International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 41-48, 2013, ISSN: 2319–8656

HANDLING CROSS-LAYER ATTACKS USING NEIGHBORS MONITORING SCHEME AND SWARM INTELLIGENCE IN MANET

G. Indirani
Department of CSE
Annamalai University
Annamalai nagar- 608002,
India

K.Selvakumar
Department of CSE,
Annamalai University,
Annamalai nagar- 608002,
India

ABSTRACT: The standard MAC protocol widely used for Mobile Adhoc Networks (MANETs) is IEEE 802.11. When attacks in MAC layer are left as such without paying attention, it could possibly disturb channel access and consequently may cause wastage of resources in terms of bandwidth and power. In this paper, a swarm based detection and defense technique is proposed for routing and MAC layer attacks in MANET. Using forward and backward ants, the technique obtains mean value of nodes between the first received RREQ and RREP packets. Based on this estimation, the source node decides the node as valid or malicious. Moreover the MAC layer parameters namely number of neighbors identified by the MAC layer, number of neighbors identified by the routing layer, the number of recent MAC receptions and the number of recent routing protocol receptions are used to determine the node state. The source node uses these two node state estimation techniques to construct the reliable path to the destination. This proposed technique improves the network performance and at the same time prevents attackers intelligently.

KEYWORDS: MANET, MAC, RREQ, RREP, Neighbors monitoring scheme

1. INTRODUCTION

1.1 Mobile ad-Hoc networks (MANETs)

A Mobile ad hoc network is a collection of wireless mobile nodes that can allow people and devices to communicate with each other without the help of any existing centralized infrastructure. A MANET is a self configuring network to form an arbitrary and temporary network. Here each mobile node can function as a router or host. Often the topology of MANET changes as nodes are mobile. Here the routing protocol plays a major role in determining the routes required for communication between the source and destination through the intermediate nodes. The MANET gets new attractive applications since they offer good communication in the changing environment. The MANET can be used in the applications such as rescue operations, tactical operations, environmental monitoring, conferences, connecting soldiers in battlefields and social or business application such as Public and Personal Area Networks.[1] The weaknesses of ad hoc networks are dynamic topology, lack of infrastructure, exposure of nodes and channels [2].

1.2 General attacks in MANET

The MANETs are more prone to security att acks when compared to the wired networks. Due to the restricted features of the MANET such as restricted protection of every individual node, uneven behaviour of connectivity, deficit of certification authority, centralized monitoring or administration, security is difficult to maintain in these networks. In such a wireless network, attacks can enter either from inside the network or from outside. In any case, each node in MANET has to be ready for facing attacks. In particular, an attack from a compromised node inside the network is destructive and difficult to get identified. [3] Attacks in MANET are generally classified as active and passive attacks which are described below.

1.2.1 Active attacks:

An active attack causes various degrees of damage to the network depending on the type of attack. It is further classified into two categories of attacks such as internal and external attack.

- The internal attacks are performed by the compromised nodes that belong to the network.
- The external attacks are performed by the nodes that are not part of the network.

Wormhole attack, black hole attack, Byzantine attack, information disclosure and resource consumption attack are some of the examples of active attacks.

1.2.2 Passive attacks

In this attack, the attacker does not interrupt the regular behavior of the network but intrudes the data exchanged in the network without changing it. This type of attack is difficult to identify as the normal operation of the network is not affected. [3] [4]. There is an attack which is specific to the passive attack whose brief description about it is given below:

- **Snooping:**

  Snooping refers to the illicit use of another person's data. This may refer to watching e-mail informally that is displayed on another's computer screen or observing other people typing. Also more complicated snooping involves a software program to examine the process of a computer or network device. [5]

1.3 Cross layer attacks

Cross-layer attacks emerge from lack of interaction between MAC and routing layers. These attacks propagate from the MAC layer, where they are manifested as Denial of Service (DoS) attacks, to the routing layer, causing serious degradation of network performance in terms of the achieved throughput, latency and connectivity. An attacker can cause congestion in the network by either generating an excessive amount of traffic or by generating specific traffic patterns that prevent certain nodes from communicating with other nodes. [6]

1.3.1 Effects of cross layer attacks

(i) This type of attack exploits the vulnerability of a particular layer (attack point) to launch the attack, but ultimately aspires to disrupt the operations of another layer (target point) [7]

(ii) By incorporating cross-layer information and network communication into the jamming attack, a resource-constrained adversary can significantly increase the efficiency of the attack by targeting specific communication channels, helping to counteract the effect of the anti-jamming systems [9].

(iii) Reduces the attacker's probability being detected.

(iv) Reduce the cost to conduct the attack successfully

(v) Achieve the attack goals that may not be feasible through attack activities in a single layer.

1.3.2 *Issues of cross layer attacks*

(i) It is possible to modify/develop anomaly detection in each individual layer.

(ii) Cross layer defense architecture can be possible which may be based on all the layers and also individual layers.

(iii) The capability of attackers gets even more strengthened by the presence of cognitive radio. [9]

(iv) Due to the anonymization of the networks, the cross layer attackers have increased their efficiency [10].

1.4 Problem identification

The security issues in ad hoc routing have been extensively studied. However, attack strategies that target interaction between MAC layer and routing layer have not been fully addressed. A new class of attacks, cross-layer attacks, emerges from lack of interaction between MAC and routing layers. These attacks propagate from the MAC layer, where they are produced as Denial of Service (DoS) attacks, to the routing layer, causing serious degradation of network performance in terms of the achieved throughput, latency and connectivity.

In the previous works, only routing attacks considered (i.e) network layer attacks. As an extension work, cross-layer attacks are going to be considered which include both MAC and network layer and provide a detection technique using the same SWARM techniques.

2. LITERATURE REVIEW

Patrick Tague et al [8] investigate a class of coordinated jamming attacks in which multiple jammers collaboratively apply knowledge about the network layer functionality to efficiently reduce the throughput of network traffic. They show how a constrained optimization framework can be used to characterize coordinated jamming attacks and allow the impact of the attack to be quantified from the perspective of the network. Using this network-centric interpretation of jamming attacks, a network designer can attain a greater understanding of the potential threat of jamming. To illustrate their approach, they propose and evaluate a variety of metrics to model the attack impact, serving both as adversarial objective functions and as network evaluation metrics

Wenkai Wang et al [9] has proposed cross layer attacks and defending the cross layer attacks in cognitive radios. The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. However, the attackers do not necessarily restrict themselves within the boundaries of network layers. In this paper, they design cross-layer attack strategies that can largely increase the attackers' power or reducing their risk of being detected. As a case study, we investigate the coordinated report-false-sensing data attack (PHY layer) and small-back-off-window attack (MAC layer). Furthermore, they propose a trust-based cross-layer defense framework that relies on abnormal detection in individual layers and cross-layer trust fusion.

John Felix Charles Joseph et al[14] has proposed a cross-layer based routing attack detection system for ad hoc networks. Previous work that uses mostly audit trails collected from the routing protocol suffers from inadequacy of features to construct a reliable model for detecting anomalous routing behavior. On the other hand, use of linear detectors lead to very high false positives and false negatives because of the inherent on-linear nature of the feature space. In this work, these issues are addressed by collating features from multiple protocols at different layers and using a non-linear detector based on Support Vector Machine (SVM). The consequent problem of computational expense of the detection process is addressed by a combination of novel data reduction techniques. Simulation results show that the performance of the proposed CRADS is far superior than conventional protocol-specific detection systems.

Andriy Panchenko et al [10] have proposed a cross layer attack on anonymizing networks. Network layer anonymization protects only some of the user's personal identification information, namely network addresses of the communicating parties. However, even if the lower layers of communication provide perfect protection for the user's profile, information leakage on the application layer destroys the whole effort. Currently, all widespread implementations of anonymizing networks do not use a holistic approach and therefore, neither filter nor actively warn users about information leakage from the upper layers, which may look innocent to the end user. The extend existing work on security of anonymizing networks to take into account additional information leakage from the application layer. Further they show, under which conditions and how this kind of information can be used not only to build an extensive user profile at "low costs", but also to speed up traditional attacks that are targeted at the network layer identification of users' peer partners

Lei Guang et al [11] demonstrate a new class of protocol-compliant exploits that initiates at the MAC layer but targets ad hoc on-demand routing mechanisms. A misbehaved node implementing this type of attacks completely follows the specifications of IEEE802.11 standard and the existing on-demand routing protocols. However, it can cause routing shortcut attacks or detour attacks. They detail the exploits against two on-demand routing protocols: AODV and DSR. They evaluate the impact of such attacks on the network performance and propose Prevention from Shortcut Attack and Detour Attack (PSD) to mitigate their impacts.

A.Rajaram et al [12] have developed a trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, they provide link-layer security using the CBC-X mode of authentication and encryption

3. PROPOSED SOLUTION

3.1 Overview

In this paper, a swarm based detection and defense technique for cross layer attacks is proposed in MANET. The technique makes use of ant colony based optimization (ACO) technique to detect attacks in the MANET. During route discovery time, the source broadcasts RREQ message and the destination responds with RREP message. In this broadcasting, each intermediate node stores the time of first received RREQ and RREP packets. The source injects forward ant (FA) to compute the mean value between received time of RREQ and RREP packets. The backward ant (BA) updates this information and reaches the source node. While receiving the mean value of nodes, the source compares mean value with predefined threshold value and marks node as valid and malicious node. To detect MAC layer attack, each node in MANET calculates D_n using four parameters namely number of neighbors identified by the MAC layer, number of neighbors identified by the routing layer, the number of recent MAC receptions and the number of recent routing protocol receptions. When D_n is zero the node is identified as the valid node otherwise the node is identified as the malicious node. When the source constructs path to the destination, it chooses the path such that the path contains only the valid nodes by omitting malicious nodes.

3.2 Network architecture

In MANET, IEEE 802.11 is used as a standard MAC protocol. The Distributed Coordination Function

(DCF) in IEEE 802.11 combines Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) with a Request to Send/Clear to Send (RTS/CTS) handshake technique to avoid collisions. Both hidden node and exposed problems are solved using RTS/CTS handshake mechanism. At MAC layer, data transmission channel is divided by inter packet gaps, which are termed as Inter Frame Spaces (IFS). Further, channel access can be provided to the nodes based on its priority. [13]

3.3 Swarm based node monitoring strategy

The MAC and routing layer must support each other to detect attacker and adversaries during the operations in MAC layer. It is possible to have more attacks in MAC layer. The attacker may pretend the channel as busy such that no node or user transmits their data. This attack consequently leads to DoS attack in the network, which drastically reduces the network performance. To detect and prevent such kind of attacks, our technique utilizes swarm based node monitoring strategy.

When the source has data to be transmitted, it broadcasts RREQ message and the destination broadcasts back the RREP message towards the source. While receiving RREQ message, each intermediate node records the time of first RREQ packet it has received. The RREQ packet is kept tacked with its RREQ sequence number. Similarly, each intermediate node stores the time and sequence number of first RREP packet it has received. The table that contains this information is known as counter table (C- Table). The format of C-table is shown in table – 1.

To monitor the network, the source periodically injects forward ants (FA) in the network. Each FA travels towards random destination to collect mean time between received times of RREQ and RREP packets. While returning from the destination, the backward ant (BA) updates this mean time in its pheromone table. Finally, the BA reaches the destination.
Every source has mean table (MN-Table) to store the mean times of nodes collected by ants. When the BA reaches the source node, it updates the mean value of nodes in M-Table. Let Th_{rd} be the route discovery threshold value. The source compares the mean value of every node with Th_{rd}. Mean value of nodes less than or equal to Th_{rd} are noted as valid nodes. Nodes that have mean value more than Th_{rd} are noted as malicious node.

Algorithm-1

1. Let Th_{rd} be the route discovery threshold value

2. Consider n_i be the mobile node, where i=1, 2…n and mv_i be the mean value of node i

3. Each node stores time of first received RREQ and RREP packet in C-Table

4. FA and BA collect and update mv values of intermediate nodes in M-Table

5. Source compares mv_i with Th_{rd}

5.1 If ($mv_i \leq Th_{rd}$) then

5.2 Node is considered as valid node

5.3 Else if ($mv_i > Th_{rd}$) then

5.4 Node is considered as malicious node

6. End if

While constructing path from source to destination, the source considers the valid nodes rather than malicious nodes.

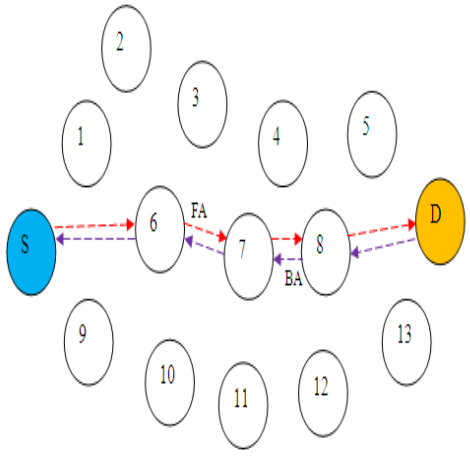

Figure-1 Mean value collection using Forward and Backward ants

Intermediate Node ID	Source ID	Destination ID	Received Time of RREQ Packet	Sequence Number of RREQ Packet	Received Time of RREP Packet	Sequence Number of RREP Packet

Table-1 Format of C-Table

3.4 Neighbors monitoring scheme

In this section, four parameters are monitored for each and every node in the MANET[14]. They are

1) Total number of neighbors found by the MAC layer which is denoted as N_{MAC}
2) Total number of neighbors found by the routing layer which is denoted as N_R
3) Total number of receptions found by the MAC layer which is denoted as R_{MAC}
4) Total number of receptions found by the routing layer which is denoted as R_R

Using these four parameters, D_N is calculated using the formula.

$$D_N \approx (|N_{MAC} - N_R|) \frac{(R_{MAC} - R_R)^2}{R_{MAc} + R_R} \quad (1)$$

Algorithm-2

1. *Let S and D be source and destination respectively*
2. *Let* D_N *be the value calculated for every node in the network.*
3. *If (*D_N *= 0) Then*

   3.1 The node state is a valid node

4. *Else if (*D_N *not equal to 0) Then*

   4.1 The node state is a malicious node

5. *End if*

This state of node is maintained by each node in MN-Table. The MN-Table has the following format,

Node ID	Mean Value	Node State

Table-2 Format of MN-Table

3.5 Data transmission through secure channel

While selecting path, the source uses the two node state detection techniques described in section 3.3 and 3.4. The source selects the path to the destination such that it contains only the valid nodes. Thereby, our technique provides defense against MAC layer attacks.

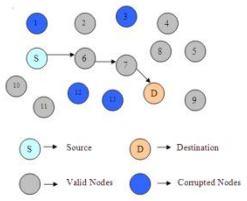

Figure-2 Secure Data transmission

4. SIMULATION RESULTS

4.1 Simulation model and parameters

Here the Network Simulator Version-2 (NS2) is used [14] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol is used. It has the functionality to notify the network layer about link breakage.

In this simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. The numbers of nodes are varied as 20, 40, 60, 80 and 100. It is assumed that each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In this simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in table 3

No. of Nodes	20, 40, 60, 80 and 100.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
No. Of Attackers	1,2,3,4 and 5.

Table 3: Simulation Settings

4.2 Performance metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Average-end-to-end Delay: It is the total time delay taken by the nodes to transmit the data to the receiver.

Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

Here the Swarm Based Detection and Defense Technique using Neighborhood monitoring scheme for Routing and MAC layer Attacks (SBDT-NB) is compared with Cross-Layer Attack vs. Cross-Layer Defense (CACD) [9].

4.3 Results

A. Based on attackers

In the first experiment, the number of attackers are varied as 1, 2, 3, 4 and 5 in a 100 node network.

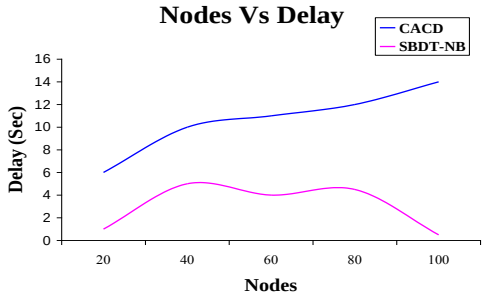

Figure 3: Nodes Vs Delay

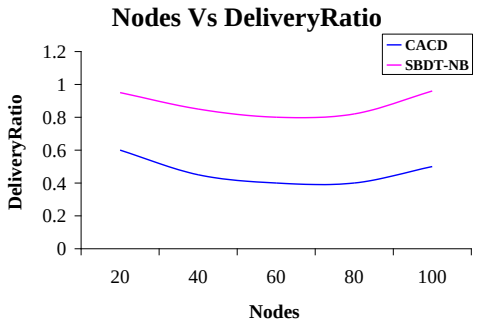

Figure 4: Nodes Vs Delivery Ratio

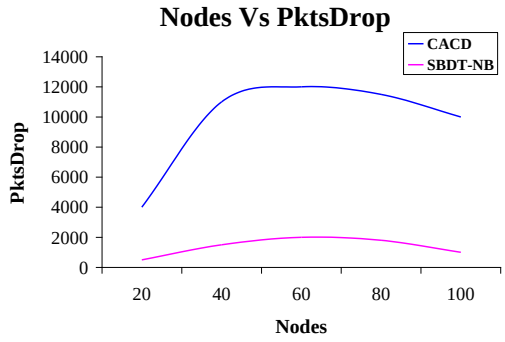

Figure 5: Nodes Vs PktsDrop

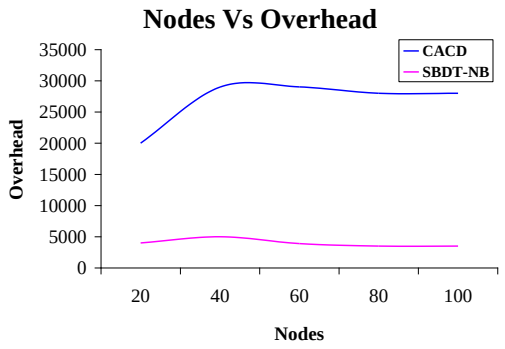

Figure 6: Nodes Vs Overhead

From figure 3, we can see that the delay of our proposed SBDT-NB is less than the existing CACD technique.

From figure 4, we can see that the delivery ratio of our proposed SBDT-NB is higher than the existing CACD technique.

From figure 5, we can see that the packet drop of our proposed SBDT-NB is less than the existing CACD technique.

From figure 6, we can see that the overhead of our proposed SBDT-NB is less than the existing CACD technique.

B. Based on nodes

In the second experiment we vary the number of nodes as 20, 40, 60, 80 and 100.

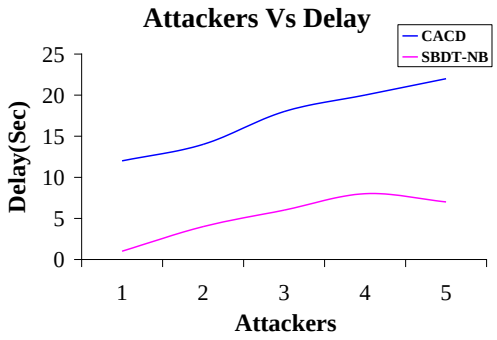

Figure 7: Attackers Vs Delay

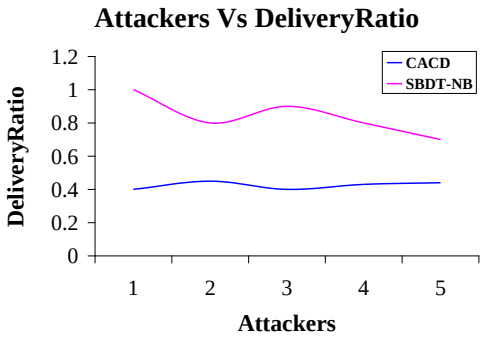

Figure 8: Attackers Vs Delivery Ratio

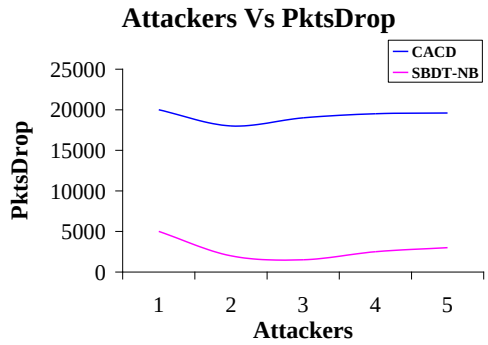

Figure 9: Attackers Vs Drop

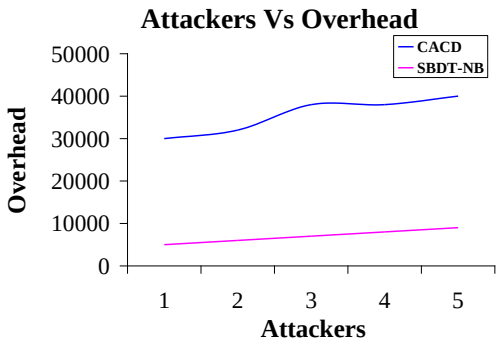

Figure 10: Attackers Vs Overhead

From figure 7, we can see that the delay of our proposed SBDT-NB is less than the existing CACD technique.

From figure 8, we can see that the delivery ratio of our proposed SBDT-NB is higher than the existing CACD technique.

From figure 9, we can see that the packet drop of our proposed SBDT-NB is less than the existing CACD technique.

From figure 10, we can see that the overhead of our proposed SBDT-NB is less than the existing CACD technique.

5. CONCLUSION

In this paper, a swarm based detection and defense technique with neighborhood monitoring scheme is proposed for cross layer attacks in MANET. Using forward and backward ants, the technique obtains mean value of nodes, which is the difference between first received RREQ and RREP packets. While receiving the mean value of nodes, the source compares mean value with predefined threshold value and marks node as valid and malicious node. Further, using the four MAC layer parameters the node state is identified. Using, these two node state estimation technique, the source constructs path to the destination by omitting the malicious nodes. The performance of our technique is proved through simulation results. This Proposed technique prevents attackers wisely and improves network performance.

6. REFERENCES

[1] Sevil , Sen, John A. Clark, "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks", Proceedings of the second ACM conference on Wireless network security 2009

[2] Yian Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", International journal of computer applications, 2011

[3] Sureyya Mutlu, Guray Yilmaz, "A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs", IARIA Seventh International Conference on Networking and Service, 2011

[4] N.Shanthi, DR.LGanesan and DR.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad Hoc Network", Journal of Theoretical and Applied Information Technology, 2009

[5] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet Communication, International Journal of Computer Science and Security (IJCSS), 2009

[6] Svetlana Radosavac, Nassir Benammar and John S. Baras, "Cross-layer attacks in wireless ad hoc networks", 38th Conference on Information Sciences and Systems (CISS), Princeton, March 17-19 2004

[7] Kaigui Bian, Jung-Min Park, and Ruiliang Chen, "Stasis Trap: Cross-Layer Stealthy Attacks in Wireless Ad Hoc Networks", K. Bian, J.M. Park and R. Chen, "Stasis Trap: Cross- Layer Stealthy Attacks in Wireless Ad Hoc Networks", In Proceedings of IEEE GLOBECOM, 2006.

[8] Patrick Tague, David Slater, Guevara Noubir, and Radha Poovendran, "Quantifying the Impact of Efficient Cross-Layer Jamming Attacks via Network Traffic Flows", Network Security Lab (NSL), University of Washington, Tech.Rep., 2009.

[9] Wenkai Wang and Yan (Lindsay) Sun, Husheng Li, Zhu Han, "Cross-Layer Attack and Defense in Cognitive Radio Networks", IEEE GlobeCOM, 2010

[10] Andriy Panchenko, Lexi Pimenidis, "Cross-Layer Attack on Anonymizing Networks", IEEE International Conference on Telecommunications, (ICT 2008), pp-1-7, 2008.

[11] Lei Guang, Chadi Assi, and Abderrahim Benslimane, "Interlayer Attacks in Mobile Ad Hoc Networks", Springer, Mobile Ad-hoc and Sensor Networks Lecture Notes in Computer Science Volume 4325, pp 436-448 , 2006

[12] A.Rajaram, Dr. S. Palaniswami, "The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks", International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010

[13] Yihong Zhou, Dapeng Wu and Scott M. Nettles, "Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems", in proceedings of the Workshop on BWSA, BROADNETS, USA, 2004.

[14] John Felix Charles Joseph∗ , Amitabha Das∗ , Boon-Chong Seet†, Bu-Sung Lee, "CRADS: Integrated Cross Layer approach for Detecting Routing Attacks in MANETs", WCNC proceedings,2008

[15] Network Simulator: http:///www.isi.edu/nsnam/ns