International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 4, August 2016, pp. 1779~1784
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i4.10008

A Generic Review on Effective Intrusion Detection in Ad hoc Networks

G. Gopichand, RA. K. Saravanaguru
School of Computing Science and Engineering, Vellore Institute of Technology University, Vellore, India

Article Info

Article history:

Received Jan 28, 2016
Revised Jul 12, 2016
Accepted Jul 25, 2016

Keyword:

Ad hoc network
Multi hop schemes
Intruder
Intrusion detection system

ABSTRACT

Ad hoc network is specifically designed for the establishment of a network anywhere and anytime, which does not have any fixed infrastructure in order to support the mobility of the users in the network. The network is established without using any access points or base stations for communication implemented in multi hop schemes. Hence we call an Ad hoc network as a collection of nodes which are mobile in nature with a dynamic network infrastructure and forms a temporary network. Because of dynamic topological changes, these networks are vulnerable at the physical link, and they can easily be manipulated. An intruder can easily attack the Ad hoc network by loading the network resources which are available, such as wireless links and energy (battery) levels of other users, and then starts disturbing all the users. This paper provides a comparative survey on the various existing intrusion detection systems for Ad hoc networks based on the various approaches applied in the intrusion detection systems for providing security to the Ad hoc network.

Corresponding Author:

G.Gopichand,
Dept of Software Systems, SCOPE,
VIT University, Vellore (Tamil Nadu),
India.
Email: gopichand.g@vit.ac.in

1. INTRODUCTION

Intrusion detection mechanism is one of the most important research area which has various potential applications for the current generation. Intrusion detection is a tool which fights against the cyber-attacks of the real world which threatens critical systems. Malicious behavior detection is the primary objective of the Intrusion detection system in a dynamic network [1], which detects the damages caused in the network by violating authenticity, availability, confidentiality, integrity, non-repudiation or privacy; as an example, a node in a mobile telephony network masquerades as another node so as to defeat the integrity of the billing function. Selfish behavior is a non-community minded action; which can be explained with an example, where a node in a Wireless Ad hoc Network does not forward packets. The term adversary is used to refer to an undesirable node that specifically exhibits malicious or selfish behavior. This differentiation is made as it is critical to consider the attack model while evaluating a defensive mechanism. An Intrusion Detection System performs two main functions: Collecting data regarding suspects and analyzing the data. In this paper we had given a detailed description of these functions performed by intrusion detection systems and given a comparative analysis of the procedure implemented by the intrusion detection systems in performing those functions.

An intrusion detection system is capable of identifying the adversaries those have crossed the border of the network. A simple approach to find intruders is to view the nodes which have anomalous network traffic profiles. In this survey paper we discuss about intrusion detection. Specifically, we classify

the efectiveness of existing IDS techniques of the Ad hoc networks based on the various factors shown in the Figure 1.

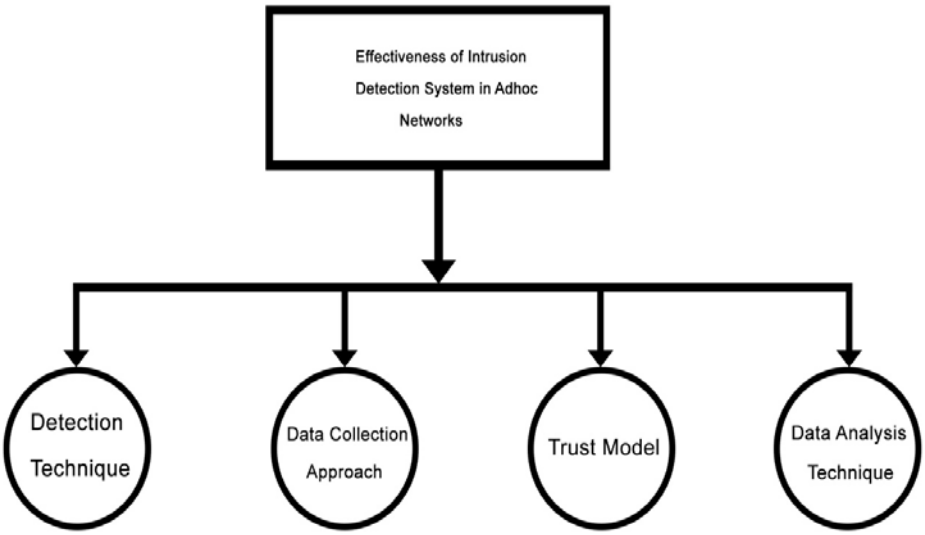

Figure 1. Factors on which the effectiveness of IDS is based

2. BACKGROUND

Here, we first describe about the various existing instrusion detection technique applied for Ad hoc network, which are named as anomaly based intrusion detection technique, signature based intrusion detection technique, specification based intrusion detection technique and reputation based techniques. Figures 2 and 3 shows the detection technique dimension and gives a comparison on the various detection techniques.

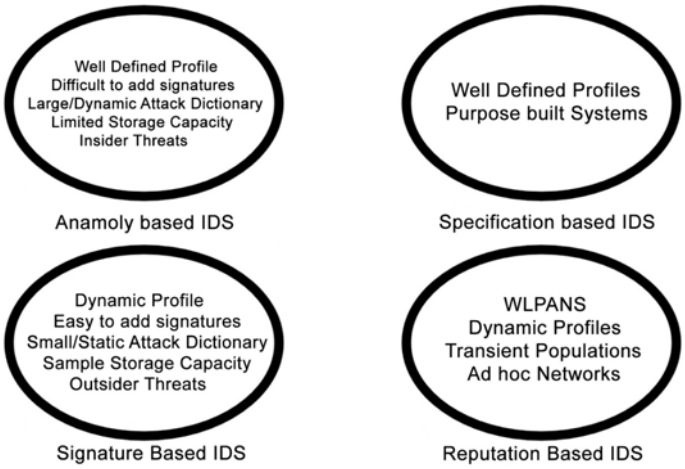

Figure 2. Dimensions of intrusion detection systems

2.1. Anomaly based intrusion detection technique

Anomaly based intrusion detection technique possess certain runtime features that are different from that of the ordinary, which can be defined in 2 ways, The first way is with respect to the history of the test signal (unsupervised) and the second way is with respect to a collection of training data (semi-supervised). Clustering is a main example of unsupervised machine learning [2]. The semi-supervised approach, train with a set of truth data and the unsupervised approach, train with live data [3].

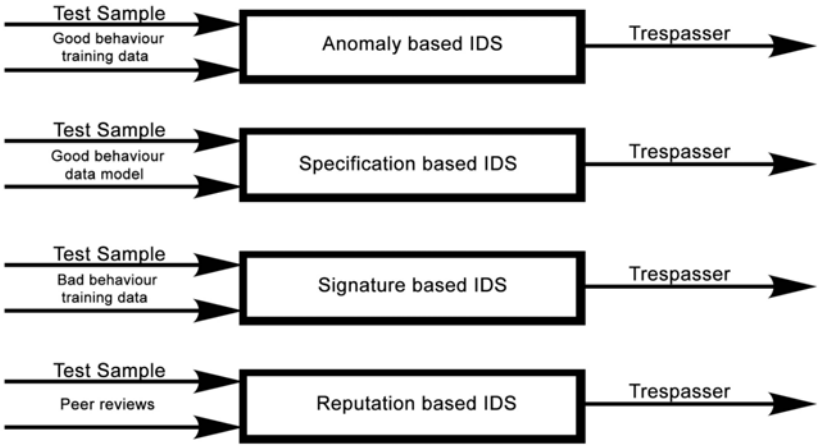

Figure 3. Comparison of the various intrusion detection techniques

The primary advantage of anomaly based intrusion detection techniques is that they doesn't look for something specific, and hence it eliminates the necessity of fully specifying all known attack vectors and keep this attack dictionary updated. The main disadvantage of this technique is its susceptibility to false positives. Chandola et al. [4] has provided a brief survey of anomaly based intrusion detection technique that is general to all applications.

2.2. Specification based intrusion detection technique

Specification based intrusion detection exhibits an abnormal performance at the system level; in contrast with anomaly based intrusion detection which analyzes specific user profiles or data flows. Specification based intrusion detection techniques normally exhibits legitimate behavior and indicates an intrusion when the system departs from this model. The First key advantage of specification based intrusion detection technique is low false negative rate. Based on the definition, these techniques only react to known bad behavior; theoretical basis is a bad node which will disrupt the formal system specification. The second key advantage of this technique is the system is highly effective as there is no training/ profiling phase. The primary disadvantage of the specification based intrusion detection technique is the high effort which is required for the generation a formal specification.

Specification based intrusion detection techniques are highly effective over insider attacks as they concentrate on system disruption. On the other hand, this is said to be not the best approach for outside attackers because the specifications, for example, state machine or grammar is application-specific and responds only to the actions that are taken by an insider. An outsider may not be able to generate transitions in the governing state machine or transforms in the defining grammar.

2.3. Signature based intrusion detection technique

Signature based intrusion detection approaches possess certain run- time features which match a specific pattern of misbehavior. From some sources this technique is referred to as pattern based detection [5] or intruder profiling, misuse detection [5]-[8], supervised detection [9].

The main advantage of this technique is a low false positive rate. Based on the definition, these techniques will only react to known bad behavior; the theoretical basis shows that a good node may not exhibit the attack signature. The primary disadvantage of this is that the techniques must identify a specific pattern; a dictionary should specify each attack vector and remain current. The attack signature may be a univariate data sequence (eg: bytes transmitted on a network, a pro- gram's system call history or application-specific information flows. The main hectic task is the combination of simple data sequences into a multivariate data sequence [3].

2.4. Reputation management intrusion detection technique

The main objective of a reputation manager is to detect nodes which exhibits selfish behavior rather than violating security. Whenever, malicious behavior is identified, the reputation managers should also guard against colluding nodes. Bella et al. [10] has identified that the main problem in MANET (Mobile Ad hoc Network) reputation management is distribution of reputation scores. Reputation management techniques are mainly applicable to large networks in which establishing a priori trust

relationships is highly infeasible (eg: packets forwarded over packets sourced, packets sent over packets received and packets forwarded over non-local packets received . Reputation management is highly relevant to ad hoc network applications.

3. PROBLEM DESCRIPTION

Here, we specify the effectiveness of intrusion detection techniques when applying to Ad hoc networks. The effectiveness of intrusion detection techniques can be specified based on mainly three features they are named as Data Collection approach, Trust model, and Data Analysis Technique.A brief description of these features is given as follows :

3.1. Data Collection Approach

As discussed earlier in section 1, collecting data regarding suspects is the first main function of an intrusion detection system. There are mainly two types of data collection approaches which are used before data analysis, they are named as, behavior based collection and traffic based collection.

3.1.1. Behavior based collection

IDSs which use behavior based data collection will analyze the logs maintained by a node, to determine whether it is compromised. The first main advantage of using this approach is scalability; in large scale applications (for eg: mobile telephony and WSN) it has its effectiveness in a very high level. The next main advantage of using this approach is decentralization; this is effective for infrastructure-less applications like ad hoc networks. The primary disadvantage of this approach is the additional work that each node has to perform to collect, or analyze, their data.

3.1.2. Traffic based collection

IDSs which use traffic based collection will analyze the network activity to determine whether a node is compromised. The primary advantage regarding resource management is that the individual nodes are free to analyze or maintain their logs. The main disadvantage regarding data collection is that the effectiveness of this technique is limited by the visibility of the nodes collecting the data. Hence In terms of effectiveness this approach is said to be more effective when compared with the behavior based collection approach.

3.2. Trust Model

The trust [11] model determines the data which a monitor node can use to audit the trustee nodes. Trust models are mainly classified into two basic types, named as, multitrust and unitrust.

3.2.1. Multitrust model

Multitrust model implements the concept of using data from third parties or witnesses. Liu and Issarny [12] has referred this type of information as a recommendation. In Contrast to recommendations, Shin et al. [13] referred it as direct monitoring. If multitrust is used along with behavior based collection the key weakness observed is: the opportunity for capable adversaries to cover their tracks. Multitrust is mostly preferred in the domain of reputation management which is highly applicable in ad hoc networks.

3.2.2. Unitrust model

Unitrust model is referred to as a standalone. In contrast to multitrust model, the unitrust model will not use reported information; a unitrust model is purely based on direct monitoring. Data reliability is the primary advantage of a unitrust model; the IDS need not require to apply safeguards to tolerate or prevent biased reports from adversaries. The main disadvantage of a unitrust model is the smaller data set. Hence in terms of effectiveness, multitrust model is highly effective than unitrust model.

3.3. Data Analysis Technique

As discussed earlier in section 1, Analyzing the data is the second main function of an intrusion detection system. There are mainly two ways to analyze data, named as, pattern matching and data mining.

3.3.1. Pattern matching Analysis

Pattern matching technique is used to simply scan an input source. Signature based approaches [3],[8],[13]-[20] scans for the entries in the attack dictionary. Semi-supervised anomaly based approaches scans for the deviations from expected performance. Reputation based approaches [18],[21],[22] scans the profile data in order to measure some criteria which was established prior to deployment.

3.3.2. Data mining Analysis

The examples of data mining analysis technique are the unsupervised variants of anomaly based Intrusion detection systems [10],[23]-[25]. In some cases like machine learning, neural networks and Bayesian classifiers the combination of both pattern matching and data mining analysis techniques is performed.Hence in terms of effectiveness pattern matching analysis technique is said to be more effective when compared with the data mining analysis technique.

4. RESULTS AND ANALYSIS

In this section, it is explained with a table (Table 1), which shows the classification of various intrusion detection systems of Ad hoc networks based on the intrusion detection technique applied, data collection approach, trust model and analysis techniques.

Table 1. The classification of various intrusion detection systems of Ad hoc networks

IDS technique	Type of Detection technique applied	Type of data Collection approach used	Trust Model applied	Analysis technique used
CONFIDANT [26]	Reputation	Traffic	multitrust	Pattern matching
CORE [22]	Reputation	Traffic	multitrust	Pattern matching
Zhang and Lee Technique [8]	Anomaly	Traffic	multitrust	Data mining
Specification Based Monitoring of AODV [21]	Specification	Traffic	multitrust	Pattern matching
Sarafijanović Technique [19]	Anomaly	Traffic	multitrust	Data mining
Vigna Technique [13]	Signature	Traffic	multitrust	
Bella Technique [10]	Reputation	Behavior	multitrust	Pattern matching

From the above table it is evident that maximum number of IDS techniques are implementing the traffic based data collection technique, which is said to be more effective when compared with the behavior based data collection technique.

5. CONCLUSION

In this paper, we performed a general comparative survey on the various existing intrusion detection systems for Ad hoc networks based on the various approaches applied in the IDS for providing security to the Ad hoc network. The approaches include the various detection techniques applied and the type of data collection approach used and the trust model applied to the system and the type of data analysis technique implemented in the intrusion detection system which performs malicious behavior detection in the Ad hoc networks. As per the analysis performed it is shown that maximum number of intrusion detection techniques are implementing the traffic based approach for data collection and hence it is proved to be more effective when compared with the behavior based approach in the detection of malicious nodes in a MANET.

REFERENCES

[1] J. Kumar, "802.11 DCF in Dynamic MANET On-demand Routing," *International Journal of Informatics and Communication Technology (IJ-ICT),* vol/issue: 2(2), pp. 85-92, 2013.
[2] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *The 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, USA, pp. 275–283, 2000.
[3] V. Chandola, *et al.*, "Anomaly detection for discrete sequences: a survey," *IEEE Trans. Knowl. Data Eng.*, vol/issue: 24(5), pp. 823–839, (2012).
[4] V. Chandola, *et al.*, " Anomaly detection: a survey," *ACM Comput. Surv.*, vol/issue: 41(15), pp. 1–58, 2009.
[5] D. Farid and M. Rahman, "Learning intrusion detection based on adaptive bayesian algorithm," in *11th International Conference on Computer and Information Technology*, Khulna, Bangladesh, pp. 652–656, 2008.
[6] F. Li, *et al.*, "Behaviour profiling on mobile devices," in *International Conference on Emerging Security Technologies*, Canterbury, UK, pp. 77–82, 2010.
[7] S. Shin, *et al.*, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Trans. Ind. Inf.*, vol/issue: 6(4), pp. 744–757, 2010.
[8] Y. Zhang, *et al.*, "Intrusion detection techniques for mobile wireless networks," *Wireless Netw.*, vol/issue: 9(5), pp. 545–556, 2003.
[9] S. Zhong, *et al.*, "A clustering approach to wireless network intrusion detection," in *17th International Conference on Tools with Artificial Intelligence*, Hong Kong, pp. 196, 2005.
[10] G. Bella, *et al.*, "Managing reputation over manets," in *Fourth International Conference on Information Assurance and Security*, Naples, Italy, pp. 255–260, 2008.

[11] P. K. Krishnappa and B. R. P. Babu, "Investigating Open Issues in Swarm Intelligence for Mitigating Security threats in MANET," *International Journal of Electrical and Computer Engineering,* vol/issue: 5(5), 2015.
[12] F. Haddadi and M. Sarram, "Wireless intrusion detection system using a lightweight agent," in *Second International Conference on Computer and Network Technology*, Bangkok, Thailand, pp. 84–87, 2010.
[13] G. Vigna, *et al.*, "An intrusion detection tool for aodv-based ad hoc wireless networks," in *20th Annual Computer Security Applications Conference*, Tucson, AZ, USA, pp. 16–27, 2004.
[14] R. Mitchell and I. R. Chen, "A hierarchical performance model for intrusion detection in cyber-physical systems," in *Wireless Communication and Networking Conference*, Cancun, Mexico, pp. 2095–2100, 2011.
[15] L. Ying, *et al.*, "The design and implementation of host-based intrusion detection system," in *Third International Symposium on Intelligent Information Technology and Security Informatics*, Jinggangshan, China, pp. 595–598, 2010.
[16] Y. Mao, "A semantic-based intrusion detection framework for wireless sensor network," in *6th International Conference on Networked Computing*, Gyeongju, South Korea, pp. 1–5, 2010.
[17] Z. Xiao, *et al.*, "An anomaly detection scheme based on machine learning for wsn," in *1st International Conference on Information Science and Engineering*, Nanjing, China, pp. 3959–3962, 2009.
[18] W. Hairui and W. Hua, "Research and design of multi-agent based intrusion detection system on wireless network," in *International Symposium on Computational Intelligence and Design*, Wuhan, China, vol. 1, pp. 444– 447, 2008.
[19] S. Sarafijanović and J. Y. Boudec, "An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal, and memory detectors," in G. Nicosia, et al. (Eds.), *Artificial Immune Systems, Lecture Notes in Computer Science*, vol. 3239, pp. 342–356, 2004.
[20] H. Han, *et al.*, "Using data mining to discover signatures in network-based intrusion detection," in *International Conference on Machine Learning and Cybernetics*, Beijing, China, vol. 1, pp. 13–17, 2002.
[21] C. Y. Tseng, *et al.*, "A specification-based intrusion detection system for aodv," in *1st Workshop on Security of Ad hoc and Sensor Networks*, Fairfax, VA, USA, pp. 125–134, 2003.
[22] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *The International Federation for Information Processing TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, Portoroz, Slovenia, pp. 107–121, 2002.
[23] S. Misra, *et al.*, "Energy efficient learning solution for intrusion detection in wireless sensor networks," *Second International Conference on Communication Systems and Networks*, Bangalore, India, pp. 1–6, 2010.
[24] B. Foo, *et al.*, "Adepts: adaptive intrusion response using attack graphs in an e-commerce environment," in *International Conference on Dependable Systems and Networks*, Yokohama, Japan, pp. 508–517, 2005.
[25] J. Hall, *et al.*, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *International Conference on Wireless And Mobile Computing, Networking And Communications*, Montreal, QC, Canada, vol. 2, pp. 17–24, 2005.
[26] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol," in *The 3rd international symposium on Mobile ad hoc networking*.

BIOGRAPHIES OF AUTHORS

Mr. G.Gopichand. is currently working as Assistant Professor and Research Scholar in the School of Computing Science and Engineering at VIT University. His research work focuses network security, Intrusion Detection Systems, and Wireless ad-hoc networks.

Dr. RA. K. Saravanaguru. is currently working as Associate Professor in the Schoool of Computing Science and Engineering at VIT University. His area of interest mainly focuses Context Aware Systems, Middleware Development, VANETS, Web Services, and Cloud Computing.