DETECTING AND REDUCING THE EFFECTS OF AN ADVERSARIAL CORRUPTION OF SENSOR DATA IN LINEAR DYNAMICAL SYSTEM

Mandala Prathyusha[1], Kandula Neha[2]
[1]M.Tech, Department of CSE, [2]M.Tech, Assistant Professor, Department of CSE,
[1]Keshav Memorial Institute of Technology, Narayanguda, Hyderabad, Telangana, India.
[2]Vidya Jyothi Institute of Technology, Aziz nagar, Hyderabad, Telangana, India

ABSTRACT: Today's large-scale controls systems are present everywhere in order to sustain the normal operation of many of the critical processes that we rely on. In general control system one can identify different components including the actuators, the sensors as well as the controllers. These different components require communicating with each other; real-world attacks on control systems have in fact occurred in the past decade and have in some cases caused significant damage to the targeted physical processes. Secure state estimation is the problem of estimating the state of a dynamical system from a set of noisy and adversarial corrupted measurements. In this paper, we present a novel algorithm that uses a Satisfiability-Modulo-Theory approach to lessen the intrinsic combinatorial complexity of the problem.

Keywords: Dynamical System, Control System, Secure State Estimation.

I. INTRODUCTION

Cyber-physical systems integrate physical processes, computational resources, and communication capabilities. Examples of cyber-physical systems include transportation networks, power generation and distribution networks, water and gas distribution networks, and advanced communication systems. As recently highlighted by the Maroochy water breach in March 2000, multiple recent power blackouts in Brazil, the SQL Slammer worm attack on the Davis-Besse nuclear plant in January 2003, the StuxNet computer worm in June 2010, and by various industrial security incidents, cyber-physical systems are prone to failures and attacks on their physical infrastructure, and cyber attacks on their data management and communication layer. Concerns about security of control systems are not new, as the numerous manuscripts on systems fault detection, isolation, and recovery testify. Yet, these systems are suffered from specific vulnerabilities which do not have an effect on classical manage structures, as well as for which suitable detection in addition to identity techniques calls for to be evolved. For instance, the reliance on communique networks and preferred communique protocols to transmit measurements and control packets increases the opportunity of intentional and worst-case attacks against physical plants. On the opposite hand, statistics safety strategies, consisting of authentication, get admission to manipulate, and message integrity, seem inadequate for a great protection of cyber-physical systems. Certainly, these protection methods do no longer exploit the compatibility of the measurements with the underlying bodily manner or the manage mechanism, and they're therefore ineffective towards insider assaults targeting the bodily dynamics. The trouble of sturdy nation estimation in deterministic systems is considered in literature. For instance, the authors represent the variety of attacked sensors (and inputs) which may be tolerated while appearing nation estimation and recommend a deciphering algorithm to recover the nation. Next, Shoukry et al. Propose event primarily based algorithms to improve the performance of robust nation estimation. Additionally, Chong et al. Broaden schemes for sturdy estimation in deterministic continuous LTI systems even as formulating a notion of observability under attack. The trouble of strong estimation has additionally been considered in stochastic and unsure structures. For instance, Mishra et al. propose robust estimation schemes in the presence of Gaussian noise and characterize limitations in estimation performance in the presence of attacks. Nakahira et al. consider robust estimation with bounded noise, proposing a stable estimator in the presence of q attacks provided that the system remains detectable after removing any 2q sensors. Finally, Pajic et al. demonstrate the robustness of estimation schemes in the presence of attacks even when there is uncertainty in the system model.

II. RELATED WORK

Non-invasive attacks on cyber-physical systems pose considerable threats in conditions that may be, at instances, lifestyles critical. Such attacks are more difficult to locate at the sensor level and hence require better stage detection mechanisms. Using automobile anti-lock braking structures, we have verified each simplistic and advanced strategy of non-invasive assaults on sensor subsystems. The advanced attack illustrates a completely capable method for isolating sensors from the surrounding environment using outcomes from adaptive remarks manage idea earlier than injecting a spoofed signal. The proposed method has been evaluated for ABS sensors, wherein a small digital module is designed and carried out to expose the feasibility of the idea. Y. Shoukry, P. D. Martin, P. Tabuada, and M. B. Srivastava explored several factors of designing one of these modules, and effects acquired in real time from commercial ABS hardware lend credence to the efficacy of the assault and the hazard that comparable assaults pose.

For cyber-physical systems modeled via linear time-invariant descriptor structures, F. Pasqualetti, F. Dorfler, and F. Bullo have analyzed essential monitoring limitations. In unique, they have got characterized undetectable and unidentifiable attacks from a device-theoretic and a graph-theoretic angle. Additionally, F. Pasqualetti, F. Dorfler, and F. Bullo have designed centralized and disbursed monitors.

Raj Gautam Dutta, Xiaolong Guo and Teng Zhang introduce a challenge-response authentication primarily based approach for detection of varieties of assaults: the Denial of Service (DoS) and the delay injection, on lively sensors of self sufficient systems. The recursive least rectangular technique is used for estimation of sensor measurements while it's far below attack. With those expected measurements, safe manage inputs of the self reliant CPS are derived, which allows the system to recover and operate competently within the presence of attacks. A case have a look at changed into presented to expose resiliency of adaptive cruise manipulate gadget of ground car, leveraging their proposed solutions to counter those attacks. However, the detection technique fails whilst an adversary with ok resources can sample the incoming indicators from energetic sensors quicker than the defender. Their destiny studies will address this drawback and we can offer defence mechanisms to save you such adversaries from attacking lively sensors of independent structures.

While some earlier paintings centered at the unique instances of scalar machine and/or special shape at the attack signal, the paintings pronounced in this work makes a speciality of the case while the underlying gadget is multi-dimensional, prepared with multiple sensors and without assumptions at the knowledge of the time evolution of the assault sign. In such case, the secure country estimation trouble turns into a combinatorial hassle.

Another suite of algorithms also are proposed for the comfortable kingdom estimation without any formal guarantees on their correctness. For instance, a technique that is based on an on-line gaining knowledge of mechanism primarily based on approximate envelopes of accumulated data has additionally been recently pronounced. The envelopes are used to discover any bizarre behavior without assuming any knowledge of the dynamical gadget model. Other strategies are proposed and which robustification methods for country estimation towards sparse sensor assaults are proposed, once more and not using ensures on their correctness.

III. FRAMEWORK

Modern control systems rely on a networked infrastructure to exchange sensor information. Therefore, an adversarial attacker can corrupt sensor measurements by manipulating the data packets exchanged between various components, as has been investigated, for instance, in the context of smart electric power grids.

In this paper we focused on securely estimating the state of a nonlinear dynamical system from a set of corrupted measurements. In particular, we consider two broad classes of nonlinear systems, and propose a technique which enables us to perform secure state estimation for such nonlinear systems. We then provide guarantees on the achievable state estimation error against arbitrary corruptions, and analytically characterize the number of errors that can be perfectly corrected by a decoder. To illustrate how the proposed nonlinear estimation approach can be applied to practical systems, we focus on secure estimation for the wide area control of an interconnected power system under cyber-physical attacks and communication failures, and propose a secure estimator for the power system.

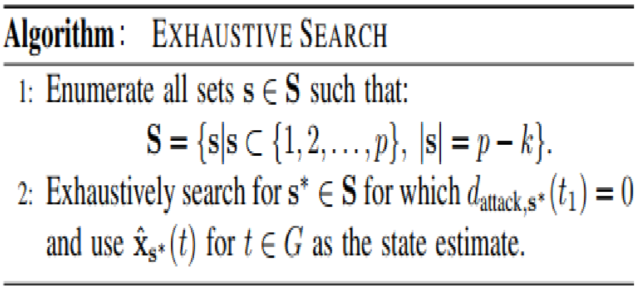
We alternative to techniques from formal methods to develop a sound and complete algorithm that can efficiently handle the combinatorial complexity of the state estimation problem; we show that the state estimation problem can be cast as a satisfiability problem for a formula including logic and pseudo-Boolean constraints on Boolean variables as well as convex constraints on real variables.

A. Optimal Secure State Estimation Problem

- Consider the linear dynamical system under attack Σa as defined, and a k-adversary satisfying assumptions are;
- A k-adversary can corrupt any k out of the p sensors in the system.
- The adversary's choice of κ is unknown but is assumed to be constant over time (static adversary).
- The adversary is assumed to have unbounded computational power, and knows the system parameters (e.g., A and C) and noise statistics.

However, the adversary is limited to have only causal knowledge of the process.

To solve this problem, we can implement an algorithm that is;



```
Algorithm: EXHAUSTIVE SEARCH
1: Enumerate all sets s ∈ S such that:
       $S = \{s | s \subset \{1, 2, \ldots, p\}, |s| = p - k\}.$
2: Exhaustively search for $s^* \in S$ for which $d_{attack,s^*}(t_1) = 0$
   and use $\hat{x}_{s^*}(t)$ for $t \in G$ as the state estimate.
```

IV. IMHOTEP-SMT SOLVER

IMHOTEP-SMT, a solver for the detection and mitigation of sensor attacks in cyber-physical systems. IMHOTEP-SMT receives as inputs a description of the physical system in the form of a linear difference equation, the system input (control) signal, and a set of output (sensor) measurements that can be noisy and corrupted by a malicious attacker. The output is the solution of the secure state estimation problem, i.e., a report indicating:

- The corrupted sensors,
- An estimate of the continuous state of the system obtained from the uncorrupted sensors.

Based on this estimate, it is then possible to deploy a control strategy, while being resilient to adversarial attacks. The core of our tool relies on the combination of convex programming with pseudo-Boolean satisfiability solving, following the lazy satisfiability modulo theory paradigm.

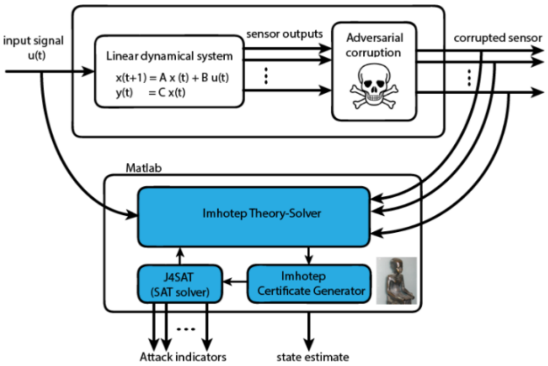


Fig1. Process of IMHOTEP-SMT solver

IMHOTEP-SMT is a unique solver that mixes results from formal strategies (Satisfiability Modulo Theories) and convex optimization to come across, in real time, if a fixed of sensor measurements amassed from a dynamical system is corrupted through an opposed assault. IMHOTEP-SMT is being applied to comfy country estimation for numerous programs, e.g. Robot, car, and aerospace cars, clever grids, industrial refinery. IMHOTEP-SMT currently supports systems that may be described via a linear dynamical model. However, in a close to future it'll be prolonged to some training of nonlinear systems.

IMHOTEP-SMT can always stumble on any compromised sensors inside the absence of measurement noise and while the numerical tolerance is 0.

V. CONCLUSION

We conclude that in this paper we proposed a sound and complete algorithm which adopts the Satisfiability-Modulo-Theories paradigm to undertake the intrinsic combinatorial complexity of the secure state estimation problem for linear dynamical systems under sensor attacks. At the compassion of our proposed SMT detector recline a set of routines that exploit the geometric structure of the problem to efficiently reason about inconsistency of sensor measurements as well as improve the runtime performance.

REFERENCES

[1] Y. Shoukry, P. D. Martin, P. Tabuada, and M. B. Srivastava, “Non-invasive spoofing attacks for anti-lock braking systems,” in Workshop on Cryptographic Hardware and Embedded Systems, ser. G. Bertoni and J.-S. Coron (Eds.): CHES 2013, LNCS 8086. International Association for Cryptologic Research, 2013, pp. 55–72.

[2] C.-Z. Bai and V. Gupta, “On kalman filtering in the presence of a compromised sensor: Fundamental performance bounds,” in American Control Conference (ACC), 2014, June 2014, pp. 3029–3034.

[3] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Sept 2009, pp. 911–918.

[4] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454–1467, June 2014.

[5] F. Pasqualetti, F. Dorfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[6] M. S. Chong, M. Wakaiki, and J. P. Hespanha, “Observability of linear systems under adversarial attacks,” in The 2015 IEEE American Control conference (ACC), 2015, accepted.

[7] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. Pappas, “Robustness of attack-resilient state estimators,” in ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), April 2014, pp. 163–174.

[8] Y. Shoukry and P. Tabuada, “Event-triggered projected luenberger observer for linear systems under sensor attacks,” in IEEE 53rd Annual Conference on Decision and Control (CDC), Dec. 2014.

[9] S. Farahmand, G. B. Giannakis, and D. Angelosante, “Doubly robust smoothing of dynamical processes via outlier sparsity constraints,” Trans. Sig. Proc., vol. 59, no. 10, pp. 4529–4543, Oct. 2011.

[10] C. Barrett, R. Sebastiani, S. A. Seshia, and C. Tinelli, Satisfiability Modulo Theories (SMT), Chapter in Handbook of Satisfiability. IOS Press, 2009.