"Overall_Thesis - Copy.doc"

**Top sources of plagiarism:**

- % 0.2 Words # 87
- % 0.1 Words # 48
- % 0.1 Words # 27
  - http://www.slideshare.net/ENGMSHARI/adhoc-networks

**Top referenced sources:**

124 - Ok / 22 - Failed

**Important notes:**

- Wikipedia: [not detected]
- Google Books: [not detected]
- Ghostwriting services: [not detected]
- Anti-cheating: [not detected]

**Detailed document analysis:**

- **Table of Contents**
  - CHAPTER 1 6
    - 1.1 INTRODUCTION 6
    - 1.2 INTRODUCTION 7
    - 1.3 BACKGROUND OF STUDY 9
  - 1.3.1 Basic Principle of MANET 10
  - 1.3.2 Routing Protocols in MANET 14
  - 1.3.3 Application in MANET 17
  - 1.4 SECURITY ISSUES IN MANET 19
  - 1.5 MOTIVATION 21
  - 1.6 PROBLEM STATEMENT 23
  - 1.7 RESEARCH AIM AND OBJECTIVES 24
  - 1.8 RESEARCH METHODOLOGY 25
  - 1.9 THESIS ORGANIZATION 28
- CHAPTER 2 31
  - LITERATURE SURVEY 31
  - 2.1 INTRODUCTION 31
  - 2.1.1 Studies towards Routing Protocols of MANET 32
  - 2.1.2 Existing Methodologies for Secure Routing on MANET 42
  - 2.2 RESEARCH GAP 59
  - 2.3 SUMMARY 61
- CHAPTER 3 62
  - SECURE ROUTING IN MOBILE AD-HOC NETWORK 62
  - 3.1 INTRODUCTION 62
  - 3.2 EXISTING ROUTING PROTOCOLS IN MANET 66
  - 3.2.1.1 Table Driven routing Protocols or Pro-Active. 67
  - 3.2.1.2 Reactive (On Demand) routing Protocols 69
  - 3.2.2 Hybrid Routing Protocols 72
  - 3.2.3 Hierarchical Routing Protocols 73
  - 3.2.4 Geographical Routing Protocols 74
  - 3.3 ISSUES IN ROUTING PROTOCOLS OF MANET 76
  - 3.3.1 Scalability 77
  - 3.3.2 Quality of Service (QoS) 78
  - 3.3.3 Energy Conservation 78
  - 3.3.4 Security Issues 79
  - 3.3.5 Authentication Problems in MANET 90
  - 3.3.6 Malicious Behaviour of Nodes 92
  - 3.3.6.1 Security Solution to Defend Malicious Behaviour 96
  - 3.4 SUMMARY 99
- CHAPTER 4 100
  - TECHNIQUES FOR NODE-TO-NODE AUTHENTICATION 100
  - 4.1 INTRODUCTION 100
CHAPTER 1
INTRODUCTION

1.1 PREAMBLE

This chapter discusses about the preliminary information of the Mobile Adhoc Network (MANET), where the significance is laid on the persistent issues in the area of MANET. Out of various problems existing in MANET, the proposed study particularly focuses on the potential security threats unexplored in prior studies. A research work has been carried out to mitigate the security issues in MANET, which is the core goal of illustration in this thesis. Hence, the primary objective of this chapter is to create the reader understands about the domain of the research, the inherent characteristics and security issues in performing communication process in MANET. This chapter also discusses about the problems being identified in this study, motivational factors for the proposed study followed by aims and objectives. Finally, the chapter discusses about the thesis organization to give a blue-print of thesis formations.

1.2 INTRODUCTION

With the emergence of the wireless technology as well as mobile computing, there is a greater extent of demands of wireless adhoc network in the area of computer communication. In this regards, it has been seen that Mobile Adhoc Network (MANET) has been under constant source of attention among the global researchers in past two decades [1]. Till date, there are some notable enhancements in MANET in various aspects; however, some of the issues associated with the communication process in MANET still remain unsolved. This section will thereby introduce the primary domain of research and will elaborate the readers about its fundamental principle of operation, its issues, and proposed system to circumvent such issues [2]. MANET consists of set of nodes where the nodes can be any form of computing devices e.g. laptops, smart phones, PDA, tablets etc [3]. The basic structure of the MANET is exhibited in Fig.1.1.[pic]

"Figure 1.1 Basic Structure of MANET" From the Fig.1.1, it can be seen that MANET consists of mobile nodes that are connected to each other using a wireless medium. The mobile nodes perform arbitrary movement and therefore give rise to dynamic topology in MANET [4]. The mobile nodes formulate self peer-to-peer communication and hence there are no centralized resources to control the communication process in MANET. This feature of MANET permits seamless communication as well as it also invites various Quality-of-Service (QoS) issues as well as security issues [5]. For more illustration of these facts, the "Sub-Section *2.1.1" will elaborate various existing studies and implementation techniques, *Section 2.2* to demonstrate the research gap and flaws associated with the different existing techniques.

1.3 BACKGROUND OF STUDY

In the existing wireless networking principle, the usage of mobile networks as well as cellular technology assist multiple mobile users to get connected. However, such technology renders the services using infrastructure, which is expensive in nature. Such limitations are overcome by adopting MANET [6]. In MANET, the mobile node does communication with each other without any aid of any infrastructure and therefore, it can be said that all the mobile nodes acts as routers. The evolution of MANET is not recent and its evolution history dates back to 1972 where the re-known institution named DARPA (Defense Advanced Research Projects Agency) has started working on PRNET (Packet Radio Networking) giving rise to SURAN Project (Survivable Adaptive Radio Network) [7]. Such projects were basically inspired from radio packet switching process. Soon after 1972, micro-electronic technology was found to take a quick pace resulting in successful integration of nodes with networking protocols called as /adhoc/ /nodes/ for first time in history. Various researchers have also investigated the possibility of incorporating flexibility and independence from infrastructure. Soon, some significant applications has been evolved that were adopted in military applications e.g. Global Mobile Information System (GloMo) [8].

However, the faster pace of the investigation took place in 1980. Various researchers were found to participate in the investigation process and successfully they came up with some significant policies to enhance the performance of MANET [9]. Such advancement in research also extended the MANET applications from military to wearable computer network, defence satellite network, etc. Various partners e.g. IETF (Internet Engineering Task Force) and Working Group of MANET has highly assisted to boost up the technology to support various challenging application in most adverse environment. However, majority of the problems and issues are set up to be originated from routing protocols in MANET [10].

1.3.1 Basic Principle of MANET

The technology and working principle supported by MANET gives higher range...
of flexibility and potential networking principles to perform communication among the mobile nodes in most adverse condition [11]. MANET principle supports node with self-organizing capabilities that assist them to dynamically organize them with each other for furnishing the required network operationality in the infrastructure less communication environment. Therefore, it can be said that MANET supports multi-hopping networking principle considering adhoc network as the core block. An elaborated understanding of the classification of the wireless network says that it is mainly classified into two type e.g. i) static adhoc network and ii) mobile adhoc network. In static adhoc network, the mobile nodes could be highly portable in size and thereby static in nature. In mobile adhoc network, the nodes are always in mobility with unequal velocity with respect to each other. Such forms of network can also make themselves functional by incorporating large scale network. All the nodes in MANET operate from a limited availability of channel capacity (or bandwidth) in presence of time-varying network topology. Essentially, MANET is classified into i) VANET (Vehicular Adhoc Network), ii) Intelligent VANET, and iii) i-MANET (Internet-based MANET) [12]. There are various set of application in MANET that ranges from static to small scale network constrained by energy, mobility factor and extreme dynamics in the networks.

The design principle of MANET routing protocols thereby encounters various significant challenges. The prime and critical requirements of MANET applications calls for an effective link scheduling, techniques to identify network organization, and routing protocols [13]. The traditional routing protocols are not applicable in MANET owing to the challenges in its dynamic network topologies. Hence, there is a requirement for an effective routing protocol that can sustain such challenges in MANET. In this regards, it was seen that majority of the existing routing protocols in MANET works in shortest path principle. Although such principle works out very effectively in small scale and static network, but they are again not directly applicable in large scale routing in MANET. Various factors responsible for such issues originates from basic working principle of MANET networks itself e.g. loss of transmission path, variable quality of link, higher energy drainage, interference, and obviously dynamic topology [14]. Hence, summarizing the essential principles of MANET can be enlisted as following:

1. Limited Bandwidth*: In MANET, the mobile nodes play multiple role at same time. For an example, one node can act as source node, destination node, and intermediate node at same time. Hence redciring all communication channel based on direction of communication will also require sufficient support of bandwidth. As the links may be symmetric or asymmetric with presence of noise in presence to time varying network topology so there is a higher consumption of bandwidth even to maintain normal communication process [15].

2. Dynamic Topology*: In MANET, all the mobile nodes are free to move at any part. They may able to go in or go out in a specified direction from transmission area of other nodes without any prior indications. Till date there is no such technique to determine the next possible position of the mobile nodes. Hence, this dynamic mobility characteristic of MANET occasionally gives rise to intermittent link breakage and finally results in substantial overhead on the routing protocols. It is also one of the reason to all the problems in MANET, be it QoS or security [16].

3. Limited Energy*: In MANET, the mobile nodes are backed up by external battery as the source of power supply. A MANET nodes significant depletes energy even the nodes are not transmitting any data packet. A required amount of control messages are always required to be exchanged among the nodes to ensure that all the nodes are in listening mode. Hence, the energy consumption is more in MANET nodes. With the declination of residual energy, the performance of routing and processing the data degrades resulting in security issues as well as link breakage too. After dynamic topology, characteristics of limited energy are also another significant issue in MANET [17].

4. Limited Security Features*: Owing to decentralized nature of MANET, it is near to impossible for one mobile node to get authenticated with other one. However, there exists various security algorithms which ensure so, but none of them provides fail-proof security [18].

1.3.2 Routing Protocols in MANET*

The prime purpose of routing protocol in MANET is to generate a set of rule that can understand the existing environment and routing requirements of the mobile nodes and can generate a policy to perform error-free transmission of control message and data packet with less attempts of re-transmission mechanism. However, such objectives are very hard to realize in MANET owing to inherent characteristics of dynamic topology. Primarily, there are 13 different kinds of routing protocols in MANET found in the literatures e.g. i) (DSDV) ii) Global State Routing (GSR), iii) (CGSR) iv) Chain Gateway Switching Routing"
Although there exists various routing protocols, still the routing protocols need to be critically analyzed with respect to MANET. Hence, some of the factors that impact the performance of the routing protocols in MANET are as follows:

* Bandwidth Efficiency*: Bandwidth plays a significant role in ensuring an effective data delivery in MANET. As the bandwidth comes under restricted resources in MANET, so the routing protocols must ensure that they support optimal data delivery in the available bandwidth itself [20].

* Support of Distributed Network*: The architecture of MANET is basically highly distributive in nature. Hence the routing protocol should be equally applicable to all the mobiles present in the environment considering the distributed need [21].

* Supportability of On-Demand Routing*: The on-demand routing protocols should target to identify the most utilized and less utilized links in order to ensure the effectiveness of on-demand routing protocols like AODV. This could significantly reduce congestion too [22].

* Supportability of Proactive Routing*: The proactive routing protocols must check the adequacy of the network resources for the speeding up the table-driven approach. This can significant enhance the data delivery [23].

* Ensuring Optimal Security*: Owing to decentralized nature of MANET, it is essential that routing protocols must ensure optimal security by identifying the forms of malicious activities in MANET [24].

* Energy Efficiency*: Owing to dynamic topology in MANET, the routing protocol must ensure that it considerable preserves significant amount of residual energy of the mobile nodes without affecting the performance of it [25].

* Supportability of Heterogeneity*: MANET consists of different nodes of different hardware characteristics. Hence, the routing principle should ensure that it supports the data delivery with optimal communication performance on multiple hardware devices even in dynamic topology [26].

*1.3.3 Application in MANET*

The application of MANET varies to case to case, however, it bears the similarity in this respect that wherever there is a need for faster data transmission in adverse condition without much support of infrastructure, MANET can be used. Following are the applications of MANET:

* Defense and Military Applications*: At present, MANET is deployed in various tactical operations in defense and military. The usage of Unmanned Aerial System (UAS) on battlefield, cognitive radio, software defined radio, smart antenna techniques are integrated with MANET system to track the opponent's strategy of defence [27].

* Rescue Operation*: Various types of geographic region afflicted by natural calamities can be monitored and tracked using MANET system. It is also possible to know the location of the victim and thereby provide necessary rescue support [28].

* Free internet connectivity*: There exist various selection schemes of gateway in MANET to support free internet connectivity. Using adhoc network, it is now highly possible to access internet without any direct connectivity of internet in the mobile nodes [29].

Other increasingly growing applications of MANET are highlighted in Table 1.1.

<table>
<thead>
<tr>
<th>No.</th>
<th>Applications</th>
<th>Services rendered in MANET</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fire Support</td>
<td>Healthcare</td>
</tr>
</tbody>
</table>
In mobile adhoc network, all the mobile nodes are free to move in any direction and perform self-organizing networks. This fact will mean that mobile nodes are usually assumed that all the other mobile nodes will perform cooperation in forwarding the data packet to the destination node. Unfortunately, owing to the decentralized nature of the MANET, it is actually not possible for a node to purely authenticate another node in the process of communication. Moreover, at present there is no standard and fail-proof algorithm or technique to ensure participation of the mobile node. In the existing system, trust and altruism is the only policy adopted by the nodes to perform communication. Hence, this is the potential loopholes in terms of security and gives rise to all sorts of security breaches [30].

There are essentially two types of attacks in MANET e.g. i) internal attack and ii) external attack. In internal attack, the attackers usually performs various malicious activities (like eavesdropping) to gain an illegitimate access to the regular mobile nodes. Similarly, in external attack, the attackers perform such a malicious activity that causes traffic jamming or corrupt the node that furnishes the services. The attacks are again categorized into two type’s e.g. i) active attack and ii) passive attack. Active attack is an intentional type of attack, where the attack too bears some cost of energy and resources of their own to generate an attack. Passive attack is unintentional that is causes due to absence of node cooperation in MANET. Some of the significant types of attacks in MANET are Sybil attack, wormhole attack, black hole attack, sink hole attack, byzantine attack, detouring attack etc.

It was also studied in various literatures that security breaches have different patterns, where the various mitigation techniques were already discussed till date. But the biggest issues with all the mitigation principles are they are symptomatic in nature. The term/symptomatic/ will mean the security algorithm safeguards against certain type of attack but it overlooks the performance of the MANET system. Hence, it is required to understand that security in MANET is still in infancy stage, which requires significant investigations towards fail-proof authentication principle as well as understanding the pattern of attacks.

*1.5 MOTIVATION* 

There are several sources of motivation to carry out the work in the direction of security of MANET. Following are some of the concrete points that have acted as motivating factors:

*1. Cost-Effective Futuristic Applications in MANET*: The futuristic applications of the mobile adhoc network calls for integrating various other networking applications too. Some of the upcoming applications where MANET will be integrated will be cloud application, optical network, multi-carrier networking principles like OFDM, etc. Hence, such applications will provide cost effective communication support to the mobile users. As such forms of reconﬁgurable network also have massive technical complexities, hence, it is expected that ensuring optimal security will be utmost challenging task till date. Therefore, there should be enough investigations leading to generation of cost-effective solutions towards enhancing the secure communication in MANET [31].

*2. Standard and Consisted Research Attempts:* The security issues in MANET are being researched from past 20 years and yet no established security protocols exist till date that can withstand majority of the lethal threats in MANET. Although the existing research-frameworks can act as a good guidelines to carry out the future work, but still there is a need of better benchmarked techniques to solve security issues in routing protocols in MANET. Hence, a research in this direction towards formulating benchmarked security principle can ease off the complexity in this field to a significant extent [32].

*3. Unsolved Issues:* There are various security issues in MANET that are yet unsolved e.g. i) majority of the security protocols are resistive towards a specific types of attacks, where other forms of attacks cannot be mitigated using the same algorithm, ii) majority of the studies are focused towards detection and prevention principle considering the established patterns of attacks, iii) not much work is carried out to understand the patterns of attack or scrutinize the dynamic behavior of malicious node. Moreover, there are less studies towards association of energy factor from malicious node viewpoint. Hence, there are various unsolved areas, which require significant attention, while carrying out the work towards mitigating security breaches or strengthening routing protocols in MANET [33].

*4. Ignored Area:* Applicability of non-cryptographic method to control security threats is one of the highly ignored area in MANET for ensuring security. Although there are few studies done on authentication system in MANET, but studies towards authentication...
node using another node doesn't exist to large extent. Usage of strategic decision making principle and mathematical modelling to understand the dynamic patterns of intruder is another significant ignored area. Hence, such areas should be testified to check how far it is applicable in MANET and till what extent it can provide robust security in routing policies in MANET [54].

1.6 PROBLEM STATEMENT

The proposed study considers the security problems associated with the routing protocols in MANET by identifying the facts that i) it is critically challenging task to ensure robust authentication policy to validate the nodes in dynamic and large scale environment. and ii) there is a need of mathematical modelling to review the patterns of attacking strategy in MANET. The problem statement associated with the proposed study is: "It is a computational challenging task to design a technique that can support highly resilient node-to-node authentication/system and mechanizes a mathematical modelling to discretize the malicious behavior to optimally resisting the most lethal attacks in MANET."

1.7 RESEARCH AIM AND OBJECTIVES

The primary aim of the proposed study is to design a robust and highly resilient technique for ensuring security of routing protocol in MANET. The secondary aim of the proposed study is to frame a mathematical model that can review the most challenging behavior of the lethal threat in MANET and thereby propose a solution to resist it. In order to carry out the above research aim, following objectives are set:
- To perform an in-depth investigation of the existing literature towards security incorporations in routing protocols in MANET and extract research gap.
- To analyze and propose a fair secure routing model by designing Node-to-Node Authentication mechanism.
- To design a strategic model for understanding node misbehavior using Surveillance of Malicious Behavior Pattern (SMBP) approach.
- To analyze and develop the security aspects of the SMBP algorithm and improve its efficiency.

1.8 RESEARCH METHODOLOGY

In this research proposal, the prime focus is laid on the security threats and challenges in MANET. There are two main parts of it, in the first part the study focuses on different security aspects and how these issues to be resolved? In the second part, the study will go for an implementation of MANET network in programming tools where, a MANET network is developed with different routing protocols and compared results with respect to various performance parameters in order to develop a better understanding of routing protocols with respect to different network situations. Second a MANET network is developed with an intruder and discussed an integrity aspect in the network. Finally a scenario is developed about information security. The proposed study has adopted the principal of constructive research that develops solutions to a problem. Here we will divide our work into two models theoretical model and simulation model. In the theoretical model we will study different security issues and their solutions. In the simulation model we will run simulation with MANET configuration and try to learn mechanisms which will help us to enforce security in Mobile Ad Hoc Networks.

*Figure 1.2 Schema of Adopted Research Methodology*

Fig.1.2 represents the adopted research methodology that can be visualized into two categories e.g. i) Node-to-Node Authentication mechanism and ii) Design of SMBP Framework. Fig1.2 shows the architecture formulated to design the proposed system. A closer look into the architecture shows that it is designed using three main blocks e.g. i) block for mapping MANET network, ii) block for implementing node-to-node authentication policy, and iii) block to study the pattern of malicious nodes. The design details of the blocks are as follows:
- **Block-1**: This is the preliminary design where the problems being formulated for insecure routing in MANET plays a critical role in design process. The design considers few initial parameters of nodes e.g. radio range, configuring and checking the availability of neighbor nodes, configuring the dimension of network, and key-design in cryptography. The mobility model used is RMM (random mobility model). The design in this part also considers various secure attributes of key management along with generation of control messages and architecture to support secure routing system.
- **Block-2**: This is the first core design that is responsible for performing node-to-node authentication mechanism. In this process, the system takes into account the routing history and proposes an algorithm to ensure privacy and confidentiality in the secure routing process using cryptography. The design also supports significant key-agreement process as well as designing of control message as per the authentication requirements. This block ensures the secure authentication scheme even in large scale network.
- **Block-3**: This block is the most critical part of design implementation of the proposed study that introduces a novel mathematical modelling using strategic decision making principle called as mechanism design. This part of the study completely focuses on understanding all sorts of attacking strategy possibly chalked out by the malicious node and attempts to differentiate malicious node from regular nodes as it is quite problematic for understanding the difference between malicious and regular nodes in many cases. The design principle considers that malicious nodes will not invoke any attack in preliminary stages in order not to get caught. The malicious node waits for a uncertain and unpredictable favorable time to invoke an attack. This problem is the pivotal point of focus in this part of the study.
The organization of the proposed thesis is as follows:

- **Chapter 1: Introduction**: This is the preliminary chapter of the thesis that mainly discusses about the preamble and background of the study. The chapter also discusses about the motivational factor, problem statement, research aim and objectives along with methodology.

- **Chapter 2: Review of Literature**: This chapter discusses about all the existing techniques, algorithms, and models available in literature that claims to resist security threats in routing protocols in MANET. The chapter illustrates the effectiveness of the work along with explicit discussion of research gap.

- **Chapter 3: Secure Routing in MANET**: This is the theoretical chapter that will elaborate the researchers about the significant issues and problems of security breaches in routing protocols of MANET.

- **Chapter 4: Technique for Node-to-Node Authentication**: This chapter will introduce a technique that formulates highly secure authentication policy in large scale MANET. The chapter will also discuss the particular problems being addressed, proposed model, projected methodology, and accomplished outcomes.

- **Chapter 5: Surveillance of Malicious Behavior Pattern**: This chapter will present a mathematical modeling using mechanism design for the purpose of understanding and reviewing the tactics of intruding strategies for malicious nodes. The chapter will also discuss the particular problems being addressed, proposed model, projected methodology, and accomplished outcomes.

- **Chapter 6: Conclusion**: This is the concluding chapter that will recapitulate the essential findings of the thesis, thesis contribution, scope and limitation, as well as tentative direction of future work.

---

**CHAPTER 2**

**LITERATURE SURVEY**

**2.1 INTRODUCTION**

Study towards secure routing protocols which are present in Mobile Ad hoc network ensures the efficient and secure routing protocol framework development methodologies that has gained extraordinary growth and researched from more than a decade. A MANET is considered as an independent collection of mobile devices that are connected with each other and maintain communication with each other in a cooperative manner over a distributed wireless and infrastructure less network in order to provide necessary network functionality to the dynamic topologies. This proposed survey study provides insight into the various potential and efficient routing protocols of Mobile Ad hoc networks and discusses numerous technical challenges detected by the past protocol designers. These challenges include authentication, integrity, dynamic and challenging environments and some risk factors such as network or overall system overload etc. The proposed study is inclined to investigate the performance analysis of the frequently used development methodologies of the secure routing protocols which are designed to mitigate the various communication issues and the malicious attacks associated with the mobile ad hoc network. Therefore this chapter investigates and discusses some of the significant literatures till date related to the safe routing of mobile ad hoc network.

Liu et al [35] investigated the influence from various cryptographic processes which are required for unidentified features. Overload considers both the increased control packet size and prolonged processing delay. Results and performance analysis have been carried out based on extensive simulation study. Comparison has been made in the basis of standard or unprotected on-demand scheme AODV to show the cost efficiency associated with the various anonymous on-demand schemes.

Rai and Singh [36] have found that need of implementation for secure routing protocols are in a scorching question where no general algorithms have found that are suitable against various network attacks for example wormhole, rushing attack etc. Survey has been done to gather the various issues of routing attacks of Mobile Ad-hoc network and solutions.

Jawandhiya et al [37] have described some security attacks which are vulnerable to the network for the lack of trusted centralized authentication issues and limited resources. This paper highlights various
prominent attacks for providing a brief performance analysis on attacks. Shawkat et al [38] presented a comparison analysis which is based on three securing routing protocols of MANET. Discusses various issues related to the data transmission such as malicious threats, attacks and penetrations. Experimental outcomes are highlighted and a set-up has been designed to show that how different types of MANET protocols handle the situation of various dynamic environments according to different scalability factors.

Patwardhan et al [39] discussed and presented about the design and the implementation details of the proposed system and elaborated several scenarios and various secure routing and disturbance detection mechanisms. This paper analyses the issues involved with implementation and deployment of the secure routing protocols. Interesting results are evaluated in this study where some practical considerations for deployment of nodes are there.

In case of MANETS, this area caught the attention of significant researchers for its intrinsic capabilities of instant communication. The study of Mamatha and Sharma [40] analysed the various issues, environment variations, some of the implementation and protocol issues which are connected with the MANET environment.

Farid and Prahladachar [41] deliberated the traditional AODV routing protocol and various security issues which are connected to this routing scheme. A survey of various security approaches has been done in order to secure the AODV in a mobile Ad hoc network. The experimental comparisons and the investigation approaches are performed to determine the performance metrics of the secure version of AODV and the Traditional AODV.

The performance analysis associated with various routing protocols have been surveyed by Sarkohaki and Shahram [42] where a discussion has been made in the basis of OLSR protocol and the improvements to be done on this protocol. The classification of various routing protocols is also discussed along with various proposed techniques.

Jasim [43] introduced the effect of jammer in MANET where it is also presented that how routing protocols can improve the network performance of a MANET in terms of some parameters. This study discusses about some of the prominent MANET routing protocols such as OLSR (Proactive Routing Protocol), DSR (Reactive Routing Protocol), TORA and GRP (hybrid Routing Protocol), OPNET modeler (v14.5) have been apply for the assessment of the HTTP applications such as (Delay, Throughput, Data dropped, Traffic receiving and send mechanism).

Thamizarasi and Vinoth [44] have discussed about the various existing routing schemes which provides only anonymity and unlink ability. This paper also gives an overview and implementation details about an efficient privacy-preserving routing protocol USOR which can be utilized to achieving content un-observability by employing unidentified key establishment. A route discovery process has been executed for finding the destination node.

Hoebeke et al [45] has done a survey and the conducted study gives an overview of the various advantages of Ad hoc networks and discusses the various technical issues which creates challenges for the protocol designers such as routing, service and resource discovery, internet connectivity, billing and the security.

A thorough study one by Chrysooula et al [46] presents the performance evaluation metrics and comparison of three MANET routing protocols and their real life scenarios.

The recent study of Gagandeep et al [47] focuses on routing protocols and security issues associated with the MANET which provides a secure architecture for secure and reliable communication. The attacks which are against MANET infrastructure are divided into active and passive attacks. This study discusses about some of the vulnerable attacks of MANET.

Sakalley and Kumar [48] discussed about various routing protocols associated with mobile Ad hoc network. Those protocols are considered for three types. This research focuses on the comparative study of various MANET secure routing protocols and mainly gives the overview of unicast routing schemes.

Ramana et al [49] have conducted a survey on the authentication of MANET and the trust based routing where they have discussed about the ways to enhance the security and the robustness of the network. It is also generalized that data authentication is constructed successfully when the import authorization and source authentication are pooled together.

Manupriya [50] analyses the major activities associated with the black hole attack where a malicious node advertise itself by replying the false route packet to the source node and initiate the route discovery process. In this study the Ad hoc on demand vector routing algorithm is applied for the simulation, results and performance metrics are implemented using NS-2 environment.

Parvinder and Suman [51] have done a survey on secure routing protocols
which are present in mobile Ad hoc network where they have analysis various scenarios associated with the Ad hoc networks and provides an overview of vulnerable attacks those have an effect on the performance of the network infrastructure and discovers the security issues which are yet to be analyzed for giving proper solutions, the result analysis of this study helps readers to efficiently minimize the routing attacks. Sharma et al [52] have made a brief survey of most standard protocols which uses the table driven approach. Some security issues of on demand approach are also discussed in the proposed study. The performance metrics give the better resolution to the future researchers to continue and to mitigate the issues associated with the MANET infrastructure.

Wu et al [53] provided a survey of network layer attacks and countermeasures in MANET. The proposed survey study gives an overview various susceptible attacks based on protocols stack and security attributes mechanism. The study represents some defensive techniques which follows the order of the layered protocol stacks. An overview of MANET intrusion detection systems (IDS), which are reactive approaches to thwart attacks and used as a second line of defenses have also been discussed.

Gupta et al [54] have been focused on the routing issues and addressed an introduction to the mobile Ad hoc networks, issues associated with the routing and overview of security mechanism of MANET. Possible solutions to mitigate various types of routing issues and protecting the security mechanisms also have been discussed in this proposed study. The security mechanisms include availability, integrity, authentication and non-repudiation. The study says security issues can be well-addressed if it is possible to design a method which very much relevant mechanism for authentication, key distribution and intrusion detection.

Bhuvana and Ragul [55] evaluated the performance analysis of various MANET protocols especially an intrusion detection system which is used to observe and evaluate the activities of the nodes, and the study determines the performance of various security protocols by security rules. Various security issues and many dynamic topologies have been discussed and security issues are discussed in this paper.

Dasgupta et al [56] focused on the study of various rushing attacks which are implemented by the malicious nodes on the AODV routing protocol, the performance analysis and the simulation graph shows the various issues associated with our previous research works and also demonstrates that the functionality of the AODV protocol stops in presence of any rushing attack.

Sen et al [57] presents some security issues which are specific to the MANET and classified the various attacks/attackers who are against the MANET distributed network. Various proactive reactive solutions have been also discussed in the proposed survey study where an overview of intrusion detection is given.

Rani and Dhir [58] focus on the detailed review of Ad hoc network infrastructure and its protocols and different types of networks in detail. This study introduces the dynamic mobility concept associated with the MANET topology and the behavior of the nodes as in the Mobile Ad hoc network the nodes are moving from one place to another within this moving network any node can join or leave the network. Security and immediate reply of different types of nodes is the main concern of the Mobile Ad hoc network.

Sardar and Majumder [59] have done a survey on different types of trust based secure routing protocols where trust mechanism is used as an alternative of the cryptographic technique, the study also discussed about the benefits of trust mechanisms such as trust mechanism is used for securing the data forwarding by isolating the malicious nodes with their security mechanism.

The study of Raghavendram et al [60] discussed about the current challenges in Mobile ad hoc network. Attacks MANET comprises various types of harmful attacks those have potential to detect the network operation. A literature survey has been done for collecting some important information which are linked with various types of attacks in mobile ad hoc network, the proposed study reach on a conclusion that there is no algorithms that are suitable well in contradiction of the most commonly known attacks. For providing a complete security solution to the MANET environment it is important to develop a framework with prevention, detection and reaction mechanisms. This study gives a comprehensive revision and detail classification of the attacks which are very susceptible against mobile ad hoc networks.

Sangulul and Naveen [61] have done survey on some of the efficient security techniques which are available in the mobile ad hoc network. The Analysis and interpretation of the proposed study says that the SMT scheme generates good outcomes in all aspect as compare to SPREAD and SDMP which only can provide the security solution but creates system and network overhead. It has been analysed by the survey study that sometimes the computationally efficient algorithms are well enough to maintain the confidentiality of the MANET. Restrictions of Limited resources such as processing capacity, limited power capacity and the size require more efficient encryption mechanisms for secure routing of MANET.

*2.1.2 Existing Methodologies for Secure Routing on MANET*

Taneja and Kush [62] proposed a new protocol EESSRP (Energy Efficient, Secure and stable Routing Protocol) to combine various factors like security, power and stable routing as secure and stable routing on MANET is very hazardous tasks due to the highly dynamic environment. An experimental analysis using NS-2.34 has been done for performing some experimentation where packet delivery ratio, average end to end postponement, throughput, normalized routing load and packet loss are
considered as performance parameters.

Abujassar and Ghambari [63] proposed a new algorithm based on DBRT (Destination Sequenced Vector Table) for improving the existing proactive protocols such as DSDV (Distance Vector Routing Protocol) with the help of a backup routing table to give multiple alternative routes. The result analysis shows the new protocol does not reduce the network performance without being affected by overload of the upgradation issues of the new back up routing table.

Haboub and Ouzzif [64] used a security and mobility aware mechanism for improving the "Ad hoc on demand Distance Vector" (AODV) map-reading protocol. The aim of this study is to be protected from the resource exhaustion attack and to change the packet transmission frequency periodically and to have a more consistent network.

Soni and Chandravanshi [65] have presented a newly Intrusion Detection system (IDS) algorithm which is designed to prevent the selfish node attack of "Mobile Ad hoc network". The behavior of selfish nodes includes unnecessary flooding of the data packets over the network and abort all ongoing transmission between the reliable nodes. This study simulated the performance metrics of selfish node attacks in ad hoc networks and represented and evaluated the network performance of different performance metrics.

Papadimitratos and Haas [66] have introduced a novel approach for route discovery technique that optimize the harmful effects of such malicious nodes for providing the correct connectivity of the information. The proposed scheme gives assurance that the fabricated, compromised or re-played route replies would either be vanished or never comes back to the querying nodes.

Lavanya et al [67] proposed an enhanced and secure routing protocol and the performance metrics of this proposed scheme has been compared with the existing Ad hoc on demand vector routing (AODV), Dynamic Source Routing (DSR) and Zone routing Protocols (ZRP) on the basis of delay, jitter and throughput with the use of Qualnet simulation software.

Yavuz et al [68] proposed a new multi-tier adaptive military MANET secure routing protocol which uses the hybrid cryptography and concept of signcryption. This protocol gives innovations to the secure military MANET communication.

Proposed technique implements hybrid key management algorithm for combining the benefits of both decentralized protocols with single point failure resistivity. The proposed network structure provides flexibility for Mobile Backbone Network (MBN) tiers. Karthheesan and Srivastava [69] proposed a distributed certificate authority (DCA) scheme in order to deliver a secure routing and authentication. This study mainly focuses on the data authentication and integrity for MANET. The desired level of security provided by the proposed architecture based on the policy of the user where the execution of corresponding security models has been found.

Vishwakarma and Chopra [70] investigated the use of evolutionary computation algorithms for manufacturing interruption detection programs of MANET. The proposed system includes the knowledge based intrusion detection technique for detecting various malicious attacks of MANET. Experimental results of the proposed algorithm are compared with normal AODV. The experimental results show more efficiency than the existing studies.

Gopinath et al [71] has presented a novel approach which is known as mobility based system for detecting the malicious nodes of the MANET. The proposed system includes execution of trust vector parameters which is extended to the existing DSR. The result analysis of the proposed system gives the better detection efficiency, packet delivery Measurements, low delay and overhead than the existing schemes.

Zhao et al [72] proposed a risk aware response technique for systematically adjustment with the identified routing attacks where the risk aware method includes the concept of extended dempster-shafer mathematical theory of evidence. The result analysis gives the effectiveness of the proposed algorithm with the consideration of Data packet delivery ratio and the routing cost.

Anil and Reddy [73] introduced a study of routing protocols where they have proposed a novel approach for designing a secure Mobile Ad hoc network which alleviates various types of routing attacks. The system recognizes the vulnerability of the routing attacks over MANET. Highly Contrastive results are shown by the performance analysis of the proposed technique which has been compared with the various previous routing algorithms for mitigating the issues.
Zalte and Ghorpade [74] proposed a secure token for mitigating the issues of dynamic topologies which are associated with MANET; the proposed system includes Cryptographic AES algorithm and hashing algorithm SHA2.

Sweetha and Bhupathi [75] have proposed a scheme for minimizing the effect of packet dropping mechanism which is based on the cooperative participation of nodes in MANET. The study offers some resolutions for packet drop attacks and improves the efficiency of the network performance.

Lou et al [76] represents the overview of the system architecture associated with the Mobile Ad hoc network and investigate analyses the major design issues of the MANET infrastructure. The result analysis shows the proposed SPREAD is more reliable as compare to other routing mechanisms which provides some certain security and a certain degree of reliable communication without compromising the security. Simulation results provide the Efficiency of the proposed technique.

Weng [77] presented various security problems of MANET along with the currently proposed techniques and discussed various solutions related to the proposed techniques. Security issues elaborated in this study are routing, Data forwarding, issues connected with key management and intrusion detection systems (IDS).

This study has been conducted by Zhao et al [78] where a Multipath Routing Single Path transmission (MARS) scheme has been proposed which combines the multipath routing and the single path data transmission and end to end feedback technique for providing a complete protection against the misbehavior of malicious nodes. The result analysis shows the proposed scheme deliver more efficiency and better network performance and considerable protection and security against malicious attacks.

Singh et al [79] have done simulation based performance evaluation of the proposed AODV, OLSR and ZRP routing protocols. The discusses about the upgradation techniques of the ZRP protocol where the proposed designed goals are Quick route configuration, route acquisition delay, low mobility scenarios. The study gives a considerable overview of the routing in intra zone.

Marti et al [80] described two techniques for the improvement of throughput put which is present

Plagiarism detected: 0.02% of this document is located in:
http://www.patents.com/us-7310335.h... + 3 more resources!

which the source nodes agrees

to transmit the data packets but they fails. To mitigate this issue the proposed Watchdog and Pathrater techniques are introduced, the simulation results of the proposed techniques with the use of packet through put and percentage of overhead.

Kong and Hong [81] proposed a routing protocol named Anonymous on-demand map-reading protocol for

Quotes detected: 0.01% of this doc is quoted by quote signs:

"mobile Ad hoc network"

which is deployed in the hostile environment; two issues associated with the secure route configuration have been addressed here. The design of ANODR follows a novel security concept which is

Quotes detected: 0.01% of this doc is quoted by quote signs:

"broadcast with trapdoor information"

The study used simulation and performance analysis to validate the effectiveness of the proposed system.

Manikandan et al [82] organized a study where an identification of existent security intimidations in mobile ad hoc networks has been manage in order to achieve the security services to mitigate the vulnerable attacks of the MANET. These studies gather various important information's and focuses on finding the related work for secure direction-finding in MANET.

Nargunam et al [83] proposed a novel cluster based security technique for protecting the Mobile ad hoc network data link layer and the network layer operations of transmitting data packets over the multi hop wireless channel. The proposed cluster technique can manage the network topology efficiently and no overlapping clusters are made by the cluster creation algorithm.

Gong and Bhargava [84] proposed a protocol named NSIPRP which is based on native immunization technique of mobile nodes, the immune reconfiguration techniques are used for protecting the confidential information against the collaborative attacks. The routing performance of the proposed system has been compared with the other existing position based routing algorithms such as the AODP.

Gopinath et al [85] has proposed a reputation mechanism for defending
various routing attacks of MANET. The proposed system has been evaluated with discrete event simulator environment, the simulation results evaluates the performance metrics of the reputation based system which detects the DoS attack and provide better solution for misbehaviour detection efficiency, packet delivery ratio, packet dropping ratio and routing overhead latency.

Kumar et al [86] developed a new algorithm technique called reputation based technique to mitigate various vulnerable attacks of Mobile Ad hoc network, the proposed technique is evaluated with the discrete event simulator environment which shows that the reputation based system detects and isolates the DoS attack and provides better effectiveness and performance efficiency to the MNAET network infrastructure for avoiding various malicious behavior.

Richhariya and Kausik [87] proposed a study of survey where they have elaborated various routing attacks in the network layer according to the study A

"mobile ad hoc network"
is a set of mobile nodes which are wireless and maintains a dynamic topology without any pre-existing infrastructure. Attacks in the MANET are categorized as Passive or Active Attack. Attacks depend on whether the connectivity of the network has been interrupted or not.

Zhao [88] proposed some introduction and background problems which are associated with various routing attacks of Mobile Ad hoc network. Novel solutions are proposed for evaluating the network performance of the proposed system. This study says that the operation of MANET does not depends on the pre-existing infrastructure. Performance evaluation has been done to contrast the issues present in the existing studies.

Rajaram and Palaniswami [89] have developed a trust based security model on a MAC-layer approach which is useful for the confidentiality and the authentication of the data packets which are transmitting over the network both in network and data link layer of MANET. In this survey study a trust based packet forwarding scheme for the detection of the malicious nodes. This packet forwarding scheme can be useful for make a malicious node isolated. A link layer security protocol also has been designed using CBC-X mode of authentication mechanism and encryption mechanism. The result analysis shows that MAC-layer security protocol obtains high packet delivery ratio and delay; overhead can be avoided with the high speed communication.

Kiran N and Kumar [90] present a novel technique which is associated with the process architecture applicable for secure mobile commerce framework where the hybrid mobile ad hoc routing protocols have been entrenched in a real time scenario. The proposed research study addresses the deployment of mobile commerce framework which is a very much emerging trend in mobile Ad hoc network scenario. Majority of the existing system suffers from QoS or the Efficiency of the secure protocols. The real time experimental analysis has been experimented with various hardware's. This proposed study provides various constraints, requirements of security, and concepts which are very much essential for creating a mobile commerce robust application model.

Nasser and Chen [91] have proposed an intrusion detection system to overcome the weakness of the watchdog method and named the proposed system as Ex-watched dog. The main feature of the proposed system is that it has an ability to detect the malicious nodes and then proceeds to protect the network. The performance evaluation and the simulation results presents a graphical representation which shows that the proposed system reduces the overall system overhead and does not increase the throughput.

The proposed study done by Mishra [92] gives the details of proposed Adaptive-SODV algorithm which

http://pluto.ksi.edu/~cych/cis370/eb...

is an extension of the existing AODV protocol which have some filtering strategies to enlarge the effectuality of the network. The performance evaluation of the proposed system has been done and a comparison also has been evaluated with the existing routing protocols using simulation.

Mohamed and Abdullah [93] addressed the issues of MANET which are associated with the security approach based on both immunity and multi-agent paradigm. This study discusses about the immunity based architecture which has been designed for simulating the immune behaviour for making the mobile Ad hoc domain self-detecting, reacting and healing against various malicious attacks.

Hoepner and Gong [94] presented two full working identity-based authentication and key exchange mechanism (IDAKE) for mobile ad-hoc network. The study discusses about pre-shared secret keys and efficient key management for designing MANET-IDAKE protocol which is designed for performing some specific requirements of MANET. The performance metrics of the proposed technique have discussed and the result analysis shows the
Ramya et al. [96] proposed an innovative technique which is called Hybrid Security Protocol, to enhance the strength and stability of the mobile Ad hoc networks. The proposed technique includes integrity, confidentiality and authentication mechanisms for secure and reliable communication of data. The Hybrid Security Protocol adopted the concept of Cryptographic technique based on Elliptic Curve Cryptography Dual-RSA algorithm for verification and MD-5 which is used for integrity. The study gives an overview that the arrangement of symmetric and asymmetric cryptographic techniques provides better security with integrity.

Zhang et al. [97] design a software framework for evaluating and developing secure Mobile Ad hoc network where the design of the software framework includes three major features, where the first one is the environment which is developed on a wireless network simulation tool and supports repeatable experiments. Secondly the framework adds an attack imitation layer with the required APIs for the further development. Third feature includes the extensible attack library which is composed by a full set of basic attacks. The study demonstrates the design of Intrusion Detection System (IDS), and the experimental outcomes greatly simplify the issues associated with MANET environment.

Kong et al. [98] proposed a solution for omnipresent security services for mobile hosts, the design and the implementation of the proposed framework gives an overview of certification authority functionality with threshold secret sharing mechanism. The study employed localized certification scheme for enabling the various omnipresent services. The updating of the secret share services also has been done to enhance the robustness against break-ins of the network. The effectiveness of the proposed framework design has been analysed by graphical simulation and the implementation. The proposed system model has activated to cope up with several scenarios where it can be plugged as value added security services into many networking environments such as cluster based middle ware and storage area network.

Juneja and Misra [99] have proposed a Tropical Intrusion Detection technique for detecting the packet drop attack (PDA) which affects the functionality of AODV MANET routing protocol. The proposed study shows that the performance of the TID security policy increased to gain the overall throughput of the network. The experimental analysis of the proposed mechanism shows the improvement reduction in end to end delay and the routing overhead are 14.0% and 5.5% respectively.

Liu et al. [100] proposed a novel hierarchical and anonymous on-demand routing protocol to increase the routing efficiency of the MANET. In order to guarantee secure routing, packet receiving acknowledgement and for the effectiveness of the network the proposed routing protocol is designed and able to tackle various limitations associated with the MANET.

Sharma et al. [101] proposed a secure routing protocol known as SNAODV (Secure Node AODV) for the prevention of various malicious attacks of MANET. The Result Analysis shows the effectiveness of the proposed protocol, and the proposed protocol maximizes the through put of the overall network as compare to AODV.

Patil et al. [102] proposed a new secure routing protocol which is called as "Enhanced AODV" (E-AODV) which is the extended version of existing AODV protocol. The proposed protocol ensures an enhanced packet delivery ratio over the Mobile ad hoc network also minimizes the end to end packet delivery ratio. The performance analysis provides a quality of service to the overall Mobile ad hoc network environment. The performance analysis and implementation results are shown to evaluate the network performance.

Sahoo et al. [103] proposed a new routing protocol and named it MyRouter, the protocol has been designed using network simulator. Packet release ratio, End to End Delay is considered as a performance parameter for evaluating the effectiveness of the proposed system. Comparison also has been done with MANET routing protocol OLSR on basis of efficiency of the performance.

Jin et al. [104] implemented a secure routing protocol which is known as FLSI (Adaptive Fuzzy Logic based Security Level Routing Protocol) to alleviate various challenges associated with MANET. The simulation and the performance has been carried out by network simulator NS-2. The study also establishes the feasibility of the protocol. Experiment and analysis under various scenarios have been performed and outcomes have been analysed to measure the effectiveness of the proposed methodology. Yadav et al. [105] have presented a fuzzy based decision for checking a node is impure by black hole or not. The identification of the malicious attack over the node have been detected by the proposed technique which provides the solution to reduce the loss of packets in the internet.
"2.2 Research Gap"

After revising so many papers which are included in the proposed study it has been found that most of the existing studies related to secure routing in mobile ad hoc networks which implements and analyses new routing protocols for the prevention of various routing attacks in MANET are repetitive in nature. Better Comparative Analysis with respect to the proposed techniques and various performance parameters are significantly missing. As the comparative analysis with respect to various performance parameters are very much essential for the reader to understand the most efficient techniques till date which assist the reader to continue the further research for mitigating the various issues related to that domain. No significant outcomes could be resulted after reviewing the existing studies where repetitive nature of implementations has been adopted. Few benchmarked studies have been found as majority of the papers highlighted in section 2.1.1 and 2.1.2 are not benchmarked at all. This situation creates a very much challenging environment for the readers to understand the reliability of the various existing studies towards secure routing techniques. As the benchmark studies help the authors for proving under the necessary conditions that their proposed technique and experimental outcomes are superior to someone's work. If those important information are missing from the existing studies then adoption of such work are hardly accepted by the future researchers. It can be seen and reviewed from the existing prior studies that majority of the authors have adopted the performance parameters which are less effective in nature. It is also observed from the various past studies that adoption of Quality of service (QoS) parameters such as energy, bandwidth, jitter, latency are very much less as the possibility of using much effective performance parameters should be presented in the existing studies.

"2.3 Summary"

This chapter discusses about the various proposed techniques which are inclined to investigate the performance analysis of the frequently used development methodologies of the secure routing protocols which are designed to mitigate the various communication issues and the malicious attacks associated with the mobile ad hoc network. The various existing studies and implementation techniques are discussed in the section 2.1.1 and 2.1.2 respectively. Section 2.2 highlights the research gap and flaws associated with the various existing techniques.

"Chapter-3"

Secure Routing in Mobile Ad-Hoc Network

The previous chapter has discussed the prior literatures where various techniques of mitigating security issues were discussed. It was found that various techniques have their own advantageous features towards addressing security issues in performing routing over Mobile Adhoc Network (MANET) as well as there exists a significant pitfalls of majority of the techniques discussed in form of research gap. This chapter will act as a theoretical backbone of the proposed study where core routing policies, their technical issues, and mechanism to resist the adversaries are discussed.

"3.1 Introduction"

"Mobile Ad Hoc Network" (MANET) is considered as a collaboration of various wireless devices or nodes which can be applicable for representing a complex distributed network where the connectivity between various mobile nodes do not require any type of fixed infrastructure. Fig 3.1 illustrates the dynamic nature of wireless mobile nodes where the network topology uses self-organized behavior in node deployment. The network topology of MANET infrastructure includes some essential characteristics of wireless nodes where nodes will have capability of moving rather than staying fixed in a specific location [106].

It is specified that the features of MANET includes many challenges in the real life scenario where many limitations are being imposed in case of network layer protocols. Mobile Ad-hoc networks introduce various challenges as compared to wired network as it is infrastructure less and connected with limited resources. Due to resource constraints it faces various challenges such as error prone broadcast channels, limited bandwidth, hidden and exposed terminal problems, frequent topology changes, power constraint and various security issues. Security issues are one of the most prominent challenges in the section of routing topology of MANET usually more exposed to the possibility of being attacked due to its wireless communication channel and the lack of proper Centralized Authentication mechanism. Security issues in MANET are usually concentrated into two major parts one is establishing secure route and the other one is securely data transmission. So it is important to design an efficient routing algorithm to avoid routing attacks in a communication channel [107].
3.1 Some Advantages of Mobile Ad-hoc network:

- Low cost of deployment: No expensive resources are required for the positioning of wireless nodes.
- Fast and Easy deployment: In MANET, wireless nodes are very easy to place anywhere as no cables are needed for the configuration of nodes and deployment time is also can be shortened.

// Self-Organization // The nodes have self-organizing characteristics where they align themselves to get connected to each other

*Figure 3.1 Overview of Mobile Ad-hoc Network*

3.1.1 Some Advantages of Mobile Ad-hoc network:

// Fast and Easy deployment: In MANET, wireless nodes are very easy to place anywhere as no cables are needed for the configuration of nodes and deployment time is also can be shortened.

// Self-Organization: The nodes have self-organizing characteristics where they align themselves to get connected to each other

*Figure 3.2 protocol stack of Mobile Adhoc Network*

Fig.3.2 highlights the formation of the protocol stack in MANET that essentially includes 5 categories of layers e.g. application, transport layer, network layer, data link layer, and physical layer. The prime discretion in the standard protocol stack and that of MANET is mainly in the network layer. In MANET, mobile nodes are usually considered to act as routers and adopt the standard adhoc based routing technique to perform communication among each other. It is also found that various protocols were found executed on each layer.

*3.2 EXISTING ROUTING PROTOCOLS IN MANET*

Categorization of various routing protocols in MANET can be done in the basis of routing strategy and network structure. The map-reading protocols can be separated into three types of categories such as 1) Flat routing, 2) Hierarchical routing, and 3) Geographic position assisted routing (Fig.3.3).

*Figure 3.3 Classification of routing protocols in MANET*

3.2.1 Flat Routing Protocols

Flat routing protocols are divided mainly into two categories, the first one is proactive and other one is reactive (on demand) routing protocols.

3.2.1.1 Table Driven routing Protocols or Pro-Active.

Pro-active MANET protocols are also called as table driven routing protocols are used in active routing environment in which the time intervals between wireless nodes maintain a table contains the information associated with more paths and every single node will maintain an absolute picture of the network. Each wireless node maintains a route table according to the changes of information which are made by the router. When some changes are made in the network topology, as well as if the original path shows invalid path configuration, in that time if any new path is established and update within the network topology, all the nodes of the "Mobile Ad hoc net work" determination receive the update message on its status path. After continuous updating of the route paths, the routing table of a particular node will be ready and it will be available whenever needed. This protocol results some drawbacks, where it is notice that with the increase of mobility of the nodes, the traffic overhead of the node can be engendered while each node maintains a routing table and evaluates these unnecessary routes. Therefore this excessive amount of energy depletion is not desired so the Proactive protocols with low node mobility do perform best or it is suitable in an environment where the nodes transmit data packets frequently.

Some of the proactive protocols are

- Optimized Link State Routing (OLSR)
- An *
**3.2.1.2 Reactive (On Demand) routing Protocols**

When a wireless node wants to transmit some packets to another wireless node in that time the source node run a route discovery process and call a path and stores the information of the path in a register. The portability of the nodes causes some significant issues of mobility as the mobility of the node is responsible for the constant change of the network topology. It is not easy to track down the topology condition as too many resources are needed and consume so much energy for signaling.

Reactive Route protocols were induced to cope up with this type of environment. These protocols have been designed with the concept where no need to keep up an image of the entire network topology as it is constantly altering, so whenever a node needs to transfer a data packet to its targeted node at that time it will initiate a route discovery process in the fly to find out a pathway. Reactive protocols set up their routes on demand, the reactive or on demand protocols establish a route when a wireless node needs to transmit data to another node to which it does not have any route. This kind of protocols is usually designed with the concept of flooding the system network with Route reply (RERP) and Route Request (RREQ) messages.

**3.2.1.3 On Demand Driven protocols there are various types:**

* AODV - "Ad-hoc On Demand-Distance Vector Routing-Protocol"

The AODV routing protocol obtains routes with the use of reactive or on demand approach, a route is constructed when a node needs to transmit data packet to another node. This protocol uses destination sequence number for packets for identifying the most recently used path.

* DSR - Dynamic Source Routing Protocol"

"Dynamic Source Routing" (DSR) is a routing protocol which is mainly designed for wireless mesh networks. This protocol is similar to AODV and...
finds a route on demand.

* TORA-Temporally Ordered Routing Protocol*

TORA is also a type of Reactive or on demand protocol or algorithm which is used mainly for routing packets data in Ad hoc networks. It is also used to achieve high degree of network ability for handling a rising amount of work in an accomplished manner.

* ABR-Associatively Based routing protocol*

The **Associatively Based Routing** (ABR) protocol is respect as one of the latest techniques for routing; it requires a latest concept of routing mechanism which is recognized as the degree of involvement stability.

* SSA-Signal-Stability Based Adaptive Routing-Protocol*

**Signal Stability Based Adaptive Routing protocol** is a hands-on routing protocol which selects routes in the basis of signal strength connecting between the location constancy and nodes.

* LAR-Location Aided Routing Protocol*

Location Aided Routing Protocol is also a type of on demand protocol which utilizes the location information to provide better performance routing of the Ad hoc networks.

**3.2.2 Hybrid Routing Protocols**

As proactive and reactive protocols are effective in oppositely different circumstances but Hybrid Routing protocols are used to balance the functionality of both protocols. As proactive protocols have some restrictions that it is only applicable to the small domains whereas Reactive protocols are applicable to the nodes which are easy to locate outside those domains. Examples of hybrid protocols

* ZRP- Zone Routing Protocols*

**Zone Routing Protocols** are hybrid routing protocols of wireless networking that utilizes the concept of both proactive and reactive protocols for sending data packets over the network.

* WARP-Wireless Ad hoc Routing Protocols*

Wireless Ad-hoc routing protocols (WARP) adopted the concept of distance vector routing protocol, which has been used to sketch mechanisms for a secure data exchange mechanism and optimize the route loops.

**3.2.3 Hierarchical Routing Protocols**

As the size of the (MANET) "Mobile Ad hoc network" increases with the time as a result the flat routing protocols may give too much routing overhead, to overcome this problem hierarchical routing protocols are preferable. Examples of Hierarchical Protocols are.

* HSR-Hierarchical State Routing*

Higher State Routing Protocols uses the concept of hierarchical technique where cluster heads at lowest stages can become the members of the higher stages.

* ZRP-Zone Routing Protocol*

ZRP is also a hybrid networking routing protocol works to speed up the Packet delivery and reduce the computing and processing overhead of nodes present in the MANET.

* CGSR- Cluster Head Gateway Switch Routing Protocol*

It is also a type of hybrid and link state routing protocol which maintains some formation of clusters and Gateway switch for data packet forwarding.
The landmark routing protocol (LANMAR) follows the concept of landmark for scalable routing of the MANET.

**3.2.4 Geographical Routing Protocols**

There are two approaches which are found in the area of Geographic mobile ad hoc networks:

1. Actual geographic coordinates (It is acquired through Global Positioning System)
2. Reference points in some fixed coordinate system.

There is an advantage of geographic map-reading protocols in the scope of Mobile Ad hoc network as they avoid the network wide searches for the destination nodes.

These protocols decrease the probability of control overhead in the network. The main constraints of these protocols are, all nodes must access their geographical coordinates all the time to utilize the functionality of the geographical routing protocols. The routing table updating must be done so fast as compared to the mobility rate of the nodes to make the location based routing so effective. This is because geographical location of nodes in MANET shifts so fast.

Examples of Geographical Routing Protocols are

- Geo-Cast (Geographic Addressing and Routing)
- DREAM - "Distance Routing Effect Algorithm for Mobility"
- GPSR-Greedy Perimeter Stateless Routing

**3.3 ISSUES IN ROUTING PROTOCOLS OF MANET**

There are varieties of challenges that concern the sketch and implementation of routing protocol in MANET. These challenges pose effects on the performance of the protocol. The major issues while designing routing protocol in MANET includes, 1) Quality of Services Optimization (QoS), 2) Energy Efficiency 3) Multicasting 4) Routing 5) Node Cooperation 6) Scalability and 7) Security Issues. The main Challenges associated with the MANET protocols are discussed below.

**3.3.1 Scalability**

Scalability can be defined as whether a network will be able to provide a certain level of service which can be acceptable even though the network consists of large number of nodes. Scalability is one of the mainly important open issues in Ad hoc networks, as MANET can be affected by nature as it originates some kind of scalability oriented issues in its capacity. Throughput will be decreased if a non-cooperative network uses omni-directional antennas. In a non-cooperative network one node acquires only one tenth of the theoretical data rate of the network interface.

There should be some set of limits for scalability of a network which are set by the routing protocols, some tasks such as Route Gaining, service location, and encryption key exchange these are the examples which are responsible for the considerable overhead of the network. These prototypes...
will increase with the rapid development of the network. In dynamic environment as a huge amount of broadcast messages are generated due to topology changes so proactive routing protocols are not suitable for the dynamic environment. Reactive protocols allows network to increase its size and to optimize the route acquisition latency. The minimum route acquisition latency is the maximum diameter of the network size and the minimum node traversal time for the route request packet. There are so many requirements to be fulfilled in case of capacity and scalability in different real time scenarios to generalize the solutions.

*3.3.2 Quality of Service (QoS)*

Quality of Service is a key to develop and fulfill incipient requirements of various heterogeneous applications and to deliver the best quality of services. QoS of Mobile Ad hoc network has become more competitive now days than even before. As the MANET is moveable in nature so the QoS cannot be taken for granted because of the link quality variation, QoS routing strategies, routing algorithms and protocols are to be verified thoroughly in future for example Perkin who has discussed about a new IMCP message (QoS Lost) which is defined to inform the end point of the route to initiate a new route discovery process.

*3.3.3 Energy Conservation*

As Mobile

**Quotes detected:** 0.01% of this doc is quoted by quote signs:

"Ad hoc network"

do not have any set infrastructure so it depends on portable limited power sources. Energy consumption issues have become one of the major problems in Ad hoc networks. Despite of using lower power consumption sources it will be appropriate from the aspect of networking to reduce the power of transceiver (the device’s in networking interface) which is one of the largest sources for power depletion. At the MAC layer this can be done by placing the receiver into sleep mode or using a transmitter which can have variable input power. From the energy management point of view power control and scheduling at MAC layer as well as with energy constrained and delay constrained routing mechanism of network layer.

*3.3.4 Security Issues*

Security is major crucial areas of Ad hoc networks, as various wireless nodes use the open shared medium which is possibly vulnerable to various malicious attacks such as Denial of Services (DoS). Absence of centralized network management or proper authentication makes the network prone to malicious attacks such as infiltration, eavesdropping, interference etc. Due to lack of proper infrastructure the Ad hoc network has become very insecure and security in MANET is considered as a major Roadblock for various commercial applications. In the concept of MANET topology various cryptographic methods are being considered as challenging to compute the task of key distribution and refresh. Mostly the current research efforts are made towards on the security of data which are being forwarded from node to node. One of the existing techniques to conquer the highly security issues is to build a self-organized public key infrastructure for Ad hoc networks Cryptography. Another challenging issues associated with Ad hoc networks are node cooperation, interpolation, multicast and theoretical limitations [109]. Another common idea to divide the data into N pieces and send to different nodes along with destination using separate routes is called secure routing, where the original message is rebuilt with the use of any (M out of N) pieces of the message packet. However security is considered as a major problem in the field of Mobile Ad hoc network. Golden age of study explore in the scope of MANET is assumed to be considered after the positive and logical explanations of the functional problems on the underlying layers. Technologies oriented with the communications whereas the recent development of smart antennas, software radios are under process, bring some new research direction along with the motivation to the area of Ad hoc network securities. Various issues pertaining to routing protocol in MANET is pictorially shown in Fig.3.4 [pic]

**Figure 3.4 Diagrammatic Representation of routing protocol issues**

**In MANET**

Malicious Attacks of network are separated into two parts, one is a. Internal Attack and another one is b. External Attack. In case of Internal Attack the Attacker intends to get regular entrance to the network without correct approval and attempt gain the entrance to the network activities, this strategies can be made either by some malicious imitations where it can act of pretending to be another authorized node for the purpose of deception else It wants to make a settlement with another nodes in the basis of mutual concession and wants to carry out its malicious behaviour. The concept of External Attacks says the adversary do acts of aiming to disrupt the network by causing congestion, propagation of fake routing information and disturb the network environment from various services. Current Mobile Ad hoc Network organization is susceptible to cause the physical harms of the network by introducing two various types of strike: Passive Attacks and Active Attacks.

**Quotes detected:** 0.01% of this doc is quoted by quote signs:

"Active Attack"

is a threat caused by the misbehaving nodes which can carry some energy costs to perform the
disruption. On the other hand passive attacks are mainly improvised to avoid the coordination between nodes with a purpose to store up or save the emmrges regardless of other nodes. Nodes are considered to be malicious if they are aiming to damage the other nodes by network outage and nodes which are responsible for making passive attacks to save the consumption of their power source for their own communication purpose are determined to be selfish nodes. Different types of attacks are classified with respect to alteration, embodiment, fabrication wormhole and absence of cooperation some of the attacks are discussed over here.

I. "Network layer Attack"
V Black Hole Attack
V Byzantine
V Wormhole
V Spoofing
V Sybil

I. "Black Hole:"
Black hole attack can introduces a probability where a malevolent node can inoculate false route replies with respect to the route requests which it has received from the other nodes and pretends like it has the shortest distance towards destination node (Fig.3.5). The fake replies can be answerable for disturbing the network traffic via the malicious node for the employment of eavesdropping or it performs this fake denial of service to block the network traffic with the received packet dropping mechanism.

II. Byzantine Attack:
This attack involves some compromised intermediate nodes where it is found that these nodes work as a whole and brings out some vulnerable attacks such as routing loops, forwarding packets on non-optimal paths and selectively dropping packets as a result the network services as well as the routing services can be affected and disrupted badly (Fig.3.6). It is seemed that the Functionality of the network is optimal in the point of view of nodes though it may be evaluating the Byzantine behavior. Possible Byzantine behavior in table driven protocols shows the possibility of the malicious nodes
V Promoting high readiness to forward control packets;
V Indorsing false links in the field of Hello packet;
V Indorsing false information's in a

III. Wormhole Attack:

A. "Network layer Attack"

Spoofing is also a special type of reliability attack where a node is compromised and program to mimic the other legitimate nodes, this nodes can be affected due to lack of authentication in the recently used routing protocols (Fig.3.6). The spoofing attack results distortion in the present network topology and causes the network looping and partitioning of the network. Absence of Integrity and authentication problems introduce fabrication attacks that generate the enormous and fake routing messages.

IV. Spoofing Attack:

Figure 3.7 Diagram of a Wormhole Attack

*Figure 3.5 Problems of Black hole Attack*
In this type of attack some non-existent nodes can be copied by a malicious node where it can be seen that several malicious nodes will be combined together which is known as Sybil attack (Fig.3.9). In this kind of attack, an attacker could be able to disorder the system performance of a network by introduce a huge number of pseudonymous attributes to obtain a huge amount of large influence. The vulnerability to Sybil attack of a reputation system has a dependency over cheap generation of the identities where it is also found that the degree from which the reputation system receives inputs from attributes and entities that have a set of trust entities to make them trustworthy entities where the system treats all the attributes in a same way. The attack is done to disrupt all, the network services when cooperation is necessary and the trust model based configuration scheme and secure allocation scheme can be affected by this. There is no alternative well planned way to prevent this attack. A few techniques which are called as "validation techniques" be able to used to defeat this attack and will able to terminate the masked hostile attributes. A local entity is defined to accept a remote identity this technique adopts the central authority mechanism which ensures a "one-to-one" communication between an identity and an entity or sometimes a reverse look up also accepted by this technique. Some techniques which are introduced to prevent the Sybil detection establish on the connectivity characteristics of the social graphs that can be able to prevent the damage caused by Sybil attacker. Some techniques cannot be able to defeat Sybil attacks as some systems are too much vulnerable to wide-spread small-scale Sybil attacks.

V RREQ Flood Attack: The flood attack hosts unnecessary transmits the data packets into the network to delay normal operation of the network.

V RREP Route loop Attack: A routing loop is a path which is used the same node more than once [110].

Authentication problems is one of the major security problems associated the "Mobile Ad Hoc Network" and the wired and the wireless network community also could be affected by this problem. Authentication mechanism is generally accomplished in two ways one is direct authentication and another is indirect authentication. In case of direct authentication mechanism a pre-shared symmetric or asymmetric keys are used by both the parties for the purpose of validating each mobile nodes as soon as the network flow of the data among them. An alternative measure of Public key infrastructure (PKI) is also used for which is known as public key infrastructure is used to validate the communicating nodes. Though Public Key Infrastructure is a very secure infrastructure for communication system which follows the concept of asymmetric cryptography, hence in this asymmetric cryptography process requirement of processing and communication resources is quite high. This voracious condition for resources makes the...
PKI based infrastructure more prone to the DoS attacks. Kerberos is a symmetric key based indirect authentication mechanism for the security and the efficient communication system which includes various significant mechanisms those are non-existent in other authentication techniques, includes:
1. Resisting the malicious activity towards identify of the client and server.
2. Identification of various types of lethal attacks, e.g. replay attack.
3. Generation of highly secure communication channel between the mobile nodes.
4. Performing authentication among the mobile nodes.
5. Resisting the disclosure of the secret key in the network [111].

"3.3.6 Malicious Behaviour of Nodes"

The vulnerabilities discussed in this chapter gives intruder a path to find the legitimate nodes and create them malicious in nature, this segment also explore about the malicious and the normal-behavior of a node. At primary normal behavior of a node is defining after that the malicious behavior.

" Normal Behaviour" - In an Ad hoc network when some operation is executed to achieve some goal for an example - all the data packets are delivered from source to destination node). The normal behavior of node includes these five security principles which are i) Confidentiality, ii) Integrity, iii) Availability, iv) Authenticity, and v) Non-repudiation.

[pic]

"Figure 3.11 Normal Behavior of Nodes"

These normal activities can be described with the assist of the above Fig.3.11, someplace packets from S to D are carried out with the conserved highly security principles. Other nodes

Quotes detected: 0.02% of this doc is quoted by quote signs:

"N1, N2, N3, N4, and N5" are the intermediates node, which are used for deliver the packets.

" Malicious Behaviour" - When a node split any of the high security principles and is therefore considered under any attack (Fig.3.12). Such nodes display one or many of the following behaviour:

" Packet Drop" - It drops or leaves the packet and do not deliver it.

" Battery Drained" - A malicious node can waste the power by execute unreasonably processes.

" Buffer Overflow" - A genuine updates cannot be to store further, because of a node under attack fills up the buffer memory with fake updates.

" Bandwidth Consumption" - a malicious node always try waste as much as the bandwidth so that legitimate nodes cannot able to use it further.

" Stale Packets" - Attackers inject stale packets into the network to cause delusion in the network.

" Delay" - In delivery packets any malicious node can consciously delay.

" Link Break" - The malicious node stays between them by the affects of two legitimate nodes from interface with each other.

" Message Tampering" - The content of the packets delay down by a malicious node.

" Malicious Node Entering" - A malicious node can appear in the network without any verification mechanism.

" Denying from Sending Message" - Sometimes Malicious nodes do not approval to deliver the packets to other legitimate nodes.

" Fake Routing" - A malicious node can build a disturbance of all operations or refer fake routes to the legitimate nodes in command to obtain the packets, whichever there is a path existing between any nodes or not.

" Node Not Available" - An intruder can separate the node from taking part in any procedure so as to make slow down when the source node selects another way of alternative path.

" Stealing Information" - Malicious nodes can take the information like the location, content, sequence number to use it for upcoming attack.

" Session Capturing" - When two legitimate nodes begin interface with each other that period , a malicious node can gain their session so as to steal some meaningful data.

" Others" - There are various ways also in which a node behaves in a malicious manner. The usual and the malicious behaviour of a node described below can be simply understood by the algorithm-N1 N3 N4 N2 [pic]

"Figure 3.12 Malicious Behaviors of Nodes"

"3.3.6.1 Security Solution to Defend Malicious Behaviour"

Various solutions to resist the security threats from malicious behavior in MANET are as follows:

" Security through Cryptography" - in

Quotes detected: 0.01% of this doc is quoted by quote signs:

"Ad Hoc Network" - the data is direct sent with the utilize of cryptographic mechanism. Cryptography is defined as to renovate (or encrypt) the original information (which is required to be sent) into the unknown organization. Even if the intruder by any chance able to entrance the content of the packet, he will face problem for understanding the format of the data packet. Cryptography is also can be symmetric which includes the same functionality of keys for encryption and decryption of the data and asymmetric includes two different encryption and decryption keys for the data packets. This proposed security technique can be applicable for protecting the truthfulness and privacy of data. Techniques like
MD5

“Message Digest 5”

- Digital Signature, MAC

SHA

“Secure Hash Algorithm”

are deploy for conserving the high security principles.

- Security through TTP (Trusted Third Party) · This service arises in the picture when the security techniques which can be applicable for transmitting data to the nodes in a MANET is systematized by the some trusted third party authority. A common example of can be represented by Public Key infrastructure (PKI) in which a consign third party like Certifying Authority (CA) that is responsible for issuing a certificate to the genuine nodes of the network where it will happen after the completion of the authenticating procedure. This preserves verification security principle. A different example can be taken as watchdog node which continues observes of all the nodes for availability.

- Security through IDS (Intrusion Detection Systems) · Intrusion Detection System in ad hoc network is able for monitoring the malicious behavior of nodes. It is found that the thought of Anomaly based IDS technique is utilized in such method where any irregularity in the network endorses an attack. Profiles can be designed into the database of IDS which is the standard method of a node. These profiles are complete under training period. Such profiles can whichever is dynamic or static in nature. IDS can be multiply inside various nodes or can even work as TTP.

- Security through Secure Protocols · In recently the investigational outcomes present that many protected protocols have been suggested and intended for providing better highly security services to the network. Protocols like

- Security through Secure Protocols · In recently the investigational outcomes present that many protected protocols have been suggested and intended for providing better highly security services to the network. Protocols like

SAR

“Secure Aware Ad-Hoc Routing protocol”

Efficient Security

“Efficient Security

... Ad-Hoc On Demand Distance Vec
tor” (ES-AODV),

“Secure Efficient Ad-Hoc Distance Vector Routing-Protocol” (SEAD),

ARAN

“Authenticated Routing for Ad Hoc Networks”

are the different examples of highly secure routing protocols. These protocols are progress and apply using the attention of cryptography system, certification system and further highly security solutions.

- Security through other methods - Several algorithms and models contain be suggested which can be applicable for the guarantee in noting and avoiding the malicious behavior of nodes is discussed. Such approaches essential the thought of above security solutions like certification system, cryptography, intrusion detection system etc [112].

3.4 SUMMARY

This chapter has discussed about the security protocols in Mobile Adhoc Network and mainly discussed about the security threats in MANET. It able to be search that there are various security attacks on the routing protocols in MANET, where the existing solutions towards resisting it are much narrowed. Hence, the proposed system identifies the security issues pertaining to routing protocol in MANET and introduces a framework with an efficient algorithm to resist it. The prime extraction of this chapter is that although there are various techniques to mitigate attacks, but still it is highly required to understand the patterns and characteristics of the
malicious nodes and identifying their potential traits in behavior. The next chapter will introduce a technique that adopts mechanism design to understand the behavior of malicious nodes in large scale MANET and introduces a novel mathematical technique to resist the adversarial activity in MANET.

CHAPTER 4

TECHNIQUES FOR NODE-TO-NODE AUTHENTICATION

The previous chapter has discussed about the theoretical background of the proposed study, where various security issues and vulnerable situations in mobile adhoc network is discussed. The chapter has emphasized that ensuring an effective security policy in mobile adhoc network with optimal communication performance is quite a challenging task. This chapter introduces a novel technique that performs node-to-node authentication scheme using cryptographic approach and probability theory. The chapter also discusses about the research methodology as well as algorithm description in illustrative manner with briefing of outcomes accomplished from simulation study.

4.1 INTRODUCTION

The inherent characteristics of mobile adhoc network are found to be responsible for majority of the loopholes be it in quality of service or security breaches [113]. As discussed in the prior chapters about the characteristics of mobile nodes, it can be added that mobile nodes also exhibit a peculiar behavior unintentional in different types of traffic situation [114][115]. There are more to investigate regarding the suspicious behavior of mobile nodes as there are no centralized methods to perform authentication in mobile adhoc network. Such decentralized nature often invites various types of attacks e.g. denial of service, rushing attack, node capture attack, which drastically intrudes the system and renders potential harm to the resources being shared in the network. Hence, there is a need to design a robust authentication mechanism that can ensure both strong encryption processes as well as ensure better communication process with integrity, confidentiality, privacy, and non-repudiation.

4.2 PROBLEM IDENTIFICATION

The mobile node in Mobile Adhoc Network exhibits typical characteristics owing to dynamic topology which makes the entire system more challenging [116]. Although the mobile nodes are more inclined to set up their communication process with other mobile nodes using any available routing protocols, but sometimes setting up a precise routing seems to be quite vulnerable situations. It is to be known that a mobile node in mobile adhoc network plays a multiple role at same time. An illustrative example of a mobile node playing multiple roles is exhibited in Fig.4.1

Figure 4.1 Scenario of Communication in Mobile Nodes

Fig.4.1 expresses a scenario, where it can be shown that a sender node A is trying to communicate with destination node C using multihop approach considering B as an intermediate hop. This is a very normal scenario considered on any routing principles. However, a closer look in the actual scenario will change the perception and will bring forth the reality behind this. It can be seen that node A acts as sender node and at the same time, it also acts as destination node for node P. Node B also acts as intermediate node for the destination node Q, while it also plays as a destination node for node R. Similarly, node C acts both as a sender as well as intermediate node. This typical example shows that a simple communication in mobile adhoc network arises from multiple source points, which generates a massive overheads and leading to maximum consumption of memory of almost all the mobile nodes. Hence, every mobile node will require certain extent of resources to be consumed in order to process the data accordingly based on the instantaneous roles played by each mobile node. Hence, this results in large extent of end-to-end propagation delay. Hence, it can be said that delay is also an inherent characteristics of large scale mobile adhoc network.

However, our interest in these special characteristics is that such characteristics may be mimicked by the malicious nodes too, where the malicious nodes will have fewer chances to get caught. Mobile Adhoc Network works on decentralized architecture where there is no way one node can get authenticated to each other. Usually the if any node is found to assist in packet forwarding mechanism in mobile adhoc network, they can considered as authenticated node and soon they can join the network. A malicious node can thereby perform eavesdropping and can gain access to the private information of the network, where their reputation and trust values will keep on increasing [117]. Such increment in trust value will result in massive and collateral damage. Another unique characteristics to be discussed in this viewpoint is that, when the mobile node (which plays a multiple role in one instance of time) get overloaded with request messages to be processed, they will either choose to i) hold the incoming packets for a certain duration of time or ii) may choose to reject the request of packet forwarding. Although this is one of the regular characteristics of a normal nodes in large and dense traffic in mobile adhoc network, but such phenomenon can also be replicated by the malicious nodes.

Hence, in short, we can terminate that the problem statement of this chapter of thesis as - "Owing to dynamic topology and characteristics of multiple role adaption in mobile nodes, it is quite challenging task to differentiate malicious and normal nodes that renders the authentication/system more and more vulnerable."

4.3 PROPOSED SYSTEM

The prime aim of the proposed system is to formulate a framework that can
In the above equation, the value of the new variable $\gamma$, called as PDF = $\gamma$. PAT + (1-$\gamma$). PNR = $\gamma$. PAT + 1 - $\gamma$ will assist in data forwarding process can be modeled as, hence, it is quite unlikely that such mobile nodes will assist in data forwarding process. Therefore, if $\gamma$ is equivalent to zero than altruistic factor, lies with the range of [0, 1], PAT is the probability of forwarding process. Therefore, the probability (PDF) that such mobile node is all the possibility of the existence of the mobile nodes with altruistic behavior exhibition. Such types of mobile nodes will attempt to safeguard their resource consumption by misutilizing resources of other mobile nodes. 4.4.2 Mobile Node Design As discussed in Fig.4.1 that a mobile node plays a multiple role, where the overheadd possibility is quite higher as a mobile node plays a role of i) sender, ii) receiver, and iii) intermediate at a same instance of time in the limited size of memory. There is all the possibility for a node to drop the incoming request from other nodes owing to this buffer overrun situation. Hence, a mobile node can definitely exhibit altruistic behavior if the traffic load is quite higher [120]. Although, this is a very normal behavior, but such behavior can be possibly mimicked by a malicious node, and this process will make the highly challenging ground to distinguish the regular and normal mobile nodes. The proposed system considers the standard adoption of IEEE 802.11b protocol for each mobile node to perform communication with each other. IEEE 802.11b offers a potential rate of transmission that will assist to establish a strong interconnectivity among the mobile nodes. Normally, a mobile node has no much constraint about its resources, but majority of the devices in mobile adhoc networks e.g. smart phones, tablets, laptop runs on limited capacity of battery. Hence, there is all the possibility of the existence of the mobile nodes with altruistic behavior exhibition. Such types of mobile nodes will attempt to safeguard their resource consumption by misutilizing resources of other mobile nodes. Hence, it is quite unlikely that such mobile nodes will assist in data forwarding process. Therefore, the probability (PDF) that such mobile node will assist in data forwarding process can be modeled as:

$$PDF = \gamma \cdot PAT + (1 - \gamma) \cdot PNR = \gamma \cdot PAT + 1 - \gamma$$

In the above equation, the value of the new variable $\gamma$, called as altruistic factor, lies with the range of [0, 1], PAT is the probability of data forwarding by mobile node with altruistic behavior which is less than 1 (=$0.1$). PNR is the probability of the data forwarding for regular forwarding of the data packet. Therefore, if $\gamma$ is equivalent to zero than the mobile node can represented as normal node, which will mean that it will be always assists in forwarding the data packet with higher probability (PDF=1). On the further hand, if $\gamma$ is equivalent to 1, than the mobile node can be thought of exhibiting the altruistic behavior with lower...
value of probability of data packet forwarding (i.e. PDF= PAT=0.01). Hence, the formulation of the altruistic factor assists in identifying the malicious behavior of the mobile nodes.

32 ALGORITHM IMPLEMENTATION

The design of the proposed system is done using Java environment on normal 32 bit machine with 4 GB RAM. The algorithm targets to establish an enhanced authentication system for all the communicating nodes present in the simulation area. The presented technique is developed considering the possible vulnerable condition arising from the dynamic topology as well as altruistic behavior exhibited by the mobile nodes. The backbone design of the algorithm in this chapter of the thesis is intended to furnish a better security policy that can understand the behavior of the nodes based on the communication principle and then based on the significance of the vulnerability, the proposed system provides sufficient security system to perform authentication of the sender to intermediate nodes and iterates till it broadcasts the data packet to the target node. In this process, there is a higher likelihood that a mobile node being underwent buffer overrun and thereby it exhibits temporarily altruistic behavior to retain its resources. However, there is no assurance that such properties of altruistic cannot be replicated by the malicious nodes too, in which case, it will be highly challenging to distinguish regular nodes to malicious nodes.

Hence, the design of the algorithm mainly performs following contribution:
1. The algorithm intends to capture the communication behavior of the mobile nodes and performs a simulation study to understand the discrete behavior of the mobile nodes.
2. The algorithm doesn’t intend to find the malicious nodes as it is not achievable to do so. We assume that attacker module is highly strong in their own algorithm design and keeps on updating their malicious programs. Hence, designing an algorithm to catch hold of attacker will be most expensive idea, which is out of scope of this thesis.
3. The algorithm formulates a discrete set of behavior for regular nodes as well as malicious nodes, where the malicious node is assumed to mimic the altruistic behavior of the regular node to initiate an attack.
4. The algorithm using a typical use of hash based cryptographic approach as well as digital signature for performing encryption of the data. The technique will use both private and public key to carry out the encryption process.
5. The algorithm is designed based on probabilistic theory that assist in evaluating the extreme cases of sustenance of the proposed techniques.
6. The algorithm is designed mathematically using bilinear maps of cryptography, which insists that only the nodes that are authenticated could be transmitted the original data.
7. Interestingly, the algorithm also stimulates the malicious nodes to participate in data packet forwarding process in order to gain trust or reputation factor. The algorithm ensures that malicious nodes or nodes with altruistic behavior should assist in forwarding the data, but however, it will not be permitted to gain any forms of access in the original data packet.
8. The proposed algorithm is developed to ensure confidentiality, integrity, and non-repudiation in the secured communication process in mobile adhoc network.
9. The proposed algorithm allocates a trust attribute to those mobile nodes which completely assists in forwarding the data packet securely to the destination nodes.
10. The proposed algorithm allocates a reputation attribute to those mobile nodes which failed itself to send the data packet to the target node but forwarded the data packet to the nodes in proximity, there assuring superior data delivery process with optimal security.

*4.5.1 Algorithm for Enforcing Packet Forwarding*

The design principle of the algorithm for enforcing the data packet forwarding consists of 4 methods e.g. i) initialization of the process, ii) data packet generation, iii) data packet forwarding, and iv) mechanism to provoke the mobile nodes to forward data packet. The proposed system uses the principle of pairing-based cryptography [121] for this purpose.

The system considers H and HT as the dual multiplicative cyclic group [122] of equivalent prime order p. Hence, if the system will consider H and HT have inclusion of pairing protocols that can generate a cost-efficient map of bilinear pairs, which will mean that [pic] (4.1).

The above eq. (1) holds good for all the values of a, b ∈ Zr and for any values of h1, h2 ∈ H. A closer look into this formulation will tell that proposed system considers the computational complex attack module with a specification of (h, ha, hb, hc) for any h ∈ H as well as with unknown a, b ∈ Zr, there will not any technique to be executed in an anticipated polynomial time for computing hab with impractical feasibility. Hence, the system defines the formulation of bilinear mapping principle to generate Hgen as a probabilistic technique considering the security attribute / as input and generates an output of (r, h, HT, f), where r can be a l-bit size of any prime digits, H, HT can be two groups with sequence of r, h ∈ H can be represented as a generator. The system also considers f: H x H x HT as a cost-efficient and scalable map of bilinear principle. Further discussion of each steps in the algorithms are as follows:
"i) Initialization of the Process": The proposed system considers N number of mobile nodes. The system also considers the inclusion of trusted authority to obey the similar system attributes. Therefore, for a considered security attribute a, the generations of the bilinear attributes can be represented as \((r, h, H, HT, f)\) by adopting \(\text{Hgen}(a)\) function. The system considers the hash operations of standard cryptography as \(\text{Hash}:[1, 0]^*\) will results in \(Z_r\) by opting a symmetric cryptographic technique \(E\). This module will generate a system attributes of \((r, h, H, HT, f, \text{Hash}, E)\) by adopting \(\text{Hgen}(a)\) function. The system then computes the associative public keys as \(y_i\) that is equivalent to \(h^x \)i. While processing for security, each mobile node also formulates a matrix to enroll its Individual Trust Factor (ITF) as well as Individual Reputation Factor (IRF) with the trusted authority. The proposed system considers that there exists an external module called as certificate authority that is responsible for certifying all the public keys to be used.

"ii) Data Packet Generation": The prime purpose of this module is to perform generation of data packet that will be required to get it ciphered while performing transmission of the data packet. Hence this module will be responsible to generating the encrypted data to the network targeting the other mobile nodes to accept it for performing decryption. Hence, the system considers a sender node \(N_s\) posses both private as well as public pairs of keys \((x_s, y_s = h^{x_s})\) at a specific position \(P_s\) is interested to forward a data packet \(\text{pkt}\) to the recipient mobile node \(N_d\) with a pair of key as \((x_d, y_d = h^{x_d})\) at a specific position \(P_d\). The steps for incorporating security to be considered by sender node \(N_s\) will be:

1. The shared key of static nature will be required to be computed between \(N_s\) and \(N_d\)

\[
\text{(4.2)}
\]

2. The system uses an encrypted digital signature \(\sigma\) on \(\text{pkt}\) considering sender node, location information of sender and recipient node, node provocation policy involved, and time to live information of the data packet and on \(\text{D}\) as

\[
\text{(4.3)}
\]

3. The interesting point in the operation involved in this step is that when any intermediate mobile node \((P_i)\) is normal or malicious nodes is willing to achieve the gain by forwarding the \(\text{pkt}\), it should initially cross-check with the reputation value of the sender's node and will be required to perform validation of the digital signature using,

\[
\text{(4.4)}
\]

4. If the reputation factor of the sender node is found to be acceptable (means reputation of the source should be less than thresholded value of reputation), the system allows the node to performing digitally signing operation as:

\[
\text{(4.5)}
\]

The above equation can also be said to be acknowledgement message that send the signature information along with position information of the interested node to the sender node \(N_s\). Once the source nodes receive this, it performs next phase of operation.

1. The sender (or source) node will be required to cross-validate the newly generated acknowledgement message by,

\[
\text{(4.6)}
\]

2. If the above equation is found to be valid, the source node \(N_s\) generates a signature \(\sigma_1\) on \((\text{pkt}\|n_1\|P_s\|TS)\) as

\[
\text{(4.7)}
\]

Or else, the source node rejects the incoming acknowledgement. Hence, this step ensures that source node checks the signature and sends the data packet to the next neighbor node.

"iii) Data Packet Forwarding": Now, when the next node (or intermediate) mobile node is authenticated by the source node, its main responsibility hold for forwarding the

"data packet"

Therefore, when an intermediate node finds in new location of its mobility that certain amount of data packet \(D\) cannot be carried by them (even if they are in good proximity of destination node \(N_d\)), it will send the

"data packet"

to the next neighbor node using algorithm for data packet forwarding. The characteristics of the algorithm will be executed by all the neighbor nodes who will be holding the data packet in next interval of time. Finally, the algorithm ensures the fail-proof forwarding of the data packets.

"4.5.2 Algorithm for Data Packet Forwarding"

*Input*: Nodes, time, data packet
*Output*: node performs data packet forwarding.
"Start"
1. "If" a mobile node \( n_i \) attempts to transmit \( D \) with \( T \) time (sec)
2. "Then"
3. \( n_i \) ensure feasible position of \( P_{i+1} \) that \( n_{i+1} \) can hold \( D \).
4. "If" position \( P_{i+1} \) is in proximity to \( N_d \) than \( P_i \)
5. \( n_i \) transmits \( D(n_{i+1} \)
6. "Else"
7. \( n_i \) increases its holding time to check \( n_{i+2} \).
8. "End"
9. "Else"
10. \( n_i \) drops \( D \)
11. "End"
"End"

The above discussed algorithm is responsible for forwarding the data packet considering the situational analysis of the mobility and the occurrences of the appearance of neighbor nodes. The intermediate node \( n_i \) at a particular position \( P_i \) is now considered to be prepared for towards the data packet to the next near node \( n_{i+1} \), where the ciphering process is sequentially considered as follows:

- When an intermediate node is ready for transmitting the data packet \( D \) to the immediate neighbor nodes, it will be required to check the availability of the reputation factor of the sender node \( N_s \) as well as its validity of the digital signatures. If the reputation factor of the sender node is found to be valid, the next node \( n_{i+1} \) performs digital signing as follows:

\[
\text{[pic] (4.9)}
\]

The above equation represents the digital signature that is considered as an acknowledgement message to the prior node \( n_i \).

- Once the message of acknowledgement is received, the intermediate mobile node will perform following validation:

\[
\text{[pic] (4.10)}
\]

If the above equation is satisfied, than the intermediate mobile node \( n_i \) evaluates,

\[
\text{[pic] (4.11)}
\]

Finally, the node transmits the data packet \( D \) to the next node \( n_{i+1} \).

- After the verification of the digital signature, the intermediate mobile node \( n_{i+1} \) will now look for next best opportunity to forward the data packet \( D \).

*4.5.3 Mechanism to Provoke the Mobile Nodes to Forward Data Packet*

This module of the proposed system is responsible for ensuring the fact that all the mobile nodes to be provoked to participate in packet forwarding process. When the data packet is collect by the final intermediate mobile node \( n_N \), it forwards all the information of the digital signatures to the trusted authority that allocates either trust or the reputation to the mobile nodes that assists in data packet forwarding process. It is performed in following phases:

- The trusted authority basically performs cross checking of the authentication of the digital signatures received from the final intermediate mobile nodes. If the digital signatures are found to be authenticated trusted authority carried out its sequential operation or aborts the connections.
- The trusted authority checks for the position information of all the possible communicating mobile nodes and estimates the original distance from the final intermediate nodes.

This part of the study performs some of the interesting operation by allocation of trust as well as reputation to the mobile nodes. The system performs two possible situations e.g. i) An intermediate mobile node carry the data packet and forwards it to destination node, and ii) An intermediate mobile node carry the data packet, fails in forwarding to the destination node.

The above mentioned situations are high possibility in the dynamic topology of mobile adhoc network. The system considers two terms trust and reputation, where the higher emphasis is given to the trust factor. The trust factor is something which even the normal node as well as malicious node will try to gain. A normal node after attaining trust factor can ensure the robustness of authentication system among the each intermediate node. However, the malicious nodes will also attempt to gain an access to trust factor for intruding inside the network and provide collateral damage. Interestingly, the authentication is highly dependent on the digital signatures and its generation process, where the malicious nodes will be provoked that if they assists in forwarding the data packet they gain a trust factor. In case the malicious node attempts to do so, they get a trust factor but owing to absence of any digital signatures they will never gain any access to the data packet. For the second situation, if the mobile node fails to onward the data packet to destination node but forwards the packet \( D \) to next hop, it gains reputations. Hence, at any condition, the nodes are getting authenticated without any possibility of intrusion from malicious node.

*4.5.4 Algorithm for Trust and Reputation System*

*Input*: Position information, digital signature
*Output*: Allocation of trust and reputation
*Start*:
1. Retrieve the position information from digital signatures
2. Estimate the original distance among the intermediate nodes
3. For \( i=1 \) to \( N \)
4. "If" \( D(N_d) \)
5. Allocate trust factor
6. Or "Else"
7. Allocate reputation factor
8. "End"
"End"
The proposed system is mainly responsible for ensuring integrity as well as repudiation of the communication process and thereby assists in evolving with a robust authentication scheme among the mobile nodes. The algorithm ensures that whenever a mobile node wants to join the network it is mandatory for it to transmit a message containing information about key agreement for its neighbor nodes for obtaining a secret message to be shared.

4.5.5 Algorithm for Cryptographic Incorporation

The cryptographic protocol implementation of the proposed system is carried out considering the key agreement process of the mobile nodes, where emphasis is given for the neighbor mobile nodes mainly. This part of the proposed system is mainly responsible for ensuring integrity as well as repudiation of the communication process and thereby assists in evolving with a robust authentication scheme among the mobile nodes. The algorithm ensures that whenever a mobile node wants to join the network it is mandatory for it to transmit a message containing information about key agreement for its neighbor nodes for obtaining a secret message to be shared.

4.5.6 Algorithm for Ensuring Authentication of Communication Mobile Nodes

"Input": sender node, intermediate node, key
"Output": Authentication between two nodes.
"Start"
1. Ns(broadcast) (msg1), where msg1=Kreq, ReqID, Naddress, PKs
2. Response (msg2)(Nn, where msg2= Kres, ResID, Neigh address, Nneigh address, PKN
3. PRNG(Ks)
4. E=Enc(Ks)
5. Transmit(msg3)(ni+1, where msg3=Kpass, E
6. get ACKmsg from ni+1
7. Ks(ni+1
8. Dec(Kpass ack, ReqID, Hash(Ks))(ReqID)
"End"

The proposed algorithm mainly performs authentication of sender and intermediate nodes and continues until the data packet is being forwarded to the destination node. For performing the mutual key agreement process, the sender nodes will be required to perform broadcasting of a control message with the neighboring nodes. The control message (msg1) will consists of request for key agreement (Kreq), id of the request message (ReqID), address of the sender node (Naddress), and public key of the sender node (PKs). This control message after receiving by the neighboring node ni will send one acknowledgement back to the sender node as a response (msg2). The contents of the response message are response of the key agreement (Kres), id of the response message (ResID), address of it (Neigh address), and public key of it (PKN). The sender node that generate a secret key (ks) using pseudorandom number generator (PRNG), which is again utilized to carry out the encryption process of the same key. The sender node sends the pass key information (Kpass) as well as Encrypted data to the intermediate node and waits for an response in terms of acknowledgement. After receiving the acknowledgement, an intermediate mobile node carry out the decryption process using its private key and send the response back to sender node to complete the mutual key agreement process.

It is to be noted that although there are two types of keys (PKs) and (PKN) that acts as public key for the sender mobile node as well as intermediate mobile node, but all the nodes in the simulation area is considered to have their own pair of both public as well as private key.

The proposed system is inspired from RSA-based generation of cryptography by ensuring self-generation process of secret key. The communicating mobile nodes do have a possession of the array of neighboring nodes along with address of neighboring nodes, position information of neighboring nodes, and a shared secret key. Hence, after the successful completion of negotiation process, the mobile nodes are successfully done with authentication process.

4.6 RESULT ANALYSIS

For the purpose of performing comparative result analysis, the proposed system considers the work done by Zhang et al. [123] who has introduced a technique for pair wise key establishment policy in sensor networks. The study of Zhang et al. [123] was chosen for the following reason e.g. i) the aim of Zhang et al. [123] is similar to us, ii) the method of using pair wise key establishment is similar to us, iii) Like proposed system, Zhang et al. [123] is also focused on node capture attacks, and iv) it is one of the good benchmark study recently in research community pertaining to group communication in wireless sensor network.

"Figure 4.3 Analysis of Time Complexity"
"Figure 4.4 Analysis of Storage Complexity"

The outcome shows that Zhang et al. [123] approach significantly takes more processing time with the increase of iteration, where each iteration will signify increasing data dissemination process. Although authors have discussed a robust accomplishment of computational complexity in their research paper, but when the attacker module is changed, the outcome shows to no enhancement in processing time. Proposed system uses a novel approach where cryptographic encryption is extremely less and more is mathematical modeling for encrypting joint key, for which reason, the recursive process in encryption is reduced and system potentially updates the used key in very faster track. Hence proposed system is observed with less time complexity. Fig.4.4 shows the storage complexity of the proposed and existing system. Zhang et al. [123] has adopted AES algorithm with 128 bit encryption technique along with storage of the keys in the matrix. However the proposed system is independent of any such things. Neither proposed system stores any joint key after performing encryption nor it is broadcasted for which reason the storage factor is almost uniformly distributed with flexible size of keys. The proposed study is the first of its kind to exhibit the fact that
encryption with lower values of standard 128 bit with security options more than existing cryptographic protocols.

*4.7 SUMMARY*

This chapter has discussed about the novel technique for performing authentication of all the communication nodes. The algorithm provides the study significance by formulation the encryption policy to be applicable between only two communication nodes i.e. sender nodes and intermediate nodes, which is iterative to encapsulate all the possible intermediate nodes till it reaches its destination. The similar environment of adversary will be considered and further investigated using mechanism design in the next chapter that will bring out more potential analysis of malicious activities in large scale mobile adhoc network.

**CHAPTER 5**

SURVEILLANCE OF MALICIOUS BEHAVIOUR PATTERN

The previous chapter has discussed about a secure authentication scheme that occurs between a sender node and an intermediate node using a robust mathematical modelling. The outcome of the system were benchmarked with the existing system and found to effectively address the issues of authentication among the communicating mobile nodes in the network. The present chapter will further extend the mathematical modelling using mechanism design where the objective is to extract the patterns of malicious behavior of the nodes in highly uncertain and unpredictable condition of mobile adhoc network. The chapter will also highlight about the methodology being adopted, algorithms being implemented, and analysis of outcomes.

5.1 INTRODUCTION

In mobile adhoc network, it is quite a challenging aspect to understand the behavior of the node. This fact is also discussed in the prior chapter. There are various ways a malicious node can copy the behavior of regular node, where it becomes quite a difficult task to identify the good and bad intention. Hence, it is required that a mathematical modelling be designed which can keep on monitoring the behavior of the node, and then based on any forms of attack, it can read the pattern of the malicious activities to be performed by the adversarial node. Hence, in order to accomplish this, mechanism design as well as probability theory will act as a highly effective tool to understand and map the complicated behavior of the malicious node. Hence, this chapter will introduce such technique that can be used for performing surveillance system to monitor the malicious behavior of the mobile node.

5.2 PROBLEM IDENTIFICATION

The proposed study has developed a quantified hybrid model that will be used by the network mobile nodes and stakeholders of the applications in mobile adhoc network to evaluate the extent of successful decision making for selecting the particular security measures and its associated development methodologies. As priorly discussed in Chapter 4, security system pertaining to authentication of mobile nodes in mobile adhoc network includes various variables that affect the quality of data delivery both intrinsically as well as extrinsically; hence, the proposed quantified model adopts strategic decision making theory as well as probability theory to mathematically model it. The design principle is majorly based on mechanism design [124] which can potentially map both strategic decision making as well as probability theory. The reasons for adopting mechanism design in this chapter of thesis are as follows:

Existing techniques for solving highly complex problems with maximum unknown variables can be done using Fuzzy Logic [125], Neural Network [126], and Genetic Algorithm [127]. But, all such models are highly dependent on training as well as database, which will mean that more the size of available training data, more accurate is the outcomes. In the area of software project development, there are various unseen circumstances like skill gap, requirement volatility, attrition rate, poor selection of quality standards etc, which are computationally complex process to be modeled. Such modeling requires strong set of assumptions as well as real-time constraint for performing reliable
decision making. Mechanism design is based on probability theory as well as consideration of real-time constraints that permits the decision maker to evaluate the outcomes of their adopted decision by scrutinizing their payoffs. Mechanism design is completely independent of any training data as with the evolution of process (or interactions), the data becomes highly intellectual to furnish more information without any training process involved in it. Hence, owing to less computational complexity while processing unlike Fuzzy Logic, Neural Network, Genetic Algorithm, mechanism design is one of the best selection to consider modelling the highly complex scenarios of software development methodologies.

Consideration of mechanism design includes the scenario where the actors (mobile nodes) are supposed to adopt their decision that can strongly influence their performance as well as their neighbor node's performance too. Interestingly, as it is designed based on probability theory, it lays strong emphasis on hypothetical frameworks that allows easier analysis for the interactions of the mobile nodes involved in the simulation study of mobile adhoc network. Hence, mechanism design can be used to check the level of effectiveness of the decision implicated by the security mobile nodes in mobile adhoc network. It also provides the highly contentful and conclusive information for the most complex data structure in the software development methodologies by allowing designing a mathematical model with most critical real-time variables with high constraint factors.

Hence, it can be seen that adoption of mechanism design is the most appropriate selection for designing the proposed quantified hybrid model that considers various real-time security constraints, performs mathematical modelling, and consistently evaluates various uncertainties factor and impending attributes influencing successful implementation of an effective surveillance system to monitor the malicious behavior of mobile nodes in mobile adhoc network.

"5.2.1 Rationale of the Model"

In the existing system, Parker [128], one of the most acclaimed authors of security systems in mobile adhoc network, in his book "Observational /Techniques for Detecting Malicious Behavior in Adhoc network" has written some of the critical difference from operational viewpoint of development methodologies between conventional and high-performance network in mobile adhoc network. The discussion laid a foundation of the fact that there are multi-dimensional complexities in different activities carried out in high-performance applications in mobile adhoc network, where the key factors for high-performance systems are identified as energy consumption, bandwidth consumption, trust, and reputation system. In reality, the computational framework to mitigate malicious attack in mobile adhoc network is practiced in the present time using intrusion detection system [129] and intrusion prevention system [130]. Parker was always in support of adopting mathematical and empirical principles as it has already exhibited its success in various type of attacks in mobile adhoc network e.g. denial-of-service attack [131], Sybil attack [132], routing attack [133] etc. Reputed author Pathan [134] in his book "Security of Self Organizing /Network" has also emphasized the adoption of mathematical approach, where it was discussed that decision making theory could look fair in reading theoretically, but complicated to bring the theory in real-time implementation. Hence, the author suggested that if mathematical modelling is difficult to be adopted for first timers who are more inclined towards conventional practices, there is better alternative for that. Mathematical modelling could be possibly integrated with slight adjustment in the existing process management for mapping the malicious behavior of mobile nodes to ensure that there are better opportunities in both detection as well as in prevention process. However, such standard theories essentially prove that there is a high scope of improvement using the leading mathematical modelling with the existing probability theory for enhancing the quality of the surveillance system development. Hence, this section will discuss about a mathematical modelling that is designed with utmost care both analytically and practically to validate the outcomes of its applicability in real-time scenario of malicious activities in mobile adhoc network.

"5.2.2 Need of the Model"

Following are the justified reasons for highlighting the genuine need of mathematical modelling:

* Lack of Mathematical Approaches*: Various real-time constraints like energy, dynamic topology, routing selection, bandwidth consumption are some of the critical parameters behind security systems of tracking the behavior of mobile nodes. However, all such parameters are near to impossible to ascertain as they cannot be framed as discrete variable, for which reason, there is no such software or framework existing till date that can perform analysis of the effectiveness of the model for future requirements. In the existing system, all the prediction [135] of success or failure of the security systems model exists based on the availability of resources and without any types of consideration of the real-time constraints. Hence, such models are definitely less reliable in long run and calls for various amendments during various stages of developing security system to track the malicious behavior of mobile nodes in mobile adhoc network. Hence, a new model is required that can overcome such issues.

* Presence of Uncertainty in Process*: The areas of security system in mobile adhoc network are shrouded with various uncertainty issues, which cannot be modeled or computed directly. The computation performed with available resources may give reliable solution for
present requirement, but doesn’t ensure when the requirements or real-time constraints keeps on changing, which is very frequent in any simulation study. Hence, such uncertainty environment cannot be designed using deterministic technique and only probabilistic technique can solve this as the variables and event in our cases are completely of random nature that can be effectively evaluating using stochastic principles.

* Few Cost Effective Approaches*: At present, various intelligence e.g. Artificial Intelligence, Genetic Algorithm, Bio-Inspired Algorithm do exists in the area of predictive analysis that are already in use from last decade. One of the most challenging issues in such technology is that they are pretty expensive in nature and their outcomes depend on the training dataset, which is heavily time consuming and depends upon programmer skills. Obviously, such principle lacks decision making instantly, which is also a part of computation. Hence, we need a soft computing technique, which is not only about cost reduction but should also emphasize on increased production efficiency.

Therefore, keeping all the important facts discussed above, the prime objective of this part of the study is to design a mathematical model that can perform analysis of the malicious behavior of mobile nodes using probabilistic theory as well as strategic decision making theory for understanding the underlying connectivity of various impacting factor responsible for success / failure of security system in mobile adhoc network.

### 5.3 RESEARCH METHODOLOGY

The proposed mathematical model is designed using strategic decision making theory where the modelling principle is done on the basis of the level of effectiveness represented by the set of specific action / behavior that a mobile node adopts. The design principle considers only mobile nodes based on the studies of Parker [136] which laid emphasis on the mobile nodes mainly. The prime reason behind this is to understand the effectiveness of the standards and the working principles towards protocol process management laid by intermediate nodes or trusted mobile nodes. It is important to highlight one potential consideration while developing this model that any clusters in mobile adhoc network will not directly able to implement a new security protocol and hence the model assist in implementing a hybrid nature of security systems by integrating probability theory, stochastic principle, mathematical modelling, and mechanism design. It is highly possible to adopt this hybrid model without involving any cost or undergoing much re-engineering process to overview the malicious activities of mobile nodes. Hence, the prime objectives of the design principle are:

- To ensure that mobile nodes stick to the protocol of the new security algorithm using the proposed mathematical model.
- To ensure that mobile nodes are guided about their imprecise decision in the entire surveillance cycle by continuously monitoring their defects and further reducing it.

The system formulates the decisive structure of such mobile nodes and attempts to understand their behavior with an aid of the proposed mathematical model. The prime actors involved in this model are as follows:

* Normal Nodes (NN)*: The system defines the normal mobile nodes as a node that are known for their correct decision towards data packet forwarding as well as identifying the potential threats in the simulation area and adhering to the standards of protocols by continuous monitoring in their surveillance system. Some of the prime characteristics set of actions defined for NN are:
  - Protocol-Compliance (C): This action will mean that mobile nodes will always cooperate with the proposed protocol for carrying out surveillance system where the core principles designed from mechanism design, probability theory, and strategic decision making theory. Each cluster has one mobile node with certain distinct roles and responsibilities.
  - Protocol-Violations (D): As the entire process management is still human-oriented and expert’s opinion, hence, there are quite possibilities that mobile nodes may decline certain sets of protocols which they find it as inappropriate with positive intentions.
  - Identify and Reporting the Threat (R): This set of action can be determined as the reporting procedure, which plays a critical role in identifying the threats in the surveillance system in front of the entire clusters.

* Adversarial Node (AN)*: The system defined selfish mobile nodes as a mobile node in the simulation study who is characterized by low efficiency in their decision making principles towards ensuring standardized protocol of surveillance system. The decision adopted by them is assumed to affect the clusters as well as neighbor node’s performance as well as results in risk in almost every stage of security system. Hence, existing of AN is detrimental to cost effective production and superior quality assurance in an effective surveillance system in mobile adhoc network. Just like NN, each cluster have one AN and is mathematically characterized by following set of action:
  - Protocol-Compliance (C): The definition of protocol-compliance for AN is almost same as NN, however, there is a distinct difference being made for better accuracy in the mathematical modelling. The AN chooses to perform protocol-compliance in the cluster for negative purposes. It is said that if AN starts showing their inefficient characteristics, they have the higher
chances to get monitored by the NN using /Identifying and/ /Reporting the Threat/. Hence, in order to hide their inefficient decision implementation, the proposed design principle considers AN to perform protocol-Compliance in the initial level. Hence, it can be seen that mathematically, the action protocol-Compliance, which is represented as a variable, is quite confusing as both AN and NN bear the same variable. However, the difference is that probability of risk is quite lower for NN and quite higher for AN when they adopt the action protocol-Compliance (C).

/Protocol-Violations (D)/: The definition of protocol-Violation is quite same for both AN and NN; however, there is again a unique difference between them. NN chooses protocol-Violation for productive purpose, while AN chooses protocol-Violation for unproductive purpose; unfortunately, it can be intentional or unintentional. The prime difference is that probability of model crash is very low for NN and very high for AN.

/Invoke Threat (A) and Spread Threat (F)/: This set of action is the prime characteristics of AN. Owing to adoption of inefficient decision; the proposed system performs C in the initial level, which is followed by action D. Hence, adoption of action D results in increased vulnerability level of the model implementation that is represented by risk factor F in one cluster. However, owing to chains in process management, it is quite possible that risk factor (A) spreads to one another cluster hence cumulatively affecting the production and quality assurance of entire cluster.

The invocation of risk and model crash is carried out by the AN with an intention to disrupt process management and thereby to waste the organization resources. Adoption of D strategy by NN also leads to failure of the surveillance management and protocol violation just like the F strategy of AN but unlike the NN, which do not receive any kind of payoff when they employ D-Strategy, the AN get payoff for invoking threat or risk factor to the proposed model.

The system presents two types of strategies: pure and mixed strategies. A pure strategy governs a complete specification of actions to be adopted by a mobile node, while a mixed strategy is basically about allocations of a probabilistic factor to each of the pure strategies adopted. The design of the proposed mathematical model is inspired from staged interaction in decision-making theory which is simple set of interactions to be played by mobile nodes at individual time slots. The system considers rationality among the mobile nodes actor as both NN and AN having the tendency to escalate their respective utility. Concept of Bayesian Nash Equilibrium (137) is developed considering the existing belief system of mobile nodes which is further enhanced using the concept of sequential rationality for multi-staged interaction where the strategy of the mobile nodes should yield optimal results in the course of interaction. Hence, the proposed system aims to explore the perfect Bayesian equilibrium of this interaction as an enhancement to existing Bayesian Nash Equilibrium.

The system also considers the existence of selfish mobile nodes, where it is assumed that certain NN may choose to behave selfishly at some time. This may be due to the fact that the NN is facing various significant resource constraints at that particular instance of time. Hence, some NM may behave selfishly only at some events but it doesn't mean it has a consistent harmful intention for deteriorating the effectiveness of surveillance system mobile adhoc network. Time is considered as an important factor in the proposed framework wherein the same is categorized into slots and mobile nodes should select their probably best strategies concurrently at the preliminary interaction of each time slot.

"5.3.1 Interaction of Entities"

This section basically introduces the actual scheme that has been formulated for the purpose of designing the proposed framework.

5.3.1.1 Elements of the Model

The proposed system presents a modelling of regular process interaction between NN and AN as a dynamic Bayesian network and later on finding the perfect Bayesian equilibrium of the proposed study. The statistical behavior of the mobile node is scrutinized and outcome of the every process interactive round is recorded for the purpose of analyzing the pattern of erroneous behavior of mobile nodes present in the simulation environment. The framework considers that the private and confidential information should be maintained for type of mobile nodes, which is usually of AN or NN. The AN forms a statistical belief system towards the mobile nodes which are present in the associated cluster and persistently updates the value (belief) to the actions of associate mobile nodes in due course of progress in process interaction. On the other hand AN are able to track the belief which NN form for them possess.

The study considers that every action of the mobile nodes is very critical and significant that also depends on the counter actions already undertaken by the quality control mobile nodes (Trusted Authority). The optimal outcomes of the responses for both the types of the mobile nodes are guided by the specific actions performed by the other mobile nodes. A specific value of reputation is initialized by a NN and thereby possessing the potential capability of assessing the type of mobile nodes depending upon the updated value of belief as well as specific value of reputation that can be also termed as threshold. On the other hand, the ongoing risk
of getting identified is persistently being calculated by AN. The AN performs a decision action termed F for spreading risk on multiple associated clusters depending on the amount of risk and anticipated cost of loss of network resources.

The proposed scheme does not limit the phenomenon of selfishness being exhibited by the NN in some stages of the process interaction. There is no degree of selfishness that can approximate the mischievous behavior demonstrated by the AN.

"Figure 5.1 Considered Scenario of the Proposed System"
The important parameters that has been considered in the proposed formulation are as highlighted in Table 5.1

"Table 5.1 Important Parameters of the Proposed Framework"

| List of Actions to be performed by Mobile nodes (EM/IM) |
| Arisk (Action of A) | Acop (Action of C) | Adec (Action of D) | Aspread (Action of F) |
| Arep (Action of R) |
| List of Gain and Cost of Adopted Actions |
| Grisk (Gain of Arisk) | Gcop (Gain of Acop) | Grep (Gain of Arep) | Gcs (Cost of Acs) |
| Cs (Cost of Asc) | Cspread (Cost of Asspread) | Ccs (Cost of Acs) |
| List of Opinion Formulation |
| Opuncer (Opinion of uncertainty) | Opdisbelie (Opinion of Disbelief) |
| Opbelief (Opinion of Belief) |

Table 5.2 Other Associated Parameters

| F | Failure of non-positive alarm |
| ? | EM probability |
| ? | Probability of Risk by IM |
| ?cop | Quantity of identified cooperation |
| ?drop | Quantity of identified threat |
| ? | Probability of cooperating by EM |
| ?/? | Profile of Strategy/Equilibrium strategy |
| Thuncer | Threshold of uncertainty value |
| (E.) | ? | Anticipated value / Standard deviation |
| (SF) | Selfishness Factor associated with a EM reflecting the degree |
| of Selfishness |

5.3.1.2 Cluster-based Process Interaction

The proposed framework has formulation of cluster which represents a logical region of highly interconnected processes of proposed surveillance system. It can be seen in Fig 5.1. The formulation of the cluster is done, where the mobile nodes can independently depart or associate with the certain process within the cumulative simulation environment. For the purpose of authentication, the model assumes prior experience verification system where the mobile nodes identity is governed by the successful delivery of data packet in past that is fixed to a certain value for computational purpose. The secondary assumption in this phase is that whenever a mobile node wants to join the cluster, the other candidate mobile node previously residing in that cluster will allocate their initial belief value towards the newcomer.

The system also performs the similar phenomenon for AN. Whenever an AN arrives into a cluster never visited before the candidate mobile node of new cluster will treat the AN as a newcomer and allocate the same initial belief. The challenging scenario in this assumption is that at the time when the AN attempts to re-associate with a cluster, the AN can actually act as a novice mobile node exploiting the identity which is dissimilar from the mobile node that was used in its previous stay. The conceptualization of the same is supported by a fact that it is not feasible to monitor the behavior of mobile node outside the cluster. In a nutshell, it will mean that when an AN performs action of spreading threat F, it basically resets the reputation value posing a threat to quality surveillance system.

The design of the cluster in a simulation study may be possibly done in structured or an adhoc manner. In structured manner, a frequently trusted mobile node is selected as a culture head. The cluster head will only gather the information related to reporting action to be performed by NN when it identified its associated mobile node as AN. However, in the adhoc manner, all mobile nodes within that cluster get the circular of reporting information by the NN.

In case of positive report information, the AN identified will be penalized. However if the NN reporting action about the identification of AN turns out to be nothing more than a false alarm, the liability of NN will be badly affected. The proposed framework doesn't focus on the aspect of verifying the falsification of the alarm type for penalizing the AN.

However, on order to normalize this falsification issue, the proposed system considers anticipated gain of legitimate reporting action (Grep) and anticipated failure of non-positive alarm (F) for performing evaluation of the outcomes.

"2 Threat Monitoring"
The discussion of this section is with the aid of Fig 5.1, where it
can be seen that a NN can select to adopt an action related to cooperation or decline and similarly AN can select to adopt an action related to A or C. The refusal of a mobile node to participate in process surveillance management system exclusively the reporting action is termed as decline while when the mobile node makes themselves available for progressing the data packet as per the protocol, it is called as cooperate action. Success in such process management is only acceptable when the mobile node at both the ends get cooperated i.e. adopt Acop. On the other hand, the phenomenon of risk action eventually leads to unwanted resource wastage as well as detriments of the process in mobile node in proposed software development methodologies. NN can adopt decline strategy either trying save itself from possible risk from a AN (owing to adversarial decision of AN) or for that matter when its available resources do not allow it to participate current process of surveillance system (which may occur owing to battery drainage, less availability of bandwidth etc). Adoption of risk strategy can be used by the AN to process and thereby implement erroneous decision to be adopted for process management for tracking malicious system leading to error or resource cost overrun with obvious errors. Interesting point to observe is that AN gets payoff for a successful risk factors, whereas the NN gets none. This is how, it is possible to segregate AN to NN in the proposed mathematical model.

Using the remote technologies of ICT in an wireless networking, a mobile node can monitors all the exercised logs from past behavior of mobile nodes in their clusters (or in other clusters too), but they cannot understand the cause of any process disruption or any failures of protocol implementation. This phenomenon in an organization is referred to as threat monitoring in specific clusters. Hence, the parameters e.g. ?, ?, and ? are formulated for better distinction of actions of different mobile nodes.

"5.3.3 Modelling Strategies"

The proposed mathematical model make use of strategic decision making model that can be considered as a cognitive process resulting in judging the course of action out of various possible options. As discussed in prior section, above mobile nodes can identify whether the opponent mobile nodes had cooperated (adopted Acop) in the current stage of process by means of threat monitoring. However the NN can't identify the type of opponent by means of only threat monitoring in one cluster alone since it can't discover whether the failure of process management and reducing defect density was really caused by suspected opponents Adec or Arisk. Thus, requiring for NN to form belief about their opponent's kind which is based on the entirely of work and outcome evidence fetched. The NN thus continuously evaluates the option of belief (Opbelief) and adequacy of evidence (Opuncer) for the opponent mobile node based on the feedback from the threat monitoring in each clusters. With every successful process interaction trials the NN increases the ?coop by 1, when a surveillance of malicious process management fails the NN checks for the opponent's strategy. If the opponent had opted for Adec / Arisk than only the value of ?drop would be increased otherwise no updating of reporting system will take place in the current stage of the process interaction. A threshold policy is being followed by an NN to take reporting decision against the opponent mobile node. If this threshold is not reached the NN should cooperate or decline based on the current beliefs it holds for the opponent and the selfishness attribute of itself.

AN are modeled to be rational, thus will continuously evaluate the trust factor for itself with the NN. It also follows a decision rule to spread threats towards implemented process (F) in order to evade being reported (R). Hence, it is really difficult for NN to trace the extent of risk factor (protocol-violation and model crash) AN just by the basis of current actions or step being taken. This fact is almost equivalent to what actually happens in real-time environment too. The proposed model uses both soft and hard thresholding factors to map the characteristics of AN.

The model does not consider the process being controlled between the two AN as there is no utility for AN in doing so, in other words the AN's capability to identify other AN is not restricted. Thus a decision process can be controlled between two actors one which has to be NN anyways. Consequently two cases evolve now, case i) NN versus AN and case ii) NN versus NN. Therefore, the decision process for the NN will be same in both the case, and thereby the sequential rationality of the staged process will be explored.

"5.3.4 Multi-Stage Process"

The proposed mathematical model considers multi-stage dynamic Bayesian Signaling network. Bayesian network are developed considering probability theory and mechanism design that permit accepting the curtailed information of the mobile nodes. While designing Bayesian network, each mobile nodes is set with certain classified information that has significant impact on the evolution of the process with other mobile nodes are considered to possess information of the belief system about the classified data. These values of belief are signified by probability distribution and revised by applying Bayes' rule in case of availability of novice information on security process management. The mobile nodes select their best possible action during the progress of tracking the malicious behavior of mobile nodes as per the classified and belief information available.

The proposed system considers signaling concept of the decision making theory where the mobile nodes update their beliefs with progress of the process. Usually, there are two categories of mobile nodes in the study e.g. i) mobile nodes and ii) neighbor nodes. The private information is basically an inherent property of mobile nodes where, it decides to transmit a specific circular about protocol according to the need of proposed security protocol development method. However, the neighbor nodes...
interprets cost as the certain amount of resources consumed for implementing a particular new process. Therefore, the IM gains Grisk from feasible set of strategies excluding Adec acquire cost. The model considers for both the type of mobile nodes, all the mobile nodes, and also its type (IM/NN) after completion of every phase of process activity adopted by the NN. Hence, in the proposed framework, the mobile nodes x is considered as mobile nodes which can be either IM or NN and mobile nodes y as a neighbor members whose type is always efficient and towards Protocol compliance. The mobile nodes (x, y) are endowed with a utility based on own actions, the actions adopted by its associated mobile nodes, and also its type (IM/NN) after completion of every phase of defined process. The utility indexes are tabulated in table 5.3.

"Table 5.3 Tabulation of utility index considered"

<table>
<thead>
<tr>
<th>Acop</th>
<th>Adec</th>
<th>Arisk</th>
<th>Aspread</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, -Ccop)</td>
<td>(0, 0)</td>
<td>(0, -F-Crep)</td>
<td>(-Cspread, -Ccop)</td>
</tr>
<tr>
<td>(Gcop-Ccop)</td>
<td></td>
<td></td>
<td>(-Cspread, 0)</td>
</tr>
<tr>
<td>(-Ccop, 0)</td>
<td></td>
<td></td>
<td>(-Cspread, -Crep)</td>
</tr>
<tr>
<td>(0, 0)</td>
<td></td>
<td></td>
<td>Grep-Crep)</td>
</tr>
<tr>
<td>(-Grep-Ccop)</td>
<td></td>
<td>Grisk-Ccop)</td>
<td></td>
</tr>
<tr>
<td>(Grisk-Crisk , Acop</td>
<td></td>
<td>Acop</td>
<td></td>
</tr>
<tr>
<td>(Arep</td>
<td>Adec</td>
<td>Arep</td>
<td></td>
</tr>
</tbody>
</table>

Considering Mobile nodes x is IM: (x's utility, y's utility)

<table>
<thead>
<tr>
<th>Acop</th>
<th>Adec</th>
<th>Arisk</th>
<th>Aspread</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, -Ccop)</td>
<td>(0, 0)</td>
<td>(0, -F-Crep)</td>
<td>(-Cspread, -Ccop)</td>
</tr>
<tr>
<td>(Gcop-Ccop)</td>
<td></td>
<td></td>
<td>(-Cspread, 0)</td>
</tr>
<tr>
<td>(-Ccop, 0)</td>
<td></td>
<td></td>
<td>(-Cspread, -Crep)</td>
</tr>
<tr>
<td>(0, 0)</td>
<td></td>
<td></td>
<td>Grep-Crep)</td>
</tr>
<tr>
<td>(-Grep-Ccop)</td>
<td></td>
<td>Grisk-Ccop)</td>
<td></td>
</tr>
<tr>
<td>(Grisk-Crisk , Acop</td>
<td></td>
<td>Acop</td>
<td></td>
</tr>
<tr>
<td>(Arep</td>
<td>Adec</td>
<td>Arep</td>
<td></td>
</tr>
</tbody>
</table>

Considering Mobile nodes x is NN: (x's utility, y's utility)

The system considers for both the type of mobile nodes, all the feasible set of strategies excluding Adec acquire cost. The model interprets cost as the certain amount of resources consumed for implementing a particular new process. Therefore, the IM gains Grisk from successful accomplishment of risk action Arisk which is also dependent on the selection of strategies by the associate mobile nodes in different clusters. This fact is also supported by the phenomenon of risk of model crash which is made successful when the NN y chooses Adec. However, the AN can also confuse the clusters by selecting Acop in order to mislead the NN y. But, in case of single staged process, AN doesn't gain by selecting Acop as its goal (risk) varies from the action selected (Adec). This is totally reverse in case of NN which gains Gcop after adopting action for protocol-Compliance cooperation Acop.

Another fact is if the NN to adopt action of decline Adec, it doesn't gain anything. In the final phase of this strategy adoption, when AM chooses to depart to another cluster by selecting its action Aspread, the AM also estimates the risk of being identified and subsequently penalized by quality control neighbor. Hence, the model considers anticipated gain for Aspread as the dynamic risk factor that maximizes when the NN y collects the data. In case the NN selects the action Arep, it attains gain value Grep if the report is positive (i.e. it has identified x as IM) and the framework is considered to successfully identify the AM. The threat of adoption of reporting strategy by the NN is that if the report has identified as false indication, the NN damages it accountability and bears a loss F.

"5.4.1 Model's Belief System"

The proposed model adopts multi-stage Bayesian process where the NN /y/ will require revising its belief value depending on the progress of process involved in existing surveillance system. It has been seen that different types of reputation system deploys Bayesian inference for understanding the trust factor of mobile nodes which is usually categorized...
into belief and disbelief in the proposed framework. The system thereby deploys the usual update policy for belief $B$ as $\{\text{cop} / (\text{cop} + \text{drop})\}$. However, deploying the same standalone actually overlooks the possible cost for false positive that is critical for the NN to attain sequential rationality.

It has been explored that uncertainty in opinion of type of mobile nodes is the prime reason for false positive information generated by NN. The proposed model assimilate the uncertainty-aware reputation system into decision method of NN and utilize a third factor called Opuncer for signifying NN's opinion towards the other type of mobile nodes $x_i$: $(\text{Opbelief}, \text{Opdisbelief}, \text{Opuncer})\{0,1\}$. 

\begin{align*}
\text{Opbelief} &= \text{cop} / (\text{cop} + \text{drop}) \\
\text{Opdisbelief} &= \text{drop} / (\text{cop} + \text{drop}) \\
\text{Opuncer} &= 12 \cdot \text{Opbelief} \cdot \text{Opdisbelief} / (\text{Opbelief} + \text{Opdisbelief})
\end{align*}


*$5.4.2$ Designing Staged Process*

The mobile nodes are rational in nature which will mean that NN will have higher tendency to identify AN and perform reporting action while AN will adopt a strategy that reduces the possibility of itself getting identified and thereby invoke risk in the organization's cost. Again the method does not consider the process being controlled between the two AN as there is no utility for AN in doing so, in other words the AN's capability to identify other AN is not restricted.

Figure 5.2 illustrates the single stage process, where the nature decide the kind of the mobile nodes $x_i$, and the kind is $x_i$'s private information. The mobile nodes $y_i$ possess current belief formation that $x_i$'s type is risky that is signified by the probability factor $\theta$. Hence, according to Bayes' rule, $\theta$ and $(1-\theta)$ are computed as (Stone, 2013, p. 411):

$\theta = \frac{\text{?drop}}{(\text{?cop} + ?\text{drop})}$

$(1-\theta) = \frac{\text{?cop}}{(\text{?cop} + ?\text{drop})}$

When a new mobile nodes joins a cluster the existing mobile nodes within the cluster assign preliminary values as $\text{?cop} = ?\text{drop} = 1$ (i.e. $\theta = 0.5$ and Opuncer $=1$) for the new comer, which shows that there is no evidence at this point of time or there complete uncertainty in the option of the mobile nodes.

*Figure 5.2 Single Stage Process Design*

The proposed model initially considers adopting of two types of strategies i.e. pure and mixed strategy for finding the Bayesian Nash Equilibrium. Nash Equilibrium refers to a situation where in a mobile nodes can benefit from changing the strategy unilaterally when the other mobile nodes is continuing with its strategy. Nash Equilibrium for a single stage process is referred as BNE. To accomplish complete sequential rationality among the mobile nodes in the process, the system aims to explore the Perfect Bayesian Equilibrium (PSE) of this process as an enhancement to the existing BNE. The discussion of the adopted strategy could be further divided into following

*4. Pure Strategy Adoption*

In pure strategy formulation, the strategy profile can be represented under two scenarios. In the first case the AN $x_i$ will always invoke risk (Arisk) while in the second case it will always invoke cooperate (Acop). In the first case the strategy profile of mobile nodes $x_i$ can be represented as:

$x_i = \{\text{Arisk if AN, Acop if NN}\}$

The above formulation would mean that $x_i$ always adopt Arisk if it is AN and Acop if it is NN. Therefore the anticipated payoff $Ey(Ai)$ of $y_i$ adopting the Agile Strategy $y_i = \text{Acop}$ or $y_i = \text{Adec}$ are:

$Ey(Ai) = ? \cdot (\text{Grisk - Ccop}) + (1-\theta) \cdot (\text{Gcop} - \text{Ccopp})$

$Ey(Adec) = 7.0 + (1-\theta) \cdot 0$

The formulation of $Ey(Acopp)$ and $Ey(Adec)$ basically indexes two cases. In the first case, the associated mobile nodes $x_i$ is considered as AN. As per mobile nodes $y_i$'s existing belief system, this case surfaces with the probability of $\theta$. As mobile nodes $x_i$ will adopt A/risk/ action, the payoff of mobile nodes $y_i$ in such situation will be $(-\text{Grisk} - \text{Ccopp})$ and 0 respectively. In the second type of case, $x_i$ is a NN surfacing with a probability $(1-\theta)$. The payoff of mobile nodes $y_i$ in this situation will be $(\text{Gcop} - \text{Ccopp})$ and 0 respectively. If $Ey(Acopp)$ $> Ey(Adec)$, the mobile nodes $y_i$ will choose to adopt Acop as best possible action.

$Ey(Acopp) > Ey(Adec)$

As $\text{Grisk} - \text{Ccopp} > 0$ (Gcop - Ccop) $> 0$

Therefore, when the computed probability $\theta$ $(\text{Gcop} - \text{Ccopp})/ (\text{Grisk} + \text{Gcop})$, the Bayesian Nash equilibrium strategy pair for mobile nodes $x_i$ and $y_i$ is:

$\{x_i, y_i\} = \{\text{Arisk if AN, Acop if NN}, \text{Acop}\}$

But, this fact changes when $\theta > (\text{Gcop-Ccop})/ (\text{Gcop} + \text{Grisk})$ as there is no existence of pure strategy BNE. Consequently, when the AN $x_i$ adopts Arisk, the preeminent response for mobile nodes $y_i$ in this case will be to adopt Adec. But, if the NN $y_i$ adopts the action Adec than AN may chose to adopt Acop as the best possible reaction as Crisk may by higher compared to Ccop in some critical and sensitive scenarios for AN.

In the second scenario, the AN $x_i$ may select pure strategy Acop. In this situation, the NN $y_i$'s best reaction will be to adopt Acop without considering for $\theta$. But, in case NN $y_i$ adopts the action Acop, then the AN may adopt the action Arisk that minimized to the prior situation. The
profiles may be represented as $(\sigma_x, \sigma_y) = \{(A_{cop} if AN, A_{cop} if NN), A_{cop}\}$ which is definitely not Bayesian Nash equilibrium.

"B. Mixed Strategy Adoption"

This phase of discussion considers possible circumstances of Mixed strategy Bayesian Nash equilibrium. It was shown in Table 5.1 that $\sigma_x$ signifies the probability of AN $x$ to adopt the action Arisk, and $\sigma_y$ signifies the probability of the NN $y$ to adopt the action Acop. Therefore, the anticipated payoff of mobile nodes $y$ while adopting Acop and Adec are:

$$E_{y}(A_{cop}) = \sigma_y (G_{cop} - C_{cop}) + (1 - \sigma_y)(G_{cop} - C_{cop})$$
$$E_{y}(A_{dec}) = \sigma_y G_{cop} + (1 - \sigma_y) C_{cop}$$

In order to render selection among Acop and Adec have no impact on NN $y$'s utility i.e. Imposing $E_{y}(A_{cop}) = E_{y}(A_{dec})$,

$$E_{y}(A_{cop}) = E_{y}(A_{dec})$$
$$\sigma_y (G_{cop} - C_{cop}) + (1 - \sigma_y)(G_{cop} - C_{cop}) = \sigma_y G_{cop} + (1 - \sigma_y) C_{cop}$$

$$\sigma_y = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$$

Therefore, the AN $x$'s strategy for equilibrium will be to adopt the action Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. The anticipated payoff for AN $x$ for adoption the action Arisk and Acop are respectively as:

$$E_{x}(A_{risk}) = \sigma Grisk + (1 - \sigma) (-Crisk) = \sigma Grisk - Crisk$$

Similarly as above, $E_{x}(A_{cop}) = \sigma G_{cop} + (1 - \sigma) C_{cop}$

Therefore, AN $x$'s strategy for equilibrium will be to adopt the action Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. The anticipated payoff for AN $x$ for adoption the action Arisk and Acop are respectively as:

$$E_{x}(A_{risk}) = \sigma Grisk + (1 - \sigma) (-Crisk) = \sigma Grisk - Crisk$$

Similarly as above, $E_{x}(A_{cop}) = \sigma G_{cop} + (1 - \sigma) C_{cop}$

Hence, the Bayesian Nash equilibrium of the stage process can be finalized as:

When $\sigma > \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$, AN $x$ chooses to adopt Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. After $\sigma > \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$, AN $x$ chooses to adopt Acop in order to save itself from being caught, which will complete the sequential rationality of the mobile nodes. The operations carried out in the proposed strategy are discussed as below

*i) Designing Reporting Action*

The proposed model considers sequential rationality only in the situation when the anticipated payoff of the mobile nodes is higher in the progress of the process for the strategies played by its opponent. The NN $y$ after adopting action Arep against mobile nodes $x$ can fetch two responses. i) Either mobile nodes $x$ was identified to be inefficient and $\sigma_x$ can fetch two responses.

When $\sigma_x > \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$, AN $x$ chooses to adopt Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. After $\sigma > \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$, AN $x$ chooses to adopt Acop in order to save itself from being caught, which will complete the sequential rationality of the mobile nodes. The operations carried out in the proposed strategy are discussed as below

ii) Designing Random Switch over in Clusters*

*ii) Designing Random Switch over in Clusters*

When formulating the Bayesian Nash Equilibrium (BNE) for a single stage process, Acop and Adec / Arisk needed to be considered. However we are still left with two important mobile node's actions, a NN can report another mobile nodes as inefficient by adopting Arep while a AN can adopt Arisk to deternine the genuine risk (cost overrun). Hence, NN should compute $\delta F$ (Private subjective value exhibiting the NN's properties) in case of order to satisfy the sequential rationality, the NN $y$ should choose to adopt action Acop only when:

$$\sigma_x \delta F > \delta G$$

Therefore $\sigma_x \delta F > \delta G$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Hence, the threshold $\delta F$ is computed as the state that forms $\sigma_x \delta F > \delta G$.

When $\sigma_x \delta F > \delta G$, AN $x$'s strategy for equilibrium will be to adopt the action Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. In order to satisfy the sequential rationality, the NN $y$ should choose to adopt action Acop only when:

$$\sigma_y \delta F > \delta G$$

Therefore, AN $x$'s strategy for equilibrium will be to adopt the action Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. Hence, $\sigma_x \delta F > \delta G$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Therefore, the threshold $\delta F$ is computed as the state that forms $\sigma_x \delta F > \delta G$.

When $\sigma_x \delta F > \delta G$, AN $x$'s strategy for equilibrium will be to adopt the action Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. Hence, $\sigma_x \delta F > \delta G$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Therefore, the threshold $\delta F$ is computed as the state that forms $\sigma_x \delta F > \delta G$. Hence, $\sigma_x \delta F > \delta G$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Therefore, the threshold $\delta F$ is computed as the state that forms $\sigma_x \delta F > \delta G$.

When $\sigma_x \delta F > \delta G$, AN $x$'s strategy for equilibrium will be to adopt the action Arisk with $\sigma = \frac{G_{cop} - C_{cop}}{G_{cop} - C_{cop}}$. Hence, $\sigma_x \delta F > \delta G$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Therefore, the threshold $\delta F$ is computed as the state that forms $\sigma_x \delta F > \delta G$. Hence, $\sigma_x \delta F > \delta G$ would mean circumventing the possibility of achieving gains during from the subsequent stages. Therefore, the threshold $\delta F$ is computed as the state that forms $\sigma_x \delta F > \delta G$.
When AN attempts to switch to some other cluster (Aspread) after implementing erroneous process in software development process, the anticipated gain of the AN will be to avoid getting detected by the NN. The system defines the risk factor as the anticipated loss of being reported. Accordingly \( \text{Risk}_{\text{factor}} = P(\text{detect}) \cdot \text{Grep} \), where \( P(\text{detect}) \) is the probability of getting detected by the NN. Hence, AN computes anticipated gain by employing the Aspread as:

\[
\text{Ex (Aspread)} = \text{Risk}_{\text{factor}} - C_{\text{spread}}
\]

When the condition \( \text{Ex (Aspread)} > \max \{\text{Ex (Arisk)}, \text{Ex (Acop)}\} \) is met when the AN should switch over to a new cluster by employing the Aspread.

The AN possess the precise information about the surveillance process management system as well as costing record between them and AN and hence, it can accurately compute the belief of NN. The AN is also expected to have sufficient information about the organization as well as complete development manifestos hence it knows the statistical information of loss of false report \( (F) \) for the NN. When there are large numbers of mobile nodes in simulation area, the false alarm \( (F) \) should comply with standard normal distribution. The AN could know the mean (expected value) and standard deviation for \( (F) \) with the network. \( P(\text{detect}) \) is equivalent to the probability that the current \( ? (1-\text{Opuncer}) \) will pass NN's threshold \( (T) \).

\[
P(\text{detect}) = P(\frac{? (1-\text{Opuncer})}{G_{\text{rep}} + F} > \frac{G_{\text{rep}} + F}{G_{\text{rep}} + F})
\]

\[
= P\left(\frac{? (1-\text{Opuncer} \cdot (G_{\text{rep}} + F)}{G_{\text{rep}} + F} < 1\right)
\]

\[
= \Phi\left(\frac{G_{\text{rep}} + F}{(1-\text{Opuncer} \cdot (G_{\text{rep}} + F)}
\]

\[
= \frac{\Phi}{1-\text{Opuncer} \cdot (G_{\text{rep}} + F)}
\]

Thus, we have,

\[
\text{Where,} \quad \Phi
\]

Hence, it can be seen that an AN benefits from selecting its optimum value for \( ? \) when invoking Arisk and latter bypass penalization with the aid of deporting to a new cluster (Aspread). The AN persistently needs to compute the risk of residing and managing further within a cluster.

*Algorithm for Mobile nodes* "\( y \)"s PBE strategy **"\( y \)"***

1. A: if \( ? (1-\text{Opuncer}) \leq (F + C_{\text{rep}}) / (G_{\text{rep}} + F) \)
2. Report \( x \) as AN by adopting Arisk;
3. goto B;
4. else
5. if \( ? \leq (G_{\text{cop}} - C_{\text{cop}}) / (G_{\text{cop}} + G_{\text{risk}}) \)
6. Adopt Acop with a probability of 1;
7. else
8. Adopt Acop with a probability of \( (G_{\text{cop}} - C_{\text{cop}}) / (G_{\text{cop}} + G_{\text{risk}}) \);
9. end if
10. Updated ?cop and ?drop to evaluate new values for ? and Opuncer;
11. goto A;
12. B: end if

*Algorithm for AN-type Mobile nodes* "\( x \)"s PBE strategy **"\( x \)"***

1. A: if \( E_i(F) \leq \max(\sum_i E_i(A), E_i(C)) \)
2. Switch to a new cluster by adopting Aspread;
3. goto B;
4. else
5. if \( ? \leq (G_{\text{cop}} - C_{\text{cop}}) / (G_{\text{cop}} + G_{\text{risk}}) \)
6. Adopt Arisk with a probability of 1;
7. else
8. Adopt Arisk with a probability of \( (G_{\text{cop}} - C_{\text{cop}}) / (G_{\text{cop}} + G_{\text{risk}}) \);
9. end if
10. Track NN values for ? and Opuncer;
11. Update Ey(Aspread);
12. Goto A;
13. B: end if

*iii) Modeling Selfish Behavior*

The proposed scheme does not limit the phenomenon of selfishness being exhibited by the NN in some stages of the process which ordinarily should always reveal collaboration. Existence of selfish mobile nodes is being considered, wherein it is assumed that certain NN may choose to behave selfishly at certain instances. Selfishness may be exhibited due to two reasons; either the mobile nodes tries to behaverationally to save its resources or otherwise there may exists some circuitry or technical issues with the NN at particular instances of time. However in both the cases the end result is common the NN refuse to take part in the surveillance process management leading to model crash and thus adopt an action of decline (Adec). We shall not be going to the sophistication of why the mobile nodes are exhibiting selfishness rather try to capture the selfishness as a discrete quantity in our mathematical model. Although, some NN may behave selfishly only at some events but it doesn't mean it has a consistent harmful intention for deteriorating the surveillance process management system in a simulation area. It needs to be clearly understood that there is no degree of selfishness that can approximate the malevolent behavior demonstrated by the AN.

In the proposed system the behavior of mobile nodes is completely governed by the strategy they are adopting. So the selfishness characteristic also needs to be imposed upon the strategies alone. It was
shown in Table 5.1 that /SF/ signifies the degree of selfishness exhibited by an NN. /SF/ represents the possibility of a NN adopting decline strategy Adec when it should have actually cooperated (Acop) based on its current beliefs it is holding.

Embedding selfishness into the strategies of NN:
Pure strategy will become: Acop with a probability of (1-/SF/)
Mixed Strategy will become: Acop with a probability of (1-/SF/). ((Crisk - Ccop) / Grisk)

*Algorithm for Proposed strategy for surveillance of malicious behavior*
1. A: if ? (1- Opuncer) ? (F + Crep) / (Grep + F)
2. Report /x/ as AN by adopting Arep;
3. goto B;
4. else
5. if ? ? (Gcop-Ccop) / (Gcop + Grisk)
6. Adopt Acop with a probability of /SF/;
7. else
8. Adopt Acop with a probability of /SF./ ((Crisk - Ccop) / Grisk);
9. end if
10. Updated ?cop and ?drop to evaluate new values for ? and Opuncer;
11. goto A;
12. B: end if

The above formation leads to two implications. One the NN only exhibit selfishness while playing the cooperate strategy Acop. They never exhibit selfishness when they want to report the other mobile nodes proved inefficient by adopting Arep. This is because otherwise the players (mobile nodes) will no longer be completely rational. This is also in line with the definition of selfishness that the NN are rational while controlling the process for software development methodologies. Second if the NN is assumed to be always collaborative i.e. the selfishness factor /SF/ is zero then actually there is no change in strategies.

*5.5. RESULTS ANALYSIS*

This section will discuss about the outcomes accomplished from the simulation study. Before, looking into the outcomes accomplished from the study, let us look closely to the assumptions being made for the proposed model.

The main assumption of this model is as follows:
. It is assumed that AN are also rational concerning their goals modeled perfectly without showing signs of selfishness during any stage of the process.
. It is assumed that mobile nodes by means of passive observation can track the scrum logs of the organizational as well as cluster issues.
. It is assumed that the error in observation may occur but with very low probability. Otherwise, it would be impossible to distinguish a AN by cluster monitoring.
. It is assumed that when AN switches from the cluster in which it conducted financial loss (owing to inefficient decision), it will also erase all its transaction history in that cluster with it thus making the detection process extremely difficult.
. It is assumed that mobile nodes trust can't be monitored outside the cluster.
. It is assumed that time is divided into slots and each slot represents a stage processing itself.

*Figure 5.3 Implementation Schema*
The above Figure 5.3 shows the technique adopted for implementing the proposed system using Matlab on normal 32 bit machine. The analysis of the outcome of the proposed study is carried out considering packet drop attack. The normal node involved in the proposed system is considered to perform cooperation in forwarding the data packet from one to another node and actively monitors the malicious behavior of the other mobile nodes. The simulation is carried out on 1500 x 1500 m2 considering 300 mobile nodes using random waypoint mobility model. The simulation study also considers presence of 3 to 9 number of clusters for enabling multiple communications among the mobile nodes.

For better effectiveness in the analysis of the proposed study, the results obtained in the proposed study are compared with that of Reddy [138] and Swetha [139]. There is a valid set of justification behind choosing the work of Reddy [138] and Swetha [139] as follows e.g. i) Reddy [138] has carried out a study where the authors have presented a typical technique to resist black hole attack in mobile adhoc network using game theory, which is very close to our proposed system. The author has evaluated the outcome of the study considering control overhead, data delivery ratio, and overhead on routing. Hence, the work done by Reddy [138] bears a strong resemblance to the proposed study and hence chosen to perform comparative analysis. ii) Swetha [139] have presented a technique of intrusion detection system on mobile adhoc network, where the outcomes of the study is found to be quite promising with respect to large scale mobile adhoc network. Hence, work done by Swetha [139] is chosen to understand the effectiveness of our protocol to understand the malicious behavior of the mobile nodes in large scale network.

*Figure 5.4. Analysis of Threat Identification*
Figure 5.4 shows the performance comparative analysis of the proposed system with respect to Reddy [138] and Swetha [139]. The outcome for
identification of independent routing attack on the similar network scenario shows that proposed system posses better detection rate as compared to that of Reddy [138] and Swetha [139].

"Figure 5.5 Analysis of Privacy Identification"

The outcome exhibited in Fig. 5.5 shows that proposed system has higher degree of potential to highlight the detection of intrusion in privacy property of the mobile nodes as compared to that of Reddy [138] and Swetha [139]. The prime reason behind this is proposed system consistently captures the malicious activities related to uncertainty and allocations of payoff, which make the system highly possible to investigate the real picture of intrusion in privacy. Hence, the proposed system can effectively track the malicious behavior of the mobile nodes using mechanism design and probability theory.

"Figure 5.6 Analysis of Processing Speed"

Any algorithm can be tested efficient, if they are found with nominal processing speed. Fig. 5.6 shows that processing speed of the proposed system for large network is around 2 minutes, which is quite low in comparison to work done by Reddy [138] and Swetha [139]. Although the mechanism design has complex algorithm policies, but it doesn't follow recursive function formulation for which purpose the system gets smarter on every round of simulation. With the incorporation of the continuous monitoring of the belief, trust, and uncertainties, the system is able to display much predictive behavior, where the increased simulation rounds were witnessed with continuous reduction in error rates as well as uncertainties. Hence, the processing time is lowered as compared to Reddy [138] and Swetha [139] where such methodology and formulation to identify threats were not being considered. Therefore, the outcomes are in agreement with time complexity of the algorithms.

"5.6 SUMMARY"

This chapter of the thesis has discussed about a novel technique to monitor the malicious behavior of the mobile nodes in mobile adhoc network. The formulation of the study is developed using Mechanism design, probability theory, as well as strategic decision making theory. The proposed system also formulates a policy which can identify the discrete behavior of the mobile nodes and can discourage them to participate in the routing process by a dynamic payoff allocation scheme. The protocol is tested on large scale network and outcomes were compared with the most existing research work to find that proposed system can effectively monitor the malicious behavior more discretely.

"CHAPTER 6"

CONCLUSION

"6.1 CONCLUSION"

The thesis work is focused on issues related to the security threats in mobile adhoc network. Our preliminary investigation has shown that from last two decades there has been increasing attention among the research community towards the issues in mobile adhoc network. There are primarily two reasons behind this:

* Reason-1:* The applications of mobile adhoc network is highly cost effective and has good response rate in various time critical and mission critical areas like defence, accident monitoring, vehicular networks, monitoring natural calamities. The thesis has discussed that mobile adhoc network renders a seamless adhoc based services to cater up the communication needs of the dynamic users on the move. Moreover, the introduction chapter of this thesis has put forward certain cases where mobile adhoc network finds a better scope in reconfigurable network, where there is a higher likelihood of integrating mobile adhoc network with upcoming technologies like OFDM, Cloud computing, and optical networking system. Hence, owing to higher scope and advantages, mobile adhoc network has received a positive attention and has attained a pivotal point of technical investigation in terms of networking.

* Reason-2:* The second reason for adoption of studies towards mobile adhoc network is the inherent characteristics of it. Chapter-1 and chapter-3 has discussed various theoretical backbone of the study where it was found that majority of the problems in mobile adhoc network is caused due to two reasons e.g. i) decentralized nature of the network, and ii) dynamic topology. We have also seen that owing to decentralized nature of such network, it gives rise to various quality of services issues as well as security threats. However, our focus of this thesis is towards security threats. Network security is the prominent area of attention on any investigation towards wireless network, and security threats are possibly very high on the adhoc based network. Chapter-2 has discussed about various literatures where it was seen that till date there are numerous research attempts towards mitigating security threats, but still it is one of the unsolved area of security in mobile adhoc network.
Hence the proposed study performs an in-depth review of literatures and extracted a research gap, where it is search that presented techniques towards ensuring maximum security is not sufficient. Therefore, we introduce a technique where every communicating mobile nodes must get themselves authenticated using standard cryptographic measures for optimal data security. Discussion of the proposed authentication system is elaborated in Chapter-4 of this thesis. Moreover, it was sense that it is quite challenging task to understand the malicious behavior of the mobile nodes owing to the decentralized nature of network as well as potentially stronger malicious program. Hence, we have proposed a technique which uses mechanism design to understand the malicious behavior of a node mobile and performs strategic decision making for performing secure data transmission by identifying the malicious node. Chapter-5 has discussed about this technique that is mainly meant to perform an effective surveillance of malicious nodes in large scale mobile adhoc network. The next section will discuss the thesis contribution.

6.2 THESIS CONTRIBUTION

The prime contributions of the proposed thesis are as follows:

* Secure Authentication Mechanism*: The proposed system has introduced multiple formulations of the algorithms to ensure i) secure authentication and ii) effective monitoring of malicious behavior. The algorithm designed for secure authentication has used standard cryptography as well as digital signature but in completely different fashion. It is assumed that inclusion of the cryptographic hash function calls for iterative encryption mechanism, which may increase the algorithm complexity with respect to time and storage. However, in our demonstration, the algorithm is found with very minimal time complexity as well as from storage viewpoint, it is more negligible as it only stores few information of the mobile nodes e.g. node id, transmission range, etc. Majority of the other variables are evaluated on the run time and hence there is no necessity of performing storage. Hence, it can be said that the suggest algorithm can be utilize on any low-powered embedded devices with as surety of secure authentication mechanism.

* Effective Mathematical Modelling*: Effective mathematical modelling always assists in understanding the assumptions and how far the assumptions are sustained in multiple test scenarios. Hence, the proposed system adopts the usage of mechanism design, probability theory, and strategic decision making that ensures an effective surveillance of the malicious nodes. The thesis has presented a mathematical modelling, where it is highlighted that it is quite a difficult task to identify regular and malicious nodes. The mathematical modelling used in the thesis has presented various strategies which can be possibly adopted by either regular node, or selfish node, or malicious nodes. Hence, when the random simulation is allowed to happen, the outcome found that malicious nodes do have significant characteristics that can be utilize in future for designing intrusion prevention system. One of the unique assistance in this case is that we have not attempted to work on prevention system as it is felt that our prevention policy might go stale if the adversarial module updates their malicious programs. Moreover, working on prevention system also might narrow down our contribution to only specific type of attacks. Therefore, by visualizing this fact, we have concentrated on manipulative such a mechanism where irrespective of any types of attackers, the proposed thesis can provide a solution to identify it. The proposed solution is therefore highly cost effective and is applicable to all the major threats applicable in mobile adhoc network. Till date, majority of the solutions towards security is focused on specific type of attack, whereas, we choose to design a technique, where our system is more interested to capture the adversarial tactics.

6.3 FUTURE WORK

The direction of the future work will be as follows:

1. At present, the proposed work has made a balance between cryptography and probability theory. Our future direction of the work will be to check the possibility of ensuring enforceability of the sender node to further strengthen the privacy protocol. It can be done using elliptical curve cryptography by enhancing various signatures scheme. Moreover, future work will be also to check the usage of ElGamal signature scheme to investigate enforceability. This will further strengthen the cryptographic approach and ensure more potential encryption scheme.

2. The proposed study has used graph theory, but to a slight extent. We have used bilinear map as a part of cryptography in the secure authentication mechanism. However, more security can be incorporated to enhance the data delivery rate using network traffic flow concept. Our future direction of work will be also to check usage of tree-based concept as well as advance graph theory like Menger’s Algorithm. Such technique can be utilized to highly ensure the data delivery process and also perform dual check on the data redundancies. The malicious nodes may possible use the redundant path to invoke an attack and therefore formulations of graph cut theory can possibly enhance the identification of the routes that are being used by the malicious nodes.