IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

A Review on Redundancy Management of Multipath Routing for Intrusion Tolerance in Hetrogeneous WSN

Manisha Dangi[1], Prof. R. K. Krishna[2]

Department of Computer Science &Engineering, RCERT, Chandrapur[1,2]

Abstract: Multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. We develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized. We then apply the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter. We observe that many existing trust models adopting watchdog as their monitoring mechanism do not explicitly address these weaknesses. Our goal in this paper is to demonstrate how serious insider attacks can be in WSNs.

Keywords: Network security, virtual network system computing, intrusion detection, attack graph, zombie detection.

INTRODUCTION

Insider threat is an important security issue in wireless sensor network (WSN) because traditional security mechanisms, such as authentication and authorization, cannot catch inside attackers who are legal members of the network. Inside attackers can disrupt the network by dropping, modifying, or misrouting data packets. This is a serious threat for many applications such as military surveillance system that monitors the battlefield and other critical infrastructures.

Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks . Since WSNs consist of hundreds or thousands of tiny sensor nodes, the trust mechanism is often implemented as a distributed system where each sensor can evaluate, update, and store the trustworthiness of other nodes based on the trust model.

Thus, an inside attacker can disguise its malicious behavior behind network traffic or noise. Third, we cannot ignore the fact that insiders have internal knowledge about our network and security mechanisms against attacks. By exploiting such knowledge, inside attackers can launch their attacks intelligently to avoid being detected.

We observe that many existing trust models adopting as their monitoring mechanism do not explicitly address these weaknesses. Our goal demonstrate how serious insider attacks can be in WSNs even with the presence of trust mechanism, and to introduce defending approaches to improve the trust mechanism.

PROBLEM DEFINITION

The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to virtual network system users. In a virtual network system where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the virtual network system and use its resource to deploy attacks in more efficient ways. Such attacks are more effective in the virtual network system environment since virtual network system users usually share computing resources

LITERATURE SURVEY

ISSN: 2278-0661 Volume 3, Issue 1, Dr.Balachandra,D.N.Karthek, (July-Aug. 2012), An Overview on Security Issues in Cloud Computing In this paper we have studied how security and compliance integrity can be maintained in new environment The prosperity in Cloud Computing literature is to be coming after security and privacy issues are resolved.

Vol.3, No.4, Hamoud Alshammari and Christian Bach, August 2013 Administration Security Issues In Cloud Computing, In this paper we have studied most administration security issues and concept of the Service Level Agreement or any trust third party that can control the processing over Could Computing .The solution to get more secure Cloud Computing environment is to have a strong Service Level Agreement Offering an adequate

level of security and privacy for the information that is already in the cloud.

ISSN: 2305-0012,Sina Manavi, Sadra Mohammadalian, Nur Izura Udzir, Azizol Abdullah,2012 Secure Model for Virtualization Layer in Cloud Infrastructure In this paper we have studied to propose a model to secure and proper mechanism to react reasonable against the detected attack by intrusion detection system. With the secured model (SVM) against the attack SVL model, (Secure Model for Virtualization layer)which combines virtualization and intrusion detection system, can increase the detection rate and provide protection against attacks targeting virtualization, and consequently will result in reliable cloud security the proposed model and framework will be implemented in order to compare and evaluate it with the traditional manner .

ISSN : 2248-9622, Vol. 4, Issue 3(Version 5) ,Mr. V.V.Prathap, Mrs.D.Saveetha,2014 Detecting Malware Intrusion in Network Environment In this is model we have studied three model intrusion detection Threat model,Attack Graphe model,Existing model NICE utilizes the attack graph model to conduct attack detection and prediction. NICE only investigates the network IDS approach to counter zombie explorative attacks.

VOL. 10, NO. 4 Chun-Jen Chung,Tianyi Xing,Dijiang Huang,2013 NICE:
Network Intrusion Detectin and Countermeasure Selectionin Virtual Network Systems In this paper we have studied The system and security evaluations demonstrate the efficiency and effectivenes of the proposed solution NICE, which is proposed to detect and mitigate collaborative attacks in the cloud virtual networking environment. NICE only investigates the network IDS approach to counter zombie explorative attacks. To improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system.

Shina Sheen,R Rajesh Network Intrusion Detection using Feature Selection and Decision tree classifier

In this paper we have studied three different approaches for feature selection, Chi square, Information Gain and ReliefF which is based on filter approach Intrusion Detection with feature selection was able to out perform the decision tree algorithm without feature selection Intrusion Detection approach is very useful for counter measure ijceronline.com) Vol. 2 Issue. 7 ,Prof.D.P.Gaikwad , Pooja Pabshettiwar, Priyanka Musale,Pooja Paranjape,Ashwini S. Pawar,2012 A Proposal for Implementation of Signature Based Intrusion Detection System Using Multithreading Technique

In this paper we have studied signature based intrusion detection system, using multithreading technique. The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. multithreaded technique for better intrusion detection should be distributed and cooperative by applying co-operative agents to the network.

Vol.5, No.2, Shalvi Dave, Bhushan Trivedi and Jimit Mahadevia, 2013 Efficacy of attack detection capability of IDPS based on its deployment in wired and Wireless environment. IDS logging agent inspects the data with the help of Suricata. Suricata is an open-source IDS available on all the platforms. It identifies an attack based on pre-defined signature rule-set.

Intrusion Detection and/or Prevention Systems (IDPS) represent an important line of defence against a variety of attacks that can compromise the security

IEEE 12th International Conference on Data Mining Workshops, Anand Kannan and Gerald Q. Maguire,Ayush Sharma and Peter Schoo,2012 Genetic Algorithm based Feature Selection Algorithm for Effective Intrusion Detection in Cloud Networks In this paper we have studied a new intrusion detection model in which we combine a newly proposed genetic based feature selection algorithm and an existing Fuzzy Support Vector Machines (SVM) for effective classification as a solution.

New genetic based feature selection algorithm is used to select optimal number of features from the KDD cup data set for intrusion detection.

Genetic algorithm is very helpful for intrusion detection.
978-1-4244-6005-2/10/$26.00 ©IEEE ,Aizhong Mi Linpeng Hai,2010.

A Clustering-based Classifier Selection Method for Network Intrusion Detection.

In this paper we studied the pattern recognition approach based on classifier selection to network intrusion detection and proposes a clustering-based classifier selection method.

The pattern recognition technique to intrusion detection, and proposes a network intrusion detection approach based on multiple classifier selection, called CDS. This method is very useful intrusion detection

Tal Garfinkel Mendel Rosenblum

A Virtual Machine Introspection Based Architecture for Intrusion Detection.

In this we studied an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. The pattern recognition technique to intrusion detection, and proposes a network intrusion detection approach based on multiple classifier selection, called CDS. This method is very useful intrusion detection.

Tal Garfinkel Mendel Rosenblum

A Virtual Machine Introspection Based Architecture for Intrusion Detection.

In this we studied an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. Approach for intrusion detection which co-locates an IDS on the same machine as the host it is monitoring and leverages a virtual machine monitor to isolate the IDS from the monitored host.

RESEARCH METHODOLOGY

Trust mechanism

In general, trust mechanism works in the following stages.

1) Node behavior monitoring : Each sensor node monitors and records its neighbors' behaviors such as packet forwarding. This collected data will be used for trustworthiness evaluation in the next stage. Watchdog is a monitoring mechanism popularly used in this stage. The confidence of the trustworthiness evaluation depends on how much data a sensor collects and how reliable such data is.

2) Trust measurement: Trust model defines how to measure the trustworthiness of a sensor node. introduced several representative approaches to build the trust model, which include Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach. The trust value of a node may be different when we use different trust models. For example, when a node is observed to forward the packet stimes and drops the packet Insider trust Management Intelligent inside attacks against trust mechanism Vulnerabilities in the inside attacker detection stage Average End-to-End delay Packet Delivery Ratio Energy Consumption Multi-hop Chain Topology

Inside attack detection : Based on the trust value, a sensor node determines whether its neighbor is trustworthy for collaboration (such as packet forwarding). If a neighbor's trust value is less than a certain threshold , it will be considered as an untrusted or malicious node.

Depending on the WSN's trust mechanism, the detection of such insider attacker may or may not be broadcast to the rest of the nodes in the WSN.

Moreover, we cannot keep aside the case of zero day attack where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner. In such case, the alert being real will be regarded as false, given that there does not exist corresponding node in SAG. Thus, current research does not address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to detect most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks.

CONCULSION

A trust threshold can be designed in static manner or dynamic manner. Static trust threshold might be optimal only for limited cases that we consider in the simulation. As a result, it may not be good for unconsidered situations. Meanwhile, dynamic trust threshold that adaptively changes according to situations in our network may have reasonably good results, although it may not be optimal for all situations. However, since dynamic trust threshold will be frequently computed, it must be designed in an energy-efficient way. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

REFERENCES

[1] Azahdeh Faridi et al, "Comprehensive Evaluation of the IEEE 802.15.4 MAC Layer Performance With Retransmissions," IEEE Transactions on Vehicular Technology, Vol.59, No.8, October 2010, pp. 3917-3932.

[2] Tran Hoang Hai and Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge," Seventh International Symposium on Network Computing and Applications (NCA '08), July 2008, pp. 325-331.

[3] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of Attack and Defense Techniques for Reputation Systems," ACM Computing Surveys, Vol 41, Issue 4, 2009.

[4] H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[5] "Open vSwitch Project," http://openvswitch.org, May 2012.

[6] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation," Proc. 16th USENIX Security Symp. (SS '07), pp. 12:1-12:16, Aug. 2007.

[8] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic," Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb. 2008.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002,

[10] "NuSMV: A New Symbolic Model Checker," http://afrodite.itc.it:1024/nusmv. Aug. 2012.

[11] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graphbased network vulnerability analysis," Proc. 9th ACM Conf. Computer and Comm. Security (CCS '02), pp. 217-224, 2002.

[12] X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic-Based Network Security Analyzer," Proc. 14th USENIX Security Symp., pp. 113-128, 2005.

[13] R. Sadoddin and A. Ghorbani, "Alert Correlation Survey: Framework and Techniques," Proc. ACM Int'l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST '06), pp. 37:1-37:10, 2006.

[14] L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts," Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[15] S. Roschke, F. Cheng, and C. Meinel, "A New Alert Correlation Algorithm Based on Attack Graph," Proc. Fourth Int'l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.

[16] A. Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees," Proc. IEEE Int'l Conf. Dependable Systems Networks (DSN '12), June 2012.