Cross Layer Intrusion Detection Systen in Wireless Ad hoc Network- A Reviwe

Trupti K. Marve
Department of Computer Science and Engineering
Yashwantrao Chavan College of Engineering
Nagpur, India
e-mail : trupti.marve12@gmail.com

Nilesh U. Sambhe
Department of Computer Science and Engineering
Yeshwantrao Chavan College of Engineering
Nagpur,India
e-mail:nilesh.sambhe@gmail.com

Abstract **-** Wireless ad-hoc networks is a collection of small randomly dispersed device deployed in large number that provide essential function like monitor physical and environmental condition also provide efficient, reliable communication via wireless Network, ad-hoc network are vulnerable to various type of security threat and attack,due to relative ease of access to wireless medium and lack of a centralized infrastructure. various way are possible to overcome vulnerabilities in wireless ad-hoc network from attack and threat, mostly used solution is an Intrusion detection system (IDS) that suites the security needs and characteristics of ad-hoc networks for efficient and effective performance against intrusion. In this paper we propose a cross layer intrusion detection system (CIDS) which overcome demerits such as false positive present in traditional IDS, a cross layer design framework that will exploit the information available across different layer of the protocol stack by triggering two level of detection that utilizes the knowledge of network and node condition in determining the node behavior, and enhance the accuracy of detection.

Keywords*—Wireless ad hoc network, Threat model, intrusion detection system, cross layer intrusion detection system (CIDS)*

*****

I. INTRODUCTION

Wireless ad-hoc network is a decentralized type of wireless network. It is become an important facet in our everyday lives as they are increasingly deployed in numerous application. However, their growing popularity is challenged by insecure environment and characteristics of these networks. The inherent nature of the wireless medium makes it susceptible to variety of security attacks ranging from passive eavesdropping to active interference.an ad-hoc network usually refers to any set of network where all devices have equivalent status on a network and are free to subordinate with any other type of ad hoc network device in a link range. The decentralized nature of wireless ad-hoc network makes them suitable variety of application where central node can't be trusted on and may improve the scalability of network compared to wireless managed network. They are used to connect wireless clients directly together, without the need for a wireless router or access point.

The wireless sensor network (WSN) monitors the environment or systems are particularly vulnerable to various kinds of attacks at different layers of the protocol stack. Many intrusion detection system (IDS) have been proposed to secure Wireless ad hoc network but all these systems operate in a single layer of the OSI model or network model, or do not consider the interaction and collaboration between these layers. Misuse and anomaly detection are common IDS technique that are used to study the abnormalities in the system to detect if an intrusion has occurred. The intrusion detection mechanisms complement the intrusion prevention measures and help enhance the security of the networks. In order to detect DoS attacks, conventional system use a network IDS that resides in a gateway node and monitor the network for abnormal network behavior. In wireless sensor network DDoS is a type of DoS attack where multiple compromised nodes are used to target a single node, for DDoS attack traditional IDS system fails to perform accurate diagnosis of malicious attack and increase in the rate of false positive.

In this paper we use cross layer based intrusion detection system that will exchange the information across different layer of the protocol stack and trigger multiple level of detection that utilizes the knowledge of network and node condition in determining the node behavior, and enhance the accuracy of detection cross layer based approach to detect intruders on AODV protocol. We mainly focus on security aspect of intrusion detection system for DoS attack in wireless ad hoc networks. Table 1 show an example of a classification of DoS attack based on protocol stack, there are also other different DoS attack and classification apart from the given in table.

Table 1. Protocol layer & Specific Attacks

Layers	**Attacks**
Physical	Jamming, Tampering
Data link	Collision, Exhaustion, Unfairness , Jamming
Network& Routing	Neglect and Greed, Homing, Misdirection, Black holes, packet drop
Transport	Flooding, Desynchronization

The remainder of the paper organized as follows. Section II describes Threat model and assumption, section III discusses the detecting techniques, section IV describes cross layer intrusion detection system, section V explained CIDS component, section VI concludes the paper.

II. Threat Model

In this section, we discuss the nature of the adversary model considered in our work. Some basic assumption are:

1. The adversary node attacks the infrastructure by denying service availability to the nodes in the network.
2. The adversary node is limited in terms of its energy resources just as any other node in the network.
3. Number of adversary nodes do not outnumber the good nodes in the wireless network.
4. The adversary node may or may not be an authenticated member of the network.

We briefly describe DDoS attacks in consideration as follows,

Collision:

In wireless networks, the channel is reserved for transmission through RTS/CTS packets. In spite of the channel reservation, an adversary node can induce a collision in the wireless channel by transmitting when another node in its range is already in transmission. The purpose of this attack is to either prevent access to a certain node or to exhaust the transmitting node's resources by continuous retransmissions.

Packet drop:

The adversary node can randomly drop either the control or data packets at the network layer. This results in denying service to the destination node, hence affecting the availability of the node. A misbehaving node does not take its own responsibility, i.e not relaying packets. Consequently, some victim nodes will undergo DoS. Selectively dropping or all packets for a particular network destination can accomplish it

Misdirection:

Misdirection attack (Type-1) occurs when the adversary node forwards the data packet to the wrong destination node. Such that the adversary node can receive the data packet and sent to a wrong destination, this kind of attack also called as "compound attack"

In another kind of misdirection attack (Type-II), the adversary node can deny the availability of an existing route to the destination by sending false Route Error (RERR) messages thus preventing service to the destination in the absence of alternate routes.

In our adversary model, (specific to the DoS attacks in TableI) we assume that the adversary can launch any and all of the attacks discussed above. However, because the collision attack involves the adversary node expending a large amount of energy of its own, it is assumed that the number of times the adversary repeats the collision attack is less. Other Denial of Service attacks such as packet drop and misdirection are assumed to occur more frequently in the network.

III. Detecting Techniques

Misuse and anomaly detection are common IDS technique in both wired and wireless network.

1) Misuse detection system are accurate in identifying the know attack, malicious activities of nodes and it has low false positive but cannot detect newly invented attack.
2) Anomaly based detection schemes are more effective in detecting unknown attacks how however they often result in high false positives.

Ioanna Stamouli [8] presented on Real time Intrusion Detection for ad hoc Networks(RIDAN),The RIDAN architecture utilizes timed finite state machines (TFSMs) to formally define attacks against the AODV routing process. Therefore, it follows the knowledge-based methodology to detect network intrusions. TFSMs enable the system to detect malicious activity in real-time rather than using statistical analysis of previously captured traffic. RIDAN operates locally in every participating node and depends on the network traffic a node observes.

Yu Liu and Hong Man [4], proposed the idea of a distributed IDS where cluster heads are elected and the IDS functionality is distributed among them. This approach minimizes the total processing time spent by each node. However, it may not be a suitable approach in an ad hoc network scenario, where care should be taken to avoid malicious cluster heads or prevent cluster heads from being compromised.

Liu et al [6] proposed a cross-layer based anomaly detection by adapting a rule based data mining technique. In this work, a specific feature set is defined to profile normal user behavior by correlating information obtained from the MAC and the network layers. The IDS system developed is effective in localizing the attacks within one hope perimeter. Inter layer interactions can be exploited in numerous ways for detecting intrusions in the wireless ad hoc networks. To the best of our knowledge a multi-layer detection module has not been utilized to detect DoS attacks in ad hoc networks.

In our work, we discuss a cross-layer intrusion detection model to detect malicious behavior of nodes using information from one layer in another layer, also distinguish between the normal and malicious behavior of nodes thus enhancing the detection accuracy.

IV. Cross Layer Based Intrusion Detection System(CIDS)

There are different approaches available to detect collision, packet drop and misdirection. We use an IDS to identify the malicious activities in the network. In this work, Geethapriya Thamilarasu [2] proposed a novel cross-layer based intrusion detection system (CIDS) that exploits information across the layers to effectively identify an intrusion. Multiple levels of detection is performed across different layers of the protocol stack before confirming the malicious behavior of the nodes, thus reducing false positives. Also, the approach leads to an increase in the number of nodes detected correctly, hence increasing the true positives in the network. The goal of adopting a cross-layer design approach is two folds.

1) Detecting intrusion at multiple levels of the protocol layers.
2) Exploiting the information such as energy and congestion from one layer, to more accurately detect intrusion in another layer.

We also intend to reduce the false positives normally caused in intrusion detection approaches. For example, in wireless ad hoc networks, a node can cause routing or any misbehavior due to a node's malicious intent or due to lack of

energy resources or congested buffer. It is important to consider these energy and congestion conditions of the nodes using information obtained from other layers before determining the nodes to be malicious. Also, detecting intrusions at different layers increases the information about the malicious nodes thus identifying these nodes more accurately.

A. Detecting Intrusions

The proposed intrusion detection mechanism is enabled by triggering detection across the protocol layers. There are two levels of intrusion detection- Level 1 detection and Level 2 detection.

The two levels of detection may be performed using the following two methods.
1) CIDS-I: Detection information obtained via detecting DoS attacks at one layer of the protocol stack, is shared with information from a different layer.
2) CIDS-II: Multiple detections of a DoS attack at the same layer of the protocol stack using information from other layers

B. CIDS-I

In this method, the information about a malicious node is obtained via detection from different layers. This forms the level 1 detection. Based on this information, level 2 detection identifies the truly malicious nodes in the network. Also, multiple levels of detection confirm the misbehavior caused by malicious node in the network, thus reducing the false positive rates

C. CIDS-II

In the second method, the two levels of detection occur at the same layer of the protocol stack. Similar to the first method, level 1detection is only passive monitoring of nodes to obtain information about the network. Based on the first level of detection, a level 2 detection is triggered but within the same layer. This detection often obtains the information from different protocol layers thus exploiting the cross-layer interactions. The advantage of this approach is that the nodes do not have to expend energy in performing the first level of detection. Detections from CIDS II is sent to the CIDS I as part of level 1 detection for CIDS I.

V. CIDS Component

The cross layer intrusion detection system is divided in to following components, Monitoring component, Intrusion database, Analysis Engine, Response component. Divya Bansal [16] explained following components:

- Monitoring Component: This is used for local events monitoring. The monitoring component will implement the detection algorithm. Algorithm is the core component and the efficiency and accuracy of detecting and responding intrusion is totally dependent on the algorithm.
- Intrusion Database: It consists of the records of recent misbehaviors reputation valves and malicious activity of the neighbouring nodes. The monitoring algorithm will generate a suspicious list based on the monitoring result of single layer .This will go as input to the analysis engine for further processing. This list is also sent to all neighbours who can use it as additional and decide its own response.
- Analysis Engine: It collects inputs from multiple layers in the form of suspicious list. It will correlate information to confirm intrusions. The complexity of the analysis engine will depend upon the environment for which IDS has to be deployed. However for simplicity we have considered statistical analysis of previously captured traffic approach in our analysis engine. After confirming the status of the misbehaving node, the analysis engine will update the intrusion list.
- Response Component: It is used to respond in case intrusion or malicious activity of node is detected. The response in the form of global intrusion list will broadcasted to all nodes.

VI. Conclusion

In this paper, we discuss a cross layer based intrusion detection system (CIDS) to detect DoS, DDoS attack at different layer of the protocol stack by triggering multiple level of detection that perform accurate diagnosis of malicious attack, and increase the accuracy of the intrusion detection system (IDS) which overcome the demerits such as false positive present in traditional IDS

References

[1] S.Bose and A.Kannan,"Detecting Denial sevice Attack using Cross based Intrusion Detection System in Wireless Ad Hoc Networks", IEEE international Conference on Sigmal processing,Communication and Networking, pp182-188,2008
[2] Thamilarasu.G, Balasubramanian .A, Mishra .S and Sridhar .R, "A Cross-Layer based Intrusion Detection Approach for Wireless Ad-hoc Networks", IEEE International Conference in Mobile Adhoc and Sensor Systems, pp. 1-8, 7-10 Nov, 2005.
[3] Glenn Carl, George Kesidis, Richard R. Brooks and Suresh Rai, "Denial of Service Attack Detection Techniques", IEEETransactions on Internet Computing, Vol. 10, Issue 1, pp. 82- 89, Jan-Feb 2006.
[4] Yu Liu, Yang Li and Hong Man, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad-Hoc Networks",1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 418-420, 05-09 Sept, 2005
[5] D.Novikov,R.VYampolskiy,L.Reznik,"Anomaly Detection Based Intrusion Detection",3rd International Conference on Information Technology: New Generations(ITNG'06), pp. 420-425, 10-12 April, 2006.
[6] Yu Liu, Yang Li and Hong Man, "MAC Layer Anomaly Detection in Ad-hoc Networks",6th Annual IEEE international conference in Systems, Man and Cybernetics (SMC),Information Assurance Workshop, pp. 402-409, 15-17 June, 2005
[7] PingYi,Yichuan Jiang, YipingZhong and ShiyongZhang," Distributed Intrusion Detection for Mobile Ad-Hoc Networks", pp. 94-97, 31-04 Jan, 2005
[8] Joanna Stamouli, Patroklos G. Argyroudis, and Hitesh Tewari,"Real-time intrusion detection for ad hoc networks",6th IEEE International Symposium on a World of WirelessMobile

and Multimedia Networks (WoWMoM'05)", pp. 374-380,13-16 June 2005.

[9] Ahmed Hasswa, Mohammad Zulkernine and HossamHassanein,"Routeguard: An Intrusion Detection and Response System forMobile Ad Hoc Networks", IEEE International Conference onWireless And Mobile Computing, Networking And CommunicationsVol 3, pp. 336-343, 22-24 Aug, 2005.

[10] Y. Huang, W. Fan, W. Lee and P. S. Yu, "Cross-Feature Analysis for Detecting Ad-hoc Routing Anomalies",23rd International Conference on Distributed Computing Systems (ICDCS'03), May, 2003.

[11] Y. Huang and W. Lee, "A Cooperative Intrusion Detection Systemfor Ad-hoc Networks", 1st ACM workshopon Security of ad hoc and sensor networks, pp 135-147, 2003.

[12] R. Rao and G. Kesidis, "Detecting Malicious Packet Dropping using Statistically Regular Traffic Patterns in Multi hop Wireless Networks that are not Bandwidth Limited", IEEE Global Telecommunications Conference in GLOBECOM 2003, Vol.22, no. 1, pp. 2957-2961, Dec, 2003

[13] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-4Hoc Networks",6th Annual International Conference on Mobile Computing and Networking, MobiCom 2000, pp. 275-283, Aug, 2000.

[14] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", 6th Annual International Conference on Mobile Computing and networking ModiCom 255-265, Aug, 20

[15] Jia-Jun Xiong and Jing Zhang, "A kind of multilayer intrusion detection system using mobile agent", 2nd International Conference on Machine Learning and Cybernetics, Vol 3, pp. 1951-1955, 2-5 Nov, 2003

[16] Divya Bansal, Sanjeev Sofat and Prafulla Kumar"Distributed Cross Layer Approach or Detecting Multilayer Attacks In Wireless Multi-hop Networks", IEEE Symposium on computers and informatics,pp,2011