CHAPTER 7

CONCLUSION

Today the world is daily getting equipped with a large number of communication networks as there is a continuous hunger for much faster and highly efficient communication systems. Whether it is computers, mobile phones or even ipads, all the consumer products have been utilizing networks as integral utility tools for communication where information networks do play a very significant and prominent role. The use of internet has further enhanced the requirement of information networks. Due to extensive number of applications offered by the internet, a larger population throughout the globe has started relying on such networks. These networks use different forms of transmission media for data transfer. Earlier, there was a trend when information networks were based on wiring cables for data transfer and were used for fixed computational facilities types of applications, commonly called *fixed or wired network*. However, with continual advances in technology, coupled with the advantages of price and performance, wireless media have started being deployed everywhere as the users could not afford the restriction of mobility while the data transfer has to be carried out. Moreover, the entanglement and management of wires in
wired networks has been a very cumbersome job that lead the researchers to develop another form of networks called *wireless networks* which does not involve the use of wiring cables. A wireless network is an information network which does not involve use of cables. This technology has permitted expansion of horizon in the field of communications beyond that it was thought to be earlier impossible. Among the purported benefits of wireless networks are increased flexibility, much lower installation costs, lower maintenance, and easy *"hot desking"* where users are highly mobile and need to physically share an office space or regularly rearrange the physical configuration of their office. Wireless networking is also particularly suited to conferencing where portable computers are used by most of the participants and to working arrangements where employees are frequently out of the office.

Among various types of wireless networks, Wireless Local Area Network (WLAN) is one of the most popular forms of networks. A WLAN is a type of Local Area Network (LAN) that enables two or more entities to communicate using high frequency radio waves rather than wires. Eliminating the wires to let employees work anywhere and connect remotely to information resources from mobile devices facilitates an attractive work environment thereby further increasing and making the WLAN as latest trend in present business market. Growth and deployment of WLAN has increased tremendously in recent years. Thus, day by day, WLANs are getting popular at university campuses, hotels, cafes, edifices, public hot-spots, etc. A WLAN provides important feature of mobility to its users. In addition, a mobile may connect to or leave a network anytime that enhances the scalability of these networks. In contrast to wired networking which are quite burdensome and expensive, WLANs offer noticeable ease of installation and that too at much lower expenses. These advantages seem to be very compelling, but the threat of intrusion in WLAN is a substantial deterrent.
As is generally believed that with every major advance in networking technology comes new ways to exploit it, the convenience offered by ability to connect to networks using mobile computing devices has also introduced many security issues that do not exist in the wired counterparts. The security measures that were relied on in the past to secure wired networks are now obsolete with this new network technology because WLANs use radio waves which are not restricted by any obstructions such as walls, ceilings or floors thereby making the transmitted data within the reach of even unintended recipients. Thus without using stringent security measures, installing a WLAN can be equivalent to placing Ethernet ports outside the building that makes it accessible to anyone interested in plugging into the network. Thus the fundamental constraint on the evolutionary process of WLANs has been its security.

Since security has always been a limiting factor in use and deployment of WLANs, various security algorithms, like, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA), etc., have been suggested by the researchers from time to time. WEP is a common name for IEEE 802.11b security standard that is a group of specifications for WLANs created by IEEE. This standard defined the Media Access Control (MAC) and physical layers for a wireless LAN. In pursuit to provide better security an effort has been made by Wi-Fi Alliance by providing another security algorithm known as WPA.

Although these algorithms are quite popular but it has been felt that the vulnerability and performance of these algorithms are yet to be analyzed in much detail. Since security has surfaced a prime concern in these ubiquitous networks, the study of vulnerability as well as the performance of these security algorithms has been taken up in this piece of research work. Analysis of these algorithms using test-bed approach has although been done to a certain extent by some researchers where a network having two to three nodes were considered and packets were captured manually through these
networks for the analysis. In this research work, an effort has been made to analyze the performance of WLAN with WEP and WPA as security algorithms and simulated these algorithms using popular simulation software, Network Simulator (NS-2). Here the analysis has not been just limited to 2 or 3 nodes but has been tried even upto 80 nodes. Although NS-2 has been found to be most appropriate simulation software for this analysis, but using NS-2 was a big challenge during this research, owing to open-source nature of NS-2 and lack of formal documentation. However, not only WEP was simulated using NS-2 but even two other algorithms viz., WEP-104 and WEP-BGS that were developed on the basis of WEP were simulated. WEP-BGS is so named because three people were involved in this research work and initials of their names have been used to differentiate this security algorithm from WEP. This is followed by the analysis and simulation of another upcoming security algorithm, WPA. The simulated algorithms have also been subjected to one of the most commonly affecting attacks on networks, the dictionary attack and have further been analysed and studied in terms of its vulnerability to such attacks. For performance evaluation, various performance metrics parameters viz., throughput, Packet Delivery Fraction (PDF) and End-to-End Delay (EED) have been computed through NS-2. In NS-2, the Xgraph and AWK files, so generated after simulation, have been utilized in computing and analyzing the variation of various performance metrics. As a part of this study, for the justification of simulation results and to carry out the comparative analysis of various algorithms, the ANOVA Test has also been applied. This piece of research not just identifies various performance metrics for different security algorithms but also compares the performance of such algorithms.

Since the requirements of a WLAN in terms of its performance may vary from application to application, there cannot be a common performance yard stick for WLANs. The analysis performed in this thesis work enables us to provide certain indications, so as to specify which security algorithm
should be employed for achieving a given performance metric. Since throughput is one of the prime performance parameters in a network, it has been analysed that although throughput remains constant for a given number of nodes for all security algorithms, it is lesser for a WLAN having large number of nodes in comparison with a WLAN having smaller Further, it has been observed that in case of WEP security algorithm, the throughput decreases with increase in the key length. In comparing any variants of WEP with WPA, it has been observed that the throughput for WPA comes out to be even lesser. Thus if throughput is not a constraint the users should opt for WEP-BGS or WPA which is even better.

While analysing another important parameter, the PDF, it was seen that although PDF does not get affected for any individual security algorithm for a given number of nodes, the PDF of various security algorithms is found to be different and it gets improved as we switch over either from WEP-40 to WEP-104 or from WEP-BGS and to WPA. Therefore, in terms of PDF, the use of WEP with increased key length is found to be a better option while WPA seems to be the best one.

In response to dictionary attack on WEP and its variants, it has been observed that different WEP variants behave differently and there is a marked improvement in time taken while extracting the secret key with increase in the length of total key. Hence among all IEEE 802.11b based algorithms, WEP-BGS has been found to be a better choice in terms of vulnerability to dictionary attack. In case of WPA, it was noticed that WPA is quite resilient to dictionary attack as compared to WEP which was found to be weak at all key lengths.

While simulating and analysing another important parameter, EED, it was observed that there is a large percentage decrease in average EED in WPA in comparison with various WEP variants and, therefore, WPA has been found to be better than both WEP-40 and WEP-104. However, the
average EED is found to be more in WPA when it is compared with WEP-BGS and the percentage increase is about 30%. Thus, in applications where EED is important WEP-BGS will prove better not only than WEP-40 or WEP-104 but also than WPA.

While summing up the analysis to conclude, it is observed that when WPA is employed as a security algorithm, for small decrease in throughput, there is an improvement in PDF as it increases as well as improvement in EED as it decreases, other than being resistant to dictionary attacks. Thus a trade-off with throughput is required.

However, when the analysis is supplemented by statistical ANOVA test so as to categorise the change as significant or not, the conclusion may be narrowed-down further that without affecting throughput and EED significantly, WPA algorithm has better i.e. greater PDF, in addition to being resistant to dictionary attack.

Apart from studying and analysing theses security algorithms on the basis of their performance metrics as well as vulnerability to attack, it is felt that there still a lot of scope for studying these security algorithms for their further improvements. Like, we have studied these networks only on the basis of one of the most severe attacks, i.e., dictionary attacks, but still such algorithms can be tried for various other popular attacks. Moreover, since some researchers are on the verge of developing another security protocol named WPA2 that is expected to be the full IEEE 802.11i standard and might be in practice in a couple of years, there seems to be a large scope of studying this new security protocol. Another scope of future investigation could be the exploration of other encryption techniques so as to develop some other security algorithm and its variants which can further be investigated.