CHAPTER 9
CONCLUSION AND FURTHER SCOPE OF RESEARCH

A MANET is an autonomous collection of distributed mobile nodes. Every node in a MANET works as a source and a sink, and also relays packets for other nodes. The MANETs comprises the following key features such as dynamic network topology, distributed network nature, multi-hop communication, limited bandwidth, limited energy constraints and vulnerability to malicious attacks. In order to support QoS in MANETs, the network is expected to guarantee for QoS parameters such as delay, delay variance (jitter), bandwidth and packet delivery rate, etc. To provide a support for QoS parameters and foolproof security protocol for ad hoc routing is a very challenging task due its unique characteristics. In this thesis, we have applied soft security (Trust) and hard security (cryptography) approach to design a Secure and QoS Enabled Communication Support for soft real-time application services. Our research work embeds security concepts that can prevent MANET QoS mechanisms from being tampered by malicious adversaries.

9.1 CONCLUSION
This thesis focus on various key issues of MANETs such as impact of scalability on different category of routing protocols to provide QoS-aware routing support, handling of cache coherence problem that arises in routing protocols due to mobility and performance analysis of routing protocols to provide VOIP support over Hybrid MANETs. Our research work also contributes towards providing trust conscious secure route data communication support and QoS in term of bandwidth, security for soft real time processing services.

The impact of scalability on various QoS parameters have been analyzed by varying number of nodes, packet size, time interval between packets and mobility rates in Chapter 4. As observed from overall results and discussion on different scenarios, the AODV protocol is QoS-aware routing protocol under the impact of scalability. With the increase in network size, the performance of DSR decreases due to increase in packet-header overhead size as data and control packets in DSR typically carry complete route information. At the same time
Chapter 9: Conclusion and Further Scope of Research

the performance of DSDV is not affected by under such parameters and its overall performance is less than AODV and DSR protocol.

Caching is an important part for all on-demand routing protocols for wireless ad hoc networks. Route caches in intermediate mobile node are used to reduce flooding of route requests. In Chapter 5, we have proposed an optimized dynamic cache coherence handling scheme to handle all the stale routes adverse effects such as packet losses, increase in routing overhead, increase in packet delivery latency and degradation of TCP performance that occurred in DSR protocol. The proposed scheme reduces the number of cross-interrogate (XI) signal send to different mobile node caches resulting in the reduction of routing overhead.

A generic searching algorithm based on associative cache memory organizations to speed up the searching of routes destination, if exist, in intermediate mobile node cache with a complexity O(n) (where n is number of bits required to represent the key field) is also proposed.

Multimedia real-time session services, such as voice and videoconferencing with quality of service support is challenging task over Hybrid MANETs. In Chapter 6, we have analyzed various QoS parameters on different routing protocols for the voice transmission using OPNET simulator. As observed from the results OLSR protocol is best performer as compared to all other protocols to provide voice communication support over Hybrid MANETs. The performance of TORA protocol is less than OLSR and AODV protocol, but it is better than DSR protocol. DSR protocol has minimum throughput and maximum end-to-end-delay with highest jitter and all these factors make this protocol not suitable for voice transmission.

Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints and the independent movement of component nodes. Trust also reflects the mutual relationships where a given node behaves in a trustworthy manner and maintains reliable communications only with nodes which are highly trusted. In Chapter 7, we have proposed an approach that is easily scalable to dynamically increase the trust directly or through proxy nodes. Our proposed soft security approach attains confidentiality and authentication during packets forwarding in AODV protocol. Every node establish an optimal trusted path before route the packet towards the destination. The
Chapter 9: Conclusion and Further Scope of Research

The proposed approach is based on symmetric keys that incur minimal additional overhead and preserve the lightweight nature of AODV.

Further on, this thesis concentrates on to provide Quality of Service (QoS) in term of bandwidth, security for soft real time processing services. All QoS routing protocols are intended for operation in a trusted environment in which all nodes are honest and they do not consider the disruptions that can be caused by a malicious attacker sending arbitrary (e.g. forged) routing packets. In Chapter 8, a secure QoS enabled on-demand link-state multipath routing protocol to explore efficient multipath routing and QoS provisioning in term of bandwidth and security is proposed. In ad hoc networks where finding a single path satisfying all QoS requirements is very difficult, the proposed protocol has better call acceptance rate in term of bandwidth. Another benefit of proposed protocol is its ability to provide fault tolerance, load balancing and reduce the route discovery delay. The proposed protocol mitigates several malicious behaviors and robustness under most of routing attacks (e.g. spoofing, node deletion, node insertion, modification, fabrication, routing loops and denial of service attacks), while minimizing the cryptographic computational overhead.

The design of various security schemes and analysis of different protocols for QoS-aware routing presented in this thesis will be an asset in providing security and quality of service for ad hoc networks. The present work will be of great application to provide secure and QoS enabled communication support for soft real-time applications.

9.2 FURTHER SCOPE OF RESEARCH

This thesis improves the understanding of ad hoc networks and advances the state-of the art through its contributions. Its investigation has revealed areas in ad hoc network where much work remains to be done. Some possible future directions are identified in this thesis and are presented as:

The work presented in this thesis has only explored the impact of scalability for QoS-aware routing on reactive and proactive protocols. The impact of scalability on QoS parameters for other category of protocols such as multicasting and hybrid is also of great concern. A simulation based performance study will be conducted to evaluate the proposed dynamic coherence check scheme in terms of cache hit ratio and average query latency by it with other caching strategies.
Chapter 9: Conclusion and Further Scope of Research

The research work ‘VoIP over Hybrid MANETs’ will be extended to provide the support for video conferencing and real time remote surveillance system. The SIP infrastructure used in our research work requires centralized proxies and registrar server. The further work is to analyze the performance of routing protocols for voice transmission support using decentralized SIP architecture.

The work presented in this thesis dynamically increases the trust directly or through proxy nodes. In further work, in order to make sure that the node does not perform misbehavior, we will add the mechanism that computes the direct trust of a node. The accuracy and sincerity of the immediate neighboring nodes is measured by observing their contribution to the packet forwarding so that no node perform selfishness during data transfer from sender to receiver node.

Wireless networks could be highly heterogeneous. The heterogeneity could be in terms of the roles of the nodes, their inherent capability and security. Heterogeneity implies that not all nodes or their contents can be treated equally when it comes to trust evaluations. Thus, there is need to incorporate a layer wise trust evaluation function, when investigating the trust of heterogeneous nodes.

Further on, we will evaluate the performance of our proposed model of secure QoS enabled on-demand link-state multipath protocol in real world scenario. Beside this, in future, we will incorporate route break prediction in our proposed QoS-aware routing protocol. A route break prediction scheme could aid in the quick response of the protocol to route breaks.

In this thesis, we have concentrated on network layer solutions to provide QoS-aware routing. A further trend that we have observed is that many researchers place great emphasis on the session admission (QoS route finding) capability of their protocol. In contrast, they often neglect or downplay the importance of session completion i.e. maintaining the routes and the QoS for as long as an application data session requires. However, more work on the evaluation of QoS-sensitive session completion performance with realistic application layers, would be useful.

Another major challenge while incorporating QoS in MANETs is the unreliable wireless channel. However, we have found that the majority of QoS routing protocol evaluation studies assume a perfect physical channel, ignoring the effects of shadowing and multipath
Chapter 9: Conclusion and Further Scope of Research

fading. Therefore, studying the impact of a more realistic physical layer model on QoS routing protocol performance is another interesting area of future work.

Accurate studies are required on different types of heuristic algorithms for calculating near-optimal paths with multiple QoS constraints. Comparative studies on the performance and impact of the heuristics are additional future work.

Further on, to foil the internal attacks and selfish behavior, we will incorporate another security tool such as Intrusion Detection System (IDS) with QoS-aware routing protocols and analyze them in real word environments.