

A SURVEY ON ANOMALY DETECTION METHODS FOR AD HOC NETWORKS

Marianne A. Azer
National Telecommunication Institute, Cairo, Egypt
marazer@nti.sci.eg

Sherif M. El-Kassas
American University in Cairo, Cairo, Egypt
sherif@aucegypt.edu

Magdy S. El-Soudani
Cairo University, Faculty of Engineering, Cairo, Egypt
mesloudani@menanet.net

ABSTRACT

Mobile ad hoc networks have recently been the topic of extensive research. The interest in such networks stems from their ability to provide temporary and instant wireless networking solutions in situations where cellular infrastructures are lacking and are expensive or infeasible to deploy. Despite their desirable characteristics, vital problems concerning their security must be solved in order to realize their full potential. Various security controls, such as the use of encryption and authentication techniques, have been proposed to help reduce the risks of intrusion. However since such risks cannot be completely eliminated there is a strong need for intrusion detection systems for ad hoc network security. Among intrusion detection techniques anomaly detection may prove to be more economic from the resources point of view, which is more suitable for the resource constrained ad hoc networks. Therefore, in this paper we present a survey on anomaly detection in ad hoc networks. In order to distinguish between the different approaches used for anomaly detection in ad hoc networks in a structured way, we have classified those methods into three categories: classifier based anomaly detection, finite state machine anomaly detection and the game approach anomaly detection. We describe each method in details and give examples for its applications in ad hoc networks.

Keywords: Ad hoc networks, anomaly detection, intrusion detection, security.

1 INTRODUCTION

A wireless ad-hoc network consists of a collection of autonomous peer mobile nodes forming a temporary or permanent network, that self-configure to form a network and have no pre-determined organization of available links. The broadcast nature of the radio channel introduces characteristics in ad hoc wireless networks that are not usually present in their wired counterparts. In particular, a radio channel allows a node to transmit a signal directly to any other node.

Mobile ad hoc networks are generally characterized by the lack of infrastructure, dynamic network topology, distributed operation, bandwidth constraints, variable capacity links, use of low power devices, limited CPU and memory, limited physical security, and complexity of design of network protocols. However, ad hoc wireless networks are highly appealing for many reasons. Due to their

inherently distributed nature, they are more robust than their cellular counterparts against single-point failures, and have the flexibility to reroute around congested nodes. Furthermore, mobile ad hoc networks can conserve battery energy by delivering a packet over a multihop path that consists of short hop by hop links. They can be rapidly deployed and reconfigured. Hence, they can be tailored to specific applications. Wireless ad-hoc networks are used in situations where a network must be deployed rapidly, without an existing infrastructure. The set of applications for mobile ad hoc networks is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. Until recently, these networks have mainly been associated with military applications. However, with the availability of wireless technologies such as Bluetooth and the IEEE 802.11 WLAN, and the development of next generation networks, civilian applications, such as

personal area networks, sensor networks, and disaster area networks are being envisioned.

There are recent research efforts, e.g., [1], [2], in providing various attack prevention schemes to secure the ad hoc routing protocols, i.e., authentication and encryption schemes. Such intrusion prevention measures do not address all the security concerns of ad hoc networks. This underscores the need for intrusion detection as an important security research area under the umbrella of ad hoc network security. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised [3].

For the purpose of this paper, intrusion detection techniques can be categorized¹ into misuse detection and anomaly detection. In misuse detection, decisions are made on the basis of knowledge of a model of the intrusive process and what traces it may leave in the observed system. Legal or illegal behavior can be defined and observed behavior compared accordingly. Such a system tries to detect evidence of intrusive activity irrespective of any knowledge regarding the background traffic (i.e., the normal behavior of the system). Misuse detection systems, e.g., IDIOT [4] and STAT [5], use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. A typical misuse detection system is shown in Figure 1. The main advantage of misuse detection is that it can accurately and efficiently detect instances of known attacks. The main disadvantage is that it lacks the ability to detect the newly invented attacks. In anomaly detection, for example the anomaly detector in IDES [6], a baseline profile of normal system activity is created. Any system activity that deviates from the baseline is treated as an anomaly, i.e. possible intrusion. A typical anomaly detection system is shown in Figure 2. Although this method suffers from the disadvantage of having a high false positive rate, however it has the advantages of not requiring prior knowledge of intrusions and can thus detect new intrusions. Another advantage which makes it suitable for an ad hoc network is that there is no need to store a database for attack profiles [3]. That is why in this paper we focus on the anomaly detection and give a survey on different methods used for anomaly detection in ad hoc networks, while classifying these methods to three main categories. instructions are for authors of submitting the research papers to the Ubiquitous computing and communication Journal. Please prepare your manuscripts in accordance with these guidelines.

¹ Intrusion detection systems can also be classified differently but we focus on misuse and anomaly detection as this is our scope of interest

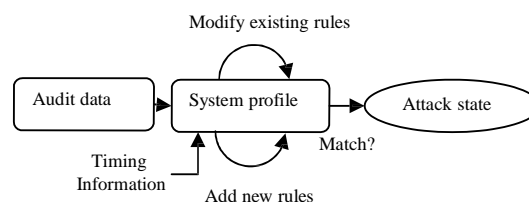


Figure 1: A typical misuse detection system

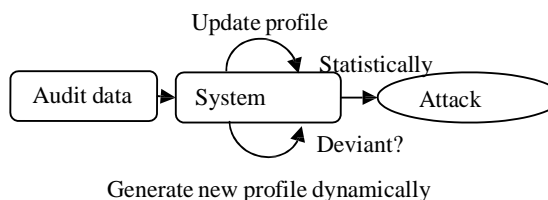


Figure 2: A typical anomaly detection system

The remainder of this paper is organized as follows. In section 2 we describe anomaly detection using a classifier and discuss its general working procedure. Section 3 considers anomaly detection using the finite state machines. Section 4 introduces the game approach concept and discusses anomaly detection using the game approach, whereas section 4 focuses on the anomaly detection using machine learning. Finally, in section 5 we conclude this paper and discuss possible future work.

2 ANOMALY DETECTION USING A CLASSIFIER

In this section we focus on the anomaly detection using a classifier. Anomaly detection depends on the idea that normal characteristics behavior can be distinguished from abnormal behavior. Referring to [7], information theoretic measures called entropy and conditional entropy are used to describe characteristics of normal information flows, and classification algorithms are used to build anomaly detection models. A classifier can be used to predict the normal incoming event given the current event. If during the monitoring phase the next event is not the one predicted by the classifier, it is considered as an anomaly. When constructing a classifier, features with high information gain [8] are needed. A classifier needs feature value tests to partition the original data set into pure subsets, each ideally with one (correct) class of data [9]. Figure 3 depicts the process for anomaly detection using a classifier described in [9].

To gain a deeper understanding of the procedure of anomaly detection using a classifier, shown in Figure 3, we consider the example given in [9]. In

that paper, two attacks were considered. The first attack was the route logic compromise and more specifically misrouting which is forwarding a packet to an incorrect node. The second attack was the traffic pattern distortion which changes the traffic normal behavior by dropping packets, injecting packets with faked source addresses, or denial of service. According to Figure 3, the most important task to start with is choosing and collecting suitable audit data for each attack. Hence, audit data was chosen to be local routing information including cache entries and traffic statistics and position locator or GPS which provide location and velocity information of nodes in the whole neighborhood. Next, comes the second step which is features construction. For the feature selection first a large feature set was constructed to cover a wide range of behaviors and a small number of training runs was conducted with the whole set of features on small data traces randomly chosen from a previously stored audit logs. Now, according to Figure 3, a classifier must be computed using training data and must test real data. Therefore, a corresponding model was built and the features whose weights exceeded a minimum threshold were selected into the essential features set. Two classifiers were chosen RIPPER [10] and the Support Vector Machine SVM light [11]. According to [9], RIPPER is a typical classifier in that it searches the given feature space and computes rules that separate data into appropriate classes. SVM Light instead pre-processes the data to represent patterns in much higher dimension than the given feature space. The heuristic is that with sufficiently high dimension, data can be separated by a hyperplane, thus achieving the goal of classification. SVM Light can produce a more accurate classifier than RIPPER when there are underlying complex patterns in the data that are not readily represented by the given set of features.

For the post processing phase; a window was chosen with a length $2l+1$, where l is a chosen parameter. For a region within the current window if the number of abnormal observation was greater than l , the region was marked as abnormal and every observation in this region as well. The window was shifted by a window size and the process was repeated until the whole trace was processed and all continuous abnormal regions were counted as one intrusion session.

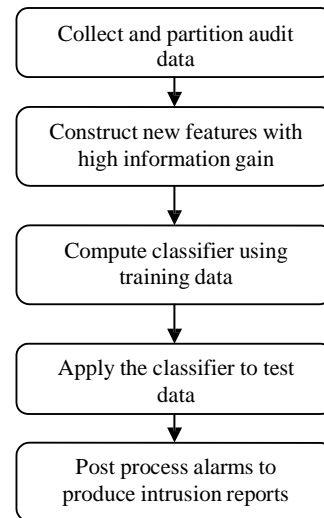


Figure 3: Anomaly detection using a classifier

The same anomaly detection approach can be applied for detecting intrusions based on anomalous behavior of neighboring nodes. For example in [12], each node monitors particular traffic activity within audio range. Intrusions are associated with pairs of IPv6 and corresponding MAC addresses.

A similar idea for anomaly detection using a classifier was proposed in [13] to investigate the performance of multi-path routing under routing attacks. It is called Statistical Analysis of Multi-path (SAM). The main idea of SAM was based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks. Hence, it was possible to examine such statistics to detect this type of routing attacks. For example, the so-called “wormhole attack” makes the tunneled link between the two attackers extremely attractive to routing requests (much less hop count than other routes), it is expected that majority of the obtained routes will contain that link. The statistics proposed were the relative frequency of each distinctive link that appears from route discovery and the difference between the most frequently appeared link and the second most frequently appeared link from one route discovery. An alternative statistic was the probability mass function (PMF) of the relative frequency of distinctive links in the set of all routes. The samples collected from the network under normal condition form the training set, and a classifier could be used to detect routing anomalies. More detailed examples for detecting abnormal updates to routing tables and detecting abnormal activities in other layers are given in [9]. Other detailed examples for detecting the route logic compromise and the traffic distortion attacks are given in [14].

3 ANOMALY DETECTION USING FINITE STATE MACHINES

A finite state machine (FSM) or finite automation is a model of behavior composed of states, transitions and actions. In this model, a state stores information about the past, i.e. it reflects the input changes from the system start to the present moment. A transition indicates a state change and is described by a condition that would need to be fulfilled to enable the transition. An action is a description of an activity that is to be performed at a given moment. There are several action types: entry action, exit action, and transition action.

The finite state machine has been used to detect attacks on the DSR protocol in [15]. First, an algorithm for monitor selection for distributed monitoring all nodes in networks was proposed and then the correct behaviors of the nodes according to DSR were manually abstracted. Using this method has the advantage of detecting intrusions without the need of trained data or signatures, also unknown intrusions can be detected with few false alarms. As a result, a distributed network monitor architecture which traces data flow on each node by means of finite state machine was proposed. A finite state machine model of local AODV behavior was used in [16]. In this model, each node does see the subset of transmissions generated by itself and its neighbors. This subset is referred to as the local routing instance

(LRI). The local node associates each transmission in a LRI with its sender and its receiver or in the case of its own outgoing broadcast RREQs with multiple receivers. Figure 4 depicts the finite state machine model of local AODV behavior, and the final states are shaded.

Transitions to timeout states occur when the local node fails to observe any additional activity for the LRI within a suitable duration. Transitions to final state (complete LRI) occur when the monitored node is observed to forward a RREP. Upon reaching a final state, the FSM is considered complete and the local node stores the completed sequence of transitions observed for the monitored node in the k^{th} LRI. These completed sequences are used to derive a matrix T containing an estimate of the probability of observing each state transition at least once during a LRI. Certain transitions can reasonably be considered more suspicious than others, especially when the corresponding value in the transition matrix is excessively large or unusually small. The conjecture of this work is that selfish behavior among the local node's neighbors can be observed in the form of aberrant transition matrices. Described at a high level, this detection approach applies a series of statistical tests to attributes extracted from the set of transition matrices for all of the local node's neighbors. The tests are designed to determine a threshold value of each attribute that separates cooperative neighbors from selfish ones.

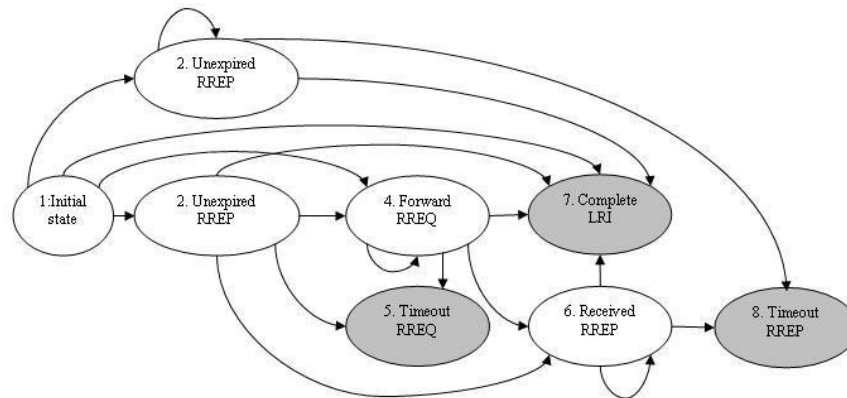


Figure 4: Finite state machine model of local AODV behavior

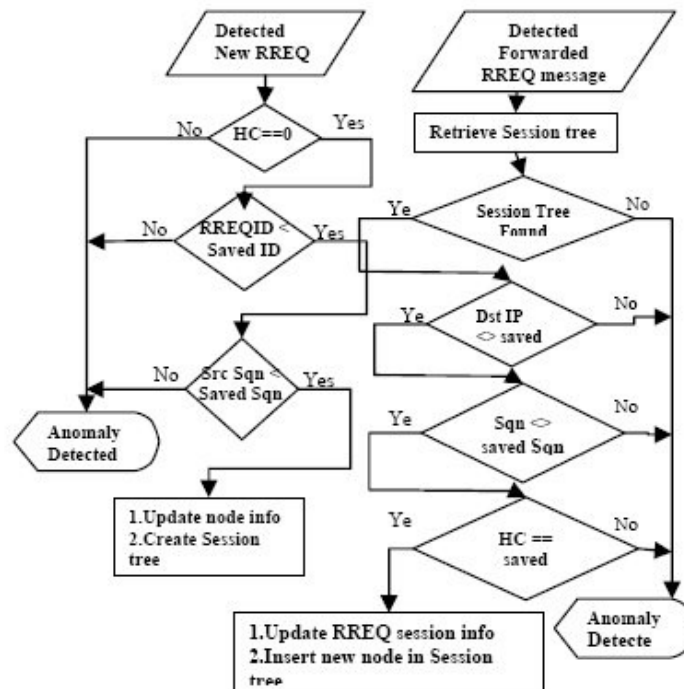


Figure 5: Analysis of RREQ messages [17]

In [17] a specification-based IDS for AODV protocol was suggested. The IDS is implemented as a two stage process. The first stage is to choose network monitoring nodes (NMs) using a clustered network-monitoring selection algorithm. In the second stage, the NM nodes run the monitoring protocol that will be responsible for monitoring the flow of the RREQ and RREP messages. The main focus of this newly devised protocol is to ensure the correct order in which the routing messages (RREQ/RREP) are exchanged as well as the integrity of the contents of these messages. To be able to analyze a RREQ-RREP flow and verify that it abides by the derived constraints each two consecutive messages need to be compared. Also different RREP flows initiated by different intermediate nodes need to be distinguished from each other, therefore an extra field identifying the IP address for the node initiating the RREP flow will also be added to the RREP header. NM nodes listen in promiscuous mode to the wireless link. Each NM node is responsible to monitor the routing traffic belonging to the nodes in its cluster. For each detected routing message (RREQ or RREP), the MAC and IP addresses of the source node are validated. If source node is one of the nodes to be monitored then the routing message will be analyzed. Otherwise neighboring NM will be informed about the detected message. On receiving messages from neighboring NMs, each NM will analyze the message contents. Therefore, the flow

chart presented in [17], and shown in Figure 5 can be considered as a finite state machine.

4 ANOMALY DETECTION USING GAME APPROACH

In this section, we focus our attention on the game theory and its applications in ad hoc networks. We first give a brief introduction about the game theory and the game approach and elaborate their uses in ad hoc networks with examples. Game theory is a branch of applied mathematics that uses models to study interactions with formalized incentive structures “games.” Game theory provides us with tools to study situations of conflict and cooperation. Such a situation exists when two or more decision makers who have different objectives act on the same system or share the same set of resources. Therefore, game theory is concerned with finding the best actions for individual decision makers in such situations and recognizing stable outcomes. Some of the assumptions that one makes while formulating a game are:

1. There are at least two players in a game and each player has two or more well-specified choices or sequences of choices.
2. Every possible combination of plays available to the players leads to a well-defined end-state (win, loss, or draw) that terminates the game.
3. Associated with each possible outcome of the game is a collection of numerical payoffs, one to each player. These payoffs represent the value of the

outcome to the different players.

4. All decision makers are rational; that is, each player, given two alternatives, will select the one that yields the greater payoff.

Game theory has been traditionally divided into cooperative game theory and non-cooperative game theory. The two branches of game theory differ in how they formalize interdependence among the players. In non-cooperative game theory, a game is a detailed model of all the moves available to the players. Non-cooperative games can be classified as static or dynamic based on whether the moves made by the players are simultaneous or not. Non-cooperative games can also be classified as complete information games or incomplete information games, based on whether the players have complete or incomplete information about their adversaries in the game. In contrast, cooperative game theory abstracts away from this level of detail and describes only the outcomes that result when the players come together in different combinations [18].

In [19], the interaction between an attacker and an intrusion detection system is modeled as a basic signaling game which falls under the category of multi-stage dynamic non-cooperative game with incomplete information. The intrusion detection game is played between an attacker and IDS. The objective of the attacker is to send a malicious message from some attack node, with the intention of attacking the target node. The intrusion is deemed successful when the malicious message reaches the target machine without being detected by the host IDS. It is assumed that an intrusion is detected and the intruding node is blocked when a message sent by a probable intruder is intercepted and the host IDS can say with certainty that the message is malicious in nature. For an IDS, the basic performance criteria is the rate of false alarms in the system. There exists a tradeoff between the reduction of false alarms by decreasing the sensitivity of the system with the increase in rate of undetected intrusions. The cost associated with an undetected intrusion is much more severe than the cost associated with false alarms. In other words, the strategy of the IDS will be to pick the optimal strategy out of its available set, in response to a message from the sending node. The choice of strategy must be based on the receivers prior beliefs, such that it is able to maximize the effective payoff by minimizing the cost due to false alarms and missed attacks. Let the probability of a particular malicious node exhibiting malicious activity be s , and the probability of the same node exhibiting normal behavior be $1 - s$. The particular choice that the attacker makes is his message. The IDS detects this decision with a probability t and misses it with a probability $1 - t$ depending on his beliefs. The game is depicted in Figure. 6, the IDS has a gain of y_{success} for detecting an attack whereas there is a cost involved whenever the IDS misses an

attack (y_{miss}) or when it raises a false alarm ($y_{\text{false alarm}}$). On the other hand, the intruder has a gain of $-O_{\text{intrude}}$ on a successful undetected intrusion and a cost of O_{caught} on being detected and blocked. False alarms have a zero cost value to the attacker.

5 ANOMALY DETECTION USING MACHINE LEARNING

In addition to the approaches described in the previous section, there is another approach, which is the anomaly detection based on machine learning. The first type that we shall introduce in this section is the Markov Chain approach. A Markov chain [20] is a series of states of a system that has the Markov property. A series with the Markov property is such that the conditional probability distribution of the state in the future, given the state of the process currently and in the past, is the same distribution as one given only the current state. In other words, the past states carry no information about future states. At each time the system may have changed from the state it was in the moment before, or it may have stayed in the same state. The changes of state are called transitions.

A Markov Chain based anomaly detection algorithm characterizes the normal behavior of the system and captures the characteristics of the temporal sequence of the system audit data by utilizing which states it moves between and with what probabilities. Normal profiles are used to characterize the normal behavior of the system. One of the difficulties using the Markov Chain to construct the normal profile is to define the states.

In [21] anomaly detection for ad hoc networks using Markov chains was presented. The statistical features of interest were collected from the routing cache of mobile nodes, such as to reflect the mobility of the network, to construct a Markov chain as the normal profile. The use of the Markov chain could capture the temporal dependency among the network activities. Vector Quantization (VQ) approach was used in this process to convert continuous raw audit data to categorized data items with minimum errors. In order to mitigate the impact of dynamics of MANETs on the construction of the normal profile, for those data items whose probability were below some threshold, they were converted into a common "rare" symbol. The output of the VQ was then used to construct a Markov chain model, which employed conditional probabilities in its transition probability matrix to represent the temporal profile of normal behavior. The Markov chain model, considering the ordering property, characterized the normal changes of the routing caches with probabilities. It determined the probability of the next valid change, given the previous N changes. The Markov chain model was then turned into a classifier, which served as the detection algorithm. Conditional entropy was

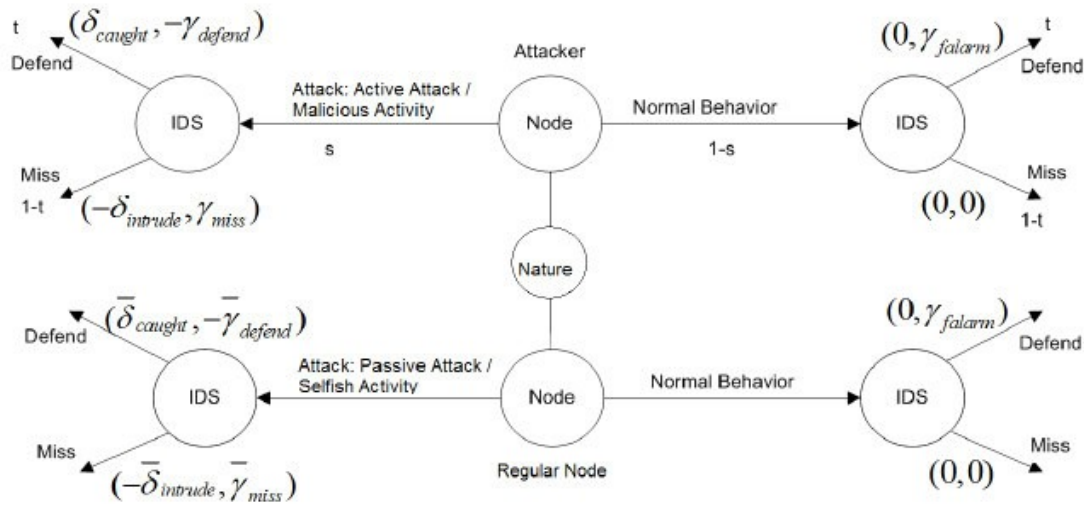


Figure 6: An Attacker-IDS Basic Signaling Game [19]

used in this process to determine the proper window size which parameterizes the Markov chain model, thus avoiding the tedious trial-and-error process. In the detection process, the distance of the current transition was defined based on the transition probability matrix recorded in the Markov chain model. A single deviation from the Markov chain did not always correspond to the occurrence of an attack. An alert was generated only when the average distance over the near past was beyond some preset threshold value. The parameters used in the detection algorithm were tuned properly using the defined performance metrics.

Two features sensitive to routing disruption attacks were used: PCR -Percentage of the change in route entries, and PCH -Percentage of the change in number of hops. They were used separately to construct the classifier and watch the performance. Simulation results showed that classifier constructed using PCH performs better compared to classifier constructed using PCR. Therefore, the classifier constructed using PCH was used as the local detection engine in a Zone Based Intrusion Detection System (ZBIDS).

Based on the locally collected statistical measures that reflect the mobility of the network, a Markov Chain is constructed to act as the normal profile, which is then used to build a classifier. Ordering property is considered and the transition probability is used to define the distance of the trace and the normal profile. The aggregation algorithm could further reduce the false positive ratio and increase the detection ratio.

A Markov Decision Process (MDP) is a model for sequential stochastic decision problems was

used in [19] to have a reward concept for IDS that will gain that reward only if it chooses the right cluster for protection. The target is to predict the future behavior of the attacker. By supposing that the past behavior of the attacker and so past states of the system are known, the system's task becomes predicting the most vulnerable node, which attacker most probably will attack. The actions change the states and the effect of the actions on the states is captured by the transition function. The transition function assigns a probability distribution to every (state, action) pair. Finally, the reward function assigns a real value to each (state, action) pair, which describes the immediate reward (or cost) of executing this action in that state. The states of the MDP for the intrusion detection system in [19] correspond to the states of the predictive model.

Each action of the MDP corresponds to one intrusion detection of a sensor node. When an intrusion is detected on node, the MDP could either accept this detection or it selects another node. The rewards of the MDP encode the utilities of detecting an intrusion. For simplicity, a constant value is assigned for the reward if the intrusion is detected.

Another type of machine learning anomaly detection is the use of Hidden Markov Model (HMM). Traditionally, people have used Markov chains to successfully model a lot of real world processes. But for some other processes, the strict assumption of Markov that next state is dependent only upon the current state will not hold, thus we need to find more generally models to deal with these processes while at the same time withhold some good properties of Markov model. These principles motivated people to generate the HMM.

HMM is a double embedded stochastic process with two hierarchy levels. The upper level is a Markov process that the states are unobservable. Observation is a probabilistic function of the upper level Markov states. Different Markov states will have different observation probabilistic functions.

In [22] a statistical framework that allows the incorporation of prior information about the normal behavior of the network and of network was presented. (HMMs) were used to provide a generative view of the dynamic evolution of the hop count distribution. Results have shown that simple attacks can be detected by an anomaly detection framework. However, detection of more complex attacks requires incorporation of prior knowledge in the HMMs.

In [23], anomaly detection was done using one class support vector machines. After having transferred the anomaly detection process into an unsupervised classification problem, a one-class Support Vector Machines (1-SVMs) [24] was used for anomaly detection, as the 1-SVM is an unsupervised classification algorithm without using the concept of clustering. It is a direct derivative of SVM algorithm and inherits all the advanced properties of SVM algorithms.

6 CONCLUSIONS AND FUTURE WORK

Due to the vulnerability of ad hoc networks, intrusion prevention measures such as encryption and authentication are used to reduce intrusions, however they cannot eliminate them. Hence, there is a strong need for intrusion detection as a frontline security research area for ad hoc network security. Among intrusion detection techniques anomaly detection is more economic from the resources point of view, which is more suitable for the resource constrained ad hoc networks. In order to give a clear vision about the use of this technique, we presented in this paper a classified survey of the methods that are used for anomaly detection in ad hoc networks. Some anomaly detection methods such as classifiers, state machines, game approach, and machine learning are suitable for well understood protocols such as routing protocols. However, since self contained protocols are limited in ad hoc networks, these approaches might not be appropriate in some cases where we need to detect attacks at, for example, the application level. We suggest the use of attack graphs for ad hoc networks. Based on this attack graph there are two methods for anomaly detection that rely basically on the constructed attack graph for intrusion detection. The first is based on the attack graph adjacency matrix and helps in the prediction of a single or multiple step attack and in the categorization of intrusion alarms' relevance. The second method used the attack graph distances for correlating intrusion events and building attack

scenarios. Therefore, this approach might be more appropriate to ad hoc networks' collaborative and dynamic nature, especially at the application level. In the future we intend to build a full ad hoc network environment and use the suggested anomaly detection approach to evaluate it and compare it with other anomaly detection techniques.

REFERENCES

- [1] Y. Hu, A. Perrig, and D. B. Johnson. Ariadne, A secure on-demand routing protocol for ad hoc networks, in Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), September 2002.
- [2] P. Papadimitratos and Z. J. Hass, Secure routing for mobile ad hoc networks, in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.
- [3] A. Mishra, K. Nadkarni and A. Patcha, Intrusion detection in wireless ad hoc networks, IEEE Wireless Communications, vol. 11, no. 1, Feb 2004, pp. 48 – 60.
- [4] S. Kumar and E. H. Spafford, A software architecture to support misuse intrusion detection, In Proceedings of the 18th National Information Security Conference, pp. 194-204, 1995.
- [5] K. Ilgun, R. A. Kemmerer, and P. A. Porras, State transition analysis: A rule-based intrusion detection approach, IEEE Transactions on Software Engineering, pp.181-199, March 1995.
- [6] T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey, A real-time intrusion detection expert system (IDES) - final technical report, Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, February 1992.
- [7] T. M. Cover and J. A. Thomas, Elements of Information Theory, Wiley, 1991.
- [8] T. Mitchell, Machine Learning, McGraw-Hill, 1997.
- [9] Y Zhang, W Lee, and Y Huang, Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET 2003.
- [10] W. Cohen, Fast effective rule induction, In Proc.12th International Conference on Machine Learning, pages 115-123, Morgan Kaufmann, 1995.
- [11] T. Joachims, Making large-scale SVM learning practical, chapter 11, MIT-Press, 1999.
- [12] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, Secure Routing and Intrusion Detection in Ad Hoc Networks, percom, pp. 191-199, Third IEEE International Conference on Pervasive Computing and Communications (PerCom'05), 2005.
- [13] N. Song, L. Qian, X. Li, Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach, ipdps, p. 289a, 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05), Workshop

17, 2005.

[14] Y. Huang, W. Fan, W. Lee, P. Yu, Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies, *icdcs*, p. 478, 23rd IEEE International Conference on Distributed Computing Systems (ICDCS'03), 2003.

[15] P. Yi, Y. Jiang, Y. Zhong, and S. Zhang, Distributed Intrusion Detection for Mobile Ad hoc Networks, *Proceedings of the 2005 Symposium on Applications and the Internet Workshops (SAINT-W'05)*, pp.94-97.

[16] B. Wang, S. Soltani, J. Shapiro, and P. Tan, Local Detection of Selfish Routing Behavior in Ad Hoc Networks, *ispan*, pp. 392-399, 8th International Symposium on Parallel Architectures, Algorithms and Networks (ISPA'05), 2005.

[17] H. Hassan, M. Mahmoud, and S. El-Kassas, "Securing the AODV Protocol Using Specification-Based Intrusion Detection," the 2nd ACM International Workshop on QoS and Security for Wireless and Mobile Networks, October 2—6, 2006, Torremolinos, (Malaga), Spain, p.p. 33-36, ISBN: 1-59593-486-3.

[18] A. Patcha and J.-M. Park, A game theoretic formulation for intrusion detection in mobile ad hoc

networks, *International Journal of Network Security*, Vol. 2, No. 2, Mar. 2006, pp. 146-152.

[19] A. Patcha and J. Park, A game theoretic approach to modeling intrusion detection in mobile ad hoc networks, 2004 IEEE Workshop on Information Assurance and Security, June 2004.

[20] J. Norris, *Markov Chains*, Series: Cambridge Series in Statistical and Probabilistic Mathematics (No. 2), 1998.

[21] Bo Sun, Kui Wu, Udo W. Pooch, Alert aggregation in mobile ad hoc networks, *Workshop on Wireless Security 2003*: pp. 69-78.

[22] A. Cardenas, V. Ramezani, J. Baras, HMM Sequential Hypothesis Tests for Intrusion Detection in MANETs Extended Abstract, Tech rept. 2003.

[23] Hongmei Deng, Roger Xu, Jason Li, Frank Zhang, Renato Levy, Wenke Lee, "Agent-Based Cooperative Anomaly Detection for Wireless Ad Hoc Networks," *icpads*, pp. 613-620, 12th International Conference on Parallel and Distributed Systems - Volume 1 (ICPADS'06), 2006.

[24] N. Vapnik, "Statistical Learning Theory", Wiley, 1998.