IJCSC International Journal of Computer Science & Communication Vol. 1, No. 1, January-June 2010, pp. 203-206

Controller Based IDS Architecture in Distributed Nodes

Kuldeep Tomar[1] Anupma Sehrawat[2] & Swati Phogaat[3]

[1]Deptt. of Computer Science, NGF College of Engg & Technology, Palwal, Haryana (India).
[1]kuldeep_karan@yahoo.com, [2]anupmasehrawat@rediffmail.com

ABSTRACT

In the past few years, the performances of wireless technology have increased tremendously. It gives rise to many new fields in the area of networking. One of field is Ad-Hoc networks. It is a network in which the members of network can directly communicate with each other with in the network without any fixed infrastructure. Securing Ad-hoc network is just as important as securing traditional wired network. Ad-hoc network have their own vulnerabilities that can't be tackled by the existing solutions. To obtain a level of security for Ad-hoc networks we have to couple IDS with Ad-hoc networks. In this paper we have presented a Controller based Ad-hoc network. Firstly we define the scope of IDS in Ad-hoc networks and then we have to focus on the challenges of IDS in Ad-hoc networks. And then finally we define the Controller based IDS. In this for a group of nodes there exists a Controller to manage all the areas of working as well as security.

1. AD HOC NETWORK (DISTRIBUTED NODES)

Ad hoc network is a type of network in which the members of the network can directly communicate to each other within the network without any fixed infrastructure such as access points or base stations. Ad Hoc network is also known as infrastructure less mobile network. Each host is incorporated with routing functionality into it. In this network, one node functions as router as well as the end point. Due to this special characteristic, ad hoc network experiences more vulnerability that brings more security concerns compared to other infrastructure networks.

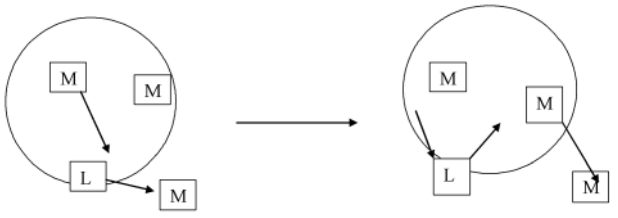

Fig 1: Ad Hoc Network Example

This figure illustrates an example ad hoc network. The network is formed by independent mobile nodes such as PDA, mobile phones, and laptop that have wireless transceivers. Here L stands for laptop and others are the mobile (M) nodes. Each circle illustrates the communication range of the node in its center. In the left side of this example, we can see that PDA that acts as source communicates with a destination, mobile phone, outside its communication (transmission) range through an intermediate node, a laptop, that locates within transmission range of source node and destination node. Moreover, mobile nodes that construct this ad hoc network can move freely inside the network. This mobility results to the dynamic change of the network topology, as shown in right side of figure 1. The participating nodes in ad hoc networks act both as end hosts and routers, forwarding traffic from the source to the destination.

2. INTRUSION DETECTION SYSTEM IN INFRASTRUCTURE NETWORKS

Intrusion detection can be classified based on audit data as either host-based, network- based, or the mixed Approach of host-based and network based. HIDS (Host based intrusion detection system) monitors for attacks at the operating system, application, or kernel level. HIDS has access to audit logs, error messages, service and application rights, and any resource available to the monitored host. NIDS (Network based intrusion detection system) monitors traffic as it flows to other hosts. IDS can also be classified, based on the detection method, into following categories.

- *Anomaly detection method:* In this method, a baseline profile of normal system is created and saved in the system. Then, the captured data which describes the current condition of the system will be compared with this profile. Some threshold value are used to determine whether the current condition can be judged as anomaly or accepted as normalcy. The difficulty to set the threshold is one disadvantage of this method. If the threshold value is set too high, it will increase the false positive that is the anomaly which is detected as normalcy. In other hand, low threshold

value will increase the false negative that is the normalcy which is detected as anomaly. Moreover, anomaly that is not caused by intrusion also flagged as intrusive in this method.

- *Misuse detection method:* In misuse detection (also called signature-based detection), decisions are made on the basis of knowledge of the attack model. The system keeps the signatures of known attacks. Then, the captured data will be compared to these signatures and any matched pattern is treated as an intrusion. While this method is able to determine intrusion with relatively low false positive and false negative rate, it cannot detect new type of attacks. Moreover, the system needs a relatively larger memory to store the attack signatures and it keeps increasing as a new signature is inputted to the system.

3. ARCHITECTURES OF INTRUSION DETECTION SYSTEM IN AD HOC NETWORKS (DISTRIBUTED NODES)

There are three types of architectures that have been proposed for IDS in ad hoc networks.

4. HOST-BASED ARCHITECTURE

The main characteristic of this architecture is that every node runs an intrusion detection system agent and independently determines intrusions as shown in the figure. In this architecture, there is no data related to intrusion detection exchanged among other nodes in the network. Hence, nodes in the same network do not know anything about the situation on other nodes in the network since no alert information is passed.

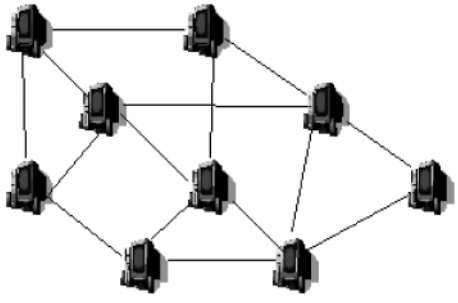

Fig 2: Host-Based Type Architecture

The merits that can be expected with this type of architecture is that there is no network overhead for the intrusion detection process such as audit data exchange.

5. HIERARCHICAL ARCHITECTURE

The second type of architecture is hierarchical model. In hierarchical architectures, networks are divided into smaller sub-networks (clusters) with one or more cluster heads that are responsible for the intrusion detection in the networks. Figure 3 shows an example of hierarchical architecture with one cluster head. This model differs from host-based architecture in the way

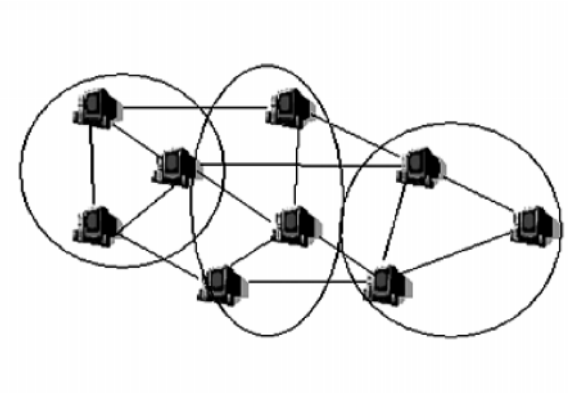

Fig 3: Hierarchical Based Architecture

that not all nodes need to host IDS agents to reduce the burden of nodes in the network. In this system, cluster heads are responsible to perform the intrusion detections in the network by intercepting all packets that are sent to their clusters and gaining local data from each of their cluster members.

6. DISTRIBUTED AND COOPERATIVE ARCHITECTURE

The third type of architecture is distributed and cooperative model. Since the nature of ad hoc networks is distributed and requires cooperation of other nodes, networks should also be distributed and cooperative as shown in figure 4. Similar to host-based architecture, Every node participates in intrusion detection and response by having an IDS agent running on them.

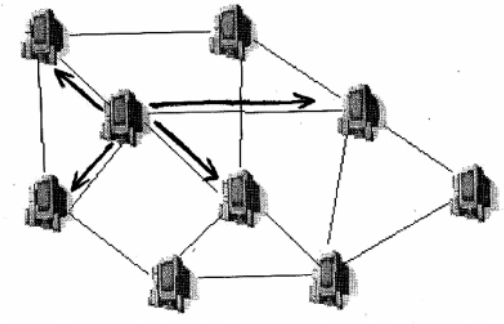

Fig 4: Distributed and Cooperative Architecture

7. CONTROLLER-BASED ARCHITECTURE

We propose a Controller-based architecture for intrusion detection system in ad hoc network (Figure 5) that belongs to hierarchical architecture model. We divide the nodes that construct the network into two types: Regular Node and Controller. The composition of these nodes are given as 1 Controller for N Regular Nodes (RNs) ($N \geq 0$), together they form a smaller sub-network that is called zone. RNs function as sensors whose tasks are collecting intrusion data locally specified on the detection algorithm that is

utilized in the network. These data can be raw data such as application log files in each node or crafted data such as the number or percentage of route change occurred in the last few minutes, etc..

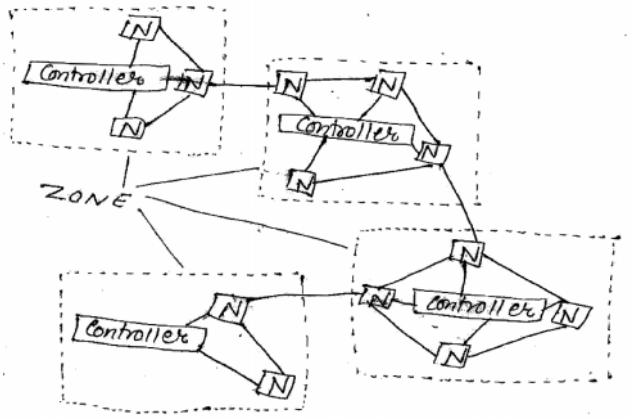

Fig 5: Controller-Based Architecture

On the other hand, Controllers function as the heads of zone to perform the intrusion detection in their zone based on the data collected from Regular Nodes added with its local data. They perform the analysis of the data and send back the result in a form of alert information to every regular node in their zones. Since ad hoc network doesn't have any fixed infrastructure, it is difficult to aggregate all intrusion data occurred in the network to one place without cooperation of all nodes. Therefore, in this architecture, all Controllers should cooperate to provide the network with more complete data for an accurate and efficient detection. The relation among nodes is best described in Figure 5. The timing of data collection is also decided in specified application or network environment. When Controllers are not in a hurry to analyze the local data, Regular Nodes can only send their data periodically. However, when Controllers detect an anomaly in the network and need to perform further analysis, they can request the data from Regular Nodes.

8. CONTROLLER SELECTION ALGORITHM

Here is the core part of our proposal architecture system: algorithm of Controller selection. In our system, Controllers are the center of zones. Choosing a Controller of a zone is equal to create the zone itself.

9. BASIC OPERATION

The architecture of Controller Selection Algorithm (CSA) is constructed by 5 functions and 3 control messages. Functions are executed at each node triggered by these specific control messages or messages from other mechanism (e.g. routing mechanism, etc) that tell about disconnection of neighbor nodes. These messages and their brief purposes are described as follows:

- Controller Declaration Message, *C* (*A*, *WA*), is used by a node *A* with weight value *WA* to declare that it has become a Controller and transmitted periodically by Controller to control the zone.
- Regular Node Submission Message, *RN* (*A*, *B*), is used by a node *A* to declare that it will affiliate to node B's zone.
- Incapability Declaration Message, INC (*A*, *WA*), is used by a node *A* to declare that it is an incapable node, a node whose weight value is too small to become Controller of other nodes.

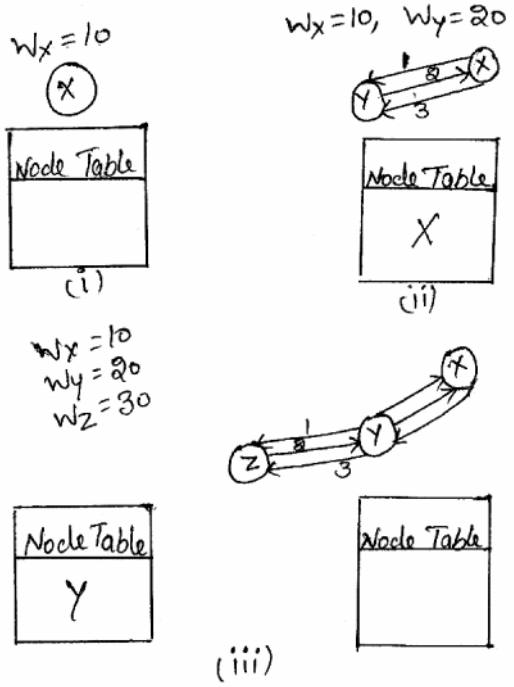

Fig: 6

For further understanding about Controller Selection Algorithm, example scenario of Controller Selection algorithm shown in Figure 6 is used. In this figure, there are 3 steps, starting from I and ending at III. Node is added one by one at every step. The process on how Controller is selected in every step is explained below.

- *Step I:* Node *X* enters the network without any other nodes in its neighbor. Thus, after waiting for several times, this node automatically becomes Controller.
- *Step II:* Node *Y* enters the network within transmission range of node *X*, hence *Y* receives message *C* (*X*, *Wy*) (indicated with number 1). that is sent by Controller *X*. Since node *Y* is having bigger weight value (20) than *X* (10), *Y* declares himself to become Controller by sending *C* (*Y*, *Wy*) (indicated with number 2). Upon receiving this message, node *X* stops being Controller and sends RN (*X*, *Y*) (packet number 3) to ask node *Y* to become its Controller. Y then registers X as its Regular Node.

- *Step III:* Node Z with weight value 30 enters the network within transmission range of node *Y*. After receiving periodical *C* (*Y*, *Wy*) (number 1) from *Y*, it sends *C* (*Z*, *Wz*) (number 2) because its weight value is larger than *Y*'s. Meanwhile, Node *X* upon receiving *C* (*Y*, *Wy*) doesn't do anything. Then, node *Y* sends RN (*Y*, *Z*) (number 3) to become node *Z*'s Regular Node. Node *X* who listens this message, starts becoming Controller again and transmits *C* (*X*, *Wx*) (number 4). Upon receiving this message, node *Y* doesn't do anything since its Controller, node *Z*, has bigger weight value than *X*. Thus the controller selection algorithm would be useful.

10. CONCLUSION AND FUTURE WORK

No doubt network security is a great area of concern but by proposing efficient architectures like the one discussed in this paper can provide us better ways to counter security threats. In the future advance mechanism or architectures would also be formulated to secure networks. Also advanced pattern matching algorithms could also be developed so as to quickly matching/detecting the related values/data/breaches.

REFERENCES

[1] Frank Stajano and Ross J. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks", *Security Protocols*, 7th International Workshop Proceedings, pp. 172-194, 1999.

[2] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks", Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, September 2002.

[3] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad-hoc Networks", *IEEE/ACM Transactions on Networking*, December 2004.

[4] G.O'Shea and M. Roe, "Child-proof Authentication for MIPV6 (CAM)", ACM Computer Communication Review, April 2001.

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

[6] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing", ACM Mobile Computing and communication Review (MC2R), **6,** No. 3, pp. 106-107, July 2002.

[7] H. Debar, M. Dacier, A. Wespi, "A Revised Taxonomy for Intrusion-Detection Systems", *Annalesdes Telecommunications*, **55,** Part 7/8, pp. 361-378, 2000.

[8] P. Brutch, C. Ko, "Challenges in Intrusion Detection for Wireless ad-hoc Networks", Proceedings in 2003 Symposium on Applications and the Internet Workshops, pp. 368-373, 27-31 January 2003.

[9] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks", 6th Int'l. Conf. Mobile Comp. and Net, Aug. 2000, pp. 275-283.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, August 2000.

[11] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)", Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02), pp. 226-336, June 2002.

[12] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", Communication and Multimedia Security Conference (CMS'02), September 2002.