Defending Against False Data Injection Attacks based Power System State Estimation

Anitha.KAnitha.S Mrs.M.SharonNisha
Department of CSE Department of CSE Assistant Professor (CSE)
Francis Xavier Engineering College Francis Xavier Engineering College Francis Xavier Engineering College
Ani618564@gmail.comAnisankar98@gmail.com Sharonnishafxece@gmail.com

Abstract

Network Forensic is one among the foremost promising approaches for the network security. Below the umbrella of network security, the network rhetorical is considered the extension of the normal security model. With the exception of the final stress on interference and detection of network attacks as in primitive network security model, the network forensics focuses on the gathering, observation and preservation of network knowledge therefore on analyse and organize traffic knowledge mistreatment clump or varied different data processing techniques for knowledge verification. Here honeypots were accustomed lure and trick attackers mistreatment network deception, by creating attainable security vulnerabilities and hasexcellent camouflage place. Additionally used were the assorted NFATs for the aim of most fidelity of information assortment. a example system is developed to gather the network logs mistreatment portae infrastructure and analyse all the logged traffic, that square measure extremely malicious in nature with massive volume of attacker's info. The tip Results of the system was to gather network knowledge that were extremely malicious in nature and were used for any investigation to urge the intelligent info concerning the attackers as proof for Network Forensics.

Introduction

With the fast development of net, human activities addicted toinfo networks also are growing. At an equivalenttime network security is tight, and alsothe existing security measures isprincipallysupported the identified facts of the passive protection model. Portae technology is associate degreerisingnetwork security supportedactivedefence technology, that by observance the activities of associatedegreepersona non grata, soweare able to analysis of the persona nongrata whose skill, victimization the tools and motivation for the invasion, thereby enhancing network security defence capability and conjointly used as proof for network forensics. At an equivalenttime, honeypots can even use thecustomoptionstopassailant, cut down the attack and also the transfer

target,
effectively frame thestandarddefensive deficiencies in info security technology, makes the protection system additionalexcellent[5].The term Forensics to be utilized in science and innovation to break down and set up actualities in criminal and common official courtrooms. Within theweb(World Wide Web) atmosphere, Forensics includes techniques and methodologies to gather, preserve and analyse network information on the net for investigation functions. It's a field of analysis and follow that has evolved as a results of increasing net usage and also the move of criminal activity. It'sconjointly argued that network forensics evolved as a response to the hacker community. Digital forensics focuses on developing proof relating digital files that relate to a laptop document, email, text, digital photograph, package program,or any alternative digital record which canbe relevant in a very legal case. And also the Network Forensics deals to gather preserve the network information evidences. It's a branch of towards watch, then examine digital media or devices. And also thecompanysecurity companies dedicat e vital resources to work the business executivelaptop attacks that still plague organization a worldwide.

Network forensics method consists of Capturing, Collection, Preparation, Acquisition, Preservation, Examination, Analysis and reportage [1]. Among these steps, Acquisition step may be a procedure that investigators collect digital proof and guarantee integrity of proof at incident website. Consequently, Acquisition step most important step for economical investigation. To Develop a Network rhetorical System, performs the subsequent tasks whereas operating with network evidences: Identification: Any digital data on the network or Artefactswhich will be used as proof. Assortment of Network information with machine learning ways for observation so preserve that information.Analyse the collected information and organize mistreatment bunch techniques. Construct the proof and verify the result on every occasion [16].

Existing System

To safely present a third party auditor(TPA), the accompanying two essential necessities must be met: TPA ought to most likely productively review the cloud information stockpiling without requesting the nearby duplicate of information, and present no extra on-line weight to the cloud client; The outsider evaluating procedure ought to get no new vulnerabilities towards client information security. Accessibility assaults can cost less assault assets contrasted and trustworthiness assaults. A natural precedent is that the aggressor utilizes a similar device to play out a Man-In-The-Middle (MITM) assault on the traded estimations among substations and the control focus. Determining skyline processes become expensive if the number of candidate concrete services is large. Genetic algorithm was not applicable when the number of concrete

services per abstract service increase. The above approaches have not explicitly considered scale of adaptation.

Proposed work

The work deals with efficient algorithms for assigning identifiers (IDs) to the nodes of a network in such a way that the IDs are anonymous using a distributed computation with no central authority.Given nodes, this assignment is essentially a permutation of the integers with each ID being known only to the node to which it is assigned. Our main algorithm is based on a method for anonymously sharing simple data and results in methods for efficient sharing of complex data. There are numerous applications that require dynamic special IDs for system hubs. Such IDs can be utilized as a component of plans for sharing/isolating correspondences transfer speed, information stockpiling, and different assets secretly and without conflict. The IDs are needed in sensor networks for security or for administrative tasks requiring reliability, Such as configuration and monitoring of individual nodes, and download of binary code or data aggregationdescriptions to these nodes. An application where IDs need to beanonymous is grid computing where one may seek services without divulging the identity of the service requestor.Businesses also have legitimate reasons to engage in anonymous communication. Avoid the consequences of identity revelation. Secure multiparty computation.

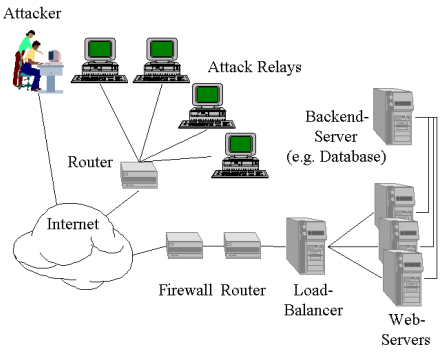

Fig1: system architecture

Mechanism

It has 5 mechanisms.They areCreation of mobile nodes,selecting group of player to coalition Formation, Establishing coalition procedure in cooperative networks, Key Generator,Bandwidth CalculationThe mobile nodes in a group (i.e., cluster) cooperatively deliver data packets among each other. The first use a social network analysis (SNA)-based approach to identify which mobile nodes have the potential to help other mobile nodes for data delivery in the same group or coalition. A distributed coalition formation algorithm is proposed which guarantees that stable coalitional structures can be obtained. We perform a comprehensive performance evaluation.Key generation is using cryptographic algorithm, this algorithm used for symmetric and asymmetric cryptographic algorithms applied to data received in Input and sent as output by the identity element.In this Module we will calculate the Bandwidth totally used by the Application. In every tab loaded bytes also calculated. The speed of the page loaded in the application also calculated.

Conclusion

Joint node and link attacks pose a serious threat to the network. In addition to network connectivity, it is also important to assess the vulnerability of the network under joint node and link networks in terms of other performance metrics such as network throughput, maximum network flow between source–destination pairs, and so on. Furthermore, the problem of allocating resource to protect the network under the joint attacks is of great importance and is the topic of our future study.

References:

[1] T. H. Grubesic, T. C. Matisziw, A. T. Murray, and D. Snediker, "Comparative approaches for assessing network vulnerability," Int. Regional Sci. Rev., vol. 31, no. 1, pp. 88–112, 2008.

[2] A. Murray, T. Matisziw, and T. Grubesic, "Multimethodological approaches to network vulnerability analysis," Growth Change, vol. 39, no. 4, pp. 573–592, 2008.

[3] A. Sen, S. Murthy, and S. Banerjee, "Region-based connectivity—A new paradigm for design of fault-tolerant networks," in Proc. HPSR, 2009, pp. 1–7.

[4] S. Banerjee, S. Shirazipourazad, and A. Sen, "Design and analysis of networks with large components in presence of region-based faults," in Proc. IEEE ICC, 2011, pp. 1–6.

[5] A. Pinar, J. Meza, V. Donde, and B. Lesieutre, "Optimization strategies for the vulnerability analysis of the electric power grid," SIAM J. Optim., vol. 20, no. 4, pp. 1786–1810, 2010.

[6] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state Estimation with respect to false data injection cyber-attacks," IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[7] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices For state estimators in power networks," in First Workshop on Secure Control Systems (SCS), Stockholm, 2010.

[8] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure Control systems: A quantitative risk management approach," IEEE Control Systems, vol. 35, no. 1, pp. 24–45, 2015.

[9] A. Teixeira, G. D´an, H. Sandberg, and K. H. Johansson, "A cyber Security study of a SCADA energy management system: Stealthy Deception attacks on the state estimator," Proceedings of IFAC World Congress, Aug 2011.

[10] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks On the smart grid," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645–658, 2011.

[11] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market Operations," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 659–666, 2011.

[12] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality

On real-time locational marginal price," IEEE Transactions on Power
Systems, vol. 29, no. 2, pp. 627–636, Mar. 2014.
[13] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences
Of false data injection attack on power system state estimation,"
IEEE Trans. on Power Systems, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.
[14] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data
Injection attack in wide-area smart grids," IEEE Transactions on Smart
Grid, vol. 6, no. 6, pp. 2725–2735, 2015.
[15] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of
Stealthy false data injection attacks in power system state estimation,"
IEEE Transactions on Smart Grid, vol. PP, no. 99, p. 1, 2016.
[16] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware
Mitigation of data integrity attacks on power system state estimation,"
IEEE Journal on Selected Areas in Communications, vol. 30, no. 6, pp.
1108–1118, 2012.
[17] K. Pan, A. M. H. Teixeira, M. Cvetkovic, and P. Palensky, "Combined
Data integrity and availability attacks on state estimation in cyberphysical
Power grids," in Proc. IEEE Int. Conf. Smart Grid Communications
(SmartGridComm), Nov. 2016, pp. 271–277.
[18] X. Liu and Z. Li, "Local load redistribution attacks in power systems
With incomplete network information," IEEE Transactions on Smart
Grid, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.
[19] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection
Attacks with reduced network information," IEEE Transactions on Smart
Grid, vol. 6, no. 4, pp. 1686–1696, 2015.
[20] X. Liu and Z. Li, "False data attacks against AC state estimation with
Incomplete network information," IEEE Transactions on Smart Grid,
vol. 8, no. 5, pp. 2239–2248, Sep. 2017.
[21] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks
With incomplete information against smart power grids," in IEEE Global
Communications Conf.(GLOBECOM). IEEE, 2012, pp. 3153–3158.
[22] 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. 49th IEEE Conf. CDC, Dec. 2010, pp. 5991–5998.
[23] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data
Injection using independent component analysis in smart grid," in Proc.
IEEE Int. Conf. Smart Grid Communications (SmartGridComm), Oct.
2011, pp. 244–248.
[24] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state
Estimation with unknown network parameters," in Proc. Systems and
Computers 2013 Asilomar Conf. Signals, Nov. 2013, pp. 1388–1392.
[25] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber –physical system
Security for the electric power grid," Proceedings of the IEEE, vol. 100,
No. 1, pp. 210–224, Jan. 2012.

[26] A. Abur and A. G. Exposito, Power system state estimation: theory and Implementation. CRC press, 2004.
[27] D. Jones, “Statistical analysis of empirical models fitted by optimization,” Biometrika, pp. 67–88, 1983.
[28] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and
K. C. Sou, “E_cient computations of a security index for false data
Attacks in power networks,” IEEE Transactions on Automatic Control,
vol. 59, no. 12, pp. 3194–3208, 2014.