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

Multiphase distributed vulnerability discovery and counter-action selection framework using OpenFlow network

Kirla Satyavathi
M.Tech,
Department of Computer Science & Engineering,
Raghu Engineering College.

Vana Tatarao
Assistant Professor
Department of Computer Science & Engineering,
Raghu Engineering College.

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

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

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.

A MANET is a special type of wireless network in which mobile hosts are connected by wireless interfaces forming a temporary network without any fixed infrastructure. In MANET, nodes communicate each other by forming a multi-hop radio network. Mobile nodes operate as not only end terminal but also as an intermediate router. Data packets sent by a source node can reach to destination node via a number of hops. Thus multi-hop scenario occurs in communication and success of communication depends on nodes' cooperation.

Security of a network is an important factor that must be considered in constructing the network. A network has to achieve security requirements in terms of authentication, confidentiality, integrity, availability and non repudiation. These security requirements rely on the availability of secure key management system in network. Fundamental goal of a key management system in a network is to issue the keys to the nodes to encrypt/decrypt the messages, to manage these keys and to prevent the improper use of legally issued keys. Absence of key management system makes a network vulnerable to several attacks [6]. Therefore, key management system is the basic and important need of a network for secure communication. A key management system normally involves key generation, distribution, updation and revocation of keys in network. The feature of MANETs such as dynamic topology, lack of centralized authority, resource constrained and node mobility are the major challenge in establishment of key management. Some techniques such as intrusion detection mechanism consume lot of nodes' battery power but cannot account for flexible membership changes. However, an efficient and secure key management system can solve this problem with an affordable cost.

On the hand, mobile ad hoc networking is multi-hop relaying, i.e. messages are forwarded by several mobile nodes from source to destination, if destination node is not directly reachable. In other words, nodes in MANET operate as not only end terminal but also as an intermediate router. Thus, multi-hop scenario occurs; where an attacker can insert, intercept or modify the messages easily in absence of secure routing protocol. This means that unprotected MANET is vulnerable to many attacks [21] such as wormhole attack [22], black hole attack [23] including node impersonation, message injection, loss of confidentiality etc.

Attacks against ad hoc networks

While a wireless network is more versatile than a wired one, it is also more vulnerable to attacks. This is due to the very nature of radio transmissions, which are made on the air.

On a wired network, an intruder would need to break into a machine of the network or to physically wiretap a cable. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer. As the intruder is potentially invisible, it can also record, alter, and then retransmit packets as they are emitted by the sender, even pretending that packets come from a legitimate party.

Furthermore, due to the limitations of the medium, communications can easily be perturbed; the intruder can perform this attack by keeping the medium busy sending its own messages, or just by jamming communications with noise.

Cache poisoning

As an instance of incorrect traffic generation in a distance vector routing protocol, an attacker node can advertise a zero metric for all destinations, which will cause all the nodes around it to route packets toward the attacker node. Then, by dropping these packets, the attacker causes a large part of the communications exchanged in the network to be lost. In a link state

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

protocol, the attacker can falsely declare that it has links with distant nodes. This causes incorrect routes to be stored in the routing table of legitimate nodes, also known as cache poisoning.

Message bombing and other DoS attacks

The attacker can also try to perform Denial of Service on the network layer by saturating the medium with a storm of broadcast messages (message bombing), reducing nodes' goodput and possibly impeding nodes from communicating. The attacker can even send invalid messages just to keep nodes busy, wasting their CPU cycles and draining their battery power. In this case the attack is not aimed at modifying the network topology in a certain fashion, but rather at generally perturbing the network functions and communications.

On the transport layer, Kuzmanovic and Knightly demonstrate the effectiveness of a low-rate DoS attack performed by sending short bursts repeated with a slow timescale frequency (shrew attack). In the case of severe network congestion, TCP operates on timescales of Retransmission Time Out (RTO). The throughput (composed of legitimate traffic as well as DoS traffic) triggers the TCP congestion control protocol, so the TCP flow enters a timeout and awaits a RTO slot before trying to send another packet. If the attack period is chosen to approximate the RTO of the TCP flow, the flow repeatedly tries to exit timeout state and fails, producing zero throughput. If the attack period is chosen to be slightly greater than the RTO, the throughput is severely reduced. This attack is effective because the sending rate of DoS traffic is too low to be detected by anti-DoS countermeasures.

Another DoS performed on the transport layer is the subtle jellyfish attack by Aad et al., that deserves particular attention. Its authors point out that, remarkably, it does not disobey the rules of the routing protocol, even if we may argue that, strictly speaking, this is not always the case. But is indeed true that the jellyfish attack is difficult to distinguish from congestion and packet losses that occur naturally in a network, and therefore is hard and resource-consuming to detect.

This DoS attack can be carried out by employing several mechanisms. One of the mechanisms of the jellyfish attack consists in a node delivering all received packets, but in scrambled order instead of the canonical FIFO order. Duplicate ACKs derive from this malicious behavior, which produces zero goodput although all sent packets are received. This attack cannot be successfully opposed by the actual TCP packet reordering techniques, because such techniques are effective on sporadic and non-systematic reordering.

The second mechanism is the same as that used in the shrew attack, and involves performing a selective blackhole attack by dropping all packets for a very short duration at every RTO. The flow enters timeout at the first packet loss caused by the jellyfish attack, then periodically re-enters the timeout state at every elapsed RTO.

The third mechanism consists in holding a received packet for a random time before processing it, increasing delay variance. This causes TCP traffic to be sent in bursts, therefore increasing the odds of collisions and losses; it increases the RTO value excessively; and it causes an incorrect estimation of the available bandwidth in congestion control protocols based on packet delays.

DoS attacks can also be carried over on the physical layer (e.g. jamming or radio interference); in this case, they can be dealt with by using physical techniques e.g. spread spectrum modulation.

In sum, Denial of Service can be accomplished over different layers and in several ways, and is quite difficult to counteract, even on a wired medium. The topics regarding a full protection against DoS attacks are beyond the scope of this thesis, and therefore are not discussed in detail.

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

Incorrect traffic relaying

Network communications coming from legitimate, protocol-compliant nodes may be polluted by misbehaving nodes.

Blackhole attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes. This is called blackhole attack by Hu et al, and is a "passive" and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.7

Message tampering

An attacker can also modify the messages originating from other nodes before relaying them, if a mechanism for message integrity (i.e. a digest of the payload) is not utilized.

Replay attack

As topology changes, old control messages, though valid in the past, describe a topology configuration that no longer exists. An attacker can perform a replay attack by recording old valid control messages and re-sending them, to make other nodes update their routing tables with stale routes. This attack is successful even if control messages bear a digest or a digital signature that does not include a timestamp.

Wormhole attack

The wormhole attack [67] is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that X is virtually invisible. This results in an extraneous inexistent A - B link which in fact is controlled by X, as shown in Figure 3.4. Node X can afterwards drop tunneled packets or break this link at will. Two intruder nodes X and X′, connected by a wireless or wired private medium, can also collude to create a longer (and more harmful) wormhole, as shown in Figure below:

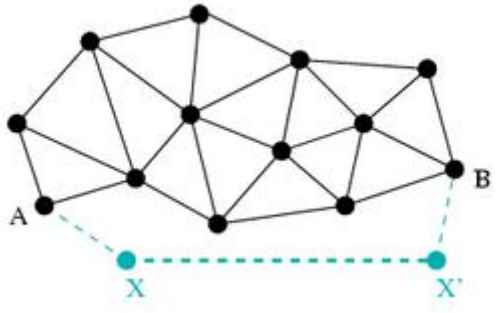


Fig: A longer wormhole created by two colluding nodes *X* and *X′*.

The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved. Furthermore, on a distance vector routing protocol, wormholes are very likely to be chosen as routes because they provide a shorter path – albeit compromised – to the destination.

Rushing attack

An offensive that can be carried out against on-demand routing protocols is the rushing attack. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors

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

are those of the attacker, then any discovered route includes the attacker.

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.

Proposed System:

In proposed system, to solve the security issues we need an intrusion detection system and we propose the preventions to the attacks. This can be categorized into two models:

1. Signature-based intrusion detection
2. Anomaly-based intrusion detection

The benefits of this IDS technique are that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack.

Modules:

- **Admin login:**
- **User login:**
- **Requesting files:**
- **Uploading file:**
- **Downloading file:**
- **Attacker:**
- **Router:**

Admin login:

Admin is login with username and password. Here admin can only do uploadfile and requesting for files.

User login:

User can register with username,password,mernory-type, email-id,digital signature and login with username,password.Here he will download the file,get the request and match the signature and send.

Requesting files:

Firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDOS attack. A DDOS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDOS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network.

Attacker:

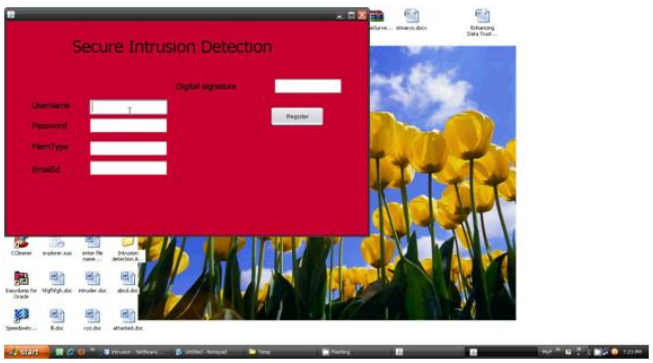
Node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers. The solution to the wormhole attack is packet leashes.

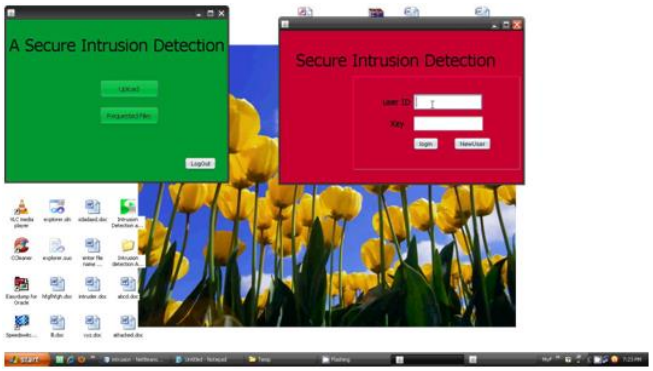
IDS Case

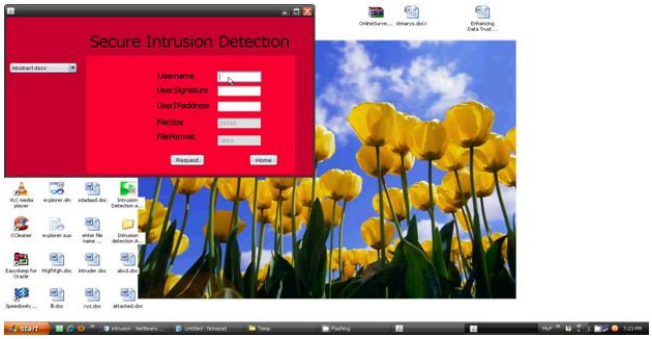
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

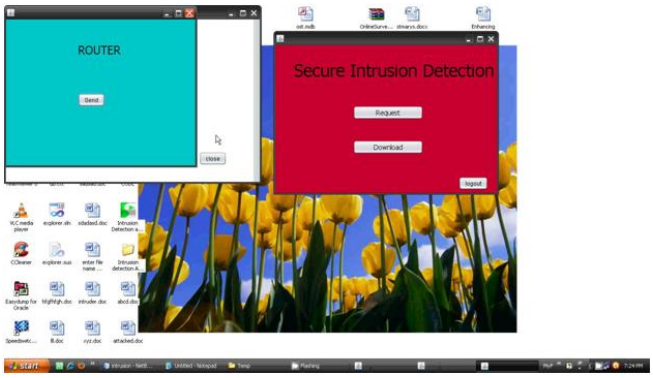
Screen Shots:

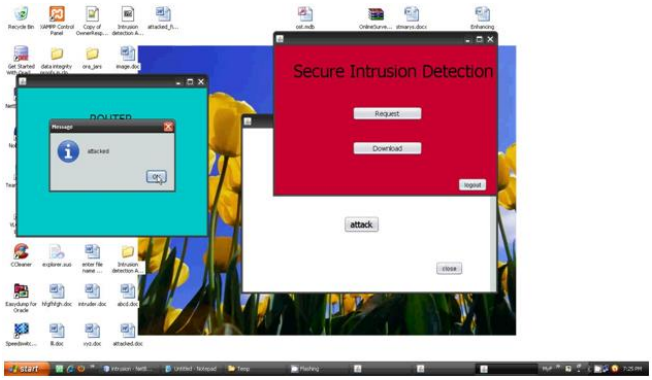


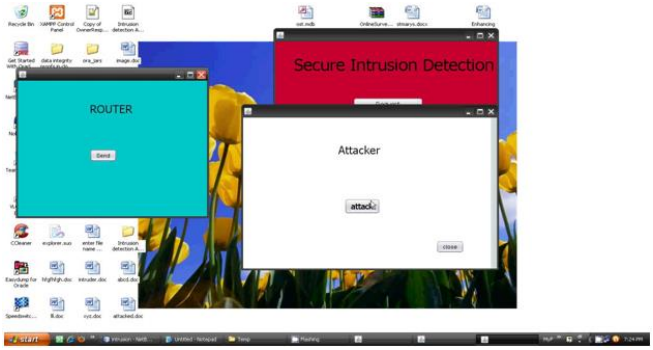


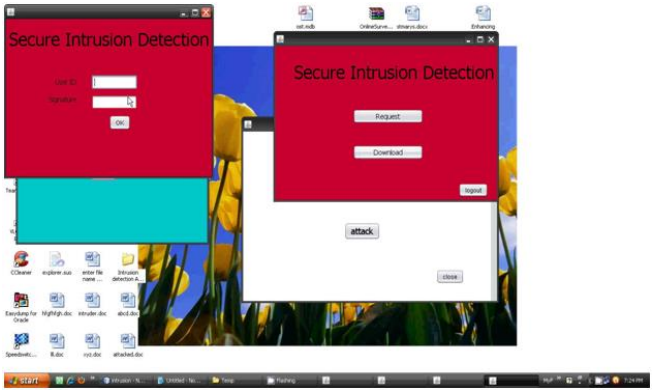


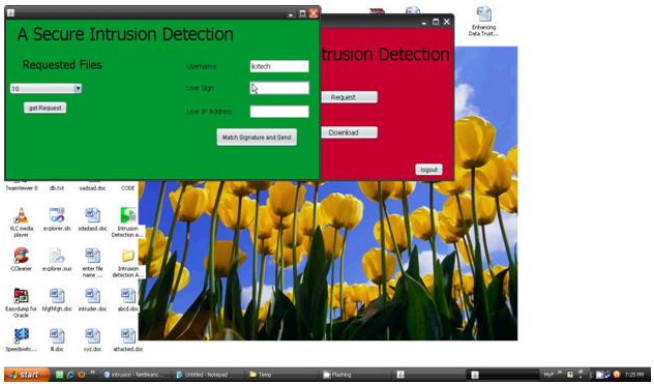
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

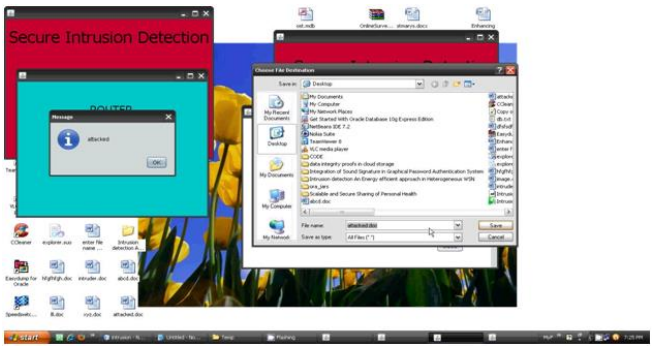


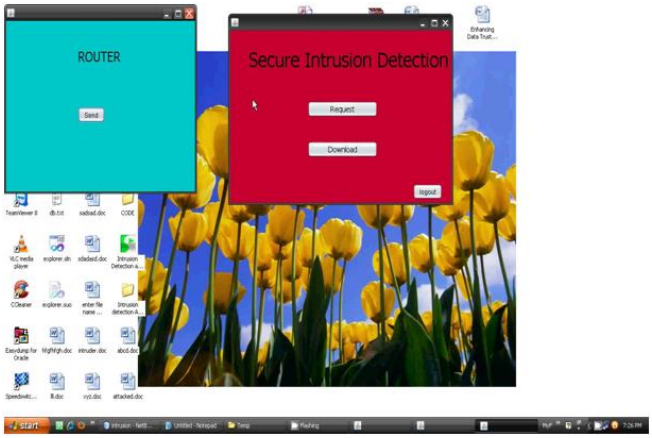












ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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;
```

CONCLUSION

In this 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.

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

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

11. Daniele Raffo, Security Schemes for the OLSR Protocol for Ad Hoc Networks, PhD Thesis, Université Paris 15 SEP 2005

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.