Chapter 6

Conclusion and Future Directions

The present research work presents the various approaches to intrusion detection in WLAN and some issue involved there in. After addressing these issues, the intrusion detection techniques have been designed in WLAN. The brief summary of the work done and important conclusions drawn from this research work are listed in section 6.1 and Section 6.2. Section 6.3 presents the scope for future work that may be helpful to the manufactures, users and the researchers engaged in this technology:

6.1. CONCLUSIONS

- The various approaches available in the literature for intrusion detection in WLAN have been thoroughly investigated. The issues involved there in like (i) the outstanding vulnerabilities and attacks in WLAN, (ii) existing wireless intrusion detection techniques and (iii) the intrusion detection tools, to analyze their performance and enhancements for WLAN are critically examined.
- The existing twenty five intrusion detection tools were analyzed by using different imperative research parameters and subsequently suggestive guidelines for the selection and design of Intrusion Detection Techniques for WLAN have been provided.
• The taxonomy was designed for intrusion detection systems (IDS) to compare and evaluate different functions, features and aspects of the various intrusion detection tools. Number of important design and implementation issues were identified, which provides a framework for evaluating or deploying intrusion detection systems.

• To address the issues involved in intrusion detection, three intrusion detection techniques have been designed in WLAN. The first proposed intrusion detection technique is cross layer based, second is MAC layer based and third one is defense architecture and distributed based technique. All the techniques are evaluated using NS2 simulator on Fedora platform. The quantitative evaluation was done using the three performance metrics i.e. false positive rate, misdetection ratio and packet delivery ratio.

In cross-layer based intrusion detection technique for wireless network, a dynamic profile of RSS values for the communicating nodes is developed, through monitoring the RSS values periodically for a specific MS or a BS from a server. Since it is not possible for an attacker to assume the exact RSS value for a sender by a receiver, therefore, it has been proven a very useful parameter for designing an intrusion detection system. The observed Time taken (TT) for RTS-CTS handshake values at the server provides a reliable passive detection mechanism for session hijacking attacks since it is an unspoofable parameter related to its measuring entity. In this technique, a combined weight value is computed from the RSS and TT. If the weight value is greater than a threshold value, then the corresponding node is considered as an attacker. The performance
of the proposed technique is evaluated practically using the NS2 simulator on the Fedora platform. The proposed technique is compared with the Radio Frequency Fingerprinting (RFF) in terms of metrics; delivery ratio, false positive rate and misdetection ratio at different transmission ranges and at different attacks rates. The simulation results show that the proposed technique attains low misdetection ratio as well as false positive rate while increasing the packet delivery ratio.

Further, a MAC Layer Based defense scheme was developed for Reduction-of-Quality (RoQ) attacks in WLAN that includes the detection and response stages. The detection technique used three status values that are obtained from the MAC layer: frequency of receiving RTS/CTS packets, frequency of sensing a busy channel, and the number of RTS/DATA retransmissions. When the number of RTS/CTS packets received exceeds a certain threshold $R_{C_{th}}$, it indicates that too many nodes are within the transmission range to compete for the channel. When the channel is sensed to be in a busy state, a node will persist in the backoff stage and stop the congestion window (CW) count. When stopping time is longer than a threshold $S_{E_{th}}$, it indicates that too many nodes are within the interference range. Thus if the number of retransmissions exceeds a threshold $R_{E_{th}}$, it will be regarded as an indicator for channel congestion. Since these status values are already available in the protocol stack implementation, the overhead required for implementing this detection scheme is very low. The proposed MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) is compared with Shrew filter (domain frequency). The simulation results show that the proposed technique
reduces the attack throughput there by increasing the received bandwidth and reducing the packet loss of legitimate users. The comparison is also made between MAC layer and cross layer based technique. The results demonstrated that Cross layer based defense scheme has better intrusion detection capability as compared to that MAC layer based defense scheme. The results of the MAC layer based defense scheme are also highly satisfactory as it perform detection as well as prevention of intruders.

Finally, two distributed wormhole detection techniques for detecting the wormhole attacks were developed. In the first technique, wormhole detection was done based on the RTT value (which is considered as the time difference between the node sending Route Request, RREQ, to the acknowledgement as Route Reply, RREP, from the destination). The RTT value may considerably higher than other successive RTT values, if there is a wormhole line between two nodes. In the second technique, wormhole detection was based on the fact that by introducing new links into the network graph, the opponent increases the number of neighbors of the nodes within its radius was proposed. If the neighboring number value for the nodes is higher than the average neighbor number, there is a suspect that a wormhole link is between the two nodes. The proposed Distributed detection techniques are compared with the normal wormhole attack scenario without applying any detection techniques in terms of different performance metrics like Received Bandwidth, Packets Dropped, Packets Received and Packet Delivery Ratio. The simulation results show that the proposed detection techniques can provide improved packet delivery ratio with less packet drops.
6.2 Findings of Research

On the basis of theoretical and experimental investigation reported in this thesis, the followings conclusions have been drawn.

- The cross layer based techniques are more effective than the Radio Frequency Finger printing (RFF) in terms of transmission range and traffic rate for the detection of both session hijacking and man-in-the-middle attacks in WLAN. The scalability from 100 meters to 400 meters can easily be achieved with high detection efficiency.

  The packet delivery ratio was improved by more than 1% whereas the misdetection ratio was significantly reduced (by more than 50%) in proposed cross-layer scheme as compared to RFF scheme when tested at different transmission ranges (100, 250, 300, 350 and 400 M) and attack traffic rates (50, 100, 150, 200 and 250kb).

  The cross-layer scheme attains low false positive rate (50% to 75% approximately), when compared with RFF scheme, which indicate the better detection efficiency of the proposed technique. The bandwidth available in the case of cross layer scheme is more than 30% approximately, and number of packets dropped was less than 25% as compared to RFF scheme.

- The MAC layer based defense architecture (which includes both detection and response stages) is more efficient as compared with Shrew filter (frequency domain method) for detecting a RoQ attack in Wireless LAN. The high detection is achieved for extended attack period upto 20 seconds, which is higher than the attack
period of Shrew attack (2.5 seconds). The received bandwidth for normal legitimate
users is also more than 18% approximately in the MAC layer based technique as
compared to Shrew for varying number of attackers (2-8) and attack period (5 Sec.
to 20 Sec.).

The packet loss due to attack was less than 600 packets in MAC layer based
technique as compared to Shrew, under varying the number of attackers and attack
periods. The detection capability of the proposed MAC layer based technique was
also more effective as compared to Shrew in terms of the delivery ratio (improved
more than 7%), the misdetection improved (less than 17% approximately) and the
false positive rate is less than 36% approximately. Further, it reduces the attack
throughput there by increasing the received bandwidth and reducing the packet loss
of legitimate users.

• The cross layer based scheme has better intrusion detection capability as
  compared to MAC layer based technique (MLDA), as cross layer technique has
  higher packet delivery ratio, less misdetection ratio and low false positive rate as
  compared to that of MLDA.

• The Distributed Techniques (which include round-trip travel time and average
  number of neighbors) are much more effective than the normal attacks scenario for
detecting the Wormhole attacks in WLAN in terms of different performance
metrics like received bandwidth, packets dropped, packets received and packet
delivery ratio. The detection efficiency was quite high even in elongated attacks of
periods upto 25 seconds and high rate upto 500kb.
As the attack period increases from 10 to 25 seconds, the packet drop was significantly less and the packets received (approximately 3% high) and bandwidth received (1% to 4% approximately) both are high in proposed technique as compared to the normal attack scenario. The packet delivery ratio was also high (by approximately 10%) in the proposed technique as compared to normal attack scenario in terms of varying time and rate.

6.3 Scope for future work

In this section, a number of open problems related to the work presented in this thesis are proposed.

• The new intrusion detection techniques in WALN are needed to be developed with the aim towards attaining low misdetection ratio and false positive rate while increasing the packet delivery ratio.

• This work can be extended to Mobile Ad-hoc Networks (MANET) and Wireless Sensor network (WSN).

• Wired networks implementation of the proposed techniques needs to be looked into.

• A lot of scope of the work is to explore the possibility of implementing intrusion detection techniques for different standards of IEEE 802.11X.

• The range, rate and users can be extended beyond the limitation of this research.

• The use of these techniques for intrusion detection in Bluetooth may be explored.