ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhanced Intrusion Detection for Zombie Exploration Attacks in Mobile Adhoc Networks

M.Srimathi[1], L.Mary Shyamala M.Tech. [2]

M.E (CSE), IFET College of Engineering, Tamilnadu, India[1]

Associate Professor, IFET College of Engineering, Tamilnadu, India[2]

ABSTRACT: Wireless networks face different security threat such that there is either a data loss or data inconsistency. Many IDS (Intrusion Detection System) models have been designed to overcome the security threats. We propose an enhanced scheme by which the IDS can act as both an intermediate node as well as a monitoring node preventing DoS (Denial of Service) at its initial stage. The HSQT (Hybrid Sequence Queue Tunneling) technique used minimizes the DoS attack and prevents an attacker node from transferring malicious packet throughout the network. It alerts the source and continues monitoring the misbehavior of the node in its coverage region. For maximum coverage we place more than one IDS node such that almost all the nodes in the scenario are covered by one IDS at least. This improved IDS is a dual purpose concentrating in any node within its coverage and isolating the active connections of the attacker node preventing considerable amount of data loss and false messages in a network.

I. INTRODUCTION

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. The intrusion detection has to be performed in decentralized system. Decentralized systems like Mobile Ad hoc Networks (MANET), Vehicular Ad Hoc Networks (VANET) and Wireless Sensor Networks (WSN).

II. EXISTING SYSTEM

There are many existing techniques are available in order to provide a secure communication in the mobile ad hoc networks. Some of the existing mechanisms are listed below.

2.1 NICE (Network Intrusion Detection and Counter Measure Selection In Virtual Network System)

Network Intrusion detection and Countermeasure selection in virtual network systems is used to establish a defence-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. The design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs.

There are two phases in NICE

- Deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic.
- Once a VM enters inspection state, Deep Packet Inspection (DPI) is applied, and/or virtual network reconfigurations can be deployed to the inspecting VM to make the potential attack behaviours prominent.

Phase 1:NICE A

The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in either Dom 0 or Dom U in each cloud server. It scans the traffic going through Linux bridges that control all the traffic among VMs and in/out from the physical cloud servers. In our experiment, Snort is used to implement NICE-A in Dom0. It will sniff a mirroring port on each virtual bridge in the Open Virtual Switch (OVS). Each bridge forms an isolated subnet in the virtual network and connects to all related VMs.

Phase 2: Deep Packet Inspection

Deep packet inspection (DPI) is normally referred to as a technology that allows packet-inspecting devices, such as firewalls and IPS, to deeply analyze packet contents, including information from all seven layers of the OSI model. This analysis is also broader than common technologies because it combines techniques such as protocol anomaly detection and signature scanning, traditionally available in IDS and anti-virus solutions.

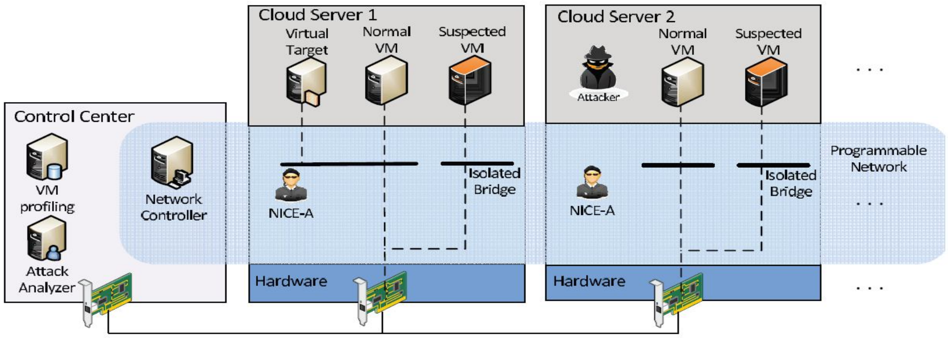

Fig 3.1: NICE Architecture Within the Cloud

The NICE framework is illustrated in Fig. 3.1. It shows the NICE framework within one cloud server cluster. Major components in this framework are distributed and light-weighted NICE-A on each physical cloud server, a network controller, a VM profiling server, and an attack analyzer. The latter three components are located in a centralized control centre connected to software switches on each cloud server (i.e., virtual switches built on one or multiple Linux software bridges).

NICE-A

The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in each cloud server. It scans the traffic going through Linux bridges that control all the traffic among VMs and in/out from the physical cloud servers.

VM Profiling

Virtual machines in the cloud can be profiled to get precise information about their state, services running, open ports, and so on. One major factor that counts toward a VM profile is its connectivity with other VMs.

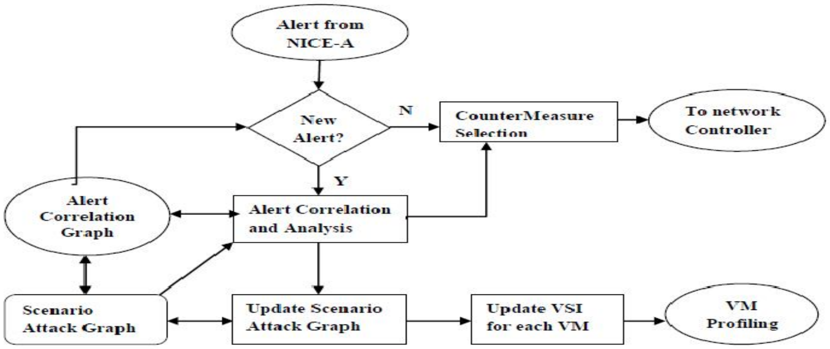

Fig 3.2: Attack Analyzer

Attack Analyzer

The major functions of NICE system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation, and countermeasure selection. The attack analyser shown as Fig 3.2.The process of constructing and utilizing the SAG consists of three phases: Information gathering, attack graph construction, and potential exploit path analysis. With this information, attack paths can be modelled using SAG. Each node in the attack graph represents an exploit by the attacker. Each path from an initial node to a goal node represents a successful attack.

III. PROPOSED SYSTEM

Wireless networks face different security threat such that there is either a data loss or data inconsistency. Grouping or clustering in wireless networks refers to the process of forming connected nodes together communication. The nodes within the cluster are connected to a controlling factor which operates communication inside and outside the group. This particular controlling factor is called the group head.

The group head is responsible for establishing communication outside the cluster. The head communicates with the head of the other group via intermediate nodes. The group formation is done by P2P technique. P2P is a point-to-point communication by which the group members are formed by the head provided the member is reachable in one hop. That means the head and group member must communicate in single hop; direct link must be available.

A HSQT queue is a type of priority queue where a closed circuit covers the entire queue as much time as the data is present in the queue. The advantage of tunnelling is that no attacker can breach the tunnelling effect. In case of a one side attack, the IDS scans and neglects packet (contaminated) and updates the packet information and status for further use. When the same kind of packet reverses for the second time, it simply checks the previous entries and denies the packet.

When there is a more than one way attack, i.e., the attackers handling more than one link to the IDS node causing traffic and initiating a DOS attack. In such a case the HSQT queue shreds up and drops the incoming packets and thus the normal queue becomes active. In this case the attackers are handled by other IDS which eliminate the threat for a particular time period within which the HSQT rebuilds to an IDS state.

3.1 Architecture of the proposed System

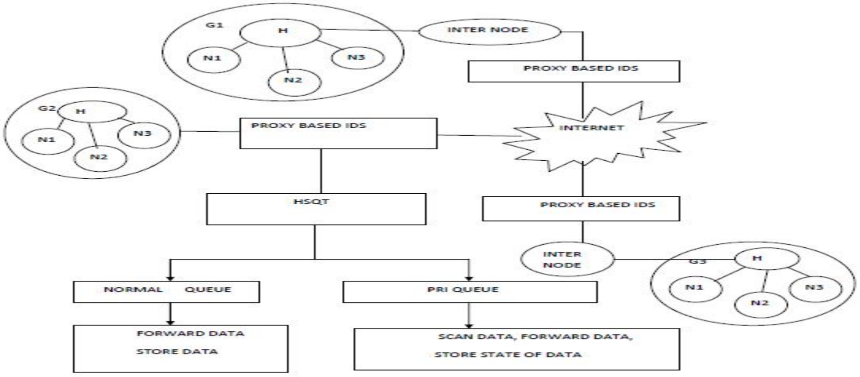

Fig 3.1 Architecture of the Proposed System

The IDS node's architecture is specially designed such that it can act as an intermediate and a NIDS node. Therefore it consists of two types of queue: normal queue and a HSQT queue. A normal queue is set active when the nodes communicate with each other and there is no misbehaviour observed. This resembles the normal data transfer between source and destination where the intermediate node buffers data transfer.

The IDS node's architecture is specially designed such that it can act as an intermediate and a NIDS node. Therefore it consists of two types of queue: normal queue and a HSQT queue. A normal queue is set active when the nodes communicate with each other and there is no misbehaviour observed. This resembles the normal data transfer between source and destination where the intermediate node buffers data transfer.

3.2 Advantages of Proposed System

- Periodic node information updates: A peer-to-peer communication protocol in which nodes periodically exchange state information about themselves and about other nodes they know about.
- Least of flooding probability: By using proxy based IDS reduce the attacker flooding probability in mobile ad hoc network because it is acting as a intermediate node and monitoring node

IV. SYSTEM DESIGN

The main module of the proposed system are

- Group Formation using P2P
- Assigning a Group Header
- Implementing a Hybrid Sequenced Queue Tunnelling

4.1 Group Formation Using P2P

The group formation is done by P2P technique. P2P is a point-to-point communication by which the group members are formed by the head provided the member is reachable in one hop. That means the head and group member must communicate in single hop; direct link must be available.

4.2 Assigning a Group Header

The Header picks the first node from the queue, sets a timer to interrupt after one quantum, and enables the active communication. If the head is still active at the end of the quantum, the active communication is pre-empted and the node is added to the tail of the queue. If the active communication finishes before the end of the quantum, the current head is released. In either case, the header assigns the nodes to the next active communication in the ready queue. The group header is subjected to change periodically. The group head is chosen by election algorithms. A best example for election algorithm in round ring algorithm.

Round Ring algorithm

1. Choose an header for the first time
2. Use a time slice till which the node remains the head
3. When the time slice period of the node exceeds, choose the next neighbouring node as head and enable active links through it.
4. Repeat through step 2 until there is an active head always.

4.3 Implementing a Hybrid Sequenced Queue Tunnelling

An IDS refers to a network framework that monitors all the nodes that are in its coverage region to avoid node misbehaviour and to update information about the misbehaviour to the nearby nodes. In a network, a common node that covers maximum nodes in a region acts as a NIDS architecture. The IDS node's architecture is specially designed such that it can act as an intermediate and a NIDS node. Therefore it consists of two types of queue: normal queue and a HSQT queue.

A normal queue is set active when the nodes communicate with each other and there is no misbehaviour observed. This resembles the normal data transfer between source and destination where the intermediate node buffers data transfer.

A HSQT queue is a type of priority queue where a closed circuit covers the entire queue as much time as the data is present in the queue. The advantage of tunnelling is that no attacker can breach the tunnelling effect. In case of a one side attack, the IDS scans and neglects packet (contaminated) and updates the packet information and status for further use. When the same kind of packet reverses for the second time, it simply checks the previous entries and denies the packet.

V. CONCLUSION

Wireless networks face different security threat such that there is either a data loss or data inconsistency. Many IDS models have been designed to overcome the security threats. We propose an enhanced scheme by which the IDS can act as both an intermediate node as well as a monitoring node preventing DOS at its initial stage. The HSQT technique used minimizes the DOS attack and prevents an attacker node from transferring malicious packet throughout the network. It alerts the source and continues monitoring the misbehaviour of the node in its coverage region. For maximum coverage we place more than one IDS node such that almost all the nodes in the scenario are covered by one IDS at least.

REFERENCES

[1] Cloud Sercurity Alliance, "Top Threats to Cloud Computing v1.0,"https://cloudsecurityalliance.org/topthreats/csathreats.v1.0pdf,Mar 2010.

[2] M. Armbrust, A. Fox, R. Griffith,A.D.Joseph, R. Katz, A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing,"*ACM Comm.*,vol. 53,no. 4, pp. 50-58, Apr. 2010.

[3] B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," *Proc. IEEE Int'l Conf.Computer Comm. and Informatics (ICCCI '12),* Jan. 2012.

[4] H. Takabi, J.B. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Securityand Privacy*, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[5] "Open vSwitch Project," *http://openvswitch.org,* May 2012.

[6] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J.Barker, "Detecting Spam Zombies by Monitoring OutgoingMessages," *IEEE Trans. Dependable and Secure Computing*,vol. 9,no. 2, pp. 198-210, Apr. 2012.