CHAPTER 5

RADICAL BLOCK TO BYZANTINE ATTACKS

The Byzantine attacks at the three layers namely data link, network and transport layers, the detection, recovery and prevention methods against these attacks handled in the thesis is presented in this chapter. The cryptography components such as encryption, hashing, secret key sharing and information dispersal algorithms used in the work are explained.

5.1 NEED FOR CROSS LAYER FEED BACK IN BLOCKING BYZANTINE ATTACKS

There is a lot of advancement in the computing world especially in resource sharing technology. It has undergone a huge change in architecture from client, server to grid and cloud, and the nodes are highly equipped, rich in configuration, small and compact, the field of applicability is almost in each and every field and has become pervasive and ubiquitous and transmission using smart and MIMO antennas.

Each and every activity depends upon the information and networking field either directly or indirectly in the present world. As the technology improves, scope for attackers and hackers also increases. There is always a need to defend the attackers and secure the communication system. A Mobile Ad Hoc Network without fixed and centralized infrastructure is less secured and paves a warm platform for abundant attacks. The various secured routing protocols and security mechanisms such as authentication, integrity,
encryption, secured association between nodes, and hashing techniques are applied as solutions to overcome these attacks.

Byzantine attacks come under the category of active insider attacks in broad classification and further into several types by the number of malicious nodes involved in the attack. Single node attacks are widely known as black hole attacks, colluding nodes are wormhole attacks and when a group of attackers jointly perform the attack, they are known as Denial of Service attacks and network overlay attacks.

Very few works were done to secure the system from Byzantine attacks and none of them have addressed all these types of Byzantine attacks with cross layer feedback to improve the efficiency of security system.

The various routing protocols were designed as a solution to identify and prevent Byzantine attacks. But when the intension of the attackers is high, they will find a new way to attack like emerging of new viruses and hacking systems to break the security of anti viruses and protection mechanism. The protocols mentioned above considers only routing and data transmission phase but the system’s security can be breached easily from the MAC layer.

The IEEE MAC protocol for wireless LAN 802.11 gives the functions carried out in MAC and physical layer. The vulnerability of 802.11 in ad hoc networks is analyzed by Anahita Sanandaji et al. (2013). 802.11 has been designed under the assumption of proper behavior of nodes whereas malicious nodes won’t obey the rules specified by 802.11. Work by Ying Zhou et al. (2006) explores the susceptibility of MAC layer to attackers. MAC layer is not secured and it is easy to deploy denial of service attack in this layer than at any other layers of MANET.
Kyasanur & Vaidya (2005) addressed the problem of selfish behavior of nodes in MAC layer and provides a solution by monitoring the nodes. Receiver is instructing the back off time for sender and it monitors packets received from sender whether it follows the schedule or violates it. As a corrective measure, penalty of maximum delay is dictated to the sender.

Cross layer approach is efficient in performance and security than that of layers working individually on security scheme. Casey et al. (2003) uses this way of cross layer feedback for efficient routing. The information of node detection and address resolution done by the MAC layer is transmitted to routing protocols to improve its multicast routing as addressed in the work by Casey. Sofiane et al. (2013) proposed a scheme to enhance the performance of TCP and routing protocols through increased interactions between them and also this interaction is used to reduce the energy consumed by nodes of MANET. The cross layer feedback conserves energy and time through avoiding unnecessary delays and transmission towards misbehaving nodes.

5.2 RADICAL BLOCKING

This work presents a solution to suppress and block all forms of Byzantine, an active insider attacks. Loyal nodes are identified by a collated code and is intimated during communication channel establishment phase of MAC layer and this authenticate the nodes as single sign on for entering into the security ring.

Nodes which provide this code can take part in further communication and only their entries are noted as loyal nodes in the ARP table, and the intruders are eliminated. Intruders or external attackers are not aware of the code, so they are noticed and rejected out in channel allocation.
phase. Byzantines are the internal attackers who know the code and had an entry into the security ring.

The hazardous Byzantine attacks are handled at two different levels - a normal security scheme and a cross layer security scheme. The threshold value is set high nearing the value of 1 for security essential applications like in combat field and vigilance system otherwise the value is set considering the normal delay and loss of data due to the mobility and ad hoc implementation of the communication network. Threshold value is between 0 and 1 including 0, 1.

When the threats are subtle, the detection, recovery and preventive measures for these Byzantine attacks operate at network and transport layers alone and when the limit crosses the normal range, a cross layer protection is invoked. This security scheme spreads across the other layers such as link layer.

The overall architecture of this cross layer approach is given in Figure 5.1.

![Figure 5.1 Triple Layer Security against Byzantines Attacks](image-url)
Full protection at one part of the network alone is not enough to prevail over the malicious nodes. MAC layer is the entry point kept open for attackers and they can execute all kinds of single, colluding and grouping attacks at this layer easily. The security ring is not complete without enough protective measures at this layer.

5.2.1 MAC Layer Attacks and Protective Mechanism

MAC layer is the subtle layer vulnerable to malicious nodes. Lot of effort is needed to break the security walls of network and transport layers, whereas it is very easy for attackers to shatter the trust and security of the MANET at MAC layer. All the work done to save the MANET from malicious nodes is of waste if the network is not secured at MAC layer.

5.2.1.1 Attacks

The two contention mechanisms used by MAC to share the bandwidth are PCF and DCF. Point Coordination function is the centralized one and can be used by infrastructure based wireless networks only. Any attack in PCF is controlled by base station or access point. Distributed coordination function is the one which suits for infrastructure less Ad Hoc networks.

Jamming the signals (RTS, CTS, and ACK), modifying the back off value, immediate access to channel before the finishing point of specified time interval and thereby limiting the bandwidth of legitimate nodes are the possible attacks at this layer.

5.2.1.2 Detection

The authentication at link layer of the MAC protocol is used as a single sign on for further communication in the top level layers. All activities
of the nodes are monitored in processing the beacon frames, probe frames, data frames, and point coordination functions.

A state table given in Table 3.1 is maintained by each node. Nodes are rated for each activity and a relative weight is added to the node for benign behavior and the relative weight is subtracted for harmful actions.

5.2.1.3 Recovery and Prevention

Parameters in the state table are modified to reflect the behavior and authenticity of nodes. This nodes behavior is collected as an aggregate weight and spread to the Laplacian matrix and the weighted Laplacian matrix \( L \) or Kirchhoff matrix \( K \) is used as the main feedback across the layers to decide whether to include or omit the node or an edge in communication activities.

Any deviation of nodes behavior in accessing the channel, response for RTS, frame forwarding activities are monitored and noted down. The malicious nodes are identified when deviation from normal behavior is high and repeated. With the help of Kirchhoff matrix, the removal of such misbehaving nodes and the links lead them that affects the connectivity of the network is predicted.

The source node sends probing signal to get the loyal nodes acceptance or status to act as movers and connectors in order to preserve the connectivity of the network. If the removal of the adversaries didn’t affect the system, normal function is carried out and any transmission from attackers is jammed.
5.2.2 Network and Transport Layer Security

5.2.2.1 Attacks

Malicious nodes affect the route discovery and route maintenance phase of the network layer by tunneling and deviate the RREQ, RREP packets in the wrong path, dropping the packets, delaying the packets, non cooperation in route establishment, providing faulty information about benign nodes, etc. All kinds of single node attacks are prohibited by secure routing. Optimized security scheme is needed for colluding attacks and further research is going on in this field. The different kinds of colluding attacks on MANET and their impact on the network are explored by Chenfeng et al. (2010).

The transport layer attacks are to block the source nodes from message transmission, not forwarding the message and giving false acknowledgements.

5.2.2.2 Detection

The feedback given by MAC layer is used in the route establishment phase to identify the misbehaving nodes. The source node has full control over the route establishment and maintenance phase. This work applies the secure routing protocol presented by Papadimitratos & Haas (2006) with an enhancement for detection of network overlay attacks and wormhole attacks.

5.2.2.3 Recovery and Prevention

The AES - Advanced Encryption Standard algorithm is used for encryption and security association and SHA-256 secret hashing technique is used for message authentication. Message is not transmitted in single path. To
recover from failure, and data loss due to Byzantine attacks, the message with limited redundancy is transmitted in multiple paths after the end nodes are securely associated by secret key.

Various codes are available for Information dispersion. Message is converted into redundant data of greater length. This added redundancy helps in reconstructing the data even if some data is lost. The codes used in adding redundancy are known as erasure codes. For choosing efficient and suitable erasure code, many codes were analyzed. Few of the erasure codes are Reed-Solomon codes, Cauchy codes, Tornado codes and Raptor codes. One such efficient erasure code is Raptor codes which a linear code is presented by Amin Shokrollahi (2006). Here data is encoded by random XOR of random number of symbols. Dispersion method for distributed communication is illustrated by Lin & Chung (2012).

After analyzing many codes, the dispersion scheme chosen for this work is by Rabin’s. Rabin disperses the message with the covariance matrix. Message is dispersed into multiple paths with the help of Rabin’s information dispersal algorithm presented in Rabin (1989). The Path metrics are maintained by each node to measure the loyalty of the nodes involved in the path and updated in the status table. The feedback got from the MAC layer and Network layer is used in data transmission through adaptive information dispersion which is explored in chapter 3. Any violation against normal condition is updated in the status table and passed to other layers.

5.3 IMPLEMENTATION DETAILS

The status table maintained at each layer by the nodes is broadcasted to other nodes to update their tables. The source has an aggregate data and transmits it to the other layers at the start of communication. This feedback acts as a key and reflected in all the activities of the three layers.
The feedback is given in the form of secured adjacency matrix- A and secured diagonal matrix-D. The weighted Kirchhoff matrix or weighted Laplacian matrix is computed from A and D by subtracting elements of A from D. This matrix is analyzed by spectral theory and used in deciding MANET’s present condition and in recovery and preventive measures.

The Kirchhoff matrix is a positive semi definite symmetric matrix. The diagonalization or spectral decomposition of the matrix decompose Kirchhoff matrix into two matrices - V with Eigen vectors as columns and a diagonal matrix of Eigen values-E. The system can be analyzed from these two Laplacian Eigen vector and Laplacian Eigen values. A study on Eigen values and Eigen vectors is called spectral theory. Spectral theory is mostly applicable in image processing. Jerome & Andreas (2009) used spectral theory for link prediction and apply it for curve fitting. A method to calculate the number of paths between two vertices is presented in the work by Jerome.

The Laplacian matrix is used to get number of paths between any two nodes and simulated to study of node or edge inclusion and removal. It also provides information about cut vertex, connectivity and partitions of the system.