ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Routing and Intrusion Detection in Wireless Mobile Ad-Hoc Networks

Ashok Kumar Gonela
MTech
Department of CSE
Miracle Educational Group Of Institutions
Bhogapuram.

Pinjala.Praveen Kumar, B.Tech, M.S, (Ph.D)
Head of Department
Department of CSE
Miracle Educational Group Of Institutions
Bhogapuram.

Abstract:
Virtually every industry and even some parts of the public sector are taking on cloud computing today, either as a provider or as a consumer. Despite being young it has not been kept untouched by hackers, criminals and other "bad guys" to break into the web servers. Once weakened these web servers can serve as a launching point for conducting further attacks against users in the cloud. One such attack is the DoS or its version DDoS attack. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based analytical models and reconfigurable virtual network-based countermeasures. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

Keywords: ***Virtual Machine, DDOS attack, Cloud computing, NICE, vulnerability detection and analytical models.***

INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing infrastructure or centralized administration. Due to the resource constraints, dynamic network topology, open network architecture, and shared transmission media wireless network are prone to different types of attacks. If the complexity of a system is high, then there are more possibilities to be exploited for attack purposes. Due to limited processing power, transmission bandwidth, and lifetime of batteries there is a restriction on handling the attacks in such networks. Dynamic network topology places a burden on routing protocols when trying to achieve short reaction and convergence times.

Open network architecture and shared transmission media make it possible to join a network without a physical connection. Any of these vulnerabilities can be exploited in a Denial of Service (DoS) attack to prevent or delay legitimate access to services [1]. Security is an important issue for any network, the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

main network security attributes are availability, confidentiality, integrity, authentication, and non-repudiation [1].

In this paper we focus on DoS attacks in wireless Ad Hoc networks. Different types of DoS attacks in wireless Ad Hoc network, impact of DoS attacks on the performance of Ad Hoc networks and the existing countermeasures.

EXISTING SYSTEM

In existing, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable applications on their virtual machines.

DRAWBACKS OF EXISTING SYSTEM

- The cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult.
- Existing work generally focuses on measuring individual vulnerabilities instead of measuring their combined effects.

EXISTING SYSTEM TECHNIQUE

- Common Vulnerability Scoring System (CVSS).

PROPOSED SYSTEM

We propose NICE (Network Intrusion detection and Countermeasure sElection in virtual network systems) to establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. We must note that 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. In general, NICE includes two main phases: deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic. A NICE-A periodically scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability towards the collaborative attack goals, NICE will decide whether or not to put a VM in network inspection state.

ADVANTAGES OF PROPOSED SYSTEM

- We propose NICE (Network Intrusion detection and Countermeasure sElection in virtual network systems) to establish a defense-in-depth intrusion detection framework.
- The area of detecting malicious behavior has been well explored.
- The proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers.

MODULES:

1. User Registration
2. Upload & Send files to users
3. Attack on Ad-Hoc Network
4. Criteria for Attack detection
5. Simulation Results

MODULES DESCRIPTION:

User Registration:

In this module, user registers his/her personal details in database.
Each user has unique id, username and password and digital signature.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

After using these details he can request file from server.

Upload & Send files to users:

In this module, server can upload the files in the database. After verify user digital signature file could be transfer to correct user via mobile ad-hoc network. Attack on Ad-Hoc Network. In this module, to see what the attack on ad-hoc is network is

Distributed Denial of Services (DDoS):

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

Criteria for Attack detection :

In this module, we use multiple nodes and simulate through different criteria are NORMAL, DDoS and IDS (intrusion detection case). Normal Case We set number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the result through our simulator.

IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behavior comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

Simulation Results In this module, we implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity.

a. Throughput

b. Packet delivery fraction

c. End to End delay

d. Normalized routing load

PROPOSED TECHNIQUE

- Scenario Attack Graph (SAG).

Algorithm

```
Create node =ids;
Set routing = AODV;
If ((node in radio range) && (next hop! =Null)
        {
                Capture load (all_node)
 Create normal_profile (rreq, rrep, tsend, trecv, tdrop)
                {pkt_type;          // AODV, TCP,
CBR, UDP
                 Time;
                 Tsend, trecv, tdrop, rrep, rreq
                }
 Threshold_parameter ()
    If ((load<=max_limit) &&
(new_profile<=max_threshold) &&
(new_profile>=min_threshold))
        {
        No any attack;
         }
Else {
         Attack in network;
        Find_attack_info ();
    }
   Else {
 "Node out of range or destination unreachable"
        }
Find_attack_info ()
        {
        Compare normal_profile into each trace value
                If (normal_profile! = new trace_value)
                        {
                                Check pkt_type;
                                Count unknown
pkt_type;
                                Arrival time;
```

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

FUTURE ENHANCEMENT

NICE only investigates the network IDS approach to counter zombie explorative attacks. In order to improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system. This should be investigated in the future work. Additionally, as indicated in the paper, we will investigate the scalability of the proposed NICE solution by investigating the decentralized network control and attack analysis model based on current study.

CONCLUSION

In this survey paper, we try to scrutinize the security issues in the wireless ad hoc networks. Due to the mobility and open media nature, the wireless ad hoc networks are much more prone denial of service. As a result, the security needs in the wireless ad hoc networks are much higher than those in the wired networks.

It has been observed that the existing IDS/IPS performs poorly in detection as well as the false positive rate is higher. It has recently been observed that Denial of Service (DoS) attacks are targeted even against the IDS. Thus, IDS themselves needs to be protected. IDS should also be able to distinguish an attack from an internal system fault.

The identification of intruder and appropriate response techniques to protect Wireless Ad Hoc Network from DoS attacks is still a challenging issue. The need to coordinate intrusion detection and response techniques and the need to respond and control the identified attacks effectively, require further research.

REFERENCES:

1. Chun-Jen Chung, Khatkar, P. ; Tianyi Xing ; Jeongkeun Lee ; Dijiang Huang, NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems, IEEE Transactions on Dependable and Secure Computing, Vlume 10, Issue 4 , Date July-Aug. 2013.

2.Mieso K. Denko " Detection and Prevention of Denial of Service Attacks in Mobile Ad Hoc Networks using reputation based Incentive Scheme" Systematics ,Cybernetics and Information ,vol.3,No.4

3. A. Mishre, K. Nadkarni and A. Patcha , "Intrusion Detection in wsireless Ad Hoc Networks", IEEE Wireless Communications, Vol. 11, Issue 1, PP. 48-60 , Feb. 2004.

4. S.P. Alampalayam, A. Kumar and S. Srinivasan " Mobile Ad Hoc Networks security- A taxonomy" in proceedings of ICACT conference, 2005,

5. Safdar Ali Soomro et l "Denial of Service Attacks in Wireless Ad hoc Networks" Journal of Information & Communication Technology Vol. 4, No. 2, 2010.

6.A.A. Ramanujam,J.Bonney,R,Hagelstrom and K.Thurber,"Techniques for Intrusion resistant Ad Hoc Routing Algorithms (TIARA)" in proceedings of MILCOM Conference,2000.

7. Y.Hu,D.B.Johnson and A.Perrig," SEAD: Secure Efficient distance vector routing for mobile wireless ad hoc networks" in proceedings of fourth IEEE workshop on mobile computing systems & Applicatons,pp3-13, 2002.

8.H.Luo and S.Lu,Ubiquitous and robust authentication services for ad hoc wireless networks" Dept. of Computer Science,UCLA Technical report TR200030,2000.

9. Sergio Marti,T.J.Giuli,Kevin Lai and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks "in proceedings of the 6th annual international conference on mobile computing and networking(MobiCom'00) Bostan 2000,pp255-265.

10.S.Buchegger and J Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes fairness in Distributed AdHoc Networks "in proceedings of MobiHoc conference,2002

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

11.P.Michiardi and R.Molva, "CORE:A Collaborative REputation mechanisms to enforce node cooperation in mobile ad hoc networks in proceedings of Communication and Multimedia Security Conference, pp. 107-121,2002.

12. Y.Huang and W.Lee "A cooperative intrusion detection system for ad hoc networks "in proceedings of ACM workshop on security of Ad Hoc and Sensor Networks,2003.

13. Y.Hu ,A Perrig and D.B.Johnson, "Ariadne : A secure on demand routing protocol for ad hoc networks "in proceedings of the 8th Annual International Conference on Mobile Computing and Networking, pp.12-23, 2002.

14.B.Awerbuch,D.Holmer,C,Nita Rotaru and H.Rubens "An on demand secure routing protocol resilient to byzantine failures," in proceedings of ACM workshop on wireless Security,pp.21-302002.