CHAPTER VII

CONCLUSIONS AND FUTURE WORK

In the previous chapter NS2 simulator further validates the "optimized secure protocol for MANET through biometric approach" under attack condition. This chapter covers the gist of the research work carried out by the optimized secure protocol through biometric approach for MANET. The concluding remarks of all the preceding chapters are summarised. It also explores the possible extension (future scope) of the proposed methodology.

7.1 INTRODUCTION

In many whereabouts a communication network is vital where there is no rooted infrastructure and neither there is time to create such a framework like military operations, law enforcement, rescue operations and personal area networking. A network developed in such situations where the nodes are mobile is called mobile ad-hoc network or a network constituted vigorously from scratch employing wireless connections composed of mobile nodes is referred as mobile ad-hoc network. Content, pace of organization and less reliance on a permanent framework when grouped with conventional wireless networks are some of the unique features provided by MANET. MANETs other than standard data networks face various challenges in terms of security and QOS due to their dynamic nature. Ad-hoc networks must be equipped with competence to emulate topology transitions as they have continuous dynamic connectivity between their various nodes.

From the literature survey it is being revealed that security and QOS are the most critical parameters for mobile ad-hoc network which are affected by various attacks due to the conventional security approaches and routing methodologies being applied. A lot of work has been done to optimize three major issues of MANET i.e. routing, security and QOS but hardly any literature is available to develop a combined approach or methodology that can enhance performance of MANET through efficient "crypt-iris based perception and authentication approach" along-with "optimized genetic stowed approach to potent QOS in MANET" together referred as "optimized secure protocol for MANET through biometric approach".
"Crypt-iris based perception and authentication approach" proves to be an efficient mechanism of securing MANET. Moreover, "optimized genetic stowed approach to potent QOS in MANET", finds the fittest path leading to an improved QOS based MANET. In this thesis, an effort is made to modify the existing secure algorithm by developing a "crypt-iris perception and authentication approach" that helps in overcoming various security breaches. Next module of this research work "optimized genetic stowed approach to potent QOS in MANET" optimizes various QOS parameters like average packet delivery ratio, average packet drop rate, average end-to-end delay and average hop count through genetic algorithm. Thus, the proposed research methodology not only doubly secures the network through crypt-biometric approach but also optimizes various QOS parameters through meta-heuristic algorithm hence, improving performance of MANET. The problem of the proposed work is to analyze and make the network more secure i.e. enhance security of MANET by overcoming various limitations and attacks faced by conventional secure routing protocols through crypt-iris based biometric approach and eventually optimize performance of QOS parameters by genetic algorithm. "Optimized secure protocol for MANET through biometric approach" is developed using MATLAB platform and results are validated through various performance parameters. Simulation results through MATLAB reveal the effectiveness of the approach in terms of security and QOS for MANET. The developed methodology is further verified through NS2 simulator under condition of attack hence, results of both the simulators validate the proposed approach as an enhanced security and QOS solution for MANET. The following section summarises concluding remarks of the preceding chapters. Future scope is discussed in the last section of this chapter.

7.2 SUMMARY AND FINDINGS

The concluding remarks and findings of all the chapters are hereby summarised below:

Chapter I has introduced the concept of communication system their fundamentals and classification followed by the description of ad-hoc networks, different attacks faced by it and parameters and methods of securing mobile ad-hoc networks. Concepts of biometrics, routing, QOS, meta-heuristic algorithms and performance parameters to analyze the proposed methodology have also been focussed upon. An exhaustive literature survey specified as state of art motivated gaps in study and problem formulation. Main objectives of the research work and complete organization of the thesis are also described in this chapter.
Chapter II has discussed various conventional routing protocols of MANET. The performance of these protocols has been comparatively analyzed by utilizing the simulated data available from literature to focus on the limitations of these conventional approaches. Comparative analysis has been done taking into consideration the various problems suffered by these approaches. The various conventional routing protocols that have been discussed in this research study revealed the fact that each routing protocol has its own advantages and limitations. A standard format that can hold various applications of ad-hoc network is not provided by any of the category of protocols. The various conventional set of routing protocols provided some limitations in one or other field like re-flooding of packets, throughput, security, congestion over network due to extensive bandwidth consumption, QOS issues not taken care of, susceptibility to various types of attacks, delay and bandwidth consumption, extensive amount of data exchange for providing authentication, excessive loss of energy due to higher processing cycles required for encryption, more latency due to invariable increase in security function, less strong mechanisms of encryption leading to more eavesdropping, no balance maintained between the security function and performance of the system and periodical refreshing of the encryption key for enhancing security of the algorithm. No specific QOS models or implementations are available for MANET. A lot of work has been done to optimize three major issues of MANET i.e. routing, security and QOS but hardly any literature is available to develop a combined approach or methodology that can enhance performance of MANET through efficient "crypt-iris based perception and authentication approach" along-with "optimized genetic stowed approach to potent QOS in MANET", together referred as "optimized secure protocol for MANET through biometric approach".

Chapter III has described the development of "crypt-iris based perception and authentication approach" in MATLAB that takes into consideration a standardized database for analysis. Biometric perception has been considered to be the most neoteric technology for sustaining security in various systems by involving exclusive identification features. The attainment of biometric perception depends upon image procurement and biometric perception system. The proffered algorithm has focused on attaining image procurement as well as biometric perception by an effective exploitation of bi-orthogonal wavelets for encoding biometric information. The biometric system has been enhanced by incorporating cryptographic features which results in better solution against various security breaches. Various results
have validated notable design and application of a novel "crypt-iris based perception and authentication approach" to protract security in mobile ad-hoc networks. By using bi-orthogonal wavelets the proposed approach has helped in the development of enhanced security solutions for MANET. Matching unlike other conventional eye recognition processes has not been done by taking one single matching criterion into consideration but in the proposed approach matching has been done through two parameters namely Hamming Distance (HD) as well as Normalized Correlation (NC) coefficient since, bit-wise comparisons are necessary. Although in theory, two iris templates generated from the same iris will have a Hamming distance of 0.0 and strongest linear relationship is indicated by a correlation coefficient of -1 or 1, weakest linear relationship is indicated by a correlation coefficient equal to 0 in conventional methods this has not been achieved. In this neotric approach normalization has been perfectly done and encoding is performed through bi-orthogonal wavelets providing a bit stream away from noises hence, achieving ideal matching conditions; Minimum Hamming Distance=0 and Maximum Normalized Correlation=1. The proposed methodology has unique feature of generating HD and NC even of non iris images and matching them by their specified percentage to the particular databases they slightly match to, that helps in recognising whether the biometric template is correct or not. Further, a two user authentication system for enhancing security of MANET has been developed and implemented involving iris signature to generate domains of ECC and private key, providing two levels of security solutions. By analyzing the proposed neotric "crypt-iris based perception and authentication approach" through two performance parameter values i.e. minimum hamming distance and normalized correlation, various security goals of MANET like authentication, confidentiality, integrity and non-repudiation have been achieved. Also occurrence of various active and passive attacks has been limited in MANET being secured by the proposed approach. No malicious node can affect the transmission of various services hence; DOS attack has been limited. No data packets could be updated, modified or altered without signature matching of the intended sender and receiver.

Chapter IV has discussed the second most critical issue for MANET i.e. to find a best fit shortest path between the source and destination and optimization of QOS parameters. For various real world scenarios, routing is required for meeting the stringent measures of QOS parameters. Meta-heuristic based genetic approach has been analyzed to optimize QOS performance of MANET by developing a simulator in MATLAB, taking into consideration various QOS parameters like average packet delivery ratio, average packet drop rate, average
end-to-end delay and average hop count. Results depict notable design and application of an optimized genetic stowed approach. Genetic algorithm has been mainly exploited for fittest shortest path selection which henceforth, has optimized the various QOS parameters like average packet delivery ratio, average packet drop rate, average end-to-end delay and average hop count. Earlier shortest route selection approaches like Dijkstra's and Bellman Ford were not able to optimize the QOS issues and hence, the performance of MANET was affected. Optimized Genetic Stowed Approach (OGSA) has provided better QOS parameters results in terms of lower packet loss, larger packet delivery ratio, lower average end-to-end delay and smaller number of hop counts when compared with the conventional shortest path selection approach. The proposed approach is quite flexible as it takes number of parameters like network length, network width, nodes transmission range, nodes traffic, speed variation factor and angle variation factor in the network configuration panel as well as number of nodes, simulation time averaging loop value in the simulation panel which have been flexibly varied, providing effective QOS solutions for MANET. Hence, simulation results have revealed that the proposed genetic based approach has optimized various QOS parameters of MANET and provided a critical performance booster for mobile ad-hoc networks when compared with the conventional shortest path selection approach.

Chapter V has focused on overcoming the limitations of conventional secure routing protocols by combining features of biometrics and cryptography to provide authentication and genetic algorithm to optimize QOS based network performance by proffered methodology. Specificity and sensitivity tests have been conducted on developed iris based biometric approach which is quite important for analyzing any biometric system. Simulation analysis has also been performed of optimized genetic stowed approach to potent QOS in MANET by comparing it with conventional shortest path selection approach (Dijkstra’s algorithm). Simulation results have justified "optimized secure protocol for MANET through biometric approach" over the conventional routing approach using MATLAB simulator. The proposed algorithm has been composed of two modules namely a "crypt-iris based perception and authentication approach" and an "optimized genetic stowed approach to potent QOS in MANET". Effectiveness of the iris based biometric approach has been stated by testing it by various specificity and sensitivity analysis which reveals a flexible simulation environment of the iris based biometric system that allows varying of the iris classes as well as images per class, providing effective values for various specificity and sensitivity parameters like TPR, TNR, FPR, FNR, Precision, Accuracy, Recall and F-Measure. Time for training various iris
classes is not very high even with increase in the number of iris classes and images per class. Also, approximately very accurate values of TPR=nearly 100%, TNR=nearly 100%, FPR=nearly 0%, Accuracy=100%, Recall=100% and F-Measure= Nearly 100% have been achieved by the neotric iris perception approach for MANET. When compared with Masek (2003) work on iris recognition which achieved FNR and FPR (with different classes per samples) as 4.580 and 2.494 on LEI database and 5.181 and 7.599 on CASIA database, the proposed methodology serves as a neotric approach achieving required values of FNR=0 and FPR=0.012346 (many parameters included in the proposed methodology are not being specified by any of the conventional approaches) leading to enhanced security solution for MANET. Similarly Abhyankar and Schuckers (2010) achieved values of FNR=0.00 and FPR=3.3 not better than the proposed approach. Also, Panganiban et al. (2011) have achieved accuracy of 94.5 in their developed iris recognition system, when compared with the proposed approach which has achieved accuracy of 96.2. Successful results of specificity sensitivity and accuracy have validated the effectiveness of the neotric iris perception approach for MANET.

Similarly, the simulations results have compared conventional shortest path selection approach and the genetic stowed approach against various parameters like network length, network width, nodes transmission range, nodes traffic, speed variation factor and angle variation factor in the network configuration panel as well as number of nodes, simulation time and averaging loop value in the simulation panel. The proposed algorithm parameters has been flexibly varied, providing effective solutions and maintains QOS which is the most critical solution for MANET. The results of the proposed methodology has been compared with the conventional shortest path selection approach providing a low packet drop rate, high packet delivery ratio, lower end-to-end delay and lower hop counts with different comparable parameters namely node transmission range, node speed, node data rate and node traffic. Even with increase in the number of nodes, simulation time and various other parameters, results have not been deteriorated. The results of simulation have validated the importance and effectiveness of the "optimized secure protocol for MANET through biometric approach” and justifies how the combination of both these methodologies which are quite critical for MANET can bring a rapid change in future as both the approaches as combination have never been utilized by any of the conventional protocols.

The proposed protocol also achieves the following QOS optimization results when compared with conventional approach of MANET, with node speed as the comparison parameter having number of nodes as 10 and 100s as the simulation time, 29% reduction in
average packet drop rate. With node transmission range as the comparison parameter having number of nodes as 20 and simulation time of 100s, 44% reduction in average packet drop rate. With node data rate as the comparison parameter having number of nodes as 30 and simulation time of 100s, 37% reduction in average packet drop rate. With node data traffic as the comparison parameter having number of nodes as 40 and simulation time of 100s, 36% reduction in average packet drop rate.

With node speed as the comparison parameter having number of nodes as 10 and 100s as the simulation time, 32% increase in average packet delivery ratio. With node transmission range as the comparison parameter having number of nodes as 20 and simulation time of 100s, 42% increase in average packet delivery ratio. With node data rate as the comparison parameter having number of nodes as 30 and simulation time of 100s, 34% increase in average packet delivery ratio. With node data traffic as the comparison parameter having number of nodes as 40 and simulation time of 100s, 37% increase in average packet delivery ratio.

With node speed as the comparison parameter having number of nodes as 10 and 100s as the simulation time, 12% reduction in average end-to-end delay. With node transmission range as the comparison parameter having number of nodes as 20 and simulation time of 100s, 14% reduction in average end-to-end delay. With node data rate as the comparison parameter having number of nodes as 30 and simulation time of 100s, 11% reduction in average end-to-end delay. With node data traffic as the comparison parameter having number of nodes as 40 and simulation time of 100s, 11% reduction in average end-to-end delay.

With node speed as the comparison parameter having number of nodes as 10 and 100s as the simulation time, reduction of average hop counts from 2.2 to 1. With node transmission range as the comparison parameter having number of nodes as 20 and simulation time of 100s, reduction in average hop count from 2.5 to 1. With node data rate as the comparison parameter having number of nodes as 30 and simulation time of 100s, reduction in average hop count from 2.1 to 1. With node data traffic as the comparison parameter having number of nodes as 40 and simulation time of 100s, reduction in average hop count from 2.3 to 1. The results of simulation have revealed the importance and effectiveness of the optimized secure routing protocol through biometric approach and specify how the combination of both these methodologies, quite critical for MANET can bring a rapid change in future.

Chapter VI has performed simulation of "optimized secure protocol for MANET through biometric approach" through NS2 under attack condition for further verification of results.
Simulation results of MATLAB as well as NS2 have justified the importance of proposed methodology. NS2 which is considered as a highly recommended simulator for MANET has been utilized for further verification of the proposed approach. The validation of "optimized secure protocol for MANET through biometric approach" is justified by simulating it under condition of attack (which is very unlikely to occur with a strong crypt-iris based approach), has revealed effective results.

Further verification of the proposed algorithm has also been done in NS2 by considering an attack condition achieving the following results compared with conventional secured AODV approach, with attack level of 5%, simulation time 3000s, number of created packets as 160, 17% increase in packet delivery ratio. With attack level of 10%, simulation time 3000s, number of created packets as 160, 17% increase in packet delivery ratio. With attack level of 15%, simulation time 3000s, number of created packets as 160, 18% increase in packet delivery ratio. With attack level of 20%, simulation time 3000s, number of created packets as 160, 12% increase in packet delivery ratio. With attack level of 25%, simulation time 3000s, number of created packets as 160, 13% increase in packet delivery ratio. With attack level of 30%, simulation time 3000s, number of created packets as 160, 11.4% increase in packet delivery ratio.

Under condition of attack delay is decreased conventionally as the malicious nodes do not send RREQ and RREP packets but in the proposed methodology, with attack level of 5%, simulation time 3000s, number of created packets as 160, an increase in average delay with 0.78. With attack level of 10%, simulation time 3000s, number of created packets as 160, an increase in average delay with 0.66. With attack level of 15%, simulation time 3000s, number of created packets as 160, an increase in average delay with 0.9. With attack level of 20%, simulation time 3000s, number of created packets as 160, an increase in average delay with 0.3. With attack level of 25%, simulation time 3000s, number of created packets as 160, an increase in average delay with 1.1. With attack level of 30%, simulation time 3000s, number of created packets as 160, an increase in average delay with 1.33, which signifies that the proposed methodology is very less affected by the attack condition.

With attack level of 5%, simulation time 3000s, number of created packets as 160, an 18% reduction in average jitter value. With attack level of 10%, simulation time 3000s, number of created packets as 160, 12% reduction in average jitter value. With attack level of 15%, simulation time 3000s, number of created packets as 160, 15% reduction in average jitter value. With attack level of 20%, simulation time 3000s, number of created packets as 160, 7% reduction in average jitter value. With attack level of 25%, simulation time 3000s,
number of created packets as 160, 15% reduction in average jitter value. With attack level of 30%, simulation time 3000s, number of created packets as 160, 12% reduction in average jitter value.

Hence, it has been stated that with number of nodes as the comparison parameter, when attack level is increased average delay and jitter of the proposed approach has been maintained. Delivery ratio of the proposed approach has also been maintained with increase in attack level which does not affect the data transmission along the network. Similarly, even when attack level is increased, throughput of the proposed approach does not falls down too heavily. Therefore, it can be specified that security of the proposed methodology is quite effective from the conventional secured approach of mobile ad-hoc networks as various QOS parameters like delivery ratio, average delay, jitter and average throughput are maintained to provide an enhanced security solution for MANET.

Simulation results and comparative analysis in respect of hamming code, normalized correlation coefficient, specificity and sensitivity tests, average end-to-end delay, average packet delivery ratio, average hop count, throughput, jitter and average packet drop rate for “optimized secure protocol for MANET through biometric approach” have been illustrated as the contributions of the proposed approach in terms of security and QOS for MANET:

**The main contributions of the research work are described below:**

1. Various simulation results have revealed notable design and application of a novel "crypt-iris based perception and authentication approach" to protract security in mobile ad-hoc networks. Unlike other conventional eye recognition mechanisms the proposed methodology exploits two matching criterion and since, normalization is perfectly done and encoding is performed through bi-orthogonal wavelets it achieves ideal matching conditions; **Minimum Hamming Distance=0 and Maximum Normalized Correlation Coefficient=1.** Various security goals of MANET namely **authentication, confidentiality, integrity** and **non-repudiation** have been achieved by the proposed methodology. Also, occurrence of various active and passive attacks has been limited in MANET being secured by the proposed approach. Hence, the neotric iris recognition approach provides enhanced security solution for MANET.

2. Finding best fit shortest path between the source and destination and optimization of QOS has been achieved in this proposed methodology by utilizing genetic algorithm. Simulation results have verified that the genetic stowed approach optimizes the various QOS parameters like average packet delivery ratio, average packet drop rate, average end-to-end delay and average hop count.
3. Effectiveness of the "iris perception approach" is stated by further verifying it with various specificity and sensitivity tests that reveal a flexible simulation environment of the biometric system. Even, varying of the iris classes as well as images per class, provides effective values for various specificity and sensitivity parameters like TPR=nearly 100%, TNR=nearly 100%, FPR=nearly 0%, Accuracy=100%, Recall=100% and F-Measure= Nearly 100%.

4. Similarly, the simulation analysis has compared the conventional shortest path selection approach and the genetic stowed approach against various parameters achieving, 36% reduction in average packet drop rate, 37% increase in average packet delivery ratio, 11% reduction in average end-to-end delay, reduction in average hop count from 2.3 to 1 hence, resulting in low packet drop rate, high packet delivery ratio, lower end-to-end delay and lower hop counts. Even with increase in the number of nodes, simulation time and various other parameters, results have not been deteriorated. The results of simulation have revealed the importance and effectiveness of the "optimized secure protocol for MANET through biometric approach" and have described how the combination of security and QOS methodologies, quite critical for MANET can bring a rapid change in future.

5. The importance of the "optimized secure protocol for MANET through biometric approach" has been determined by simulating it under condition of attack through NS2, which has revealed effective results. With attack level of 30%, simulation time 3000s, number of created packets as 160, 11.4% increase in packet delivery ratio, increase in delay value by 1.33, 12% reduction in average jitter value hence, when attack level is increased average delay and jitter of the proposed approach have been maintained, delivery ratio has also been maintained and throughput also doesn't drop off too heavily. Therefore, it has been stated that the proposed methodology is quite effective from the conventional approaches of mobile ad-hoc networks as various parameters like delivery ratio, average delay, jitter and average throughput are maintained to provide an enhanced security and QOS solution for MANET.

All the performance factors namely hamming code, normalized correlation coefficient, specificity and sensitivity tests, average end-to-end delay, average packet delivery ratio, average hop count, throughput, jitter and average packet drop rate have been optimized by proposed secure routing protocol for MANET through biometric approach both by MATLAB and NS2 simulators. This novel iris perception algorithm approach has been applied on various iris images from standardised database (Chinese Academy of Sciences – Institute of Automation-CASIA, Lion’s Eye Institute-LEI) and other databases too for providing enhanced security solution for MANET. Optimization of conventional routing algorithm of
MANET has been done through genetic based meta-heuristics approach which resulted in enhanced QOS parameters. Thus, the "optimized secure protocol for MANET through biometric approach", has enhanced the critical parameters i.e. security and QOS, which are quite essential for better performance of MANET.

In this thesis, performance of MANET has been enhanced through efficient "crypt-iris based perception and authentication approach" along-with "optimized genetic stowed approach to potent QOS in MANET", together referred as "optimized secure protocol for MANET through biometric approach". The proposed methodology not only doubly secures the network through crypt-biometric approach but has also optimized various QOS parameters through meta-heuristic algorithm hence, improving performance of MANET. Simulation of "optimized secure protocol for MANET through biometric approach" has been done through MATLAB and results are validated by various performance parameters. Simulation results obtained through MATLAB have revealed the effectiveness of the proposed methodology in terms of security and QOS for MANET. The proposed methodology has been further verified through NS2 simulator considering the condition of attack. Simulation results of both the simulators have justified the proposed methodology as an enhanced security and QOS solution for MANET.

7.3 SCOPE FOR FUTURE WORK

The novel "optimized secure protocol for MANET through biometric approach" enhances security and QOS, which are critical parameters for performance enrichment of MANET. The proposed approach is simulated in MATLAB and results are further verified through NS2 simulator under condition of attack which justifies the importance of the proposed methodology. Following future domains of research can be considered for the proposed "optimized secure protocol for MANET through biometric approach":

● For better recognition rates, the database of the iris perception methodology could be enlarged by increasing number of classes and images per classes.
● For real-time iris recognition system interface, an iris acquisition camera will be required as depicted in figure 7.1. The frame grabber could be utilized for capturing number of real time images rather than having a fixed set of iris images from a database. Then templates for each individual, one for the left eye and one for the right eye can be created, where an individual will be accepted only if both eyes match to the corresponding templates that will be stored in
the database. The rate of recognition produced for these types of optimizations need to be balanced with the increased imaging difficulty and the inconvenience to the user.

Figure 7.1 Image Acquisition Using an LG2200 Camera

- For performance improvement of the proposed methodology, some minor delay caused by implementation of meta-heuristics based genetic approach may also be looked upon and necessary measures could be adopted for reducing it.
- For further investigations, a comparative analysis can be performed by utilizing other optimization algorithms like neural network with artificial intelligence, simulated annealing, tabu-search, ant colony optimization and evolutionary computation.