International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 4, Number 1 (2012), pp. 31-37
© International Research Publication House
http://www.irphouse.com

Analysis for Intrusion Detection in Wireless Ad-Hoc Networks

Brahampal Singh

Lecturer in IT & Computer Science, Trinity Institute of Professional Studies,
Dwarka, New Delhi, India
(Affiliated from G.G.S.I.P. University, New Delhi)
E-mail: brahampal_singh@yahoo.com

Abstract

As Mobile Ad-hoc network (MANET) has become a very important technology, research concerning its security problem, especially, in intrusion detection has attracted many researchers. Feature selection methodology plays a central role in the data analysis process. The proposed features are tested in deferent network operating conditions. PCA is used to analyze the selected features. Performance reduction will occur both in speed and predictive accuracy. This paper aims to select and analyze the network features using principal component analysis.

Wireless ad-hoc networks are increasingly being used in the tactical battlefield, emergency search and rescue missions, as well as civilian ad-hoc situations like conferences and classrooms due to the ease and speed in setting up such networks. As wireless ad-hoc networks have different characteristics from a wired network, the intrusion detection techniques used for wired networks may no longer be sufficient and effective when adapted directly to a wireless ad-hoc network. In this paper, I will first provide an introduction to wireless ad-hoc networks and thereafter an introduction to intrusion detection. I will then present various existing intrusion detection techniques that can be adapted to wireless ad-hoc networks and finally propose a hybrid intrusion detection system for wireless ad-hoc networks.

Keywords: Feature selection, intrusion , Mobile Ad-hoc network (MANET), PCA- principal component analysis

Introduction

Mobile Ad-hoc Network (MANET) is an unstructured wireless network that can be established temporarily. In MANET, nodes can add-in to the network or detach from it at anytime. Thus, there is no central control on the network for the nodes to follow [20]. Intrusion detection models were introduced by Denning in 1987 and rather are a new technology [5, 20]. Intrusion detection systems can be categorized into two models: Signature-based intrusion detection [2] and anomaly-based intrusion detection. Signature-based intrusion detection uses signatures of the attacks to detect the intrusion.

A wireless ad-hoc network consists of a collection of mobile nodes that communicate with each other via wireless links without the aid of a pre-existing communication infrastructure. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart rely on intermediate nodes to forward their messages. Each node can function both as a router as well as a host.

For this paper, the mobile nodes that we are focusing our discussion on are current day laptops that have sufficient processing capability and memory to support ad-hoc networking as well as intrusion detection applications. These laptops have limited battery life only when they are unplugged from a main power source. Such mobile nodes are used to setup wireless ad-hoc networks in situations like classrooms or conferences; temporary offices like a promotional booth; emergency search and rescue missions and possibly at command posts in the military.

Vulnerabilities of wireless ad-hoc networks

Despite the convenience that comes with being able to rapidly deploy wireless ad-hoc networks and being mobile, such networks have inherent vulnerabilities that make them highly susceptible to malicious attacks.

The wireless link does not provide the same level of protection for data transmission as a wired link, allowing adversaries within radio transmission range to perform attacks against the transmitted data without gaining physical access to the wireless link. The dynamic and cooperative nature of ad-hoc networking without a centralized authority for authentication and monitoring is susceptible to attacks that breaks down or exploit the cooperative behavior of the ad-hoc routing. The mobile nodes that are roaming independently may have inadequate physical protection and can be captured and compromised. Adversaries using these captured nodes can perform far more damaging attacks from within the network and such attacks are much harder to detect since the captured nodes will contain the private keys and passwords used within the network.

Network architecture

Wireless ad-hoc networks may be configured in basically two ways, either a flat network infrastructure or a multi-layered network infrastructure. The two different configurations will determine how well an intrusion detection system can be employed in a network as well as the architecture of the intrusion detection system.

In a multi-layered network infrastructure, all nodes are not considered equal . Nodes within transmission range are organized into a cluster, and elect a Cluster-Head (CH) node to centralize routing information for the cluster. The CH nodes will in this case be more powerful devices with better resources and they form a virtual backbone of the network. Depending on the protocol, intermediate gateway nodes may relay packets between CH nodes.

Intrusion detection

Intrusion detection is defined as the method to identify "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [13]. It is pertaining to techniques that attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Hence in the context of wireless ad-hoc network, we need to identify any malicious nodes either from outside the network trying to break into or nodes that have turned bad. Bad nodes can easily disrupt or partition the network using the various forms of attacks as seen from the previous section. Detection of break-ins or attempts is done either manually or via software expert systems that operate on logs or other information available on the network.

Anomaly detection vs. misuse detection

In order to detect an intrusion attack, one needs to make use of a model of intrusion. That is, we need to know what an Intrusion Detection System (IDS) should look out for. There are basically two types of

Host-based vs. network-based intrusion detection

Most intrusion detection systems (IDS) take either a network-based or a host-based approach to recognizing and deflecting attacks. In either case, these products look for specific patterns that usually indicate malicious or suspicious intent. An IDS is network-based when it looks for these patterns in network traffic. It is host-based when it looks for patterns in log files

Online detection vs. offline detection

The classification of intrusion detection systems can be further segregated according to the timeliness of the audit data being gathered and processed. Audit data can be gathered and processed while the hosts is either online (connected to the network) or offline (disconnected from the network).

A survey of intrusion detection techniques

Problems of current intrusion detection techniques

It is difficult to apply intrusion detection techniques developed for the wired network to the wireless ad-hoc network due to the vast difference between the two networks. The main difference is that wireless ad-hoc networks do not have fixed infrastructures, and existing network-based IDSs, which rely on real-time traffic analysis, can no longer function well in the new environment. In wired networks, traffic monitoring is usually done at switches, routers and gateways. The wireless ad-hoc environment does not have such traffic concentration points where the IDS can collect audit data for the entire network and can only rely on partial, localized audit data collected from the host and from communication activities taking place within the radio range.

Besides having different network infrastructures, there is also a big difference in the communication pattern of users in the wireless mobile environment. Due to the bandwidth limitations, battery constraints and frequent disconnects, users often adopt new operations modes such as disconnected operations [12]. This suggest that existing anomaly detection models may not be able to determine that such new operations are certified and identify them as intrusions.

There also may not be a clear separation between normalcy and anomaly in the mobile environment [11].

A node that sends out false routing information could be a compromised node or merely one that is temporarily out of sync due to rigorous physical movement. Existing detection methods may find it increasingly difficult to differentiate false alarms from real intrusions.

The lack of protocol standards, an example being the lack of a standardized routing protocol makes it difficult to define intrusion attack signatures for the wireless mobile environment. Signatures are defined from the characteristics, vulnerabilities and the working topologies of the routing protocol. The lack of understanding of new applications that are being developed for the wireless mobile environment also add to the difficulty in defining attack signatures.

Reasons for choice of intrusion detection techniques

The intrusion detection techniques that will be presented in the following sections are chosen due to the suitability of the technique for anomaly detection. Anomaly detection should be the main approach for intrusion detection in the wireless ad-hoc network because it is conceivable that intrusion in this new environment will come in the form of new attacks types that are yet to be defined. These techniques can also be adapted for local and cooperative detection. The techniques can either process partial and local data on the host as well as gather more information from the neighboring hosts to perform cooperative intrusion detection.

Data mining

Data mining algorithms implemented on each mobile node can be used to analyze audit data and thereafter generate intrusion detection models. Data mining generally refers to the process of extracting useful models from large repositories of data [3]. Below are several algorithms that are particularly useful for mining audit data for anomaly detection.

A proposed hybrid intrusion detection system

Hybrid system requirements

Our hybrid intrusion detection system is designed especially for the wireless ad-hoc network although it can also be deployed in the wired network. We take into considerations, when designing our hybrid intrusion detection system, the characteristics of the wireless ad-hoc network and the problems that existing system face when being deployed in a wireless ad-hoc environment.

The dynamic and cooperative nature of the wireless ad-hoc network suggests that the intrusion detection system should be designed to be dynamic and cooperative as well. Each node should have its own intrusion detection module since it cannot rely on other nodes that may leave the network at anytime to help it perform intrusion detection. Wireless ad-hoc networks also do not have traffic concentration points that allows for intrusion detection at a centralized location and this further emphasize the need for each to have its own intrusion detection module

The proposed hybrid system (figure 5) consists of the following components; data collector, detection optimizer, detection engine, response engine and secure communication module.

Data collector

The data collector collects data at the link layer, the network layer and the application layer. Information is needed from these three different layers to perform multi-layered intrusion detection [11]. Multi-layered intrusion detection is needed as certain attacks that target the upper layer may seem perfectly legitimate to the lower layers.

Detection optimizer

Due to the limited battery life that the mobile node has, we deem that intrusion detection should be done on the basis of different levels of escalation starting from the simplest and least battery consuming intrusion detection operation to more complex and CPU intensive operation. The detection optimizer preprocesses all the audit data collected from the different layers and send the most relevant audit data to the detection engine based on the mode that the mobile node is currently operating in.

Detection engine

The detection engine performs both misuse and anomaly detection. Either the Haystack or data mining algorithms can be implemented in the detection engine.

Response engine

When an intrusion is detected, the system needs to respond appropriately. It can either sound a local alarm on the host or a global alarm on the network. The nodes can then respond to the intrusion either locally or cooperatively.

Secure communication module

The secure communication module is needed when the node needs to perform cooperatively intrusion detection as well as when sounding a global alarm. Mobile agents, the Indra approach or tunneling can be implemented for this communication module. Measurements like pixel gray levels or values of a signal at di®erent time instants [16].

In the PCA transform, the vector *x* is ¯rst centered by subtracting its mean [9, 16]:

x Ã¡ x ¡ Efxg:

In practice, the mean is estimated from the available sample *x*(1) *: : :* *x*(*T*).

The matrix *X* is a *n £ n* covariance matrix of *x*.

Cx Ã¡ EfxxT g:

It is well known from basic linear algebra that the solution to the PCA problem is given in terms of the unit-length eigenvectors *e*1*; e*2*; : : : ; en* of the matrix *Cx*. The ordering of the eigenvectors is such that the corresponding eigen-values *d*1*, : : :, dn* satisfy *d*1 ¸ *d*2 ¸ *: : :* ¸ *dn*.

Thus the ¯rst principal component of *x* is

*y*1 = *eT*
1 *x:*

Conclusion

Wireless ad-hoc networks have brought about a paradigm shift in the way we think about intrusion detection. We need to rethink methods for these new networks based on the characteristics that these networks have. In this paper, we have provided an introduction to wireless ad-hoc networks. We then proceeded to provide an introduction to intrusion detection in the context of wireless ad-hoc networking. Having understood the implications and problems in performing intrusion detection in this new environment, we performed a survey on the existing methods for intrusion detection and listed four techniques that we deemed are suitable for the wireless ad-hoc environment. We ended by proposing a hybrid intrusion detection system that allows the different techniques that we have identified to be incorporated into the system and is most suited for wireless ad-hoc networking. Link Layer Network

References

[1] A. Agah, and S. K. Das, \Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145-153, 2007.

[2] F. Anjum, D. Subhadrabandhu, and S. Sarkar.\Signature-based intrusion detection for wireless *Ad-hoc networks," Proceedings of Vehicular Technology Conference*, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[3] W. Chen, J. Yan, B. Zhang, Z. Chen, and Q. Yang,\Document transformation for multi-label feature selection in text categorization," *Proceedings of Seventh IEEE International Conference on Data Mining*, pp. 451-456, USA, 2007.

[4] H. Deng, Q. A. Zeng, and D. P. Agrawal, \SVM based intrusion detection system for wireless ad hoc networks," *Proceedings of the IEEE Vehicular Technology Conference*, pp. 2147-2151, USA, 2003.

[5] D. E. Denning, \An Intrusion Detection Model,"*IEEE Transactions in Software Engineering*, vol. 13,no. 2, pp. 222-232, USA, 1987.

[6] H. A. Edelstein, *Introduction to Data Mining and Knowledge Discovery*, Crows Corporation, Third Edition, 1999.

[7] D. M. Farid, and M. Z. Rahman, \Learning intrusion detection based on adaptive Bayesian algorithm," *11th International Conference on Computer and Information Technology (ICCIT2008)*, pp. 652- 656, 2008.

[8] Y. K. Hassan, M. Hashim, A. El-Aziz, A. Safwat, A. El-Radi, \Performance Evaluation of Mobility Speed over MANET Routing Protocols," *International Journal of Network Security*, vol. 11, no. 3, pp. 101-111, 2010.

[9] H. Hotelling, \Analysis of a complex of statistical variables into principal components," *Journal of Educational Psychology*, vol. 24, no. 7, pp. 498-520, 1933.

[10] A. HyÄvarinen, J. Karhunen, and E. Oja, *Independent Component Analysis*, John Wiley & Sons Inc., USA, 2001.

[11] Y. C. Hu, A. Perrig, and D. B. Johnson, \Rushing attacks and defense in wireless ad-hoc network routing protocols," *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 30-40, USA, 2003.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, \Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp.370-380, IEEE, 2006.

[13] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, \Cross feature analysis for detecting ad-hoc routing anomalies," *Proceedings of The 23rd International Conference on Distributed Computing Systems (ICDCS)*, pp. 478-487, USA, 2003.

[14] Y. A. Huang, and W. Lee, \A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN' 03)*, pp. 135-147, USA, 2003.

[15] B. Mukherjee, L.Todd Heberlein, and Karl N. Levitt. *Network Intrusion Detection*. IEEE Network, May/June 1994

[16] R. Janakiraman, M. Waldvogel, and Qi Zhang. *Indra: a peer-to-peer approach to network intrusion detection and prevention*. Twelfth IEEE International Workshops, Jun 9-11, 2003

[17] Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P. 1996. The KDD process of extracting useful knowledge from volumes of data. Commun. ACM 39, 11, 27-34

[18] Zhou, L. and Haas Z.,“Securing Ad Hoc Networks,” *IEEE Network Magazine*, vol. 13, no. 6, November/December 1999.

[19] S. Puttini, J-M. Percher, L. Mé, O. Camp, R. de Sousa Jr., C. J. Barenco Abbas, L. J. Garcia Villalba. A Modular Architecture for Distributed IDS in MANET. In Proceedings of the 2003 International Conference on Computational Science and Its Applications (ICCSA). Springer Verlag, LNCS 2668, May 2003

[20] Kong, J., Luo, H., Xu, K., Gu, D., Gerla, M., and Lu, S.,“Adaptive Security for Multi-layer Ad-hoc Networks,” *Special Issue of Wireless Communication and Mobile Computing*, 2002.

[21] Wenke Lee, Salvatore J. Stolfo. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC) Vol. 3, Issue 4 Nov 2000