Journal of Advances in Science and Technology

Vol. III, No. VI, August-2012, ISSN 2230-9659

REVIEW ARTICLE

INTRUSION DETECTION TECHNIQUES

www.ignited.in

Journal of Advances in Science and Technology
Vol. III, No. VI, August-2012, ISSN 2230-9659

Intrusion Detection Techniques

Gundeep Tanwar

Research Scholar, CMJ University, Shillong, Meghalaya

----------♦----------

INTRODUCTION

Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems. Although there are some differences between the traditional wired network and the mobile ad hoc network, intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. An effective IDS is a key component in securing MANETs. Two different methodologies of intrusion detection are commonly used: anomaly intrusion detection and misuse intrusion detection. Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misuse-detection systems cannot detect new types of attack. Hybrid systems using both techniques are often deployed in order to minimize these shortcomings .In the following, we discuss some typical intrusion detection techniques in the mobile ad hoc networks in details [35].

INTRUSION DETECTION TECHNIQUES IN MANET: THE FIRST DISCUSSION

The first discussion about the intrusion detection techniques in the mobile ad hoc networks was presented in the paper written by Zhang et al. A general intrusion detection framework in MANET was proposed, which was distributed and cooperative to meet with the needs of MANET. The proposed architecture of the intrusion detection system is shown below in Figure 3.1

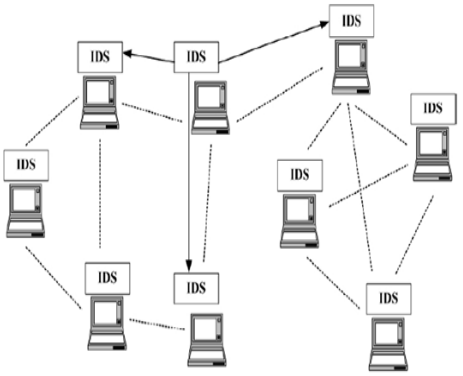

Figure 3.1: IDS Architecture for MANET

.In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behavior locally and independently, which are performed by the built-in IDS agent. However, the neighboring nodes can share their investigation results with each other and cooperate in a broader range. The cooperation between nodes generally happens when a certain node detects an anomaly but does not have enough evidence to figure out what kind of intrusion it belongs to. In this situation, the node that has detected the anomaly requires other nodes in the communication range to perform searches to their security logs in order to track the possible traces of the intruder. The internal structure of an IDS agent is shown in Figure 3.2:

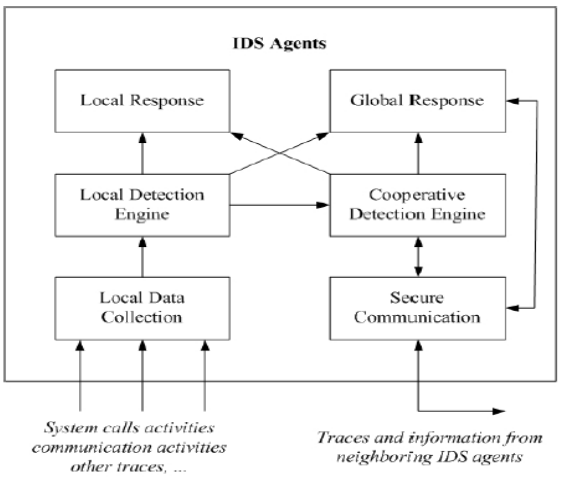

Figure 3.2: Conceptual Model for an IDS Agent

In the conceptual model, there are four main functional modules:

- Local data collection module, which mainly deals with the data gathering issue, in which the real-time audit data may come from various resources.

- Local detection engine, which examines the local data collected by the local data collection module and inspects if there is any anomaly shown in the data. Because there are always new attack types emerging as the known attacks being recognized by the IDS, the detection engine should not expect to merely perform pattern recognition between known attack behaviors and the anomalies that are likely to be some intrusions: instead of the misuse detection technique that cannot deal with the novel attack types effectively, the detection engine should mainly rely on the statistical anomaly detection techniques, which distinguish anomalies from normal behaviors based on the deviation between the current observation data and the normal profiles of the system [36].

- Cooperative detection engine, which works with other IDS agents when there are some needs to find more evidences for some suspicious anomalies detected in some certain nodes. When there is a need to initiate such cooperated detection process, the participants will propagate the intrusion detection state information of themselves to all of their neighboring nodes, and all of the participants can calculate the new intrusion detection state of them based on all such information they have got from their neighbors by some selected algorithms such as a distributed consensus algorithm with weight. Since we can make such a reasonable assumption that majority of the nodes in the ad hoc network should be benign, we can trust the conclusion drawn by any of the participants that the network is under attack.

- Intrusion response module, which deals with the response to the intrusion when it has been confirmed. The response can be reinitializing the communication channel such as reassigning the key, or reorganizing the network and removing all the compromised nodes. The response to the intrusion behavior varies with the different kinds of intrusion.

Intrusion detection module should be set in each layer on each node of the mobile ad hoc network in order to get better performance on some attacks that may seem rather legitimate to the lower layers such as MAC protocol, but are much more easier to detect in the higher layers such as the application layer. The multi-layer integrated intrusion detection and response technique can greatly enhance the performance of the IDS especially when there are large amount of attacks that can be easily caught in the higher layer but are hard to find in the lower layer.

It presents an architecture in which each of the nodes in the mobile ad hoc network should be equipped with an IDS agent, and all of the IDS agents can work independently and locally as well as cooperative with each other to detect some intrusion behaviors in a larger range.

CLUSTER-BASED INTRUSION DETECTION TECHNIQUE FOR AD HOC NETWORKS

All of the nodes in this framework are supposed to participate in the cooperative intrusion detection activities when there is such a necessity, which cause huge power consumption for all the participating nodes. Due to the limited power supply in the ad hoc network, this framework may cause some nodes behave in a selfish way and not cooperative with other nodes so as to save their battery power, which will actually violate the original intention of this cooperative intrusion detection architecture [37].

A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called clusterhead. As is defined in the paper, a cluster is a group of nodes that reside within the same radio range with each other, which means that when a node is selected as the clusterhead, all of the other nodes in this cluster should be within 1-hop vicinity.

It is necessary to ensure the fairness and efficiency of the cluster selection process. Here fairness contains two levels of meanings: the probability of every node in the cluster to be selected as the clusterhead should be equal, and each node should act as the cluster node for the same amount of time. Efficiency of the process means that there should be some methods that can select a node from the cluster periodically with high efficiency. The finite state machine of the cluster formation protocol is shown in Figure 3.3:

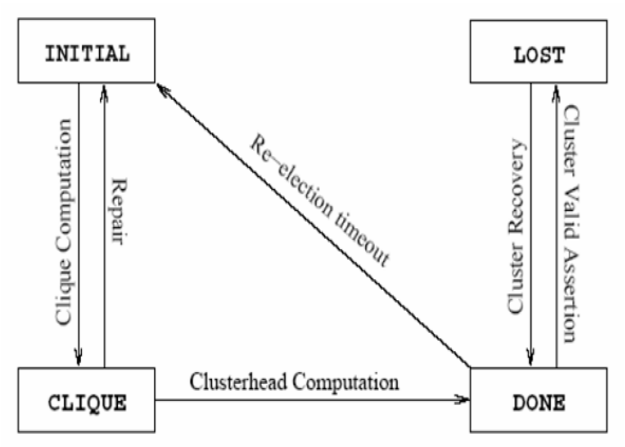

Figure 3.3: Finite State Machine of the Cluster Formation Protocol

Basically there are four states in the cluster formation protocol: initial, clique, done and lost. All the nodes in the network will be in the initial state at first, which means that they will monitor their own traffic and detect intrusion behaviors independently. There are two steps that we need to finish before we get the clusterhead of the network: clique computation and clusterhead computation. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link. The definition of clique is a little more restricted than that of cluster. Once the protocol is finished, every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the clusterhead. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol. The cluster valid assertion protocol has generally been used in the following two situations:

- The node in the cluster will periodically use the Cluster Valid Assertion Protocol to check if the connection between the clusterhead and itself is maintained or not. If not, this node will check to see if it belongs to another cluster, and if it also get negative answer, then the node will enter the LOST state and initiate a routing recovery request.

- Furthermore, there need to be a mandatory re-election timeout for the clusterhead to keep the fairness and security of the whole cluster. If the timeout expires, all the nodes switch from DONE state to INITIAL state and begin a new round of clusterhead election.

The Cluster Recovery Protocol is mainly used in the case that a citizen loses its connection with previous clusterhead or a clusterhead loses all its citizens, when it enters LOST state and initiates Cluster Recovery Protocol to re-discover a new clusterhead.

MISBEHAVIOR DETECTION THROUGH CROSS-LAYER ANALYSIS

Multi-layer intrusion detection technique is another potential research area. However, they seem not to explore deeper in this area. In this part, we will discuss the cross-layer analysis method presented by Parker et al.

The attack behaviors in the MANET, and find that some smart attackers may simultaneously exploit several vulnerabilities. at multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector. This type of cross-layer attack will be far more threatening than the single-layer attack in that it can be easily skipped by the single-layer misbehavior detector. Nevertheless, this attack scenario can be detected by a cross-layer misbehavior detector, in which the inputs from all layers of the network stack are combined and analyzed by the cross-layer detector in a comprehensive way.

As far as I know, there are several aspects that can be further explored in this area. First of all, it will be an important problem that how to make the cross-layer detection more efficient, or in other words, how to cooperate between single-layer detectors to make them work well. Because different single-layer detectors deal with different types of attacks, there can be some different viewpoints to the same attack scenario when it is observed in different layers. Therefore it is necessary to figure out the possible solution if there are different detection results generated by different layers. Second, we need to find out how much the system resource and network overhead will be increased due to the use of cross-layer detector compared with the original single-layer detector. Due to the limited battery power of the nodes in the ad hoc networks, the system and network overhead brought by the cross-layer detection should be taken into account and compared with the performance gain caused by the use of cross-layer detection method.

REFERENCES

[1] Wang, Weichao, L Yi, Bharat Bhargava. On Vulnerability and protection of Ad hoc On Demand Distance Vector Protocol. http://www.cs.purdue.edu/homes/wangwc/ICT03wangwc.pdf

[2] Jakobsson, Markus; Wetzel, Susanne and Yener, Bulent. Steal Attack on Adhoc Wireless Networks.

http://Guinness.cs.steven.edu/~swetzel/papers/stealth.pdf

[3] Martin, Frederic; Thao, Houy-Sy; Thylander, Magnus. Security in Ad-hoc Routing Protocols. http://www.comp.nus.edu.sq/~cs4274/tempapers/0304-l/group1/present.ppt

[4] Mishra, Amitabh; Nadkarni, Ketan M.; Ilyas, Mohammad, editor. Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network. CRC PRESS Publisher, 2003.

[5] Murthy, C. Siva Ram, Manoj, B. S; Ad hoc Wireless Networks: Architectures and Protocols. Prentice Hall. http://www.parc.com/zhao/stanford-cs428/readings/Networking/Royer_IEEE_Personal_Comm99.pdf

[6] Hu, Yih-Chun; Johnson, David B.; Perrig, Adrian. ARIADNE: A Secure On-Demand Routing Protocol for Ad hoc Networks. http://www.ece.cmu.edu/~adrian/projects/secure-routing/ariadne.pdf

[7] OPNET Modeler 11.0 Documentation: API Reference Manuals.

[8] Zapata, Manel Guerrero. Secure Ad hoc On-Demand Distance Vector Routing. http://www.cse.cuhk.edu.hk

[9] Sadasivam, Karthik; Vishal, Changrani; T. Andrew Yang: Scenario Based Performance Evaluation of Secure Routing in MANETs http://sce.uhcl.edu/sadasivamk/MANETII05-draft.pdf

[10] Ad hoc routing protocol list. http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols. Last accessed March 2007.

[11] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET on demand (DYMO) routing protocol. Internet-Draft Version 06, IETF, October 2006, (Work in Progress).

[12] Ian D. Chakeres and Elizabeth M. Belding-Royer. The utility of hello messages for determining link connectivity. In Proceedings of the 5th International Symposium of Wireless Personal Multimedia Communications (WPMC) 2002, volume 2, pages 504–508, Honolulu, Hawaii, October 2002

[13] Sumit Gwalani, Elizabeth M. Belding-Royer, and Charles E. Perkins. AODV-PA: AODV with path accumulation. In IEEE International Conference on Communications (ICC' 03), volume 1, pages 527–531, Anchorage, Alaska, May 2003. IEEE.

[14] Elizabeth Belding-Royer, Ian Chakeres, David Johnson, and Charlie Perkins. DYMO – dynamic MANET on-demand routing protocol. In Rebecca Bunch, editor, Proceedings of the Sixty-First Internet Engineering Task Force, Washington, DC, USA, November 2004. IETF.

[15] S.A. Razak, S.M. Furnell, N.L. Clarke, and P.J. Brooke, "Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks," Ad Hoc Networks,vol. In Press, Corrected Proof.

[16] A.P. Lauf, R.A. Peters, and W.H. Robinson, "A distributed intrusion detection system for resource-constrained devices in ad-hoc networks," Ad Hoc Networks, vol. In Press, Corrected Proof, 2009.

[17] N. Marchang, and R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," Ad Hoc Networks, vol. In Press, Corrected Proof