International Journal of Information Technology and Knowledge Management
July-December 2010, Volume 2, No. 2, pp. 305-310

A COMPREHENSIVE SURVEY ON INTRUSION DETECTION IN MANET

Sunita Sahu[1] & Shishir K. Shandilya[2]

With the progression of computer networks extending boundaries, Mobile ad hoc network (MANET) has emerged as a new frontier of technology to provide any where, any time communication. Due to its deployment nature, MANETs are more vulnerable to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, limited power and limited bandwidth. The Prevention methods like authentication and cryptography techniques alone are not able to provide the security to these types of networks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. In this paper we have surveyed various intrusion detection techniques in MANET and analyzed their fruitfulness.

Keywords: Mobile Ad-hoc Network, Security, Intrusion Detection.

1. Introduction

A mobile ad hoc network (MANET) is an autonomous system of mobile stations connected by wireless link to form a network. It does not rely on predefined infrastructure to keep the network connected therefore it is also known as infrastructure less networks. In MANET, each node can communicate with node in its range and those which are beyond the range can communicate using the concept of multi hop communication in which other node relay the packets [15]. In the MANET the network topology may change rapidly and unpredictably. To deals with this, nodes exchange information about network topology. So the functioning of the ad hoc network depends on the trust and cooperation between nodes.

The mobile ad hoc network have many salient characteristics such as dynamic topology, bandwidth constrained, variable link capacity, limited energy, limited physical security[16]. Due to these features mobile ad hoc networks are particularly vulnerable to various types of attacks. Various intrusion detection methods are developed for detecting the intrusion in the wired networks. Due to the mobility of nodes, the intrusion detection methods of wired network can not be used for MANETS.

Intrusion detection is a security mechanism which is used to identify those who are trying to break and misuse the system without authorization and those who have legitimate access to the system but misusing the privileges [28]. Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System (IDS) [21].

IDS works under following assumptions:

- User and program activities are observable.
- Normal and intrusive activities must have distinct behaviors.

The Intrusion detection System monitors the activities of the system, analyze the activities to determine that any of the activity is violating the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity. [30]

Achieving security within ad hoc networks is very difficult because of the following reasons [27]:

a. Continuous Changing Topology: In MANET, due to mobility of the nodes, topology changes very frequently.

b. Open and Vulnerable Media: Many types of attacks are possible in the ad hoc networks such as Packet dropping attack, Resource consumption attack, Fabrication attack, DOS attack, Route invasion attack, node isolation attack [15].flooding attack[16],spoofing masquerading, impersonation are possible.

c. Roaming in Dangerous Environment: Any malicious node or misbehaving node can create hostile attack or deprive all other nodes from providing any service.

Depending upon the technique used, the intrusion detection can be classified in 3 categories:

1. Misused or signature based IDS;

[1] M.Tech Scholar, PG Dept. of Computer Science & Engineering, NRI Institute of Information Science And Technology, Bhopal, India

[2] Head, PG Dept. of Computer Science & Engineering, NRI Institute of Information Science and Technology, Bhopal, India

Email: [1]sunitasahu101@gmail.com, [2]shishir.sam@gmail.com

2. Anomaly based IDS;
3. Specification based IDS.

In misuse based intrusion detection [4], also called signature based detection, a pre-written rule or pattern is used to match an attack. In anomaly detection, a normal profile of user is kept in the system and then the captured profile is compared. If IDS found any activity that deviated from the normal profile is detected as anomaly. In Specification based intrusion detection, some set of constraints are defined for correct operation of program and then operations are monitored against define constraints. A mismatch is reported as a attack.

The organization of this paper is as follows. In section 2 we discussed about the evolution of IDs system. Section 3 presents the recent scenario of intrusion Detection System. In section 4, we discuss the challenges and finally, the conclusion and future directions are given in section 5.

2. EVOLUTION

Intrusion detection in MANET is addressed by various researchers and has been a major research area. In 1987 the dinning proposed a model of a real-time intrusion-detection expert system that can able to detect break-ins, penetrations, and other forms of computer abuse [1]. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. In 2000, the S. Marti, T.J. Giuli, K. Lai and M. Proposed the "watchdog and pathrater" scheme that is used to detect & mitigate the effect of nodes that do not forward packets. Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent node to these packets. Watchdog promiscuously snoops to decide if the adjacent node forwards the packets without modifications or not. If the packets that are snooped match with the observing node's buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are flagged as having been dropped or modified.

The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious. Information about malicious nodes is passed to the Pathrater component for inclusion in path rating evaluation Pathrater on an individual node works to rate all of the known nodes in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular node's perspective. Nodes start with a neutral rating that is modified over time based on observed reliable or unreliable behavior during packet routing. Nodes that are observed by watchdog to have misbehaved are given an immediate rating of -100. It should be distinguished that misbehavior is detected as packet mishandling/modification, whereas unreliable behavior is detected as link breaks. It is shown from the experiments that these two components can well reflect the reliability of the nodes based on their packet forwarding performances. But the main problem of this scheme is vulnerability to blackmail attack [12].

In 2001 Knowledge-based intrusion detection systems was proposed by H.–Y. Chang, S.F. Wu and Y.F. Jou, which accumulate knowledge about attacks, examine traffic and try to identify patterns indicating that a suspicious activity is occurring. This approach can be applied against known attack patterns only and the utilized knowledge base needs to be updated frequently [7]. Knowledge-based systems are particularly attractive because of their low false alarm rates and high accuracy. A real-time knowledge-based network intrusion detection model for detecting link-state routing protocol attacks has been developed specifically for OSPF. In 2002, K.Paul and D westhoff proposed a approach that uses hash chain in route discovery process and an observer to detect the malicious behavior of the neighbor node and then neighbor report the behavior of the node to source node which calculate the rating for the accessed node and this rating is used to decide the malicious node but is not a pure IDS because it uses a cryptographic mechanism to detect the attacks[14]. In 2003, O. Kachirski and R. Guha proposed a sensor based approach to detect intrusion. In which multiple sensors are deployed and audit data is collected from all the sensors these data is merged to detect the intrusion [13].

In the same year, the Farooq Anjum and Dhanant Subhadrabandhu and Saswati Sarkar propossed a "signature based intrusion detection technique ",in which they assume that they knows the signature of the attack and all the system execute the IDS such nodes are said to constitute the intrusion detection subsystem. [4]. In [34], Bo Sun,Kui Wu and Udo W. Pooch introduce a geographic zone based intrusion detection frameworks that uses a location aware zone gateways node to collect and aggregate the alerts from intra-zone nodes. Gateway node in neighboring zone cans then further collaborate to perform the intrusion detection in the wide area and to attempt to reduce the false positive alarm. In Aug 2004, D. Sterne, et al. Present a cooperative intrusion detection architecture[9] that facilitates accurate detection of MANET-specific and conventional attacks. The architecture is organized as a dynamic hierarchy in which detection data is acquired at the leaves and is incrementally aggregated, reduced, and analyzed as it flows upward toward the root. The nodes at the top are responsible for security management functions.

In 2005, Ioanna Stamouli propossed RIDAN architecture which uses timed finite state machine to formally define attack against the AODV routing process. It uses a knowledge based methodology to detect the intrusion [2]. RIDAN operates locally in every participating nodes and observe the network traffic. This model can able to detect resource consumption attack, Sequence number attack and dropping routing packet attack.

In 2006 A. Karygiannis, E. Antonakakis, and A. Apostolopoulos Proposed a method to detect the critical node for MANET. Critical node is a node whose failure or malicious behavior disconnects or significantly degrades the performance of the network. After identification of critical node, these nodes are continuously monitored. To detect the critical node they used a vertex cut and edge cut approach [8]. A vertex-cut is a set of vertices whose removal produces a sub graph with more components than the original The critical node test detects nodes whose failure or malicious behavior disconnects or significantly degrades the performance of the network (i.e. introduces unacceptably long alternative paths). In an to reduce the number of tests performed, a lightweight trigger mechanism monitors network traffic and initiates a critical node test when it suspects such a condition might exist. The trigger mechanism is designed to allow false positives that the critical node test will later screen out. The only false-negatives that can occur are when there is no traffic to analyze on a cut-edge, but this condition is most likely short-lived and of no consequence. The trigger mechanism monitors the number of connections served by the test node as well as the number of packets traversing the test node. Note that the trigger itself can also serve as a lightweight alternative to the critical node test. The node performing the test is referred to as the testing node, and the node being tested is referred to as the node under test.

In [31] S.Bose, P.Yogesh and A.Kanan proposed a "Neural network approach for anomaly intrusion detection in ad hoc network using mobile agents". In this paper they used mobile agents that interact with machine, collect information. They used the user log file data obtained from local host for training the neural network for the purpose of intrusion detection. Their system obtain high intrusion detection rate and low false alarm rate

In Sept 2006 Xia Wang proposed end to end Wormhole detection method in wireless ah hoc networks [5]. They used AODV protocol. In the route discovery process the sender sets the Destination-only flag such that only the destination can able to respond to the ROUTE REQUEST packet. Once the ROUTE REQUEST packet reaches to the destination, it responds by sending a ROUTE REPLY with its current position. The sender retrieves the receiver's position from the ROUTE REPLY packet and estimates the lower bound of hops between the sender and the receiver. If the received route is shorter than the estimated shortest path, the corresponding route will be discarded. Otherwise, the sender will select the shortest path corresponding to the estimation. After the detection of wormhole by sender, it temporarily enable the path with wormhole and send the TRACE packet to the receiver through this path. This TRACE packet is forwarded by each intermediate node through the route with wormhole. When any node on the route receives the TRACE packet, it replies to sender by sending its current position and hop count to the destination node. Then the sender can calculate the increase of hop count at each node using the received position. If the increase of hop count at one node is not one comparing to its previous hop, then this node and its previous hop node are identified as the wormhole.

In Oct 2006 Yu Liu, Cristina Comaniciu and Hong Man proposed a Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks [6]. In this paper, they propose a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation. They studied the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios. The dynamic Bayesian game is a more realistic model, since it allows the defender to consistently update his belief on his opponent's maliciousness as the game evolves. A new Bayesian hybrid detection approach is suggested for the defender, in which a lightweight monitoring system is used to estimate his opponent's actions, and a heavyweight monitoring system acts as a last resort of defense.. The difference between a static and a dynamic Bayesian game is that the former does not take into account the game evolution, and the defender has fixed prior beliefs about the types of his opponent. In contrast, the latter is a more realistic game model; because the defender can dynamically update his beliefs based on new observations of the opponent's actions and the game history, and then can adjust his monitoring strategy accordingly. type of the potential attacker i can be perfectly determined The advantage of implementing the IDS system as a Bayesian hybrid IDS is that it allows to save significant energy (potentially spent on continuously monitoring the network), while minimizing the potential damage infected by an undetected attacker. This comes as a result of an interesting property of the equilibrium solution: the monitoring probability does not depend on the current belief of the defender on his opponent's maliciousness, but rather influences the attacker behavior.

In 2007, J Martin, R.Bhuvaneshwari, M.A. Bhagyaveni and S. Shanmugavel developed a secure routing approach called Resiliency Oriented Secure (ROS)which include the detection phase in routing to detect the malicious node. To detect the malicious node, they used a number of updates field in the routing table and set some threshold value for it. Whenever any node receives a routing packet that produces an update in its routing table, it increments the number of update field by one. When the count values crosses the threshold values it generate alarm signal. In the year 2007, R.Ranjana and M. Rajaram Proposed a model which does not perform any change in underlying protocol and used additional security component to detect fabrication attack, resource consumption attack and packet dropping attack[11].

In June 2008 Ningrinla marching and Raja Datta proposed "collaborative technique for Intrusion detection in MANET"[10]. In this, they proposed two intrusion detection techniques for mobile ad-hoc networks, which use collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood. The first technique is designed for detection of malicious nodes in a neighborhood of nodes in which each pair of nodes in the neighborhood are within radio range of each other. Such a neighborhood of nodes is known as a clique. The second technique is designed for detection of malicious nodes in a neighborhood of nodes, in which each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one-hop vicinity. This neighborhood is identical to a cluster as mentioned in. Both techniques use message passing between the nodes. A node called the monitor node initiates the detection process. Based on the messages that it receives during the detection process, each node determines the nodes it suspects to be malicious and send votes to the monitor node. The monitor node upon inspecting the votes determines the malicious nodes from among the suspected nodes. Their IDS is independent of any routing protocol.

3. Recent Scenario

Pasquale Donadio, Antonio Cimmino and Giorgio Ventre proposed a Grid based Intrusion Detection System (G-IDS) that uses the basic principles of the Grid computing and apply them to the intrusion detection mechanisms, in order to define a new process capable to protect networks characterized by the constantly changing of the topology. In this they used a distributed traffic analyzer that operates a real-time feedback sharing the results between the neighboring nodes of the network.[17].

S.Madhavi and Dr. Tai Hoon Kim [32] developed an Mobile Intrusion Detection System for multi-hop ad-hoc wireless network In their work the author define the monitor node whose job is to detect misbehaving node. They also describe the algorithm for detecting the packet dropping and packet delaying attack.

S Şen proposed a "grammatical evolution approach to intrusion detection on mobile ad hoc networks"[33]. They use artificial intelligence based learning technique to explore design space. The grammatical evolution technique inspired by natural evolution is explored to detect known attacks on MANETs such as DOS attacks and route disruption attacks. Intrusion detection programs are evolved for each attack and distributed to each node on the network.

4. Challenges

A number of constraints and technical difficulties faced by researchers, which are described in previous section. These. general problem must be consider for further research in this area to propose new technologies for intrusion detection in mobile ad hoc networks and some of these are:

- Unlike wired network, the mobile ad hoc network does not need any infrastructure so it is very difficult to perform any kind of centralized management and control.
- Large numbers of sensors are deployed to monitor the network activities in coordinated intrusion detection techniques. And finding optimal position of the sensors requires tactical processing and collecting data from them consumes a lot of network bandwidth.
- The resource constraint constitutes another challenge to mobile ad hoc network. The wireless channel is bandwidth-constrained and shared among multiple networking entities. At the same point computational capabilities of mobile devices are also limited and these devices are powered by batteries with its inherent limitation.
- IDS accuracy itself is a critical issue. In MANETs, the IDS monitor the activities and analyze and compare them against the security rules and accordingly generate the alarm. Because of the dynamic nature of network, most IDS suffer from the false positive and false negative alarm.
- In the MANET, the IDS is so distributed and the node itself is not trusted so IDS does not guarantees to work efficiently and should be should be some trust model
- A knowledgeable attacker can able to bypass the security rules of IDS so protection of IDS against Attacks is required

5. Conclusion and Future Directions

As the use of mobile ad hoc networks (MANET) has increased manifolds, the security in MANETs has become of paramount importance. Wireless ad hoc networks are vulnerable to many attacks because of its fundamental characteristics such as lack of centralized control, dynamic topology, limited resources and open media. These features present new challenges for intrusion detection techniques and as such, achieving security in ad hoc network is more difficult compared to wired networks. In this survey paper, we briefly explored the various intrusion detection methods suggested by the authors. We also analyzed some challenges and problems of intrusion detection in MANET. There is an utmost need of a general foundation for all intrusion detection and supporting activities that can able to adapt dynamic network conditions. These activities include detecting all types of attack on MANET; collecting, and correlating intrusion events; responding to intrusions; and managing intrusion detection and all related functions to cater for a secure communication.

References

[1] Dorothy E. Denning "An Intrusion-detection Model" IEEE Transaction on Software Engineering, 13, No. 7, Pp 222-232, Feb 1987.

[2] Ioanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari "Real-time Intrusion Detection for Ad hoc Networks" Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), 0-7695-2342-0/05 $20.00 © 2005 IEEE.

[3] Zhang Anfd Lee "Intrusion Detection System in Ad-hoc Networks" MOBICOM 2000 bostom MA USA.

[4] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative Study of Various Routing Protocols"

[5] Xia Wang" Intrusion Detection Techniques in Wireless Ad Hoc Networks".

[6] Yu Liu, Cristina Comaniciu and Hong Man "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks".

[7] H.–Y. Chang, S.F. Wu and Y.F. Jou, "Real-Time Protocol Analysis for Detecting Link-State Routing Protocol Attacks", ACM Tran. Inf. Sys.Sec., 1, Pp. 1-36, 2001.

[8] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos "Detecting Critical Nodes for MANET Intrusion Detection Systems".

[9] D. Sterne1, P. Balasubramanyam2, D. Carman1, B. Wilson1, R. Talpade3, C. Ko1,R. Balupari1, C-Y. Tseng2, T. Bowen3, K. Levitt2 and J. Rowe2 "A General Cooperative Intrusion Detection Architecture for MANETs".

[10] Ningrinla Marching and Raja Datta "Collaborative Technique for Intrusion Detection in Mobile Ad hoc Network" Ad hoc Networks, 6, Issue 4, June 2008 Page 508-523.

[11] R.Ranjana and M.Rajaram, "Detecting Intrusion Attacks in Ad-hoc Networks," Asian Journal in Information Technology, 6(7), 758-761, 2007, ISSN: 1682:3915, Macdwell Journal 2007.

[12] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad hoc Networks", In Proc. ACM/IEEE Int'l Conf. on Mobile Computing and Networking, Pp. 255-265, 2000.

[13] O. Kachirski and R. Guha, "Effective Intrusion Detection using Multiple Sensors in Wireless Ad hoc Networks", In Proc. 36th Annual Hawaii Int'l. Conf. on System Sciences (HICSS'03), Pp.57.1, 2003.

[14] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad hoc Networks", In Proc. IEEE Vehicular Technology Conf., 2002.

[15] Alekha Kumar Mishra1, Bibhu Dutta Sahoo2" Analysis of Security Attacks for AODV Protocol in Manet".

[16] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong "A New Routing Attack in Mobile Ad Hoc Networks".

[17] Pasquale Donadio,Antonio Cimmino and Giorgio Ventre "Enhanced Intrusion Detection Systems in Ad Hoc Networks using a Grid Based Agnostic Middleware".

[18] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad hoc Networks", In Proc. ACM/IEEE Int'l. Conf. on Mobile Computing and Networking, Pp 275-283, 2000.

[19] Y. F. Jou, F. Gong, C. Sargor, X. Wu, S. Wu, H. Chang, and F. Wang, "Design and Implementation of a Scalable Intrusion Detection System for the Protection of Networks Infrastructure," Proceedings of DARPA Information Survivability Conference and Exposition, 2, Pp. 69-83, January 2000.

[20] V. Madhu Viswanatham and A.A. Chari "An Approach for Detecting Attacks in Mobile Adhoc Networks" Journal of Computer Science, 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[21] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes" World Academy of Science, Engineering and Technology, 44, 2008.

[22] Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam "Addressing Security Concerns of Data Exchange in AODV Protocol".

[23] Lidong Zhou and Zygmunt J. HaasHappy Sankranti/ pongalhttp://crackspider.net/ "Securing Ad Hoc Networks" In Proc IEEE, Special Issue on Network Security, November/December, 1999.

[24] Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks".

[25] Anand Patwardhan, Jim Parker and Anupam Joshi "Secure Routing and Intrusion Detection in Ad Hoc Networks".

[26] Tom Chen SMU, Dept of Electrical Engineering tchen@engr.smu.edu http://www.engr.smu.edu/~tchen.

[27] Preetida Vinayakray-Jani "Security within Ad hoc Networks".

[28] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes".

[29] Marianne A. Azer,Sherif M. El-Kassas and Magdy S. El-Soudani "A Survey on Anomaly Detection Methods for Ad Hoc Networks".

[30] Tiranuch Anantvalee and Jie Wu "A Survey on Intrusion Detection in Mobile Ad Hoc Networks".

[31] S.Bose,P.Yogesh and A.Kannan "Neural Network Approach for Anomaly Intrusion Detection in Adhoc Networks using Agents" Internatinal Journal of Soft computing1, Medwell Online 2006.

[32] S.Madhavi and Dr. Tai Hoon Kim "An Intrusion Detection System in Mobile Ad hoc Networks" International Journal of Security and its Application, 2, No 3, July 2008.

[33] S.Sen and John Andrew Clark "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad hoc Networks" March 2009, WiSec '09: Proceedings of the Second ACM Conference on Wireless Network Security.

[34] B. Sun, K. Wu, and U. Pooch. "Zone-based Intrusion Detection for Mobile Ad hoc Networks". Int. Journal of Ad Hoc and Sensor Wireless Networks, 2(3), 2003.