A Security Architecture to Mitigate Cross Layer Malicious Attacks in Lazy Receiver Processing (LRP) Network Subsystem

[1] G. Nazia Sulthana, [2] V.K. Sharma
Department of Computer Science and Engineering,
Bhagwant University, Ajmer, India

Abstract: **--** Lazy Receiver Processing is new network subsystem architecture, which provides stable overload behavior, fair resource allocation, and high throughput under heavy load. All operating systems use sophisticated means of controlling the resources allocated to application processes. Policies like dynamic scheduling, memory allocation and swap memory are designed to ensure fair behavior of a timeshared system under various load conditions. The purpose of this paper is to provide a framework for understanding the Cross Layer attack in LRP based networks and evaluate its damage in the association. We made our simulations using NS-2 (Network Simulator version 2). Having implemented a detection and diffusion technique which simulates the cross layer attacks, we performed tests on diverse topologies to evaluate the network performance without and with malicious nodes in the LRP network. As expected, the throughput in the network was deteriorating considerably in the existence of a malicious nodes. Afterwards, proposed a solution to remove the malicious node effects in the LRP network in terms of packet delivery ratio, end-to-end delay, and throughput.

Keywords: **--** LRP, MAC, Neighbors monitoring scheme.

Introduction

1.1 Lazy Receiver Processing (LRP)

Operating systems are focused on improving bandwidth utilization and reducing network latency by resource management. Lazy receiver processing (LRP) A network subsystem [1] was proposed, which provides stable behavior, fair allocation of resources, and high throughput under heavy load. Main memory allocation and swapping are designed to ensure fair behavior of a timeshared system under various load conditions. Resources consumed during the processing of network traffic, on the other hand, are generally not controlled and accounted for in the same manner. This poses a problem for network devices that face a large volume of network traffic, and potentially spend high amounts of resources on processing that traffic. Incoming network traffic is scheduled at the priority of the process that receives the traffic, and extra traffic is discarded. This allows the system to maintain fair allocation of resources while handling high volumes of network traffic, and achieves system stability under overload.

1.2 General Attacks in Networks

The LRP networks like other are more prone to security attacks. Due restricted protection of every individual node, uneven behavior of connectivity, deficit of certification authority, centralized monitoring or administration, security is difficult to maintain in these networks. In such a network, Attacks can enter either from inside the network or from outside. [3] Attacks 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. 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]. Snooping in one of such attacks which refers to the illicit use of another person's data.

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.

1.3.1 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. [6]

(iv) Due to the anonymization of the networks, the cross layer attackers have increased their efficiency [7].

1.4 Problem Statement

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 neighbor monitoring techniques.

Literature Review

Patrick Tague et al [5] 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.

Wenkai Wang et al [6] 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.

John Felix Charles Joseph et al[11] has proposed a crosslayer 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 nonlinear 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.

Andriy Panchenko et al [7] 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.

Lei Guang et al [8] 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.

A.Rajaram et al [9] 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.

Proposed Solution

The proposed cross-layer cooperation demonstrates that MAC and routing layers would need to coordinate with each other so as to keep away from purposes of congestion and reroute traffic and with the IDS, so as to keep away from consideration of malicious nodes in the new routes or to isolate malicious nodes and spread the information throughout the network. When the source has to transmit the data, It uses RREQ and destination reply back with RREP. While receiving source notes down the time of reception & similarly each intermediate nodes notes the sequence number and the time of RREP reception and stores in Col-Table.

To monitor the network source injects packets (Forward Ants) to network which collects mean times of RREQ data from each nodes and while returning back BA (Backward Ants collects this mean time in its pheromone table. Finally, the BA reaches the destination. Every source has mean table (Mean-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 Mean-Table. Let Td be the route discovery threshold value. The source compares the mean value of every node with Td. Mean value of nodes less than or equal to Td are noted as valid nodes. Nodes that have mean value more than Td are noted as malicious node.

Algorithm-1

1. Let Td be the route discovery threshold value
2. Consider Ndi be the mobile node, where i=1, 2…n and mvi be the mean value of node i
3. Each node stores time of first received RREQ and RREP packet in Col-Table
4. FA and BA collect and update mv values of intermediate nodes in Mean-Table
5. Source compares mvi with Td

5.1 If (mvi ≤= Td) then

5.2 Node is considered as valid node
5.3 Else if (mvi > Td) then
5.4 Node is considered as malicious node
6. End if

Source only considers valid nodes to construct routing path.

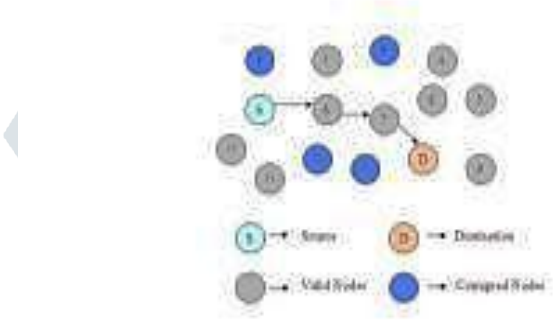

Fig-1 Routing table search

Table-1: Col-Table

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

MAC layer monitoring:

In this section, four parameters are monitored for each and every node in the MANET[11]. They are
1) Total number of neighbors found by the MAC layer which is denoted as NMAC
2) Total number of neighbors found by the routing layer which is denoted as NR
3) Total number of receptions found by the MAC layer which is denoted as RMAC
4) Total number of receptions found by the routing layer which is denoted as RR Using these four parameters, DN 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 Dn be the value calculated for every node in the network.
3. If (Dn = 0) Then

3.1 The node state is a valid node

4. Else if (Dn not equal to 0) Then

4.1 The node state is a malicious node

5. End if

This state of node is maintained in Mean-Table.

Table-2: Mean Table

Node ID	Mean Value	Node State

Simulation Model

The NS 2.35 test system is utilized to recreate the proposed approach. It is just an Object Oriented Discrete Event Simulator that stores the rundown of occasions and executes them one after the other. At once, just a single string is executed. Back end of NS 2.35 utilizations C++ event scheduler.

Numerous Protocols that are upheld by NS 2.35 are actualized at the back end C++ coding. The front end is the language called OTCL; a protest arranged Tool Command Language which is a scripting dialect used to execute C++ source documents. The front end makes arrange situations and topologies and for speedier execution of the program, the back end apparatus is utilized.

Simulation was carried out in NS 2.35 with below mentioned parameters.

Parameter	Value
No. Of Nodes	50
Model	1000 X 100
Mac Type	802.11
Routing Protocol	AODV
Packet Size	512
Simulation Time	10 mins
Traffic type	CBR

Fig-2 snapshot of malicious node detection

As shown in fig-2, when malicious node is detected, it diffuses contacts with another node to start the transmission. If the number of neighbors is larger, the probability of node M being in interference range rises and, therefore, the probability of collision with transmission of another node rises. In general, the malicious node is aware of the fact that the decisions it makes cause different back of values and different PD (they are inversely proportional). Hence, it has distinct preferences for different outcomes. Another issue is a network with multiple malicious nodes. If all the nodes are acting independently, this becomes a Prisoner dilemma problem (game Theory Approach) obviously, if all malicious nodes play the game which they try to maximize their own gain, nobody will gain an advantage.

Performance Parameters

1. End to end delay

End to End delay alludes to the time taken (average) for the packet to achieve the goal, which incorporates the route disclosure time and line taking care of time during transmission.

2. PDR (Packet Delivery Ratio)

Packet Delivery Ratio can be characterized as the proportion of aggregate packets conveyed to the object and the aggregate number of packets that were sent by the source. A high estimation of the packets conveyance proportion legitimizes better execution of the convention.

3. Throughput

Throughput can be characterized as the number of bytes sent from the sender and aggregate number of bytes received by the receiver. A high estimation of the throughput can conveyance legitimizes better execution of the convention.

Simulation Results and Discussion

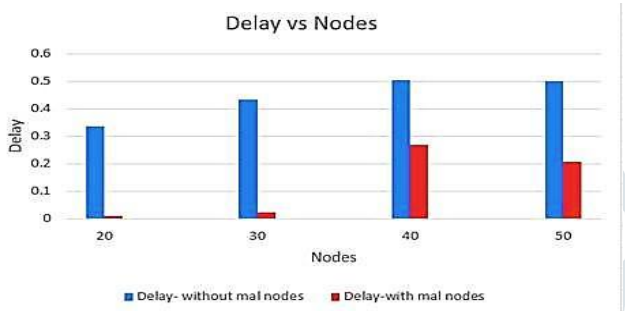

Fig – 3: Delay vs Nodes

Above Figure shows end to end delay without malicious nodes after IDS system shows reduced delay of the network compared with Malicious nodes in network. It can be seen that in the presence of high network traffic load, network is providing much lower delay after malicious nodes detected.

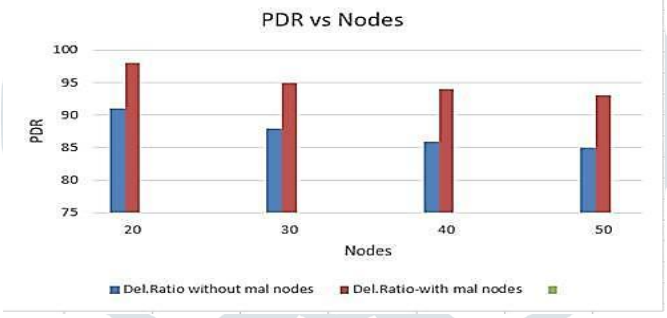

Fig-4: PDR vs Nodes

The above figure describes the graphical view of Packet Delivery Ratio in network with malicious nodes and without malicious nodes after detection using IDS system. Simulation result clearly shows that PDR without malicious node is quite higher than with malicious nodes.

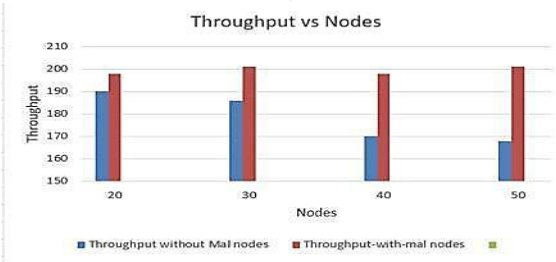

Fig-5: Throughput vs Nodes

Above Figure graphical view of Throughput without malicious nodes improved throughput of the network compared to network with malicious nodes.

Conclusion

This paper demonstrates that cross-layer interaction can drastically improve the probability of attack detection (malicious nodes) as well as the speed of detection. Sneaky attacks are not feasible in the lengthy term; however that is also dependent on the stage of traffic in the neighborhood of the malicious nodes. So the proposed IDS approach in collaboration of cross-layer targets to overcome efficient load balancing path instead of link cost based shortest path. The proposed IDS approach improving network performance. Further to improve network lifetime and QOS cross-layer architecture, based cooperative routing algorithms have to be designed for different network model.

References

[1] Lazy Receiver Processing (LRP): A Network Subsystem. Architecture for Server Systems. Peter Druschel and Gaurav Banga. USENIX Symposium on Operating Systems Design And Implementation (ODSI), Seattle,WA,Oct 1996

[2] CHEN, B., JAMIESON, K., BALAKRISHNAN, H., AND MORRIS, R. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. ACM Wireless Networks Journal 8, 5 (Sept. 2002), 481–494.

[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] 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.

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

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

[8] 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

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

[10] 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.

[11] 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

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