconnected passive dynamical systems. The passivity approach enabled to prove stability and convergence of the system to a unique equilibrium, which satisfies the criteria for the well-known War-drop equilibrium, under general assumptions on the adversary behavior and network mitigation mechanism. This allowed characterizing the delays experienced by source nodes at the steady-state.

## III. PROPOSED SYSTEM

This section describes the problem and the proposed system. Also the different components in the proposed system are discussed here.

**Problem ststement**

In this the wormhole attacks on a networked control system. Establish a link between two geographically distant regions of the network. The wormhole attack reroutes and replays valid message, it cannot using cryptographic mechanisms. The integration of existing mitigation strategy is the allocation of network flows and resulting delays. This model has three interdependent components, namely, flow allocation by network nodes, delay characteristics introduced by wormholes, and mitigation algorithms employed by the network. This

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1119-1125 www.ijaem.net ISSN: 2395-5252

framework is used for both out-of-band and in-band wormholes. In addition, using our framework, we are able to model, represent and mitigate complex wormhole attacks that simultaneously make use of both in- and out-of-band wormholes. For each case, prove that the flow allocation, wormhole delay, and mitigation components can be modeled as a passive dynamical system which allows the characterization of flow allocation and delay at the steady state. Since framework is in control-theoretic language, it enables ease of composition with control models of cyber-physical systems.

**Proposed Framework**

In proposed system the wormhole attacks on a networked control system. Establish a link between two geographically distant regions of the network. By using either high-gain antennas as in the out-of-band wormhole or colluding network nodes as in the in-band wormhole. The wormhole attack reroutes and replays valid message, it cannot using cryptographic mechanisms.

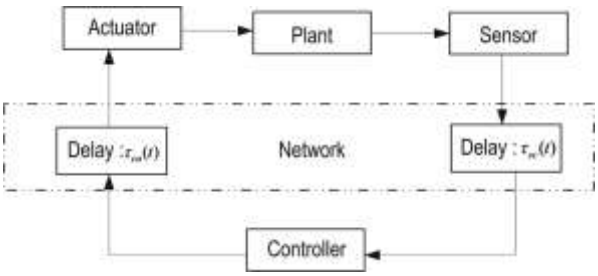


Fig 1 Proposed System

Passivity-based techniques have been used to model network flow control and derive novel flow allocation algorithms. The work of fits within the broader context of dual decomposition-based methods for designing network protocols as distributed algorithms for solving network optimization problems.

1. Network Model

Consider a wireless network of n nodes. Assume that two nodes can communicate directly if their positions are within the maximum node communication range. Denote the set of links by L, with |L| = L. In order to facilitate sensing and control of the system, network flows must be maintained between a set of source nodes S and destination nodes D. The ordered pair (Si,Di) denotes the source and destination of flow i. Assume that source Si maintains a constant rate ri, and that flows are originating from the set of sources. External flows that do not originate from S are not considered. Any source and destination pair that is not in direct radio range relies on multi-hop communication. Since the topology changes due to node sleep/wake cycles and nodes joining and leaving the network, each source Si uses a distributed routing protocol to identify a set of source-destination paths.

2. Adversary Model

The network is deployed in a hostile environment where one or more mobile adversaries are present.Assume that each adversary is capable of eavesdropping as well as recording and replaying eavesdropped messages, including routing protocol messages. By eavesdropping on routing protocol messages, the adversary determines the network topology. The adversary is also capable of physically capturing the unattended nodes. Once the adversary has compromised a node, the adversary can extract its cryptographic secrets. This enables the adversary to replace the captured node with a malicious node assuming the identity of the captured node. Malicious nodes are under the control of the adversary and are capable of colluding with other malicious nodes. Passivity-based techniques have been used to model network flow control and derive novel flow allocation algorithms.

3. Classifier Construction

The in-band wormhole is mounted using compromised nodes and their stored cryptographic keys, defenses against the out-of-band wormhole may be ineffective against in-bandwidth wormholes. The in-band wormhole, however, will incur longer delays than the out-of-band wormhole, since it relies on a multi-hop path of network nodes to forward packets. By performing statistical analysis, the network nodes can identify one-hop links with exceptionally long delays and/or packet-loss rates, which are then suspected of being wormhole links and ignored for routing purposes.

The passivity-based framework is used for modeling and mitigating out-of-band wormholes in a networked control system. The model considers the effect of the wormhole attack and mitigation on the delay and flow allocation of the network traffic. Develop a dynamical model for the flow allocation by the network nodes. Then model the delays

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1119-1125 www.ijaem.net ISSN: 2395-5252

experienced due to the out-of-band wormhole, followed by the effect of mitigation mechanisms. Lastly, consider the interconnection of these three dynamical models and characterize the flow allocation and delay at the unique equilibrium point via a passivity-based approach.

4. Delay Distribution Approach

Delay-distribution dependent sufficient conditions are derived for the deterministic exponential stability and stabilizability of the NCS, which leads to tighter bounds of input delays than existing results. The resulting controller design method is formulated as an iterative linear optimization algorithm subject to linear matrix inequality constraints. Finally, numerical examples are presented to substantiate the effectiveness and advantage of the results. The transmission delays and transmission intervals or packet losses in practice often degrade system performance and even lead to closed-loop instability. NCSs with time-varying transmission delays and intervals are also deemed as sampled-data systems under variable sampling with additional transmission delays. It is always an important problem for the NCSs to obtain sufficient stability/ stabilizability conditions with less conservatism to give tighter bounds on transmission delays, transmission intervals, and system performance.

5. Lyapunov-Krasovskii Method

Based on a delay decomposition technique, an improved Lyapunov-Krasovskii method exploit the real-time distribution of input delays in estimating the cross-product integral terms in the infinitesimal of the Lyapunov functional using a new bounding technique. With this Lyapunov-Krasovskii method, delay-distribution-dependent sufficient conditions are derived for the deterministic closed- loop exponential stability and stabilizability, and lead to tighter bounds of input delays than the ones. The resulting controller design method is also given, which is formulated as an iterative linear optimization algorithm subject to linear matrix inequality (LMI) constraints. Numerical examples are given to substantiate the effectiveness and advantage of the approach. The real-time distribution of input delays is in- corporate into the closed-loop model of the concerned NCS, which facilitates reducing the conservatism of the results using Lyapunov-Krasovskii method.

## IV. IMPLEMENTATION AND RESULTS

The finalized result model is categorized as following. Run the corresponding coding. First set the width and height of graphical user interface The delay for packets traversing the wormhole tunnel, equal to the time per packet transmission multiplied by the average number of retransmissions, is therefore given by pl =αl/(1 − Φl(rl)). In the user interface page, set the number of nodes, and fill the parameter to the corresponding nodes. The attacker node is only highlighted in order to identify the particular attacked nodes from various nodes. Malicious nodes are under the control of the adversary and are capable of colluding with other malicious nodes. Passivity-based techniques have been used to model network flow control and derive novel flow allocation algorithms. Thus the attacker node ‘f’, particular nodes path is resigned as destination and its IP address has been identified

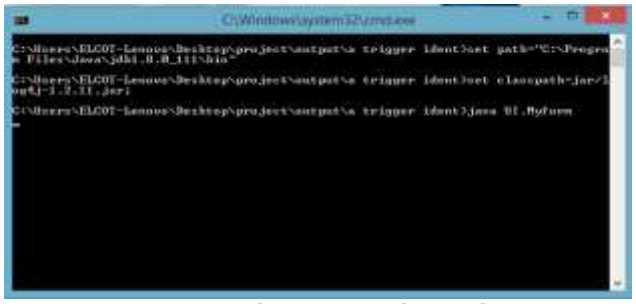

Fig 2 Run the corresponding code

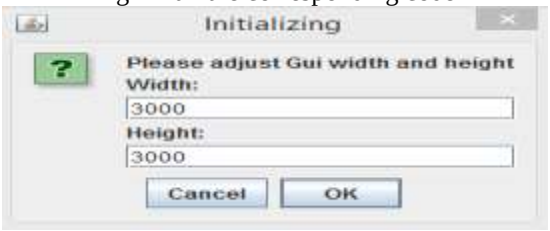


Fig 3 Initializing

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1119-1125 www.ijaem.net ISSN: 2395-5252

Fig 4 User interface page

Fig 5 Identifying attacker node

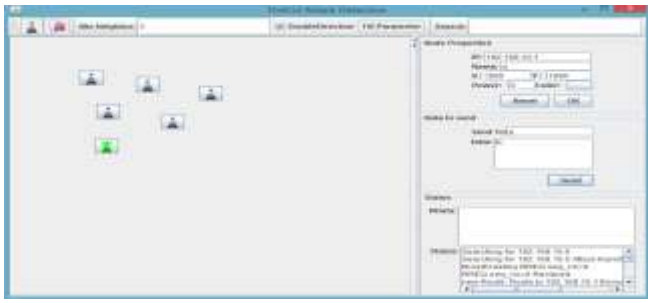

Fig 6 Attacker node is highlighted

Fig 7 Attacker node ‘f’

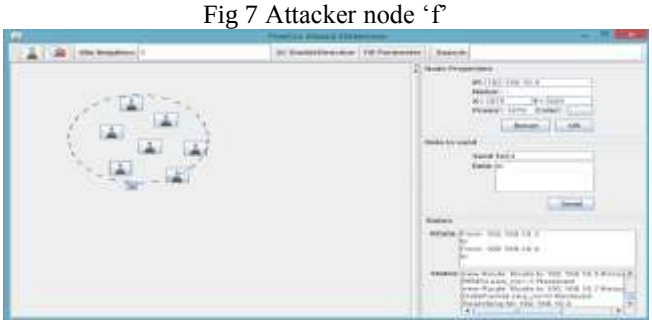

Fig 8 Preventing other nodes

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1119-1125 www.ijaem.net ISSN: 2395-5252

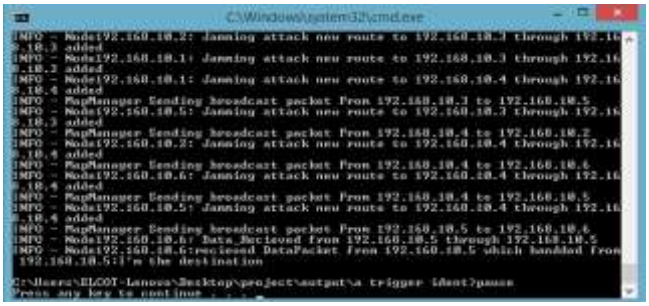

Fig 9 Identifying the IP address

## V. PERFORMANCE EVALUATION

In this section the performance of the proposed framework for Wormhole Attack on Network Control System was evaluated by calculating the processing time.

*a)* Result of two metrics

The evaluation use two metrics to evaluate our attacks precision and false positive rate (FPR) defined as follows:

Precision = True positive / True positive + False Positive

FPR = False positive / True positive + False positive

Each packet is assigned a packet leash chosen by the source, so that the packet is valid for time (R/c) + Δmax, where R is the propagation distance c is the speed of light, and Δmax is the maximum permissible value of the clock skew. When the packet traverses a wormhole, the packet violates the packet. The distances of the sender and receiver from the wormhole start and end points, respectively, and αl is the wormhole tunnel propagation time as in the previous section.

*b)* Time Model

The delay experienced by an out-of-band wormhole link is defined by the propagation time and the packet dropping rate. Hence, the negative feedback interconnection is globally asymptotically stable. The passivity based framework enables us to compose in-band and out-of-band wormholes and characterize the overall delay and flow allocation. The in-band wormhole contains colluding nodes that can modify the time stamps using valid cryptographic keys, the out-of-band wormhole mitigation is ineffective and hence adds no delay to in-band wormhole links. The in-band wormhole mitigation mechanism described in employed on the valid and in-band wormhole links. Since the out-of-band wormhole link is created using a high capacity, low-latency channel, the adversary can manipulate the delays in order to the statistical mitigation mechanism. Hence model of the impact of mitigation on the link delays are proved.

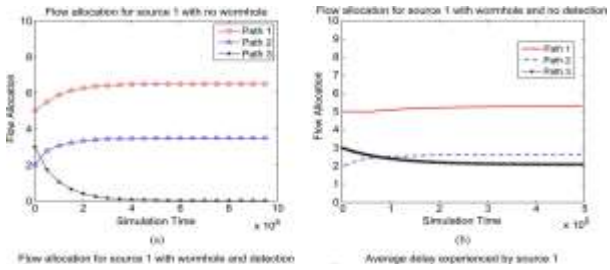

Fig 9 Proceesing Time

TABLE I. DETAILS OF NETWORK NODES

| Category | Avg | % of > 4 |
|---|---|---|
| Reachability Failure | 3.67 | 56.90% |
| Throughput/Latency | 3.39 | 52.54% |
| Intermittent Connectivity | 3.38 | 53.45% |
| Congestion | 2.65 | 28.07% |

| Category | Avg | % of > 4 |
|---|---|---|
| Security Policy Violation | 2.33 | 17.54% |
| Forwarding Loop | 1.89 | 10.71% |
| Broadcast/Multicast Storm | 1.83 | 9.63% |

## VI. CONCLUSION AND FUTURE ENHANCEMENT

The wormhole attack on a network control system, in which an adversary establishes a link between two geographically distant regions of the network by using either high-gain antennas, as in the out-of-band wormhole, or colluding network nodes as in the in-band wormhole. Wormholes allow the adversary to violate the timing constraints of real-time control systems by first creating low-latency links, which attract network traffic, and then delaying or dropping packets. Since the wormhole attack reroutes and replays valid messages, it cannot be detected using cryptographic mechanisms alone. The impact of the wormhole attack on the network flows and delays and introduce a passivity-based control-theoretic framework for modeling and mitigating the wormhole attack. Developing this framework for both the in-band and out-band wormhole attacks as well as complex, hereto-unreported wormhole attacks consisting of arbitrary combinations of in-and out-of band wormholes. By integrating existing mitigation strategies into framework, analyze the throughput, delay and stability properties of the overall system. Through simulation study, by selectively dropping control packets, the wormhole attack can cause disturbances in the physical plant of a networked control system, and demonstrate that appropriate selection of detection parameters mitigates the disturbances due to the wormhole while satisfying the delay constraints of the physical system. For the in-band case, simulation results suggest that detection mechanisms enable the source rates to converge to the same equilibrium regardless of the presence of a wormhole. The simulation results illustrate the tradeoff between the effectiveness of the network defense and the increase in delay for the out-of-band case. In particular, found that out-of-band wormhole causes large disturbances in the physical system by selectively dropping packets, and the parameters of packet leash defense can be chosen to reduce flow allocation to the wormhole while satisfying the delay constraint of the physical system. For the in-band case, simulation suggests that the network defense allows the system to reach the same flow allocation equilibrium regardless of the presence of wormhole. Though find that an adversary who creates an out-of-band wormhole can cause large disturbances on the physical plant by selectively dropping packets that are allocated to the wormhole link. In future work, would investigate whether the steady state values of our passivity framework arise as equilibrium of an equivalent dynamic game between the network and adversary.

## REFERENCES

[1] E. Altman and L.Wynter, “Equilibrium, games, and pricing in transportation and telecommunication networks,”2015
[2] Y.-C. Hu, A. Perrig and D. B. Johnson, “A defense against wormhole attacks in wireless networks”, 2014.
[3] Karlof and D. Wagner, “Secure routing in wireless sensor networks: Wormhole Attacks and Countermeasures”, 2017.
[4] P.Kruus, D. Sterne and R. Gopaul, “In-Band Wormholes and Countermeasures in OLSR Network”, 2014.
[5] P. Lee, A. Clark, L. Bushnell and R. Poovendran, “A passivity Framework for Modeling and MitigatingWormhole Attacks On Networked Control Systems”, 2013.
[6] P. Lee, A. Clark, L. Bushnell and R. Poovendran, “Modeling and Modeling Designing Network Defense against Control Channel Jamming Attack”, 2014.
[7] V. Mahajan, M. Natu, and A. Sethi, “Analysis of wormhole intrusion attacks in MANETs”, 2015.
[8] Poovendran and L. Lazos, “A graph theoretic Framework for preventing the wormhole attack in wireless ad hoc networks”, 2017.
[9] R. Song, P. C. Mason, and M. Li, “Enhancement of frequency-based Wormhole Attack Detection”, 2016.
[10] J. T. Wen and M.Arcak, “A Unifying Passivity Framework for Network Flow Control”, 2013.