EXTENDED SCALABLE AND SECURED VIRTUAL INFRASTRUCTURE FOR MOBILE ADHOC NETWORK

A THESIS

Submitted

in partial fulfillment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

IN THE DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

By

KESAVAN R

(SP08 EI DA11)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

St. PETER'S INSTITUTE OF HIGHER EDUCATION AND RESEARCH

ST. PETER'S UNIVERSITY

CHENNAI 600 054

DECEMBER 2013

DECLARATION

Certified that the thesis entitled “**Extended Scalable and Secured Virtual Infrastructure for Mobile Ad hoc Network**” is the bonafide record of independent work done by me under the supervision of Dr**. V.Thulasi Bai,** Professor, Department of Electronics & Communication Engineering, Prathyusha Institute of Technology and Management, Thiruvallur-602025. Certified further that the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred earlier.

Mr. R. KESAVAN

Dr. V. THULASI BAI

SUPERVISOR
Professor, Dean (R&D)
Department of Electronics & Communication Engineering,
Prathyusha Institute of Technology &Management,
Chennai, Tamilnadu, India.

Place :

Date :

CERTIFICATE

I hereby certify that the thesis entitled "**Extended Scalable and Secured Virtual Infrastructure for Mobile Ad hoc Network**" submitted to the St. Peter's University, for the award of Degree of Doctor of Philosophy is the record of research work done by the candidate **Mr. R. Kesavan** under my guidance and that the thesis has not formed previously the basis for the award of any degree, diploma, associateship, fellowship or other similar titles.

Place:
Date:

Dr. V. THULASI BAI
SUPERVISOR,
Professor, Dean (R&D)
Department of Electronics &
Communication Engineering,
Prathyusha Institute of Technology
&Management,
Chennai, Tamilnadu, India.

ACKNOWLEDGEMENT

At the outset I would like to thank and express my appreciation to **Dr. (Mrs) T. Banumathy, Chancellor,** who has given me an opportunity to develop my skills as a researcher and pursue my interests in the field of VLSI and signal processing. I would also like to thank **Prof. Dr. D. S. Ramachandramurthy, Vice Chancellor** (officiating) for his whole hearted support and guidance during the entire course of research. I sincerely **thank Dr. M. Shanmugam, Registrar** & COE and **Prof. Dr. S. Gunasekaran, Dean (R & D)** for their advice and guidance. I am grateful for their help and suggestions during the preparation of the thesis. I would like to thank the Management and Staff of the St. Peter's University for supporting me during my course of research and providing the necessary infrastructure whenever needed.

I am grateful to my supervisor **Dr. V. Thulasi Bai** for her unflinching support and guidance. She has been a constant source of inspiration and guidance for me at all levels in my professional path.

I would like to thank my wife, my parents and my friends for their encouragement and motivation right through the duration of my research work and preparation of the thesis. At the last but not least, I would like to express my gratitude to the GOD, the almighty.

KESAVAN R

ABSTRACT

A Mobile Ad hoc NETwork (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. For the past few years, wireless technology is growing rapidly for the day to day activity of human lives in the form of cellular phones, wireless LAN, Bluetooth, location systems, smart homes and many more.

In general, the wireless communication has divided as two types, 1) Infra-structure based wireless communication and 2) Distributed Mobile Ad hoc Wireless communication. In which, the MANET is applied wide spread across the world in many different applications such as vehicular network, location based services, monitoring and controlling of disaster, border security, under sea gas pipelines.

There are enormous research issues in the MANET, which includes optimal routing, traffic engineering, transmission control protocol, security and virtualization. The virtualization is a major research issue for the past few decades. Hence, this research work concentrates on virtualization of MANET. Virtual infrastructure provides many advantages to the users like simplicity, effective project development, potentially hostile free environment. The fixed

infrastructure may be costly and impractical for huge applications. The virtualization of MANET has two major requirements, 1) Clustering and 2) Security. This thesis concentrates on these research issues and proposed optimal methodologies.

The major requirement of wireless clustering is energy efficient techniques. Hence, an energy efficient clustering with effective node deployment is proposed in this thesis. Similarly, the major requirement of security is dynamic and effective group key management, hence dynamic group key management based security model is proposed in this thesis.

A flat or cluster less MANET architecture has an inherent scalability limitation in terms of achievable network capacity. It is seen that when the network size increases, per node throughput of an ad hoc network rapidly decreases. This is due to the fact that in large scale networks, a flat structure of networks results in long hop paths which are prone to breaking. There are some specific virtual power capable nodes functionally more capable than ordinary nodes.

Hence, the proposed work applies Artificial Bee Colony (ABC), which has been a recently developed swarm intelligence technique that proves as an optimization technique for many engineering problems. The ABC broadly is applied to many engineering applications in the literature. The proposed energy efficient clustering using ABC has proved better clustering model than the existing traditional clustering techniques.

The security issues in MANET are more challenging than those in the traditional wired computer networks and the Internet. Providing security in MANET is more difficult than in the other networking due to the resource limitations of wireless nodes. Most wireless networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored.

Moreover, the wireless communication employed by wireless networks facilitates eavesdropping and packet injection by an adversary. The combination of these factors demands security for wireless networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in wireless environments.

To ensure secrecy in MANET, messages are often encrypted using a chosen cryptographic key, which is, in the scenario of group communication, termed as group key. Only group members who know the current group key can recover the original message. Group key management means that multiple parties establish a common secret to secure dynamically.

Without relying on a central trusted entity, two people who do not previously share a common secret can create one based on the 2-party Diffie-

Hellman (DH) protocol. The DH protocol can be extended to a generalized version of n-party DH. The DH is inefficient for group of wireless nodes due to its physical characteristics.

However, more research efforts have been put into the design of a group key management protocol in the past few decades, for the sake of scalability, reliability, and security. Furthermore, group key management also needs to address the security issue related to membership changes. The modification of the membership requires refreshment of the group key. In this research work, a dynamic group key management scheme is proposed.

The performances of proposed work are analyzed on two network parameters, 1) Latency and 2) Throughput. The latency gives maximum transmission time which includes, round trip time and waiting time in the network buffer. The throughput of the network provides average data transfer during one time unit. The implementation of swarm intelligence based energy efficient ABC clustering and secured model for protecting security attacks, shows optimal result than existing methodologies.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE NO. TITLE PAGE NO.

FIGURE NO. TITLEPAGE NO.

LIST OF SYMBOLS AND ABBREVIATIONS

2G	- Second Generation
3G	- Third Generation
4G	- Fourth Generation
5G	- Fifth Generation
ABC	- Artificial Bee Colony
ACO	- Ant Colony Optimization
AODV	- Ad hoc On-Demand Distance Vector
AP	- Access Point
CGSR	- Cluster-head Gateway Switch Routing
CH	- Cluster Head
CTS	- Clear To Send
DGKMS	- Dynamic Group Key Management Scheme
DH	- Deffi-Helman
DN	- Destination Node
DoS	- Denial of Service
DRI	- Data Routing Information
EEABC	- Energy Efficient Artificial Bee Colony
EVSM	- Extended Virtual Spring Mesh
FRP	- Further Reply
FRq	- Further Request
GL	- Group Leader
IBC	- Identity Based Cryptography
ID	- Identification
IDS	- Intrusion Detection System
IMKM	- ID-based Multiple Secrets Key Management

IN	-	Intermediate Node
LAN	-	Local Area Network
LEACH	-	Low Energy Adaptive Clustering Hierarchy
MA	-	Mobile Agent
MAC	-	Medium Access Control
MANET	-	Mobile Ad hoc Network
MD5	-	Message Digest 5
ND	-	Node Deployment
NHN	-	Next Hope Node
NVS	-	Network Virtualization Substrate
PDR	-	Packet Delivery Ratio
PKG	-	Private Key Generator
PSO	-	Particle Swarm Optimization
QoS	-	Quality of Service
RREP	-	Route Reply
RREQ	-	Route Request
RTS	-	Ready To Send
RTT	-	Round Trip Time
SASVIS	-	Scalable and Secured Virtual Infrastructure
SI	-	Swarm Intelligence
TA	-	Target Authority
TCP	-	Transmission Control Protocol
TTP	-	Time Triggered Protocol
UDP	-	User Datagram Protocol
VN	-	Virtual Network
VSM	-	Virtual Spring Mesh
WN	-	Wireless Node
WSN	-	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Wireless Network

Wireless technology has been growing rapidly in day to day usage.A wireless local area network that uses radio waves as its carrier.The last link with the users is wireless, to give a network connection to all users in a building or campus. Wireless LANs operate in almost the same way aswired LANs, using the same networking protocolsand supporting the most of the sameapplications.

Wireless communication has many segments such as Infra-structure based wireless communication, ad hoc wireless communication; satellite based wireless communication, and wireless local area network (Gazis et al 2005, Surachai et al 2010). Ad hoc network is applied widespread across the world in many different applications, which include all major engineering systems.

Cellular communication has introduced packet switching in addition to circuit switching in the Second Generation (2G) and it extends the features such as multimedia service in the 2.5G, video conferencing in Third Generation (3G) and internet protocol addressing based networking in the

Fourth Generation (4G) (Bin Xie et al 2008). It is in progress to extend its capability through the Fifth Generation (5G) and it is also referred to as next generation network (Xiaohua et al 2010).

Internet access through the cellular communication has increased rapidly over the last few years. It is due to the flexibility in the handling, mobility, reduced installation time, comparatively lower initial cost and nil maintenance cost on the user perception.

802.11 is a member of the IEEE 802 family, which is a series of specifications for local area network (LAN) technologies. IEEE 802 specifications are focused on the two lowest layers of the OSI model because they incorporate both physical and data link components. All 802 networks have both a MAC and a Physical (PHY) component.

The MAC is a set of rules to determine how to access the medium and send data, but the details of transmission and reception are left to the PHY. Individual specifications in the 802 series are identified by a second number. For example, 802.3 is the specification for a Carrier Sense Multiple Access network with Collision Detection (CSMA/CD), which is related to (and often mistakenly called) Ethernet, and 802.5 is the Token Ring specification.

Other specifications describe other parts of the 802 protocol stack. 802.2 specifies a common link layer, the Logical Link Control (LLC), which can be used by any lower-layer LAN technology. Management features for 802 networks are specified in 802.1. Among 802.1's many provisions are bridging (802.1d) and virtual LANs, or VLANs (802.1q).

802.11 is just another link layer that can use the 802.2/LLC encapsulation. The base 802.11 specification includes the 802.11 MAC and two physical layers: a frequency-hopping spread-spectrum (FHSS) physical layer and a direct-sequence spread-spectrum (DSSS) link layer. Later revisions to 802.11 added additional physical layers. 802.11b specifies a high-rate direct-sequence layer (HR/DSSS); products based on 802.11b hit the marketplace in 1999 and make up the bulk of the installed base. 802.11a describes a physical layer based on orthogonal frequency division multiplexing (OFDM); products based on 802.11a were released as this book was completed.

The use of radio waves as a physical layer requires a relatively complex PHY, as well. 802.11 splits the PHY into two generic components: the Physical Layer Convergence Procedure (PLCP), to map the MAC frames onto the medium, and a Physical Medium Dependent (PMD) system to transmit those frames.

When several access points are connected to form a large coverage area, they must communicate with each other to track the movements of mobile stations. The distribution system is the logical component of 802.11 used to forward frames to their destination. 802.11 does not specify any particular technology for the distribution system.

In most commercial products, the distribution system is implemented as a combination of a bridging engine and a distribution system medium, which is the backbone network used to relay frames between access points; it is often called simply the backbone network. In nearly all commercially successful products, Ethernet is used as the backbone network technology.

Frames on an 802.11 network must be converted to another type of frame for delivery to the rest of the world. Devices called access points perform the wireless-to-wired bridging function. (Access points perform a number of other functions, but bridging is by far the most important.). To move frames from station to station, the standard uses a wireless medium.

Several different physical layers are defined; the architecture allows multiple physical layers to be developed to support the 802.11 MAC. Initially, two radio frequency (RF) physical layers and one infrared physical layer were standardized, though the RF layers have proven far more popular.

Networks are built to transfer data between stations. Stations are computing devices with wireless network interfaces. Typically, stations are battery-operated laptop or handheld computers. There is no reason why stations must be portable computing devices, though. In some environments, wireless networking is used to avoid pulling new cable, and desktops are connected by wireless LANs.

Access points are used for all communications in infrastructure networks, including communication between mobile nodes in the same service area. If one mobile station in an infrastructure BSS needs to communicate with a second mobile station, the communication must take two hops. First, the originating mobile station transfers the frame to the access point. Second, the access point transfers the frame to the destination station.

With all communications relayed through an access point, the basic service area corresponding to an infrastructure BSS is defined by the points in which transmissions from the access point can be received. Although the multi-hop transmission takes more transmission capacity than a directed frame from the sender to the receiver, it has two major advantages:

- An infrastructure BSS is defined by the distance from the access point. All mobile stations are required to be within reach of the access point, but no restriction is placed on the distance between mobile stations themselves. Allowing direct communication between mobile stations would save transmission capacity but at the cost of increased physical layer complexity because mobile stations would need to maintain neighbour relationships with all other mobile stations within the service area.

- Access points in infrastructure networks are in a position to assist with stations attempting to save power. Access points can note when a station enters a power-saving mode and buffer frames for it. Battery-operated stations can turn the wireless transceiver off and power it up only to transmit and retrieve buffered frames from the access point.

In an infrastructure network, stations must associate with an access point to obtain network services. Association is the process by which mobile station joins an 802.11 network; it is logically equivalent to plugging in the network cable on an Ethernet. It is not a symmetric process. Mobile stations always initiate the association process, and access points may choose to grant or deny access based on the contents of an association request.

Associations are also exclusive on the part of the mobile station: a mobile station can be associated with only one access point. The 802.11 standard places no limit on the number of mobile stations that an access point may serve.

Every frame sent by a mobile station in an infrastructure network must use the distribution system. It is easy to understand why interaction with hosts on the backbone network must use the distribution system. After all, they are connected to the distribution system medium. Wireless stations in an infrastructure network depend on the distribution system to communicate with each other because they are not directly connected to each other.

The only way for station A to send a frame to station B is by relaying the frame through the bridging engine in the access point. However, the bridge is a component of the distribution system. While what exactly makes up the distribution system may seem like a narrow technical concern, there are some features of the 802.11 MAC that are closely tied to its interaction with the distribution system.

1.1.1 Design Requirements for Wireless Network

In order to design robust wireless networks, the following group of important problems mentioned below have found solutions:

- **Manageability:** Wireless networks are frustratingly opaque. This leads to long delays in resolving performance and connectivity problems, as well as high manageability costs. The state of the art will be significantly enhanced by a management infrastructure for wireless networks that diagnoses problems with minimum human intervention and informs the user of ways to recover (Peter et al, 2007).

- **Capacity:** Although the bandwidth of wireless networks is steadily increasing, capacity is still a bottleneck for many applications. Any scheme that increases wireless capacity, through advanced antennas and smarter protocols will greatly impact the wireless performance of a number of applications (Toh, 2009).

- **Power Management:** Limited battery power is the Achilles heel for wireless applications. Applications and protocols for mobile computing should prolong battery life by using schemes such as maximizing sleep durations of wireless nodes, using transmit power control, or avoiding multiple wireless interfaces (Siva and Manoj, 2000).

1.1.2 Research Issues in Wireless Network

Some of the research issues (Chowdhury and Boutaba 2009, Xin Li et al 2009) in the wireless network are listed below:

- Virtualization
- Security
- Traffic Management
- Optimal routing protocols
- Providing Quality of Service

- Offering reliable services,
- Load balancing
- Transport Control Protocol (TCP)
- Effective Medium access scheme,
- Energy management,
- Scalability,
- Efficient node deployment,
- Self-organization and service discovery

When too many packets are present in the subnet or a part of subnet, the performance degrades the characteristics and functionalities of the network. This situation is called congestion (Tanenbaum 1998). Avoiding congestion and network traffic is the field of study which is termed as traffic management. Traffic management (Larry and Bruce 2000) is divided into three major sub-divisions which are Congestion Avoidance, Congestion control and flow control.

The routing protocol lies in the network layer, the task of wired routing protocol may be exchanging route information and finding feasible path, but in the wireless routing there are some more tasks added to meet the wireless environment which includes minimum power requirement, utilizing minimal network resources like bandwidth, gathering and updating link failures. Therefore, in order to provide optimal routing in the wired cum wireless environment, routing protocols need to fulfil the following major challenges and requirements.

In any network, Quality of Service (QoS) is an important parameter for evaluating the performance of the particular network. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results. Elements of network performance within the scope of QoS often include availability, throughput, latency and error rate. QoS is especially more important for the new generation of Internet applications such as Voice over Internet Protocol, video-on-demand and other consumer services. An optimal routing will satisfy the above listed attributes of the QoS (Budyal et al, 2013).

Reliability is an important metric in the performance evaluation of all types of networks. Reliability of a particular network (Pin and Li, 2013) ensures user satisfaction through higher packet delivery ratio and avoiding the smaller number of packet loss. Reliability is more important for the emergency engineering services, as it involves real time data communication. Emergency engineering services are categorized as hard real time application, in which a small amount of data loss will lead to heavy loss. Reliability and congestion control are inter-dependent issues.

Load balancing in the network will improve network efficiency and also the QoS. It will meet two types of critical situations, which are heavy load on particular links and the idle load on some other links. Heavy load in a particular network will lead to heavy packet loss and as a consequence, the network has fewer throughputs, less reliability and poor QoS. In the other links, some of the links in the subnet are always idle. If the loads are balanced, then every links in the subnet will provide reliable communication and improved QoS (Sedaghat et al, 2012).

This thesis concentrates on the virtualization and security, proposes the solution through optimal methodologies. The overviews of these two issues, virtualization and security are briefly discussed in the following section.

1.2 Overview of Virtualization

Virtualization of wireless network will provide following features, which are unavailable in a simple wireless network (Chandra, 2006):

- **Concurrent Connectivity:** A user can connect to multiple wireless networks by specifying a list of networks.

- **Network Elasticity:** The range of an infrastructure network can be extended if border nodes use virtual infrastructure to function as relays for authorized nodes that are outside the range of the Access Point (AP) (Katranaran et al, 2011).

- **Gateway Node:** A node that is part of a wireless ad hoc network and close to an AP, connected to the Internet, can use Virtual infrastructure to stay connected on both networks, and become a gateway node for the ad hoc network (Berenbrink et al, 2009).

- **Network Security:** Different groups like human resources personnel, secretaries, developers within a company may be given different permissions to access data servers. These servers could be on physically different networks. A privileged user, who has permission to access different networks, can use virtual infrastructure to simultaneously connect to multiple networks (Chan, 2012).

- **Increased Capacity:** The capacity of ad hoc networks can be increased if nodes within interference range communicate on orthogonal frequency channels (Khan et al, 2012).

- **Seamless Roaming:** The time to handoff from one AP to another is a significant overhead in mobile wireless networks. Virtual infrastructure allows a wireless node to connect to an AP without disconnecting from its previous one (Nestinger et al, 2010).

A virtualized physical wireless node appears as a multiple virtual network interfaces, where each virtual interface corresponds to a physically different wireless network. Further, virtual infrastructure also strives to achieve the following design goals when virtualizing a wireless node:

- **Transparency:** To reduce the learning curve in using the system, virtual interfaces are used appear as physical wireless nodes to the user. The user should be able to connect different virtual nodes to different wireless networks, although the node is only on one network at any instant. The architecture should ensure that packets sent to and from a virtual interface are not discarded if the node is not on the corresponding network at that instant. Further, when a machine is mobile, the virtual interface should appear disconnected when the machine moves out of the range of the network. However, it should appear connected when the machine moves back in the network range (Dey and Datta, 2012).

- **Performance:** The system should give the illusion of simultaneous connectivity on all virtual interfaces. Packet delays on a virtual interface should be minimized. The user should also be able to prioritize different virtual interfaces, so that packets on a more important network are sent and received with lesser delay (Di and Mouffah, 2000).

- **Deployability:** The system should be easy to deploy in an existing wireless network. It should work over the commonly used IEEE 802.11 standard, and with commercial wireless nodes. Nearly all of the modifications should be on the user's machines (Bravo-Torres et al, 2012).

1.2.1 Virtual Infrastructure

Virtual infrastructure provides many of the advantages of a fixed infrastructure, in terms of simplicity and algorithm development, while simultaneously tolerating an ad hoc, potentially hostile environment in which fixed infrastructure may be overly costly and impractical. There are two types of virtual infrastructure are defined, 1) virtual objects and 2) virtual nodes (Ma and Tsai, 2008).

Much like virtual objects, virtual nodes are designed to be more reliable than the individual mobile nodes in the underlying network. As long as some real nodes reside near the virtual node, it can continue to operate. If a virtual node fails (due to regional depopulation), it can recover, if mobile nodes again return to the region near the virtual node (Liang and Yu, 2010).

Moreover, a virtual node may be mobile, travelling on a predictable path through the network. The basic idea of executing algorithms on virtual mobile nodes (in contrast to static virtual infrastructure) was inspired by the development of compulsory protocols.

Each virtual infrastructure component is emulated by a set of replicas that reside near the actual location of the virtual object or node. As real devices move towards and away from the virtual component, and as real devices join and leave the system, the set of replicas changes continuously. In particular, a device is able to examine its current location and determines whether to join or leave the emulation, the use of hysteresis may well improve efficiency (Salmanian et al, 2011).

In order to maintain consistency, each replica must apply updates in the same order. One way to achieve this is to use a (local) totally ordered broadcast service that ensures that messages sent within a specific region the area of emulation of the virtual component are delivered in the same order to all active participants. When the network guarantees reliable and timely communication, it is possible to build a totally ordered communication service using timestamp-based techniques in the context of fixed-infrastructure replicated state machines.

When a node joins the emulation, it first requests a copy of the replicated state and at the same time begins participation in the totally ordered broadcast service. On receiving a copy of the replicated state, the new node can update the state (adjusting for changes that may have occurred while the replica message was in transit) and begin participating in the emulation. Unfortunately, collisions and message loss may disrupt communication, making it difficult to implement a totally ordered broadcast (Pushpalakshmi et al,2011).

In particular, the timestamp-based techniques for totally ordering messages do not adapt well to such an environment. Since it is difficult to determine when everyone has received a particular message. Most other prior techniques for implementing replicated-state machines, also do not adapt well to a wireless environment. For example, may require all the participants to communicate. In a wireless setting, the increased communication will results in increased rates of collision (JongpilJeong, 2011).

Virtual infrastructure is useful only when the virtual components perform efficiently with low latency. For each algorithm implementing virtual infrastructure, the conditional performance should be analysed.

1.2.2 *Virtual Objects*

A virtual object is akin to a reliable storage unit deposited at some known location in the network. Each real node, i.e., client, can store and retrieve information from the virtual object. The object can implement any “variable type,” and supports atomic invoke/response semantics.

A virtual object is (relatively) reliable, even though the set of real nodes that reside near—and implement—the object may be continuously changing. As long as some real nodes reside near the virtual object, it can continue to operate. Virtual objects generalize some of the previously mentioned approaches for location-aware data storage.

The most basic type of virtual infrastructure introduced in this thesis consists of virtual objects. A virtual object is akin to a reliable storage unit deposited at some known location in the network. Each real node, i.e., client, can store and retrieve information from the virtual object. The object can implement any “variable type,” and supports atomic invoke/response semantics.

A virtual object is (relatively) reliable, even though the set of real nodes that reside near and implement the object may be continuously changing. As long as some real nodes reside near the virtual object, it can continue to operate. Virtual objects generalize some of the previously mentioned approaches for location-aware data storage (Maiev et al, 2007).

1.2.3 *Virtual Nodes*

A virtual node is a natural extension of a virtual object. Instead of simply storing data and passively responding to requests, the virtual node can process data, send messages, and initiate actions. A virtual node resembles a reliable server, that is, a piece of computing infrastructure residing at some well-known location.

Clients can send and receive messages to and from the virtual node, just as they would interact with a real device. If they are near to the virtual node, they may communicate with it via “local broadcast” communication; if the virtual node is farther away, they may communicate using a GeoCast service.

Similarly, the virtual nodes may communicate with each other. Each virtual node is an arbitrary I/O automaton (without tasks or fairness), and thus can execute any arbitrary (untimed) program. Much like virtual objects, virtual nodes are designed to be more reliable than the individual mobile nodes in the underlying network.

As long as some real nodes reside near the virtual node, it can continue to operate. If a virtual node fails (due to regional depopulation, say), it can recover if mobile nodes again return to the region near to the virtual node. Moreover, a virtual node may be mobile, traveling on a predictable path through the network. The basic idea of executing algorithms on virtual mobile nodes (in contrast to static virtual infrastructure) was inspired by the development of compulsory protocols.

The basic observation in compulsory protocols is that if mobile nodes moved in a programmable way, algorithms could take advantage of the motion, providing elegant and simple solutions. They present an efficient compulsory protocol for leader election. Using virtual mobile nodes, it is possible to take advantage of compulsory protocols even in networks where the underlying mobile nodes in fact do not behave in the desired manner.

1.3 Overview of Wireless Security

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Wireless Mobile Ad hoc Networks (MANETs) and wireless networks have many applications in used for various fields. Many wireless networks have mission-critical tasks.

Security is critical for such networks deployed in hostile environments, security concerns remain a serious impediment to widespread adoption of these wireless networks.

The security issues in MANETs are more challenging than those in traditional wired computer networks and the Internet. Most wireless networks actively monitor their surroundings and it is often easy to deduce information other than the data monitored. Such unwanted information leakage often results in privacy breaches of the people in the environment (John and Samuel, 2010).

Moreover, the wireless communication employed by wireless networks facilitates overhearing and packet injection by an adversary. The combination of these factors demands security for wireless networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in wireless environments. Significant efforts and research have been undertaken to enhance security levels of wireless networks.

Security in wireless networks is complicated by the constrained capabilities of wireless node hardware and the properties of the deployment, which includes (Li and Xiang-Gen, 2008):

- The overall cost of the wireless node should be as low as possible
- Wireless nodes are susceptible to physical capture, but due to their targeted low cost, tamper-resistant hardware are unlikely to prevail. Wireless Node (WN) use wireless communication, which is

particularly easy to eavesdrop on. Similarly, an attacker can easily inject malicious messages into the wireless network.

- Advanced anti-jamming techniques such as frequency- hopping spread spectrum and physical tamper proofing of nodes are generally impossible in a wireless network due to the requirements of greater design complexity and higher energy consumption.

- The use of radio transmission along with the constraints of small size, low cost and limited energy make WN more susceptible to denial-of-service attacks.

- Ad-hoc networking topology of WN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes etc.

- Security also needs scale to large-scale deployments. Most current standard security protocols were designed for two-party settings and do not scale to a large number of participants.

- There is a conflicting interest between minimization of resource consumption and maximization of security level. A good solution actually gives a good compromise between these two.

- Since wireless nodes usually have severely constrained, asymmetric cryptography is often too expensive for many applications. Thus, a promising approach is to use more efficient symmetric cryptographic alternatives. Instead, most security schemes make use of symmetric key cryptography. One thing required in either case is the use of keys for secure communication.

- Managing key distribution is not unique to WN, but again constraints such as small memory capacity make centralized keying techniques impossible.

1.3.1 Security Requirements

The analysis of security and survivability requirements concern the design goals of scalability, efficiency, key connectivity, resilience and reliability. Security services include the following (Raji and Ladani, 2010):

- **Authentication** ensures that the other end of a connection or the originator of a packet is the node that is claimed. Access-control prevents unauthorized access to a resource.

- **Confidentiality** protects overall content or a field in a message. Confidentiality may also be required to prevent an adversary from undertaking traffic analysis.

- **Privacy** prevents adversaries from obtaining information that may have a private content. Private information may be obtained through analysis of traffic patterns, i.e. frequency, source node, routes, etc. Ensures that a packet is not modified during transmission is known as **Integrity**.

- **Authorization**: authorizes another node to update information (import authorization) or to receive information (export authorization).

- **Anonymity** hides the source of a packet or frame. It is a service that can help with data confidentiality and privacy.

- **Non-repudiation** proves the source of a packet. In authentication the source proves its identity. Non-repudiation prevents the source from denying that it sent a packet.

- **Freshness** ensures that a malicious node does not resend previously captured packets.

- **Availability** mainly targets Denial of Service attacks and is the ability to sustain the networking functionalities without any interruption due to security threats.

- **Resilience** to attacks is required to sustain the network functionalities when a portion of nodes is compromised or destroyed. In Forward secrecy a wireless should not be able to read any future messages after it leaves the network. In Backward secrecy a joining wireless should not be able to read any previously transmitted message.

- **Survivability** is the ability to provide a minimum level of service in the presence of power loss, failures or attacks. Ability to change security level as resource availability changes is the Degradation of security services.

1.3.2 Security Metrics

The following metrics are suggested to evaluate the appropriateness of security scheme for WN (Gazdan et al, 2011):

- **Security Model:** a security scheme has to meet the requirements discussed above.

- **Resiliency:** in case a few nodes is compromised, a security scheme should still protect against the attacks.

- **Energy efficiency:** a security scheme must be energy efficient so as to maximize node and network lifetime.

- **Flexibility:** key management needs to be flexible.

- **Scalability:** a security scheme should be able to scale without compromising the security requirements.

- **Fault-tolerance:** a security scheme should continue to provide security services in the presence of faults such as failed nodes.

- **Self-healing:** One of the wireless nodes may fail or run out of energy. The remaining wireless nodes may need to be reorganized to maintain a set level of security.

- **Assurance:** assurance is the ability to disseminate different information at different levels to end-users. A security scheme should offer choices with regard to desired reliability, latency, and so on.

The individual node evaluation metric scan be linked to the system performance metrics down to the individual node characteristics that support them. The end goal is to understand how changes to the low-level system architecture impact application performance (Gomathi and Gandhi, 2011).

- **Robustness:** In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible. System modularity is a powerful tool that can be used to develop a robust system.

- **Security:** In order to meet the application level security requirements, the individual nodes must be capable of performing complex encrypting and authentication algorithms. In addition to securing all data transmission, the nodes themselves must secure the data that they contain.

- **Communication:** A key evaluation metric for any WN is its communication rate, power consumption, and range. Higher communication rates translate into the ability to achieve higher effective sampling rates and lower network power consumption. As bit rates increase, transmissions takes less time and therefore potentially require less energy.

- **Computation:** The two most computationally intensive operations for a wireless node are the in-network data processing and the management of the low-level wireless communication protocols. Higher communication rates required faster computation. The same is true for processing being performed on wireless data.

- **Time Synchronization:** In order to support time correlated wireless readings and low-duty cycle operation of our data collection application scenario; nodes must be able to maintain precise time synchronization with other members of the network. Errors in the timing mechanism will create inefficiencies that result in increased duty cycles.

- **Size & Cost:** The physical size and cost of each individual wireless node has a significant and direct impact on the ease and cost of deployment. Total cost of ownership and initial deployment cost are two key factors that will drive the adoption of WN technologies. Physical size also impacts the ease of network deployment. Smaller nodes can be placed in more locations and used in more scenarios.

1.3.3 Security Attacks

The potential attacks are classified into five categories (Zheng et al, 2010):

- **Jamming Attacks -** A jamming attack occurs in the physical layer and injected to disturb sensor node communication and the transmission of messages

- **Black hole attacks -** A black hole attack appears in the network and routing layer. When it is injected, a compromised node sends messages to its neighbouring nodes, in order to transmit packets to destinations using minimal routing. However, when it receives packets from its neighbouring nodes, it may be deleted or stored in a temporary buffer. In the sender scenario, it will appear that they are sending packets into a black hole for transmission.

- **Power or Flooding attacks -** A flooding attack arises in the transport layer, leading to power supply failure. In a flooding attack, an attacker sends many message packets asking the system to establish a connection with a node, eventually exhausting its power in the process.

- **De-synchronization attacks -** A de-synchronization attack lies in the transport layer. An attacker widely broadcasts some forged packets to fake a connected message with another node or between any two peer nodes. The attacker inserts numbers in various sequences into the packet, so the receiving node actively requests that the other node send the last packet again. This type of attack jams the network and causes power overload.

- **Capture attacks -** Preventing capture attacks are difficult, if nodes are not tamper-proof and the environment is left unattended.

Most of the above attacks are eliminated using an authentication mechanism. The Intrusion Detection System (IDS) is a well-known authentication mechanism, which can be divided into two types, viz., anomaly detection and misuse detection. The anomaly detection is able to identify new types of attack but it may raises false alarms in some environment. The misuse detection is unable to identify new types of attacks, but it has a high correct-detection rate for known types of attacks (Dey et al, 2011).

1.4 Motivation

In the proposed research work, security and clustering are focused for ad hoc virtual infrastructure, as these are major research issues on effective virtualization of MANET. In clustering, energy efficient clustering with effective node deployment is proposed. In security, dynamic group key management based security model is proposed.

To ensure secrecy in MANET, messages are often encrypted using a chosen cryptographic key, which, in the scenario of group communication, is termed as group key. Only group members who know the current group key can recover the original message. Group key management means that multiple parties establish a common secret to secure dynamically. Without relying on a central trusted entity, two people who do not previously share a common secret can create one based on the 2-party Diffie-Hellman (DH) protocol.

The DH protocol can be extended to a generalized version of n-party DH. Research efforts have been put into the design of a group key management protocol for the sake of scalability, reliability, and security. Furthermore, group key management also needs to address the security issue related to membership changes. The modification of the membership requires refreshment of the group key. In this research work, a dynamic group key management scheme is proposed.

A flat MANET has an inherent scalability limitation in terms of achievable network capacity. It is seen that when the network size increases, per node throughput of an ad hoc network rapidly decreases (Bhagavathula et al, 2002). This is due to the fact that in large scale networks, flat structure of networks results in long hop paths which are prone to breaking. There are some specific virtual power capable nodes functionally more capable than ordinary nodes (Kush et al, 2009).

Hence, the proposed work applies Artificial Bee Colony (ABC) which has been a recently developed swarm intelligence technique that proves as an optimization technique. The ABC is broadly applied to many engineering applications in the literature. The proposed energy efficient clustering using ABC proved better clustering model than the existing traditional clustering techniques.

1.5 Contributions Made in this Thesis

- Proposed node authentication method.
- Proposed Scalable clustering for virtual mobile infrastructure using ABC.
- Proposed Secured Dynamic Group Key Management Scheme model.

1.6 Organization of Thesis

In chapter 1, the overview of research domain, research issue and objective are described as Introduction. In chapter 2, the related work in virtualization, secured model for virtualization, and clustering for MANET are discussed as Literature Survey. In chapter 3, the architectural design, algorithms and implementation techniques of proposed cluster based node deployment methodology are explained. The methodology, result and performance analysis of proposed Energy Efficient Artificial Bee Colony based Clustering methodology are elaborated in chapter 4. Similarly, the secured model, result and performance analysis of proposed dynamic group key management schemes are expanded in chapter 5. In chapter 6, the system design and methodology of proposed Scalable and Secured Virtual Infra Structure (SASVIS) is illuminated. Conclusion and future direction of proposed work are given in chapter 7.

CHAPTER 2

LITERATURE SURVEY

2.1 Reviews on Virtual Infrastructure

MANET is distributed as self-organizing networks that can change locations and configure themselves on the fly. A MANET is a collection of autonomous nodes that communicate with one another by forming a multi-hop radio network and maintaining connections in a decentralized manner. MANET offer quick and easy deployment of network in situations where it is not possible otherwise. MANET offer unique benefits and versatility if the environment and application are appropriate, M-governance is one such application. MANET can be the best option for m-Governance services where there is no predefined infrastructure (Liang et al, 2011).

The deployment of a MANET within an enclosed area, such as a building in a disaster scenario, can provide a robust communication infrastructure for search and rescue operations. The dynamic composition of networked appliances, or virtual devices, enables users to generate complex, strong, and specific systems. Current MANET basedcomposition schemes use service discovery mechanisms that depend on periodic service advertising by controlled broadcast, resulting in needless depletion of node resources (Mohite and Ragha, 2012).

The assumption that, once generated, a virtual device is to remain static is false; the device should gracefully degrade and upgrade along with the conditions in the user's environment, particularly the network's current performance requirements. While a Virtual Spring Mesh (VSM) algorithm provides scalable, self-organizing, and fault-tolerant capabilities required by a MANET, the VSM lacks the MANET's capabilities of deployment mechanisms for blanket coverage of an area and does not provide an obstacle avoidance mechanism.

Extended VSM (EVSM) algorithm (Derr and Manic,2011) provides the following novelties: 1) New control laws for exploration and expansion to provide blanket coverage, 2) Virtual adaptive springs enabling the mesh to expand as necessary, 3) Adapts to communications disturbances by varying the density and movement of mobile nodes, and 4) New metrics to assess the performance of the EVSM algorithm.

Presently, schemes for infrastructure-less virtual device composition and management do not consider this adaptation. Hence a distributed constraint satisfaction problem for virtual device composition in MANETs was proposed (Karmouch and Nayak, 2012) for effectiveness and efficiency.

The Internet, which is a global heterogeneous network composed of diverse wireless mobile access, home broadband, and core IP/optical networks, is perhaps the critical element in future global ICT strategy. However, the way the current Internet is managed and the way it provides services cannot match the fast changing and more demanding requirements imposed by user-end applications. Network virtualization, coupled with an effective and efficient approach to managing virtualized resources, is a key solution to the problem (Xu et al., 2012).

Table 2.1 Survey Table for Virtual Infrastructure

Sl. No.	Authors	Proposed Work
1	Liang et al, 2011	M Governance with no pre-defined infrastructure
2	Mohite and Ragha, 2012	Robust communication infrastructureusing MANET with periodic service advertising
3	Derr and Manic,2011	Extended Virtual Spring Mesh (EVSM) algorithm with virtual adaptive mesh, adapts to movement of mobile nodesand new metrics to assess the performance
4	Karmouch and Nayak, 2012	Infrastructure-less virtual device composition and management
5	Xu et al., 2012	Network virtualization coupled with an effective and efficient approach to managing virtualized resources
6	Kokkuetal., 2012	Network Virtualization Substrate with optimal slice scheduler and customizedflow scheduling
7	Pin et al., 2012	Virtual Networks with packet loss rate analysis and QoS guarantee

The design and implementation of a Network Virtualization Substrate (NVS) is effective virtualization of wireless resources in cellular networks. Virtualization fosters the realization of several interesting deployment scenarios such as customized virtual networks, virtual services, and wide-area corporate networks, with diverse performance objectives.

In virtualizing a base station's uplink and downlink resources into slices, NVS meets three key requirements isolation, customization, and efficient resource utilization using two novel features (Kokkuetal., 2012). The two features of NVS are,

1) NVS introduces a provably optimal slice scheduler that allows existence of slices with bandwidth-based and resource-based reservations simultaneously;
2) NVS includes a generic framework for efficiently enabling customizedflow scheduling within the base station on a per-slice basis.

Since wireless links are unreliable, packet loss is inevitable when the multicast service-oriented Virtual Networks (VN) are embedded into a WN. Although multicast allows the occurrence of packet loss, it is still important to ensure the packet loss rate is below a certain level for QoS guarantee (Pin et al., 2012).

2.2 Reviews on Wireless Clustering

The Clustering Problem in MANETs lies in selecting the most suitable nodes of a given MANET topology as cluster heads, and ensuring that regular nodes are connected to cluster heads such that the lifetime of the network is maximized. The development of an improved formulation of the clustering problem is discussed in the literature (Zahidi et al., 2013).

Additionally, various enhancements are implemented in the form of additions to the improved formulation, including the establishment of intra-cluster communication, multi-hop connections and the enforcement of coverage constraints (Umamaheswari and Radhamani, 2012). The improved formulation and developments are implemented in a tool designed to visually create network topologies and cluster them using state of the art generic methods.

It is also observed that while these enhanced formulations enable the generation of complex network solutions, and are suitable for small scale networks, the time taken to generate the corresponding solution does not meet the strict requirements of a practical environment.

Table 2.2 Survey Table for Wireless Cluster

Sl. No.	Authors	Proposed Work
1	Zahidi et al., 2013	Ensuring regular nodes are connected to cluster heads by reducing the lifetime of the network is maximized
2	Umamaheswari and Radhamani, 2012	Establishment of intra-cluster communication, multi-hop connections and the enforcement of coverage constraints
3	Lie et al, 2013	Cluster-based certificate revocation with vindication capability scheme

For quick and accurate certificate revocation, Lie et al (2013) has proposed the cluster-based certificate revocation with vindication capability scheme. In particular, to improve the reliability of the scheme, the warned nodes are recoverd to take part in the certificate revocation process to enhance the accuracy. The threshold-based mechanism to assess and vindicate warned nodes as legitimate nodes or not, before recovering them.

2.3 Reviews on Secured MANET

MANET has attracted much attention due to their mobility and ease of deployment. However, the wireless and dynamic features render them more vulnerable to various types of security attacks than the wired networks. The major challenge is to guarantee secure network services. To meet this challenge, certificate revocation is an important integral component to secure network communications (Rivera et al, 2008).

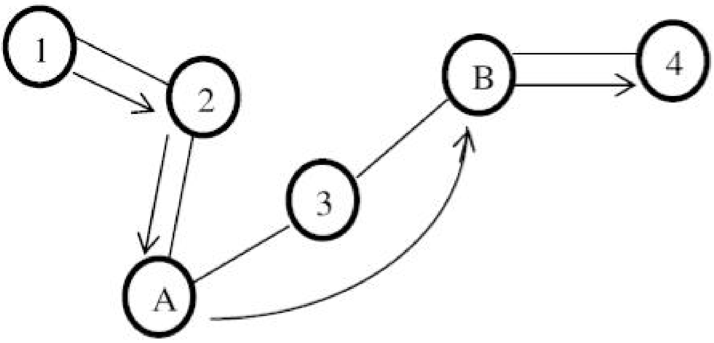
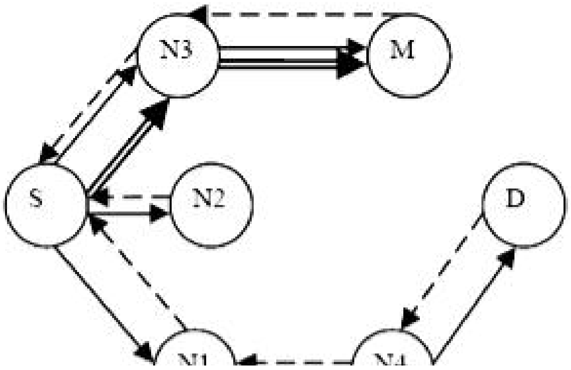


Figure 2.1 Wormhole Attack

The representation of wormhole and black hole attack is shown in Figure 2.1 and 2.2. The classification of key management scheme is shown in figure 2.3.



⇢ Route Request

→ (RREQ) Route Reply (RREP)

⇒ Data Packets Destinations Sequence Number

S <<= Source Node,

D <<= Destination Node,

M <<= Malicious Node

Figure 2.2 Black Hole Attacks

Ad hoc On-Demand Distance Vector (AODV) routing is a very popular routing algorithm that enables dynamic, self-starting, multi hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network (Dissanyake and Armstrong, 2013). An intermediate node, which takes part in packets forwarding, may behave maliciously and drop packets which goes through it, instead of forwarding them to the following node, where a malicious node falsely advertises good paths to a destination node during the route discovery process, such behavior is called black-hole attack. This attack becomes more sever when a group of malicious nodes cooperate to each other. However, it is vulnerable to the well-known cooperative black-hole attack.

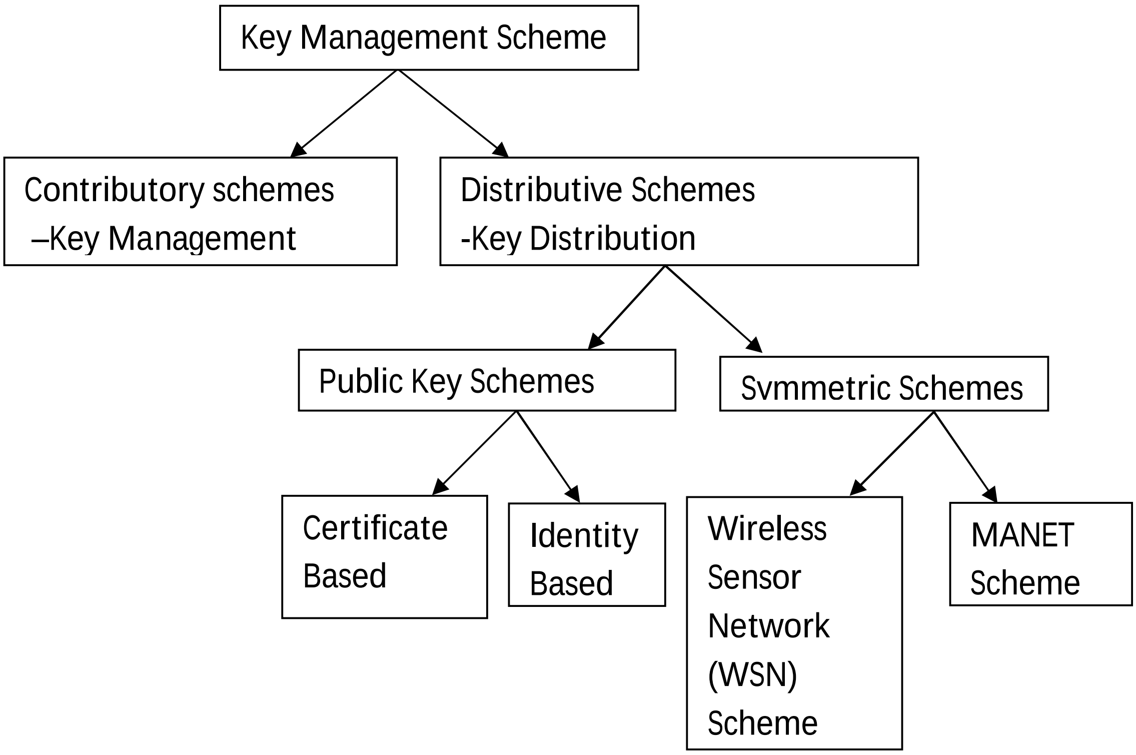

Key Management Scheme
Contributory schemes –Key Management
Distributive Schemes -Key Distribution
Public Key Schemes
Svmmetric Schemes
Certificate Based
Identity Based
Wireless Sensor Network (WSN) Scheme
MANET Scheme

Figure 2.3 Classification of Key Management Schemes

Fully self-organized MANET represent (Zafar et al, 2010) complex distributed systems that may also be part of a huge complex system, such as a complex system-of-systems used for disaster management operations. Due to the complex nature of MANETs and their resource constraint nodes, there has always been a need to develop lightweight security solutions. Since MANETs require a unique, distinct, and persistent identity per node for their security protocols to be viable, Sybil attacks pose a serious threat to such networks. A Sybil attacker can either create more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, thereby promoting lack of accountability in the network.

Secure group communication with efficient self-organizing key agreement protocol and small broadcast cipher text is essential to many collaborative and distributed applications in MANET. Chinese Remainder Theorem-based secure group communication scheme was proposed in the literature, which is able to provide confidentiality service and non-repudiation service simultaneously. All group members contribute their own public keys to negotiate a shared encryption public key, which corresponds to all different decryption keys. By using the shared public key and the respective secret key, confidentiality and non-repudiation can be obtained, both are essential to secure group communication in MANETs.

Identity Based Cryptography (IBC) has the advantage that no public key certification is needed when used in a MANET. This is especially useful when bi-directional channels do not exist in a MANET. However, IBC normally needs a centralized server for issuing private keys for different identities (Ni et al, 2011).

In MANET, many applications require group-oriented computing among a large number of nodes in an adversarial environment. In order to deploy these large-scale cooperative applications, secure multicast service must be provided to efficiently and safely exchange data among nodes. The existing literature has extensively studied security protection for a single multicast group, in which all nodes are assumed to have the same security level (Rong et al., 2009). For many applications, different users can play different roles and thus naturally be classified into multiple security levels.

As a prominent feature, a pyramidal security model contains a set of hierarchical security groups and multicast groups. To find an efficient key management solution that covers all the involved multicast groups, the following three schemes implemented: (1) Separated star key graph, (2) Separated tree key graph, and (3) Integrated tree key graph (Porkodi and Arumuganathan, 2009).

Most of the existing key management schemes concentrate only on network structures and key allocation algorithms, ignoring attributes of the nodes themselves. Due to the distributed and dynamic nature of MANET, it is possible to show that there is a security benefit to be achieved when the node states are considered in the process of constructing a Private Key Generator (PKG) (Zhu et al, 2010).

Yu et al., (2010) proposed a distributed hierarchical key management scheme in which nodes can get their keys updated either from their parent nodes or a threshold of sibling nodes. The dynamic node selection process is formulated as a stochastic problem and the proposed scheme can select the best nodes to be used as PKGs from all available ones considering their security conditions and energy states.

A fully-distributed ID-based Multiple Secrets Key Management (IMKM)scheme for effective key management in cluster-based MANET was proposed by (Li and Liul, 2010), which while ensuring secure communication in an ad hoc network is extremely challenging because of the dynamic nature of the network and the lack of centralized management. For this reason, key management is particularly difficult to implement in such networks.

The IMKM scheme was implemented via a combination of ID-based multiple secrets and threshold cryptography. It eliminates the need for certificate-based authenticated public-key distribution and provides an efficient mechanism for key update and key revocation schemes, which leads to more suitable, economic, adaptable, scalable, and autonomous key management for mobile ad hoc networks (Zaman and Karray, 2009).

MANETs are exposed to several extra threats as compared to legacy wireless networks due to their nature. The security management in MANETs, where node level security monitoring plays an integral role in maintaining security and the problem of computing the overall security level of MANETs. The security level estimation architecture, security level classification and applications is major focus in security model (Qayyum et al, 2012).

QoS routing is one of the most important functions for the integrated services networks. Security in MANET QoS routing has received increased attention recently. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense.

The MANETs can be easily adapted to m-Governance but due to their ad hoc nature MANETS are vulnerable to security attacks. Most of the research in MANETS has focused on routing issues and security has been given a low priority. The layered architecture draws huge support with its success in case of Internet. The Cross Layer Design Architecture is becoming more popular with its performance improvements. Security architecture is proposed for Cross Layer Design Architecture of MANET by Kaur (2013), which analyzes the security mechanism in m-Governance applications.

Hence, the related work which discussed above majorly focused on security architecture provided methodology for attacks, threats, and key management. Most of the recent methodologies provided appreciable result, even though optimality in key management, secured and dynamic node deployment on effective virtual infra-structure are still is an issue. Therefore, this proposed work concentrated on effective node deployment and dynamic group key management for secured communication. In addition to these issues, the energy efficient cluster is also concentrated in the proposed research work for improving the life time of ad hoc network.

CHAPTER 3

CLUSTER BASED NODE DEPLOYMENT

3.1 Objective

MANET consist of mobile nodes which can communicate with each other in a peer-to-peer fashion (over single hop or multiple hops) without any fixed infrastructure such as access point or base station. In a multi-hop ad hoc wireless network, which changes its topology dynamically, well-organized resource allocation, energy management, routing and end-to-end throughput performance can be achieved through adaptive clustering of the mobile nodes (Ali and Babak, 2010).

Clustering of MANET is an essential and efficient way of data communication. It is widely used in efficient network management, hierarchical routing protocol design, network modeling, and QoS. Clustering is defined as the grouping of similar objects or the process of finding a natural association among some specific objects or data. With an ad hoc clustering network, the nodes are separated into groups called clusters (Papadogiannis and Alexandropoulos, 2010).

The major goal of clustering is the election of an optimal cluster head and the achievement of an optimal number of clusters through division without degrading the entire network performance.

In this research work, a new energy based weighted distributed clustering algorithm is proposed which takes into consideration parameters such as connectivity, residual battery power, average mobility, and distance of the nodes to choose locally optimal cluster heads. The main objective of this algorithm is maintaining stable clustering structure with a lowest number of clusters formed, to minimize the overhead for the clustering formation and maintenance and to maximize the lifespan of mobile nodes in the system.

3.2 Overview of Wireless Clustering

Clustering is a well-known technique for grouping nodes that are close to one another in the network and to reduce the useful energy consumption. The concept of clustering consists of dividing the geographical area covered by the mobile nodes into small zones and then select from each cluster a node called Cluster head which is responsible for coordinating the communication with the nodes of the other cluster (intra cluster) and within the same cluster (Inter cluster) (Saini and trivedi, 2010).

There are usually three types of nodes in clustering networks: 1) Cluster-Heads (CH), 2) Gateway nodes and 3) Normal nodes. In each cluster, one node is elected as a CH to act as a local controller. The cluster-head needs to coordinate all transmissions within the cluster; it handles the inter-cluster traffic and delivers the packets destined for the cluster etc. Hence these cluster-heads experience high-energy consumption and thereby exhaust their energy resources more quickly than the ordinary nodes (Hai-tao, 2011).

It is, therefore, required that the cluster-heads energy consumption be minimized (optimal) thus maximizing the network lifetime. The process of cluster-formation consists of two phase's cluster-head election and assignment of nodes to cluster-heads. The size of the cluster (the number of nodes in the cluster) depends on the transmission range of the nodes in single hop cluster and the number of hops made by the cluster in multi-hop clusters.

The normal node sends or relays data to the CH which transfers the collected packets to the next hop. The gateway node, belonging to more than one cluster, bridges the CHs in those clusters. Both CHs and gateway nodes form the backbone network, yet the presence of gateway node is not compulsory in the clustering network.

Some basic advantages of the clustering scheme are:

- Only the CHs and gateway nodes form the backbone network, resulting in a much simpler topology, less overhead, flooding and collision.

- The change of nodes only affects part topology of the networks, making the topology more stable.

Only CHs or gateway nodes need to maintain the route information.

Cluster head election is a very important problem in MANET. But the existing solutions cannot be applied efficiently in wireless Ad-hoc network where the topology changes frequently and nodes links fail. The cluster structure needs to be maintained as the new mobile nodes may enter the network and the existing nodes may move out or lose their battery power. It occurs in case of both cluster head and member nodes.

Most of the existing clustering algorithms are based on criteria to choose cluster heads such as speed and direction, Position and the number of neighbours of a given node. These works have some drawbacks as a high computational overhead for both clustering and cluster maintenance.

The existing system uses different clustering schemes which are based on different parameters and are defined as below:

- Mobility based clustering
- Connectivity-based clustering
- Identifier based clustering
- Weighted based clustering

The parameters to be considered for cluster formation in each clustering schemes are as follows:

In the mobility Based algorithm, mobility of the mobile nodes behavior is utilized for cluster construction and maintenance and assigning mobile nodes with low relative speed as the cluster head.

In the connectivity Clustering Algorithm, the degree of the node is computed based on its distance from other node. The node with maximum number of neighbors is chosen as a cluster head. In the Identifier Clustering Algorithm, a unique Identification (ID) number is assigned to each node. Based upon their ID, cluster head has been selected.

In Highest Degree Clustering Algorithm in the degree of a node, the number of neighbors in each node is considered as a metric for the selection of CHs. The node with maximum degree is chosen as CH. Similarly, in Lowest ID Algorithm, A node with lowest ID is chosen as a cluster head.Distributed clustering algorithm andDistributed Mobility Adaptive Clustering Algorithm, each node has a unique weight instead of ID .If a nodes weight is higher than the neighbor, then it is elected as CH. otherwise it joins a neighboring CH.

In the Weighted Clustering Algorithm**,** the factors influenced are node degree, node distributed with its entire neighbor, node speed and time spent. Cluster head is elected by computing behavior of neighbors. All the above schemes have their own drawbacks and limitations.Hence, in this research work, each node broadcasts a beacon signal which contains the state of the node to all its neighbor nodes. Each node builds its neighbor list based on the beacon message received. The cluster head election is based on the weight value of the nodes.

In the cluster Maintenance phase, two types of operations are defined, which are

- Node Movement
- Battery Power

The node movement will be in the form of node leaving or node joining. This will have a small effect if the moving node is CH. In that case the cluster reorganization is performed using the concept of Linear Auto regression by which at a given time the future position of the node shall be predicted based on the present position. The battery power of the nodes in the clustering changes continuously.

Cluster Head power decreases rapidly compared to the cluster members. When the CH battery falls below a threshold, the node is no longer able to perform its activities and then a new head from the members is chosen. The proposed system gives a flexibility of assigning different weights, has better performance, Power of the node is saved and a stable cluster is obtained. Instead of wasting such signals and power to update the positional information, this proposed work defines a modified algorithm which is based on the criteria of Weight.

There are three efficient algorithms implemented in this proposed research work, these are:

- Weighted Clustering Algorithm
- Algorithm for node movement
- Algorithm for Battery Power

Detailed explanation of these proposed algorithms is given in the following sub-sections.

3.3 Related Work

Most hierarchical clustering architectures for mobile radio networks are based on the concept of cluster head, which acts as a local coordinator of transmissions within the cluster. It differs from the base station concept in current cellular systems, in that it does not have a special hardware and in fact is dynamically selected from among the set of stations. However, it does extra work with respect to ordinary stations, and therefore it may become the bottleneck of the cluster.

To overcome these difficulties, in our approach we eliminate the requirement for a cluster head altogether and adopt a fully distributed approach for cluster formation and intra-cluster communications. In cluster based systems, network nodes are partitioned into several groups. In each group, one node is elected to be the cluster-head while the rest of the nodes become ordinary nodes.

The cluster size is controlled by varying its transmission power. The cluster head coordinates transmissions within the cluster, handles inter-cluster traffic and delivers all packets destined to the cluster; it may also exchange data with nodes that act as gateways to the wired networks. In the cluster-based network architectures, the lifetime is strongly related to cluster-head's failure.

Cluster heads, therefore, experience high energy consumption and exhaust their energy resources more quickly than ordinary nodes do.

The procedure of cluster formation consists of two phases:

- Cluster-head election
- Assignment of nodes to cluster-heads.

Although several algorithms have been proposed in the literature, which address the problem of cluster formation, little work has been done on the energy efficient design of cluster-based networks.

3.3.1 *Clique*

Clique is a cluster formation protocol that exchanges information with 1-hop neighbors nodes are divided into mutually disjoints cluster (cliques). The protocol aims divide the MANET network into multiples small groups and guarantee that all the nodes in each clique agree on the same clique membership (Santhishree, and Damodaran, 2011).

The protocol has the following properties:

- It is fully distributed. Each node computes its clique only using the information from its 1-hop neighbors.

- Its termination is guaranteed.

- After the protocol terminates, all nodes are divided into mutually disjoint clique.

- They have consistent view on their clique membership.

The original algorithm assumes that each node knows its 1-hop neighbors and they have and unique ID.

This protocol is divided in four steps:

- Step 1: Each node exchanges its neighbor list with its neighbors, and computes its local maximum clique.

- Step 2: Each node exchanges its local maximum clique with its neighbors, and updates its maximum clique according to its neighbor nodes using local maximum clique.

- Step 3: Each node exchanges the update clique with its neighbors and derives its final clique.

- Step 4: Each node exchanges the final clique with its neighbors and checks their consistency.

3.3.2 ***Bounded-Distance Multi Cluster Head:***

Bounded-distance multi-cluster head formation algorithm is a distributed clustering using (k, r) dominating sets. Any node is said to be (k, r)-dominated if node i has at least k neighbors with distance r in D. This multi cluster head protocol allows the nodes to have several CH (redundancy) in order to have fault-tolerance for the applications. There are two different approaches for the clustering algorithm (leader-first and cluster-first), this algorithm will be included in the leader-first group due to at the beginning nodes try to find out which are its best CH and then join them.

In order to achieve clusters calculations of the dominating set of the network is generally used. The domination problem seeks to determine the minimum numbers of nodes D (called dominating nodes or cluster heads) such that any node i not in D am adjacent to at least one node in D. This problem is NP-complete.

For the (k, r)-Dominating set problem, r defines the maximum distance from nodes to their cluster-heads and k the minimum numbers of dominating sets per node. Notice that with a k greater than one, redundancy can use it to build fault-tolerant applications.

The Spohn algorithm has two main phases. The first is called election phase and here, each node elects k nodes with small ID (also including itself) with distance r. These elected nodes are not CH yet, they are only candidates. Later, the second and the last stage start. During this, cluster heads are finally elected and the rest of nodes have to associate to their dominating nodes (CH). It must have k nodes in every node’s r-hop neighborhood; otherwise the domination set k is not satisfied.

3.4 Proposed Node Deployment Architectural Design

The responsibilities of the system are designed in such a way that each subsystem performs its own functions and when integrated they represent the complete functionality of the system. The first module takes the responsibility Cluster formation and selecting the Cluster head.

Each node generates its beacon message which contains the state of the node to notify its presence to the neighbour. Each node builds its neighbour list based on the beacon message received. Cluster head election is based on the weight of the node and the node with the least weight is selected as cluster head.

The next immediate module is responsible for cluster maintenance. It deals with two distinct types of operations. First module, in cluster maintenance, deals with the maintaining the battery power using the threshold property. The CH power decreases more rapidly than the member nodes. When the cluster head battery power falls below a threshold then the node is no longer able to perform the activities of the leader and hence a new leader form the member node must be chosen.

The next module deals with node movement to the outside of the cluster boundary. When a new node tries to join in a network, the intermediate nodes are responsible for forwarding the packets from the new node to the CH of the existing group. Each node generates its join request; the requests are verified to ensure security. If the request is appropriate, new node is authenticated and included in the group.

Then the CH generates a broadcast message that includes: information about new node, for all the node members. Node leaving operation works in the same way as like the operations that involves when a node joins except that the node must have to generate a leaving notice to the CH. But, if the moving node is the cluster head, the cluster reorganization need to be performed. The CH is again selected based on the weights of the existing nodes and the node with the least weight is now again selected as the cluster head using the previous selection methodology.

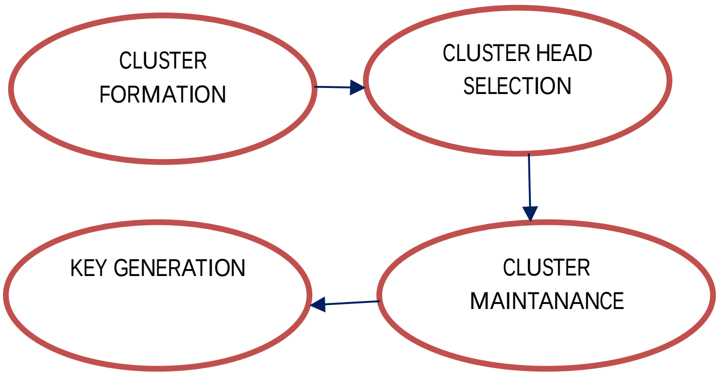


Figure 3.1 Information Flow Diagram

Initially, each node broadcasts a beacon message to notify its presence to the neighbours. A beacon message contains the state of the node. Each node builds its neighbour list based on the beacon messages received.

Step 1 : Create a node, n.

Step 2 : Node n broadcast a "Hello" message which contains the state of the node to all its neighbouring nodes. *Send_msg("Hello")* to notify its presence.

Step 3 : Each node builds its neighbour list based on the beacon messages received.

Step 4 : The elected CH broadcast a Node Deployment (ND) message to construct its cluster, all the nodes that hear the ND message and they want to join it, they must send a response message.

Based on which the CH assigns to them their identity in the network.

The election of cluster-heads is based on the weight values of the nodes and the node having the maximum energy is chosen as CH. Each node computes its weight value based on the following algorithm:

Step 1 : Broadcast a beacon signal to all its neighbour nodes in the transmission range, Process the beacon signals received from the neighbour nodes in the network and form the connection matrix.

Step 2 : Calculate energy of each node n.

Step 3 : Determine how much battery power has been consumed by each node. This is assumed to be more for a Cluster-Head when compared to an ordinary node. Because, the CH taken care of all the members of the cluster by continuously sending the signal.

Step 4 : The energy for each node is calculated

Step 5 : The node with the maximum energy is elected as a cluster-head. All the neighbours of the chosen cluster-head are no more allowed to participate in the election procedure.

Step 6 : All the above steps are repeated for remaining nodes which is not yet elected as a cluster-head or assigned to a cluster.

3.5 Result

The proposed work is simulated in Network Simulator 2 (NS2) and performance of the proposed work is compared with existing well known protocols Low Energy Adaptive Clustering Hierarchy and Cluster Head Gateway Switched Routing and proposed node deployment. The simulation environment is shown in Table 3.1.

Table 3.1 Simulation Environment

Parameter	Value
Number of sensors	50,100, 200, 300, 400, 500, 1000
Total Time of Simulation	10 Sec
Protocols Compared	Low Energy Adaptive Clustering Hierarchy (LEACH), Cluster-head Gateway Switched Routing (CGSR), Proposed Node Deployment

The performance in terms of latency, throughput and Packet Delivery Ratio (PDR) on various numbers of nodes in User Datagram Protocol (UDP) Communication are recorded in Table 3.2,

Table 3.2 Latency of Data Transmission in UDP

No of Nodes	CGSR	LEACH	Proposed Node deployment
50	65	63	61
100	81	77	76
200	100	95	93
300	123	117	117
500	152	146	144
1000	188	179	177

Table 3.3 Throughput of Data Transmission in UDP

No of Nodes	CGSR	LEACH	Proposed Node Deployment
50	165.7	170.2	170.5
100	205.2	210.9	211.3
200	202.6	208.3	208.6
300	200.1	205.6	206.0
500	197.7	203.1	203.5
1000	195.2	200.6	201.1

Table 3.3 and Table 3.4. Similarly the performance in terms of latency, throughput and PDR on various numbers of nodes in TCP Communication are recorded in Table 3.5, Table 3.6 and Table 3.7.

Table 3.4 Packet Delivery Ratio in UDP

No of Nodes	CGSR	LEACH	Proposed Node Deployment
50	94	97	97
100	93	96	97
200	93	96	97
300	93	96	97
500	92	94	95
1000	88	91	92

Table 3.5 Latency of Data Transmission in TCP

No of Nodes	CGSR	LEACH	Proposed Node Deployment
50	138	134	155.4
100	172	163	192.6
200	212	202	190.2
300	261	248	187.8
500	323	310	185.4
1000	399	380	183.3

Table 3.6 Throughput of Data Transmission in TCP

No of Nodes	CGSR	LEACH	Proposed Node Deployment
50	151.2	155.3	156.6
100	187.2	192.4	194.1
200	184.8	190.0	191.7
300	182.6	187.6	189.3
500	180.4	185.3	186.9
1000	178.1	183.0	184.7

Table 3.7 Packet Delivery Ratio in TCP

No of Nodes	**CGSR**	**LEACH**	**Proposed Node Deployment**
50	95	98	99
100	94	97	99
200	94	97	99
300	94	97	98
500	93	95	97
1000	89	92	94

The performance in terms of latency, throughput and packet delivery ratio in UDP is shown in Figure 3.1, 3.2 and 3.3. The performance in terms of latency, throughput and packet delivery ratio in TCP is shown in Figure 3.4, 3.5 and 3.6.

The latency in UDP using proposed node deployment is around 160ms when numbers of node are 50, whereas the CGSR and LEACH are higher than proposed work. In the simulation, number of nodes is increased to

100 and the latency is computed. The latency of proposed work in 100 nodes is increased to 200ms, the existing methodologies are still higher than the proposed work.

Numbers of node are further more increased to 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the latency are computed. The latency of proposed work in 200 nodes is reduced than the latency in 100 nodes. The latency of proposed work in 300 nodes, 500 nodes and 1000 nodes are reduced further.

The throughput in UDP using proposed node deployment is around 160 Kbps when number of nodes are 50 nodes, whereas the CGSR and LEACH are lesser than the proposed work. In the simulation, number of nodes is increased to 100 and the throughput is computed. The throughput of proposed work in 100 nodes is increased to 200 Kbps, the existing methodologies are still lesser than the proposed work.

Number of nodes are further more increased to 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the throughput are computed. The throughput of proposed work in 200 nodes is reduced than the throughput in 100 nodes. The throughput of proposed work in 300 nodes, 500 nodes and 1000 nodes are reduced further.

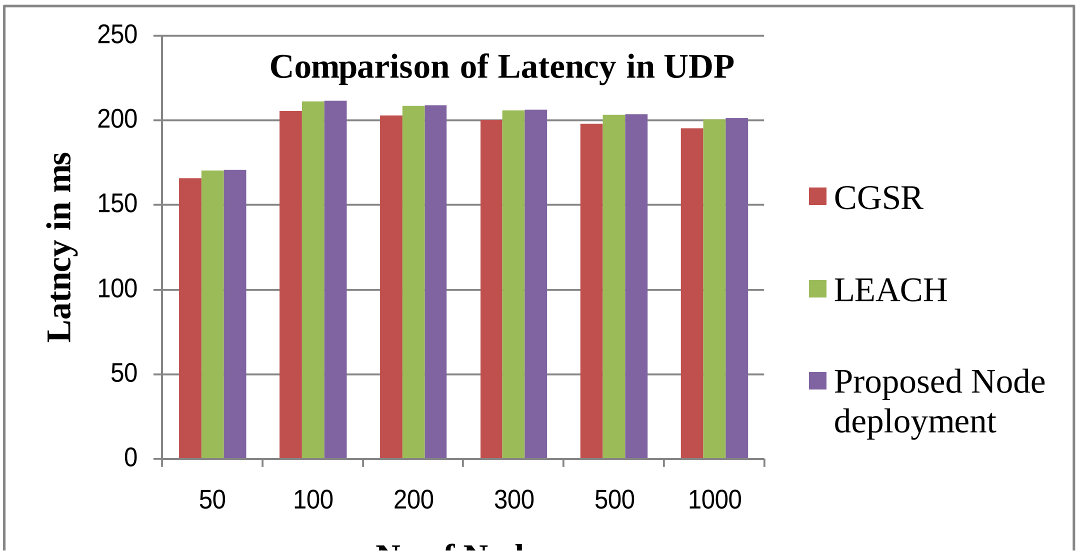


Figure 3.2 Comparison of Latency in UDP

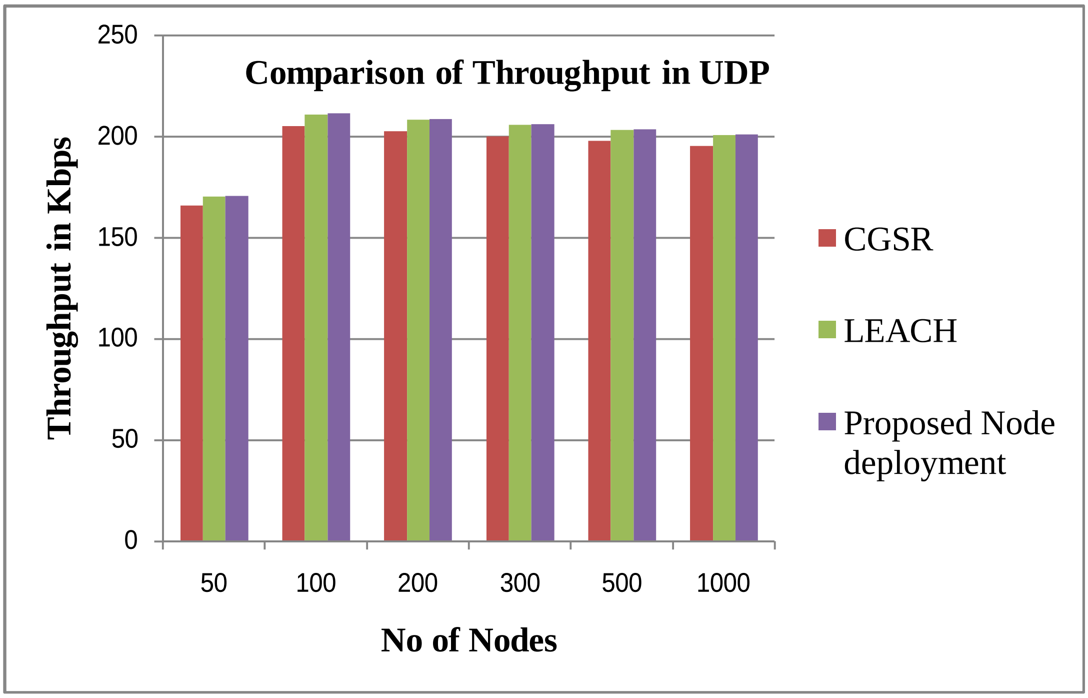


Figure 3.3 Comparison of throughput in UDP

The packet delivery ratio in UDP using proposed node deployment is around 94% when number of nodes are 50 nodes, whereas the CGSR and LEACH are lesser than the proposed work. In the simulation, number of nodes is increased to 100 nodes, 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the packet delivery ratio are computed.

The packet delivery ratio of proposed work in 100 nodes is reduced than the throughput in 50 nodes. The packet delivery ratio of proposed work in 200 nodes, 300 nodes, 500 nodes and 1000 nodes are reduced further.

The latency in TCP using proposed node deployment is around 120 ms when numbers of node are 50, whereas the CGSR and LEACH are higher than proposed work. In the simulation, number of nodes is increased to 100 and the latency is computed. The latency of proposed work in 100 nodes is increased to 200ms, the existing methodologies are still higher than the proposed work.

Numbers of node are further more increased to 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the latency are computed. The latency of proposed work in 200 nodes is reduced than the latency in 100 nodes. The latency of proposed work in 300 nodes, 500 nodes and 1000 nodes are reduced further.

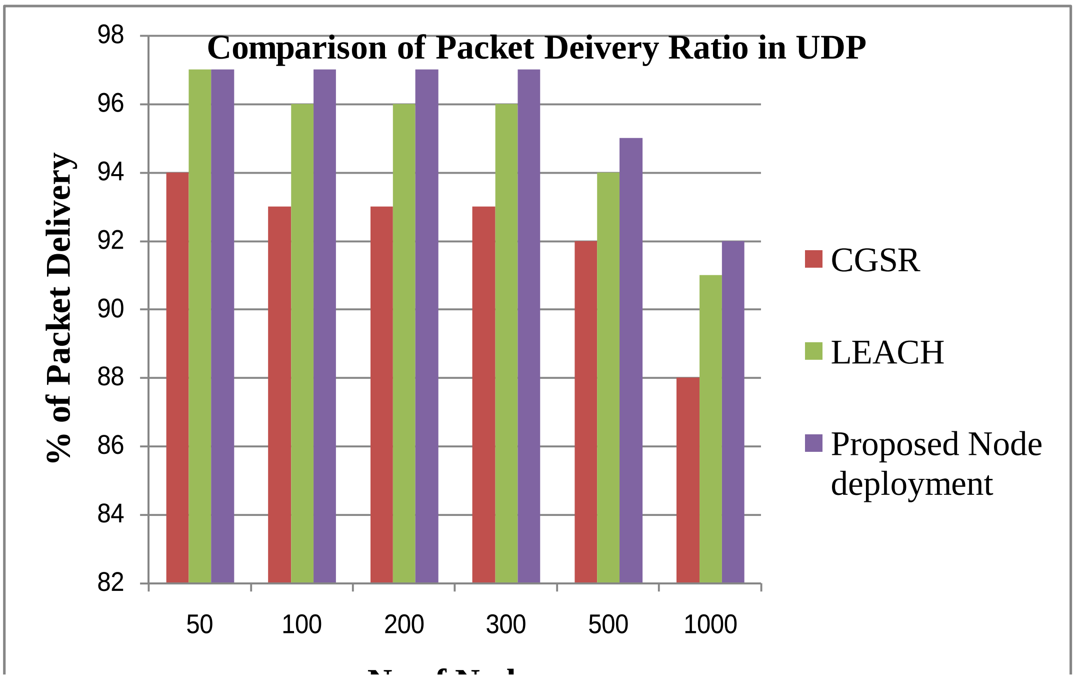


Figure 3.4 Comparison of Packet Delivery Ratio in UDP

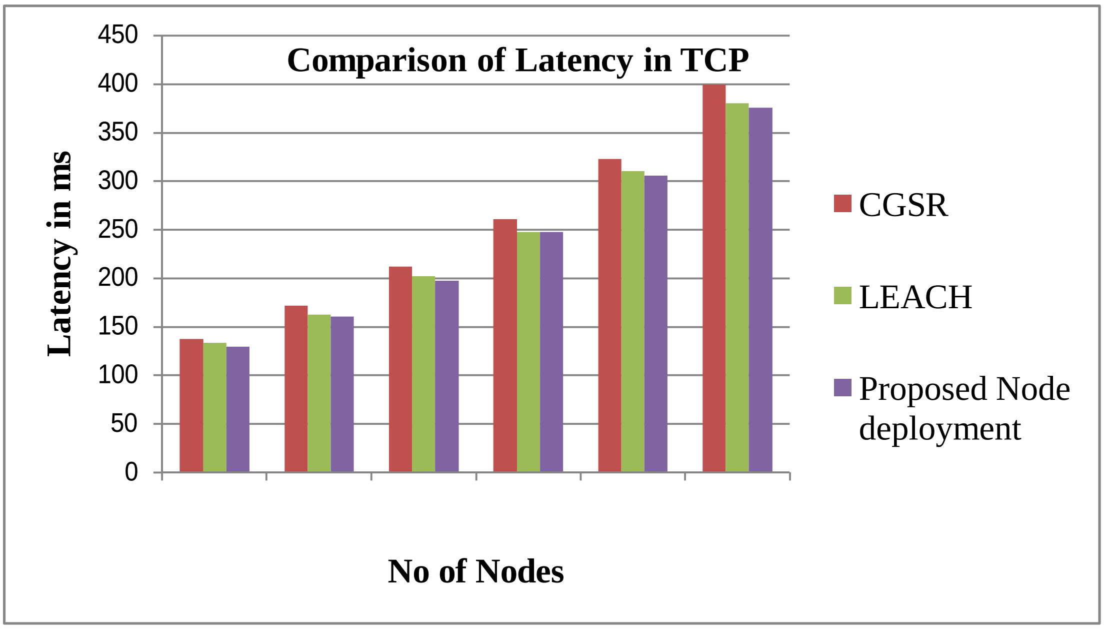


Figure 3.5 Comparison of Latency in TCP

The throughput in TCP using proposed node deployment is around 150 Kbps when numbers of node are 50 nodes, whereas the CGSR and LEACH are lesser than the proposed work. In the simulation, number of nodes is increased to 100 and the throughput is computed. The throughput of proposed work in 100 nodes is increased to 180 Kbps, the existing methodologies are still lesser than the proposed work.

Number of nodes are further more increased to 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the throughput are computed. The throughput of proposed work in 200 nodes is reduced than the throughput in 100 nodes. The throughput of proposed work in 300 nodes, 500 nodes and 1000 nodes are reduced further.

The packet delivery ratio in TCP using proposed node deployment is around 98% when number of nodes are 50 nodes, whereas the CGSR and LEACH are lesser than the proposed work. In the simulation, number of nodes is increased to 100 nodes, 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the packet delivery ratio are computed.

The packet delivery ratio of proposed work in 100 nodes is reduced than the throughput in 50 nodes. The packet delivery ratio of proposed work in 200 nodes, 300 nodes, 500 nodes and 1000 nodes are reduced further.

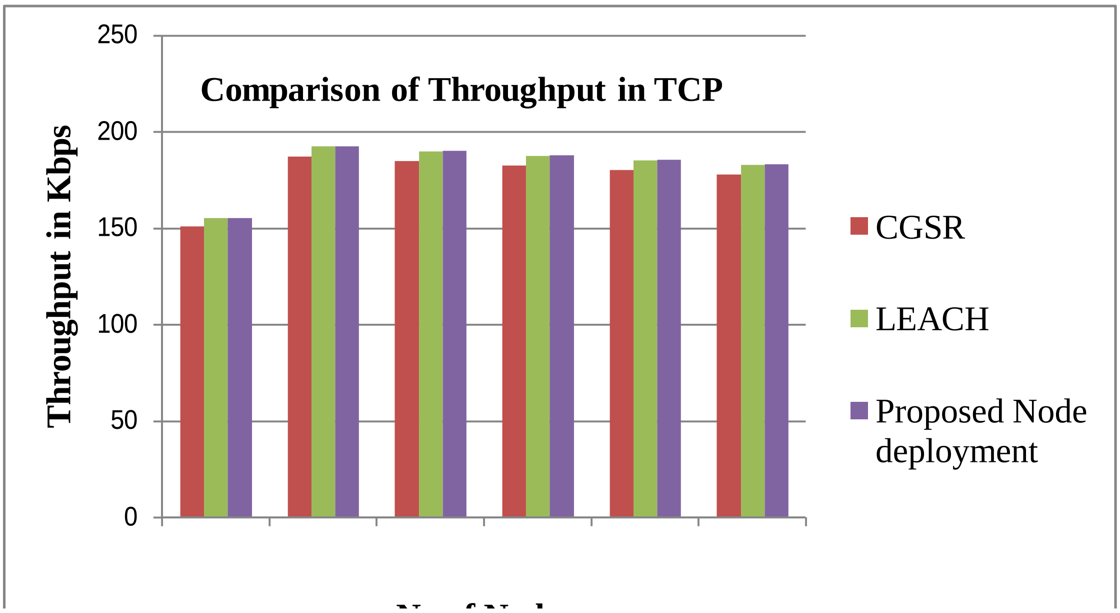


Figure 3.6 Comparison of Throughput in TCP

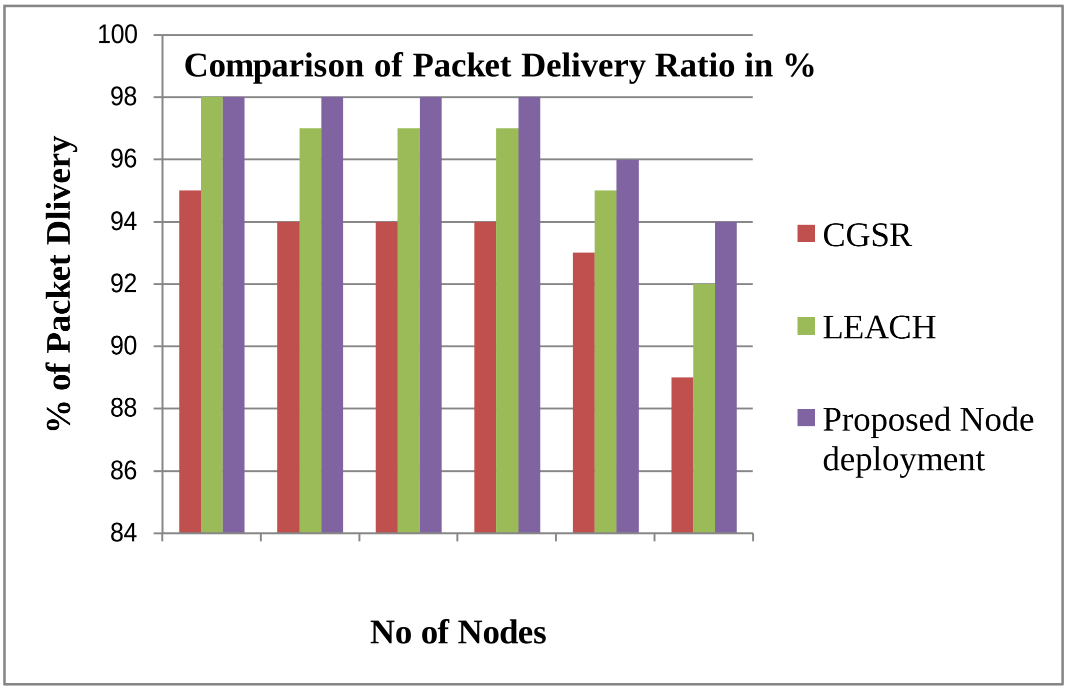


Figure 3.7 Comparison of Packet Delivery Ratio in TCP

3.6 CONCLUSION

The proposed node deployment architecture introduces a new modified weighted deployment scheme for mobile ad hoc network, where all the nodes in the network are divided into clusters. The main objective of clustering here is election of optimal cluster and the achievement of clusters through division without degrading the whole network's performance.

A method electing the cluster head by computing the weight of the node is proposed and the node with maximum energy is selected as Cluster head. Cluster maintenance is also done in case of the new node arriving and leaving the cluster. A method of shifting the ownership of Cluster head from one node to another node is used when a node leaves the cluster is done.

From the result, it is obvious that the proposed method provides effective utilization of power, minimum wastage of bandwidth and stable clustering structure, minimised the overhead, effective maintenance phase and maximised the lifespan of mobile nodes in the system.

CHAPTER 4

ARTIFICIAL BEE COLONY BASED CLUSTERING METHODOLOGY

4.1 Objective

A flat MANET has an inherent scalability limitation in terms of achievable network capacity. It is seen that when the network size increases per node, throughput of an ad hoc network rapidly decreases (Bhagavathula et al, 2002). This is due to the fact that in large scale networks, flat structure of networks results in long hop paths which are prone to breaking. These long hop paths can be avoided by using virtual node concept working as a mobile backbone network. There are some specific virtual power capable nodes functionally more capable than ordinary nodes (Kush et al, 2009).

Hence, the proposed work applies Artificial Bee Colony (ABC) which has been a recently developed swarm intelligence technique that proves as an optimization technique. The Artificial Bee Colony broadly applied to many engineering applications in the literature. The proposed energy efficient clustering of wireless networks using ABC, which proved better result in the clustering model of database (Ahmed et al, 2010) than the existing traditional clustering techniques. In order to implement the ABC in wireless network, the parameters and algorithms used in ABC are re-modified.

4.2 Overview of ABC

Swarm intelligence is a new discipline of study that contains a relatively optimal approach to problem solving which are the imitations inspired from the social behaviour of insects and animals, for example, Ant Colony Optimization (ACO) algorithm, (Dorigo et al, 1996) (Dorigo and Luca, 1997) Honey Bee Algorithms and Firefly algorithm.

The “ACO Algorithm” is a study derived from the observation of real ants’ behaviour and uses these models as a source of inspiration for the design of novel algorithms, which is the solution for optimization and distributed control problems. The honey bee mating algorithm is the growing technique, which is proposed in late 2005 for many engineering applications (Chandramohan et al, 2011a, 2011b, 2011c, and 2011d).

In the last few years, the interest in the studies of Swarm Intelligence (SI) based optimization techniques is increasing. In SI, the organisms of animals and insects are studied for solving optimization problems and patterns generation. SI groups those techniques inspired by the collective behaviour of social insect colonies, as well as other animal societies that are able to solve large-scale distributed problems. Like ACO, the ABC provides optimality in many aspects of a variety of engineering problems.

Honey bees are insects that live in large colonies (around 50,000 bees as a colony) usually containing one queen and her progeny, some 20,000–40,000 female workers and 200–300 male drones. Michael et al (2010) is a detailed study of honey bee in the biological aspect and about the foraging behaviour. There are many syndromes observed like aggression syndrome, waggling dance, from the honey bee colony which is used for solving optimization problems. Although honey bees are depicted in many cave paintings dated from 6000BC, the first recorded observations of bee behaviour were made by Aristotle.

The honey bee is a diffuse creature which can extend itself over long distances in multiple directions in order to find a large number of food sources and at the same time to find the best food source for the collection of food sources. For example, the flower patches with plentiful amounts of nectar or pollen that can be collected with less effort should be visited by more bees, whereas patches with less nectar or pollen should receive fewer bees (Huang et al, 2009).

The foraging process begins in a colony of scout bees being sent to search for promising flower patches. Scout bees search randomly from one patch to another. When they return to the hive, those scout bees that found a patch which is rated above a certain threshold which is measured as a combination of some constituents, such as sugar content, deposit their nectar or pollen and go to the "dance floor" to perform a dance known as the "waggle dance" (Jha et al, 2011).

This dance is essential for colony communication, and contains three vital pieces of information regarding flower patches: the direction in which it will be found, its distance from the hive and its quality rating (or fitness) (Andrew and Wenyan, 2010). This information guides the bees to find the flower patches precisely, without the use of guides or maps. Each individual's knowledge of the outside environment is gleaned solely from the waggle dance. This dance enables the colony to evaluate the relative merit of different patches according to both the quality of the food they provide and the amount of energy needed to harvest it.

Till date, many research activities are carried on various engineering problems, for example, Dervis and Bahriye (2009), Taher et al (2010), Dervis and Celal (2011), Hongnian et al (2010). Dervis and Bahriye (2009) and Hongnian et al (2010) are described the biological nature of real bees, the study of bionics bridges with the engineering functions, biological structures of animals and insects, and organizational principles found in the nature which mapping with the modern technologies.

In Jiejin et al (2010), the authors proposed a novel hybrid ABC and Quantum Evolutionary Algorithm for solving continuous optimization problems. ABC is adopted to increase the local search capacity as well as the randomness of the populations. These implementations have been tested on several well-known real data sets and compared with other popular heuristic algorithms such as Genetic Algorithm, Simulated Annealing, ACO and the recently proposed algorithms like improved PSO.

The computational simulations reveal very encouraging results in terms of the quality of solution and the processing time required honey bees are among the most closely studied social insects. Their foraging behaviour, learning, memorizing and information sharing characteristics have recently been one of the most interesting research areas in swarm intelligence.

Rajesh et al (2011) presented a new multi-agent based hybrid particle swarm optimization technique applied to the economic power dispatch. The earlier PSO suffers from the tuning of variables, randomness and uniqueness of solution. The algorithm integrates the deterministic search, the Multi-agent system, the PSO algorithm and the bee decision-making process. The economic power dispatch problem is a nonlinear constrained optimization problem.

Classical optimization techniques like direct search and gradient methods fails to give the global optimum solution. Other Evolutionary algorithms provide only a good enough solution. To show the capability, the author is applied to two cases 13 and 40 generators, respectively. The results show that this algorithm is more accurate and robust in finding the global optimum than another.

David et al (2010) discussed a new calculation tool based on particle swarm which named as a binary honey bee foraging. Effectively, this approach will make possible to determine the optimal location, biomass supply area and power plant size that offer the best profitability for investors. Moreover, it prevents the accurate method, which may not feasible from a computational viewpoint. In this work, Profitability Index is set as the fitness function for the binary honey bee foraging approach.

Changsheng (2011) proposed a clustering approach for optimally partitioning of N objects into K clusters. The author tested the proposed system with several well-known real data sets and concluded that the ABC performs well than the other popular heuristic algorithm in clustering, such as genetic algorithm, PSO, scatter search, and ACO. The result of all above proposals shows that the performance of the honey bee algorithm is more optimal than other existing algorithms.

Alok (2009) and Michael et al (2010) applied the ABC in the studies of computer science and engineering for network routing and minimum spanning tree. Alok (2009) designed and implemented the ABC for leaf-constrained minimum spanning tree problem and concluded that computation time in the ABC is quite small and it completely outperforms both in terms of solution quality as well as running time. The author proposes ABC based solution for the given an undirected, connected, weighted graph, the leaf-constrained minimum spanning tree problem.

This paper seeks on this graph a spanning tree of minimum weight among all the spanning trees of the graph that have at least number of leaves. This paper differs from other implementations in the following features: In the existing implementation, if the solution associated with an employed bee does not improve for a predetermined number of iterations then it becomes a scout bee. While the author proposes a second possibility in which an employed bee can become a scout. An employed bee can become a scout through collision also.

There are no limits on the number of scouts in a single iteration like other ABC algorithms. Also the number of scouts depends on the above two conditions. There can be many scouts in the iteration if these two conditions are satisfied many times, or there can be no scout if these two conditions remain unsatisfied.

Michael et al (2010) made a detailed review of bio-inspired routing algorithm such that ABC and ACO. The author discusses in some depth why biology is an appealing and appropriate place to find inspiration for computer networking research. The paper covers a review on routing research inspired by the behaviour of social insects, intrusion and misbehaviour detection research inspired by the immune system, network services modelled on the interactions and evolution of populations of organisms, research that applies techniques from the field of epidemiology, and presents a sampling of newly emerging bio-inspired research topics.

It is observed that the performance of ABC may be further improved by 1) optimal value assignment for the constants, which was assumed for almost all the previous work, and 2) the initial number of scout bee, if this is not optimally selected then there are many chances for local optima (zero-to-infinity) problem. ABC is proposed for wireless routing, which is re-modified for avoiding local optimal problem.

4.3 Proposed Eenergy Efficient ABC (EE-ABC) Clustering

The design and working nature of the proposed EE-ABC is redefined in order to provide optimality. The existing ABC has few pitfalls such as the improper number of scout bee will lead local optimal problem, slow convergence and as a result non feasible especially for computer network routing.

The bees search for food sources in a way that maximizes the ratio

$$\forall(E,H) \Leftrightarrow F(\theta_i) = \frac{E}{H} \tag{3.1}$$

Where, E is the energy obtained, H is the hop count, the number of intermediate peers, between hive to the food source. Here E is proportional to the nectar amount of food sources discovered by bees and it works to maximize the honey being stored inside the hive. In a maximization problem, the goal is to find the maximum of the objective function, F (θ).

F (θ) is the nectar ratio, shown in equation (1), $\theta \in R^P$. R^P represents the region of the search area. Assume that θ_i is the position of the ith food source; F(θ_i) represents the nectar ratio of the food source located at θ_i and it is proportional to the energy E(θ_i).

If the nectar ratio, F (θ), of the food source is higher than the minimum threshold, then the scout bee initialises the waggling dance with rhythm above the food source (which is called as dance floor). This waggling dance is a visualization technique that to transfer information to the insight worker bees. If the worker bees are beyond insight, the rhythm of scout bee may reach the worker bee. Based on the visual and or audio information from the scout bee, the worker bee from one hive or more hive will reach the dance floor (food source) for collecting the nectar.

$$T(\theta_i) = \begin{cases} \alpha \bullet F(\theta_i) & F(\theta_i) > F_{th} \\ 0 & \text{otherwise} \end{cases} \tag{3.2}$$

$$R(\theta_i) = \begin{cases} \beta \bullet F(\theta_i) & F(\theta_i) > F_{th} \\ 0 & \text{otherwise} \end{cases} \tag{3.3}$$

Where the $T(\theta_i)$ is the duration of waggling dance, $R(\theta_i)$ is the volume of rhythm, F_{th} is the minimum threshold of the nectar value and α, β are the constant which is termed as time scale factor and volume scale factor.

$$0 < \alpha < 1 \tag{3.4}$$

$$0 < \beta < 1 \tag{3.5}$$

If the value of α and β are small, then convergence becomes fast. If the value of the same is high, more precise result will occur. The bees search for food sources and collect the nectar (E). This process initiates the waggling dance on the floor for T time units (based on the equation 3.2) with an R volume of the rhythm (based on the equation 3.3).

If the dancing time of the bee is elapsed, then it will search the neighbouring dancing bee and goes to the dance floor of neighbouring bee to watch the dance as guest bee. Suppose more than one dancing bee found near, and then the bee chooses the one with higher rhythm (Rhythm of bee proportional to nectar).

The energy level of the ad hoc nodes or sensory nodes is mapped as the rhythm of the ABC. When a guest bee enters the dancing floor, the data from this guest bee is stored in the nectar (routing) table of dancing bee. The mapping of biological terms with the networking terms for the proposed ABC clustering methodology are described in table 4.1.

Table 4.1 Mapping of Biological Terminology with Network Terminology

In biological terms	**Network Routing**
Bee	Hello message
Food Source (or Flower)	Node
Nectar	Energy / Power
Nectar (or Patch) Table	Routing Table
Waggling Dance	Waiting Time
Elite Site	Cluster Head
Hive	Control Station (Real /Imaginary Node)

The working principles of proposed ABC based clustering algorithm is shown in the following pseudo code.

4.4 Pseudocode for Proposed EE-ABC Clustering Algorithm

```
Procedure_EEABC_Clustering
    Initialization
    Generate the initial population of the bees
Selection of the best bee as the queen
    Selection of the maximum number of mating flights (n)
    Main Phase
do while i ≤ n
   Initialize queen spermatheca, energy and speed.
Select α
      do while energy  > threshold and spermatheca is not full
Select a drone
       If the drone passes the probabilistic condition then
  Add sperm of the drone in the spermatheca
endif
Update Speed
Update Energy
   enddo
do j = 1, Size of Spermatheca
Select a sperm from the spermatheca
        Generate a brood by applying a crossover operator between the queen, the selected drones and the adaptive memory
Select, randomly, a worker
        Use the selected worker to improve the brood's fitness
        if the brood's fitness is better than the queen's fitness then
   Replace the queen with the brood
else
          if the brood's fitness is better than one of the drone's fitness then
   Replace the drone with the brood
endif
   endif
```

```
    **enddo**
**enddo**
**Return The** Queen (Best Solution Found)
**end Procedure**
```

4.5 Results and Discussion

The proposed work is simulated in Network Simulator 2 (NS2) and performance of the proposed work is compared with existing well known protocols. The simulation environment is shown in Table 4.2.

Table 4.2 Simulation Environment

Parameter	**Value**
Number of nodes	50,100, 200, 300, 400, 500, 1000
Total Time of Simulation	10 Sec
Protocols Compared	LEACH, CGSR and Proposed EE-ABC

The performance in terms of latency in UDP is shown in Figure 4.1.

The performance in terms of latency in TCP is shown in Figure 4.2, and the performance of proposed EE-ABC in terms of latency in UDP and TCP are compared with trend line in Figure 4.3.

The performance in terms of throughput in UDP is shown in Figure 4.4.

Table 4.3 Latency of Data Transmission in UDP

No of Nodes	CGSR	LEACH	Proposed EE-ABC
50	65	63	60
100	81	77	74
200	100	95	91
300	123	117	114
500	152	146	141
1000	188	179	173

Table 4.4 Throughput of Data Transmission in UDP

No of Nodes	CGSR	LEACH	Proposed EE-ABC
50	165.7	170.2	171.7
100	205.2	210.9	212.8
200	202.6	208.3	210.1
300	200.1	205.6	207.5
500	197.7	203.1	204.9
1000	195.2	200.6	202.5

Table 4.5 Packet Delivery Ratio in UDP

No of Nodes	CGSR	LEACH	Proposed EE-ABC
50	94	97	99
100	93	96	99
200	93	96	99
300	93	96	98
500	92	94	97
1000	88	91	94

Table 4.6 Latency of Data Transmission in TCP

No of Nodes	CGSR	LEACH	Proposed EE-ABC
50	138	134	127
100	172	163	157
200	212	202	193
300	261	248	242
500	323	310	299
1000	399	380	367

Table 4.7 Throughput of Data Transmission in TCP

No of Nodes	CGSR	LEACH	Proposed EE-ABC
50	151.2	155.3	156.6
100	187.2	192.4	194.1
200	184.8	190.0	191.7
300	182.6	187.6	189.3
500	180.4	185.3	186.9
1000	178.1	183.0	184.7

Table 4.8 Packet Delivery Ratio in TCP

No of Nodes	CGSR	LEACH	Proposed EE-ABC
50	95	98	99
100	94	97	99
200	94	97	99
300	94	97	98
500	93	95	97
1000	89	92	94

The performance in terms of latency, throughput and PDR on various numbers of nodes in UDP communication are recorded in Table 4.3, Table 4.4 and Table 4.5.

The latency in UDP using proposed node deployment is less than 130ms when numbers of node are 50, whereas the CGSR and LEACH are higher than proposed work. In the simulation, number of nodes is increased to 100 and the latency is computed. The latency of proposed work in 100 nodes is increased to 150ms, the existing methodologies are still higher than the proposed work.

Numbers of node are further more increased to 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the latency are computed. The latency of proposed work in 200 nodes is increase than the latency in 100 nodes. The latency of proposed work in 300 nodes, 500 nodes and 1000 nodes are in increasing order, however the existing methodologies are always higher than proposed work.

Similarly, the latency in TCP using proposed node deployment is always lesser than existing work.

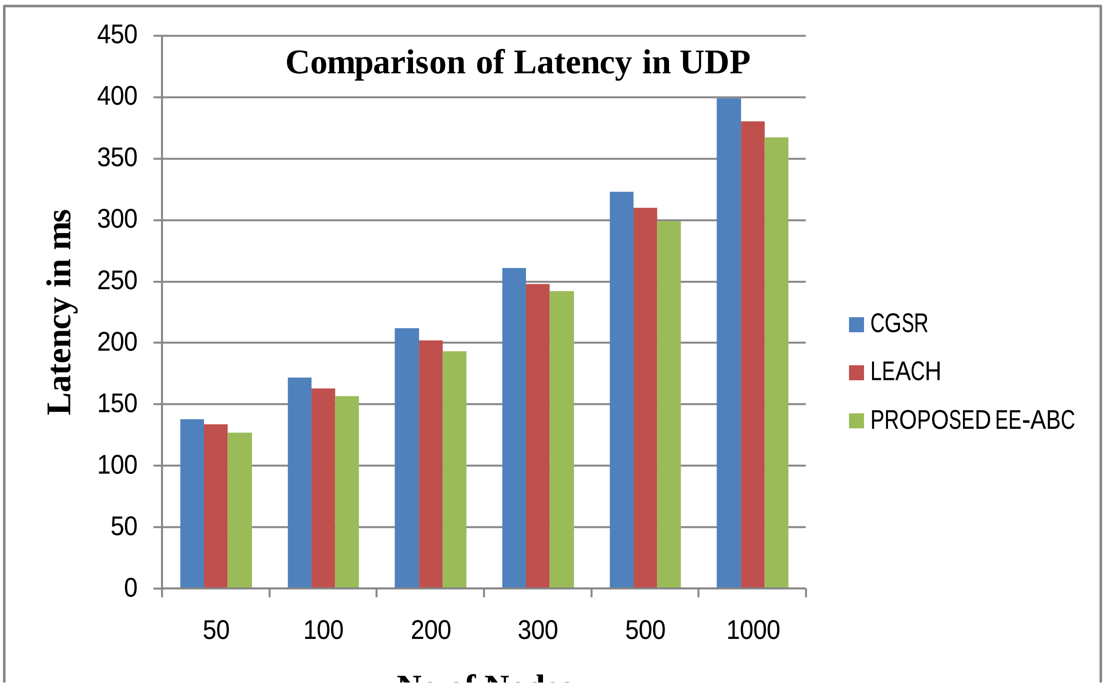


Figure 4.1. Comparison of Latency in UDP

Similarly the performance in terms of latency, throughput and PDR on various number of nodes in TCP communication are recorded in Table 4.6, Table 4.7 and Table 4.8.

The performance in terms of throughput in TCP is shown in Figure 4.5, and the performance of proposed EE-ABC in terms of throughput in UDP and TCP are compared with trend line in Figure 4.6.

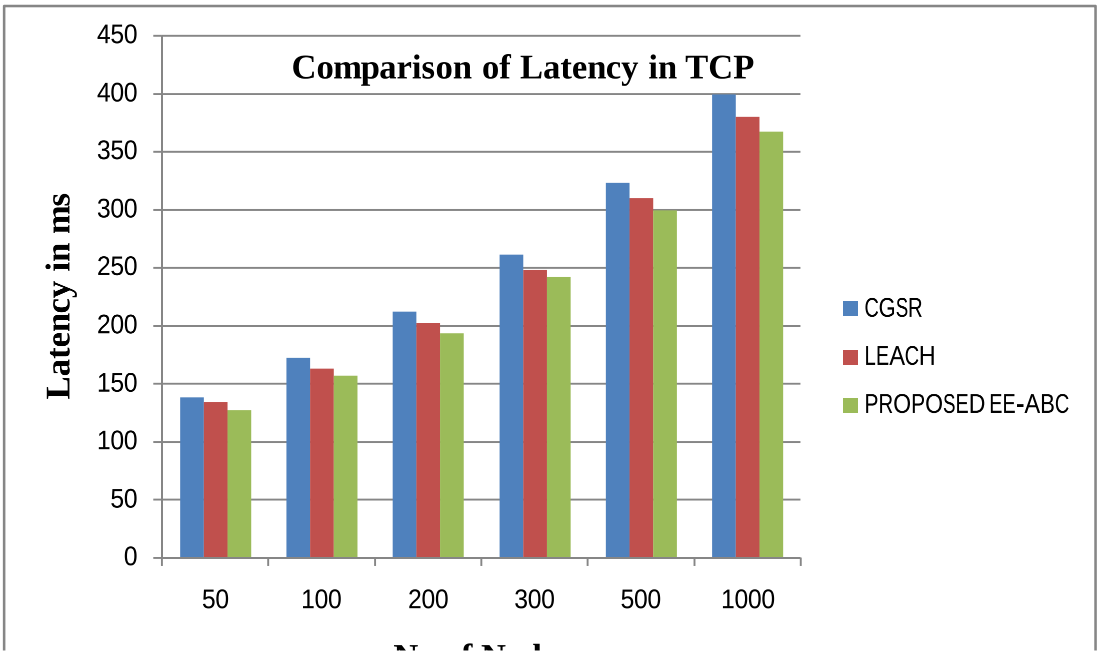


Figure 4.2. Comparison of Latency in TCP

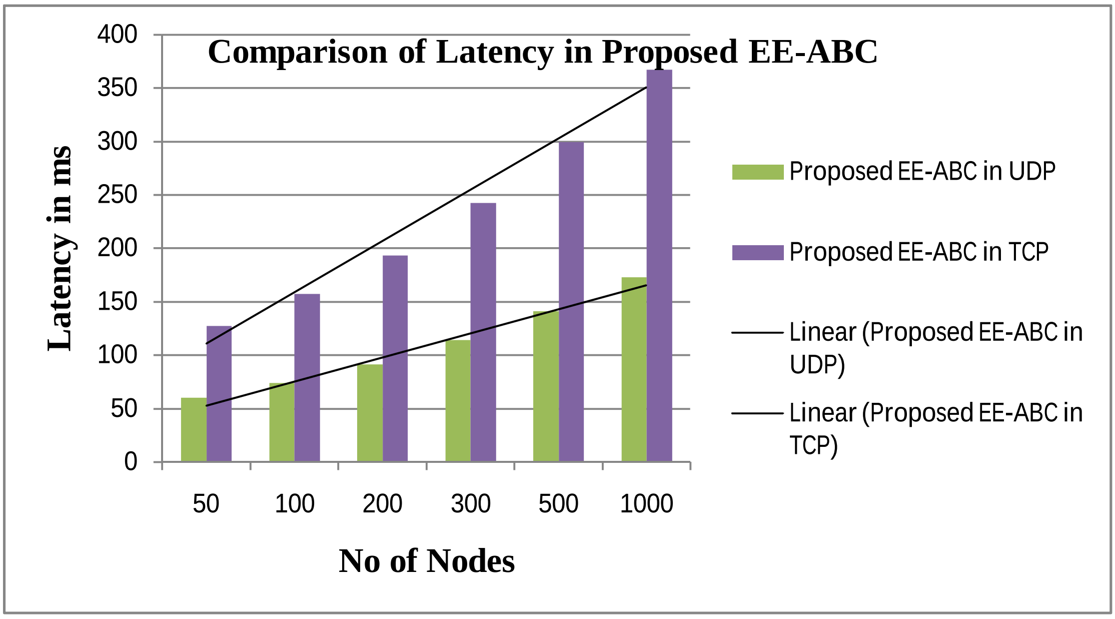


Figure 4.3. Comparison of Throughput of proposed system with linear trendline

The throughput in UDP using proposed node deployment is above 170 Kbps when number of nodes are 50 nodes, whereas the CGSR and LEACH are lesser than the proposed work. In the simulation, number of nodes is increased to 100 and the throughput is computed. The throughput of proposed work in 100 nodes is increased above 200 Kbps, the existing methodologies are still lesser than the proposed work.

Number of nodes are further more increased to 200 nodes, 300 nodes, 500 nodes and 1000 nodes, then the throughput are computed. The throughput of proposed work in 200 nodes is reduced than the throughput in 100 nodes. The throughput of proposed work in 300 nodes, 500 nodes and 1000 nodes are reduced further.

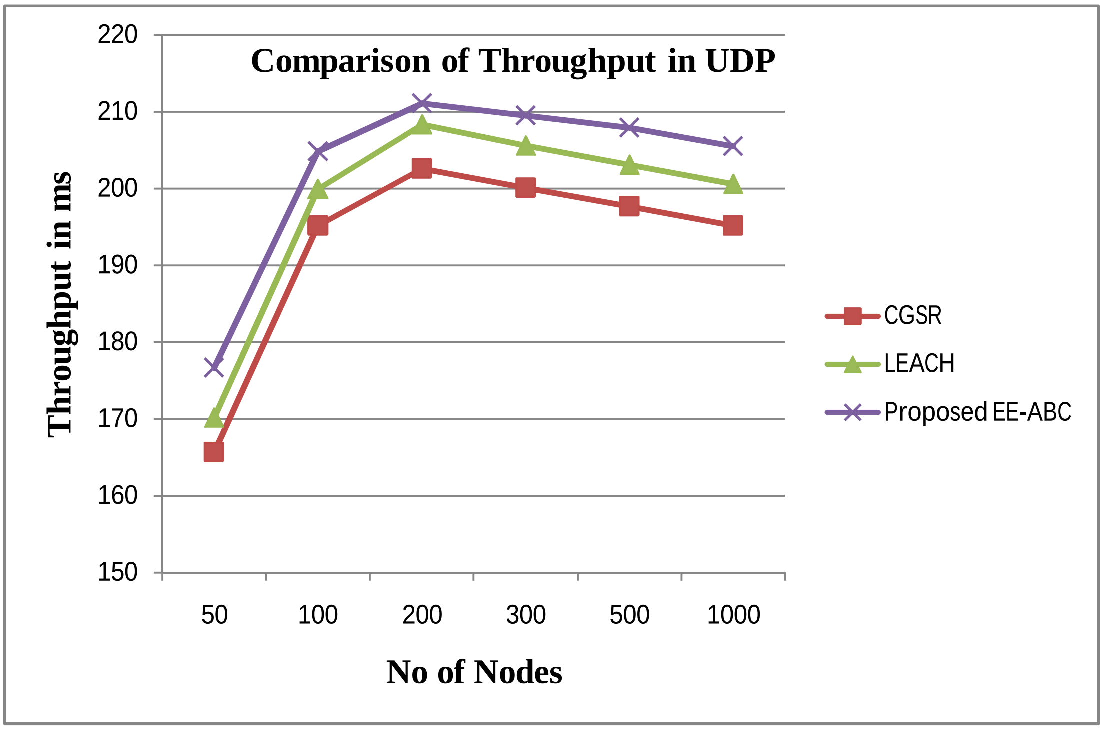


Figure 4.4 Comparison of Throughput in UDP

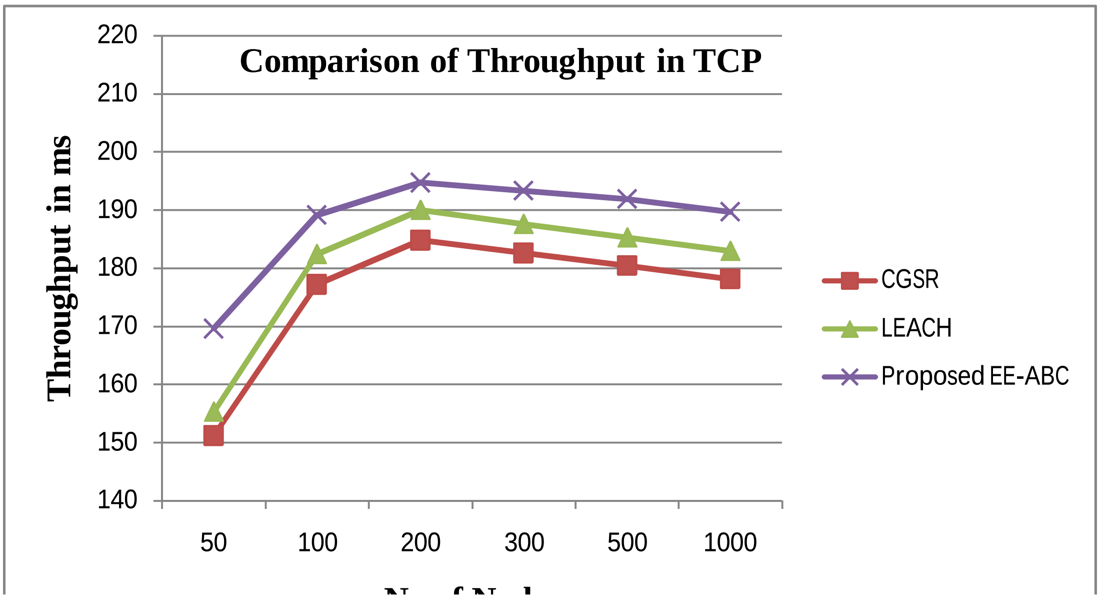


Figure 4.5 Comparison of Throughput in TCP

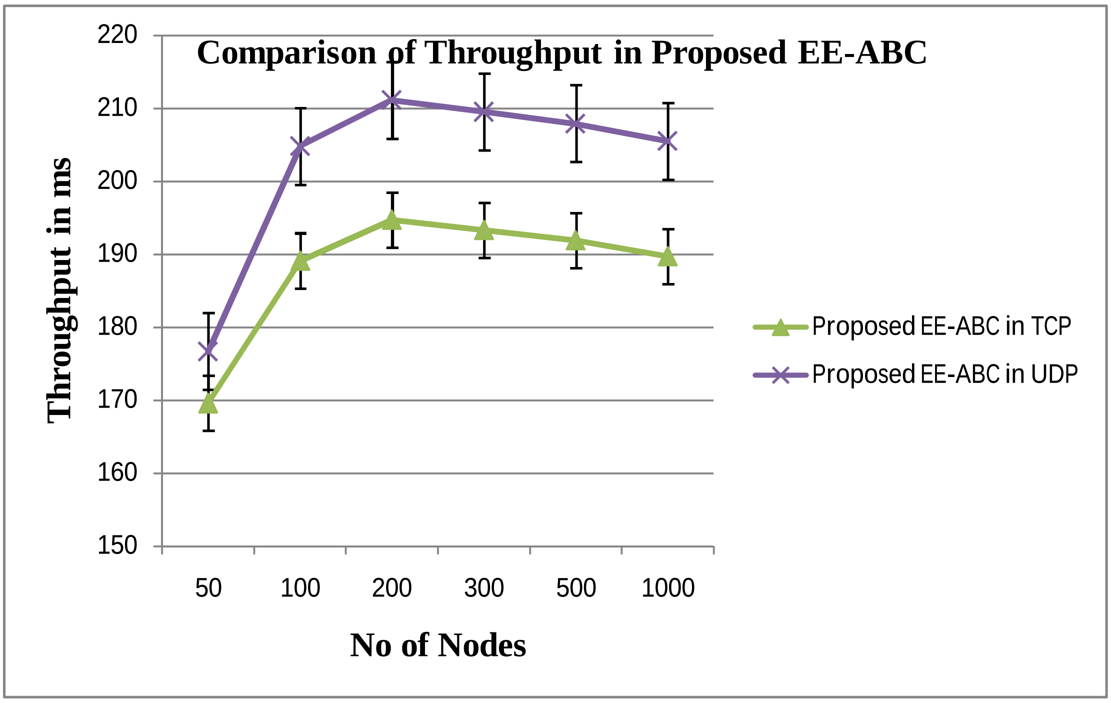


Figure 4.6 Comparison of Throughput of proposed EE-ABC with error bars

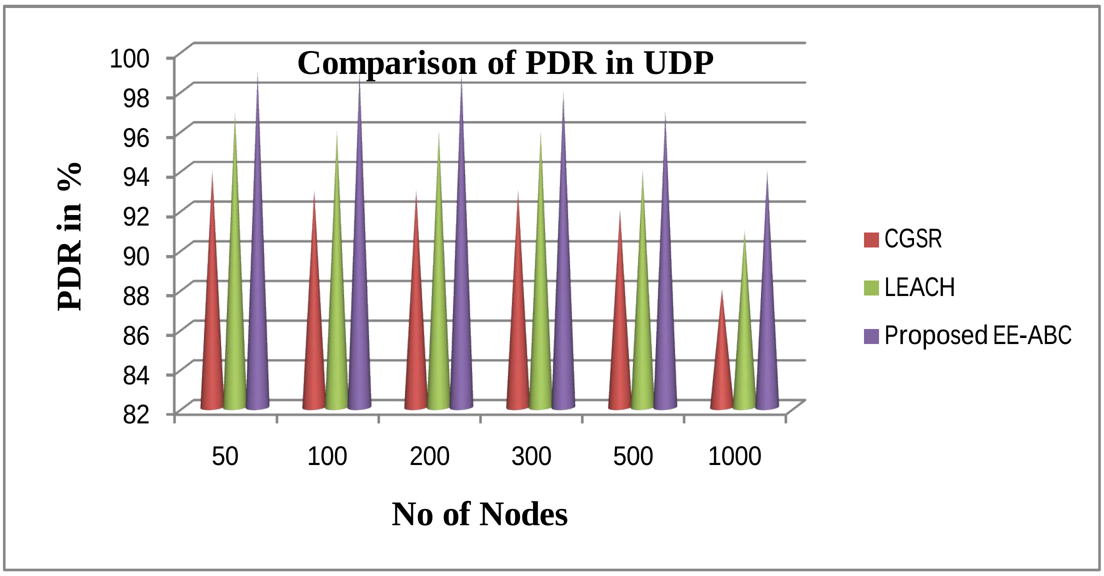


Figure 4.7 Comparison of PDR in UDP

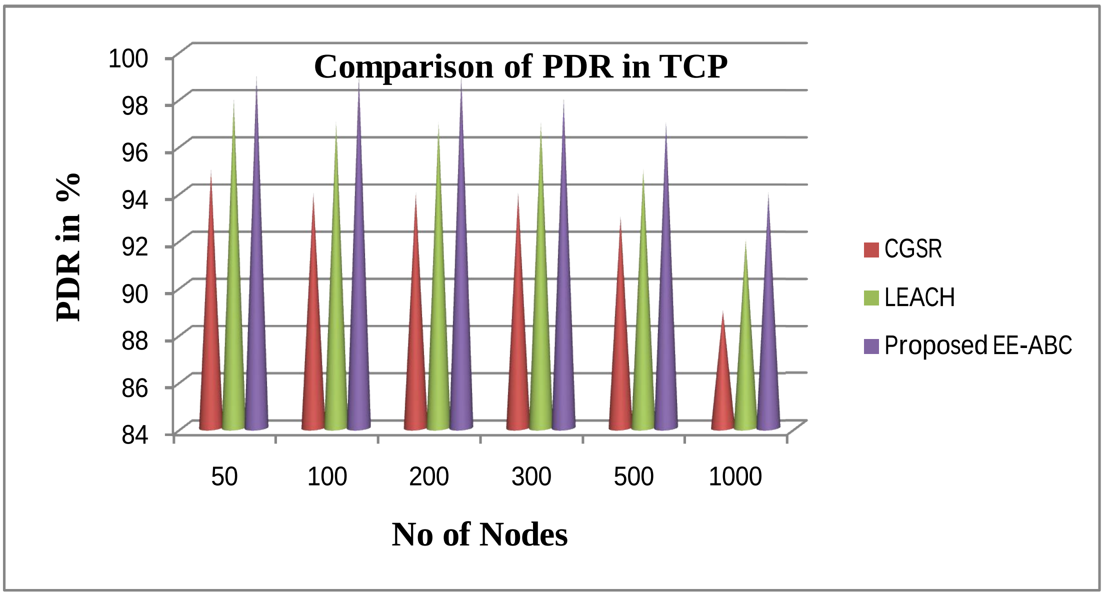


Figure 4.8 Comparison of PDR in TCP

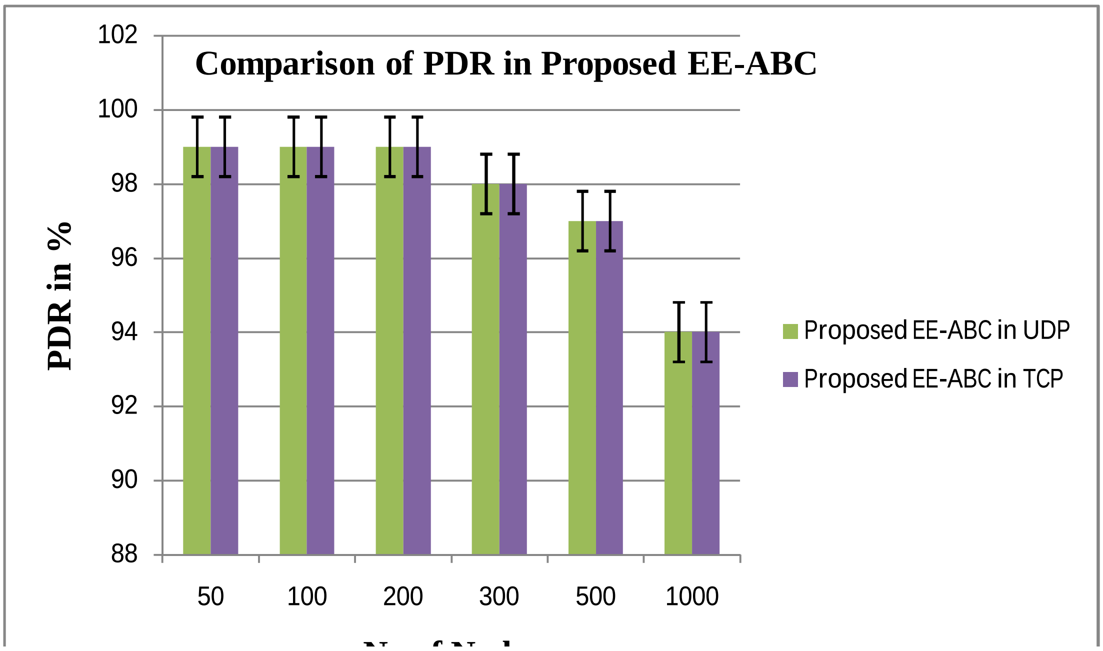


Figure 4.9 Comparison of PDR in Proposed EE-ABC with error bars

The performance in terms of PDR in UDP is shown in Figure 4.7. The performance in terms of PDR in TCP is shown in Figure 4.8, and the performance of proposed EE-ABC in terms of PDR in UDP and TCP are compared with error bars in Figure 4.9.

4.6 Conclusion

From the result and performance analysis, it is obvious that the Latency of the proposed work is improved around 5% more than LEACH and around 8% more than CGSR. Similarly the throughput of the proposed work is improved around 15% more than LEACH and around 10% more than CGSR. The throughput of the proposed work always shows above 95%. The proposed EE-ABC applies energy as the decision parameters in the proposed clustering model, the performance of the proposed work improved better than existing methodologies. Hence, it is concluded that the proposed work outperforms than the existing methodologies.

CHAPTER 5

DYNAMIC GROUP KEY MANAGEMENT SCHEME

5.1 Objective

Security of a network is an important factor in its construction. In the traditional wired networks and infrastructural wireless networks, central servers are available to provide security services for the users inside the network system. A network has to achieve security requirements in terms of authentication, non-repudiation, confidentiality, integrity and availability. The major factor in the implementation of the secured model is the key management system. The main goal of key management system is to manage the keys used by the members of the group and to protect from the unauthorized modifications, and disclosure.

There are many key management systems, in which group key optimal methodology is one of the important method. The purpose of the group key management system is to secure communication among group of nodes in MANET. The main purpose of this group key management system is to generate and distribute common secret for all group members. Various group management schemes have been proposed and are in use (Abbas et al, 2013).

This Group key management involves creating and distributing the public key (Group Key) for all group members. A group is managed and organized by the Group Leader. Group Leader keeps track of group members and identifies node failure or leaving node and disseminates the information to other group members. In this research work, a key management scheme which ensures both forward and backward secrecy with less communication is proposed. The proposed work improved throughput, Reduced Network delay and computational cost.

Virtual infrastructure achieves reliable transmission in MANET. It is affected also by the security vulnerabilities on the routing protocols. Black hole attack is the major problem that affects the virtual infrastructure. It is a severe attack that can be easily employed against routing in mobile ad hoc networks. A black hole is a malicious node that falsely replies for any route requests without having active route to specified destination and drops all the receiving packets.

Hence, in this proposed research work, in addition to the group key management, an algorithmic approach is used for analysing and improving the security of AODV. The aim of the research work is to ensure the security against black hole attack. The proposed solution is capable of detecting black hole node(s) in the MANET at the beginning and a solution to discover a safe route detects cooperative black hole attack.

5.2 Security Requirements

Wireless Network must be capable of keeping the information they are collecting private from eavesdropping. Use of encryption and cryptographic authentication costs both power and network bandwidth. This impacts application performance by decreasing the number of samples than can be extracted from a given network and the expected network lifetime. Effective Sample Rate It is the sample rate that wireless data can be taken at each individual wireless and communicated to a collection point in a data collection network. In-network processing can increase the effective sample rate.

The design requirements of the security model of the wireless network and wireless nodes are discussed in this section. The design requirements of the wireless networks are,

- **Security Vulnerabilities:** It is always advantageous to have the ability to deploy a network over a larger physical area. Multi-hop communication techniques can extend the coverage of the network; but increase the power consumption of the nodes, which may decrease the network lifetime. Additionally, they require a minimal node density, which may increase the deployment cost.

- **Energy efficiency / system lifetime:** The wireless nodes are battery operated, rendering energy a very scarce resource that must be wisely managed in order to extend the lifetime of the network.

- **Cost and ease of deployment:** For system deployments to be successful, the wireless nodes must configure themselves for any possible physical node placement. In the long term, the total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost.

- **Response Time/Latency:** Many wireless applications require delay-guaranteed service. Protocols must ensure that sensed data are delivered to the user within a certain delay. The ability to have low response time conflicts with many of the techniques used to increase network lifetime.

- **Accuracy:** Obtaining accurate information is the primary objective; accuracy can be improved through joint detection and estimation.

- **Fault tolerance:** Robustness to wireless and link failures must be achieved through redundancy and collaborative processing and communication.

- **Scalability:** As a wireless network may contain thousands of nodes, scalability is a critical factor that guarantees that the network performance does not significantly degrade as the network size increases.

- **Transport capacity/throughput:** As most wireless data must be delivered to a single base station or fusion center, a critical area in the wireless network exists, whose wireless nodes must relay the data generated by virtually all nodes in the network. Apparently, this area has a paramount influence on system lifetime, packet end-to-end delay, and scalability.

5.3 Security Attacks

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. For a large-scale wireless network, it is impractical to monitor and protect each individual wireless from physical or logical attack. Attackers may device different types of security threats to make the WN system unstable. Here in this section, is presented a layer-based classification of WN security threats and also based on the capability of the attacker and defenses proposed in the literature.

5.3.1 Outside and Inside Attacker

Outside attacks are attacks from node which is not belongs to a WN; inside attacks occur when legitimate nodes of a WN behave in unintended or unauthorized ways. To overcome these attacks, require robustness against outsider attacks, resilience to insider attacks, graceful degradation with respect to node compromise and realistic levels of security.

5.3.2 Passive versus Active attacks

Passive attacks include eavesdropping on or monitoring packets exchanged within a WN; active attacks involve some modifications of the data steam or the creation of a false stream.

5.3.3 Attacks on Information in Transit

In a wireless network, wireless node monitors the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be attacked to provide wrong information to the base stations or sinks. The attacks are

- **Interruption-** Communication link in wireless networks becomes lost or unavailable. This operation threatens service availability. The main purpose is to launch denial-of-service (DoS) attacks. From the layer-specific perspective, this is aimed at all layers.

- **Interception-** Wireless network has been compromised by an adversary where the attacker gains unauthorized access to wireless node or data in it. An Example of this type of attacks is node capture attacks. This threatens message confidentiality. The main purpose is to eavesdrop on the information carried in the messages. From the layer-specific perspective, this operation is usually aimed at the application layer.

- **Modification-** An unauthorized party not only accesses the data but also tampers with it. This threatens message integrity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer, because of the richer semantics of these layers.

- **Fabrication-** An adversary injects false data and compromises the trustworthiness of information. This threatens message authenticity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This operation can also facilitate DoS attacks, by flooding the network.

- **Replaying existing messages-** This operation threatens message freshness. The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that is not time-aware.

5.3.4 *Host-Based Attacks*

- **User compromise:** This involves compromising the users of a WN, e.g. by misleading the users into revealing information such as passwords or keys about the wireless nodes.

- **Hardware compromise:** This involves tampering with the hardware to extract the program code, data and keys stored within a wireless node. The attacker might also attempt to load its program in the compromised node.

- **Software compromise:** This involves breaking the software running on the wireless nodes. Chances are that the operating system and/or the applications running in a wireless node are vulnerable to popular exploits such as buffer overflows.

5.3.5 Network-Based Attacks

It has two orthogonal perspectives: layer-specific compromises and protocol-specific compromises. This includes all the attacks on information in transit. Apart from that, it also includes deviating from protocol; When the attacker is, or becomes an insider of the network, and the attacker's purpose is not to threaten the service availability, message confidentiality, integrity and authenticity of the network, but to gain an unfair advantage for itself in the usage of the network, the attacker manifests selfish behavior that deviates from the intended functioning of the protocol.

5.3.6 Physical Layer Attack

- **Jamming -** This is one of the DoS Attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal. Jamming attacks in WN are classified as four models, which are 1) Constant - corrupts packets as they are transmitted, 2) Deceptive - sends a constant stream of bytes into the network to make it look like legitimate traffic, 3) Random-randomly alternates between sleep and jamming to save energy, and 4) Reactive - transmits a jam signal when it senses traffic.

  In order to defend against this attack, use spread-spectrum techniques for radio communication. Handling jamming over the Medium Access Control (MAC) layer requires Admission Control Mechanisms. Network layer deals with it, by mapping the jammed area in the network and routing around the area. Algorithms that combine statistically analyzing the received signal strength indicator values, the average time required to sense an idle channel (carrier sense time), and the packet delivery ratio techniques can reliably identify all four types of jamming.

- **Radio interference attack** – This is one in which the adversary either produces large amounts of interference intermittently or persistently. To handle this issue, use of symmetric key algorithms in which the disclosure of the keys is delayed by some time interval.

- **Tampering or destruction -** Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. One defense to this attack involves tamper-proofing the node's physical package. The self-destruction and fault tolerant protocols are briefly discussed below:

  - Self - Destruction (tamper-proofing packages): whenever somebody accesses the wireless nodes physically, they vaporize their memory contents and this prevents any leakage of information.

  - Fault Tolerant Protocols: the protocols designed for a WN should be resilient to this type of attacks.

5.3.7 *Data Link Layer Attacks*

- **Continuous Channel Access (Exhaustion)**: A malicious node disrupts the MAC protocol, by continuously requesting or transmitting over the channel. This eventually leads to a starvation for other nodes in the network with respect to channel access. One of the countermeasures to such an attack is Rate Limiting to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions. A second technique is the use of time-division multiplexing where each node is allotted a time slot in which it can transmit.

- **Collision:** This is very much similar to the continuous channel attack. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change is likely to occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. A typical defense against collisions is the use of error-correcting codes.

- **Unfairness:** Repeated application of these exhaustion or collision based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms, can lead into unfairness. This kind of attack is a partial DoS attack, but results in marginal performance degradation.

- **Interrogation:** Exploits the two-way Request-To- Send / Clear To Send (RTS/CTS) handshake that many MAC protocols use to mitigate the hidden-node problem. An attacker can exhaust a node's resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbor node. To put a defense against such type of attacks a node can limit itself in accepting connections from same identity or use Anti replay protection and strong link-layer authentication.

- **Sybil Attack:** This type of attack is very much prominent in the Link Layer. The first type of link layer sybil attack is data aggregation in which single malicious node is act as different sybil nodes and then this negative reinforcements to make the aggregate message a false one. Second type is voting.

  Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here the sybil attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and of course it depends on the number of identities the attacker owns.

5.3.8 *Network Layer Attacks*

- **Sinkhole:** Depending on the routing algorithm technique, a sinkhole attack tries to attract almost all the traffic towards the compromised node, creating a metaphorical sinkhole with the adversary at the center. Geo-routing protocols are known as one of the routing protocol classes that are resistant to sinkhole attacks.

Because, geo-routing protocol topology is constructed using only localized information, and traffic, which is naturally routed through the physical location of the sink node.

- **Hello Flood:** This attack exploits hello packets that are required in many protocols to announce nodes to their neighbors. A node receiving such packets may assume that it is in the radio range of the sender. A laptop-class adversary can send this kind of packet to all wireless nodes in the network so that they believe the compromised node belongs to their neighbors. This causes a large number of nodes sending packets to this imaginary neighbor. Authentication is the key solution to such attacks. Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link.

- **Node Capture:** It is observed and analyzed that even a single node capture is sufficient for an attacker to take over the entire network. Good solution to this problem would definitely constitute an important work in WN.

- **Selective Forwarding/ Black Hole Attack (Neglect and Greed)**: WN are usually multi-hop networks and hence based on the assumption that the participating nodes will forward the messages faithfully. Malicious or attacking nodes can however refuse to route certain messages and drop them. If they drop all the packets through them, then it is called a Black Hole Attack. However if they selectively forward the packets, then it is called selective forwarding. To overcome this, Multi path routing can be used in combination with random selection of paths to destination, or braided paths can be used which represent paths which have no common link or which do not have two consecutive common nodes, or use implicit acknowledgments, which ensure that packets are forwarded as they were sent.

- **Sybil Attack:** In this attack, a single node presents multiple identities to all other nodes in the WN. This may mislead other nodes and hence routes believed to be disjoint with respect to node can have the same adversary node. A countermeasure to sybil Attack is by using a unique shared symmetric key for each node with the base station.

- **Wormhole Attacks:** An adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker. To overcome this, the traffic is routed to the base station along a path, which is always geographically shortest or use very tight time synchronization among the nodes, which is infeasible in practical environments.

- **Spoofed, Altered, or Replayed Routing Information:** The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. A countermeasure against spoofing and alteration is to append a MAC after the message. Efficient encryption and authentication techniques can defend spoofing attacks.

- **Acknowledgment Spoofing:** Routing algorithms used in wireless networks sometimes requires acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. The most obvious solution to this problem would be authentication via encryption of all sent packets and also packet headers.

- **Internet Smurf Attack:** In this type of attack the adversary can flood the victim node's network link. The attacker forges the victim's address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim. If it gets observed that a node's network link is getting flooded without any useful information then the victim node can be scheduled into a sleep mode for some time to overcome this.

- **Homing:** uses the traffic pattern analysis to identify and target nodes that have special responsibilities, such as cluster heads or cryptographic- key managers. An attacker then achieves DoS by jamming or destroying these key network nodes. Header encryption is a common prevention technique. Using “dummy packets” throughout the network to equalize traffic volume and thus prevent traffic analysis. Unfortunately, this wastes significant wireless node energy, so use it only when preventing traffic analysis is of utmost importance.

5.3.9 Transport Layer Attack

- **Flooding -** An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes. A solution proposed for this problem is the requirement that each connecting client demonstrate its commitment to the connection by solving a puzzle. As a defense against this class of attack, a limit can be put on the number of connections from a particular node

- **De-synchronization Attacks:** In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the adversary maintains a proper timing, it can prevent the end points from exchanging any useful information. This will cause a considerable drainage of energy of legitimate nodes in the network in an endless synchronization-recovery protocol. A possible solution to this type of attack is to require authentication of all packets including control fields communicated between hosts. Header or full packet authentication can defeat such an attack.

5.3.10 *Application Layer Attacks*

- **Overwhelm attack:** An attacker may attempt to overwhelm network nodes with wireless stimuli, causing the network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains node energy. We can mitigate this attack by carefully tuning wireless so that only the specifically desired stimulus, such as vehicular movement, as opposed to any movement, triggers them. Rate-limiting and efficient data-aggregation algorithms can also reduce these attacks' effects.

- **Path-based DoS attack:** It involves injecting spurious or replayed packets into the network at leaf nodes. This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station. Combining packet authentication and anti-replay protection prevents these attacks.

- **Deluge (reprogram) attack:** Network-programming system allows remotely reprogram nodes in deployed networks. If the reprogramming process insecure, an intruder can hijack this process and take control of large portions of a network. It can use authentication streams to secure the reprogramming process.

5.4 Survey on Secured MANET

Many researchers in the literature deal with virtual infrastructure concept based the battery power and signal strength. Prior work uses a simple group key management approach. The basic idea of this scheme is that a multicast tree is formed in MANET for efficient dissemination of messages including keys. It basically uses the same multicast tree structure and defines new group key agreement protocols.

Two multicast trees are constructed and maintained in parallel to achieve fault tolerance. Group members take turns as group coordinators to compute and multicast the blinded keys to all members through the active tree links. Each group member computes the group key locally by collecting the necessary keys from the group coordinator. The operation can be made in rounds and the coordinator is selected. Construction and maintenance of double multicast tree demand additional memory requirement and require additional computation on construction and maintenance. It also increases the work burden of the node which is acting as Group Leader.

Only group members who know the current group key are can recover the original message. The DH protocol can be extended to a generalized version of n-party DH. Research efforts have been put into the design of a group key management protocol for improving the scalability, reliability, and security. Furthermore, group key management also needs to address the security issue related to membership changes. The modification of the membership requires refreshment of the group key. This can be done either by periodic rekeying or updating right after a member change.

Group key management protocols can be classified into three categories: centralized, decentralized, and distributed. In the distributed method, group members themselves contribute to the formation of a group key and are equally responsible for the rekeying and distribution of group keys. Key management protocol is a critical component for securing group communications.

However, group key management for large and dynamic groups in MANETs is a difficult problem because of the restrictions on available resources and unpredictable mobility.

Group members take turns acting as group coordinators to compute and distribute intermediate key materials to group members. So, the duty of group maintenance and the burdens of computation, storage, and energy consumption are balanced among all mobile nodes. The intermediate keys are delivered through the tree links for efficiency. Each group member computes the group key locally without maintaining a logic key tree. Another important factor is to improve the performance of the overall system to achieve less end-to-end and network delay by using Secured Group Key Management Scheme.

A secure key management method in group structured MANET, where a group leader is responsible to generate, maintain and revoke the key of group members. Shifting the ownership of the group leader from one node to another node. By the time it transfers many secret info including key & function to generate key. Each time transferring this information increases overhead in network.

5.5 Proposed Dynamic Group Key Management Scheme (DGKMS)

A novel mutual authentication and key management protocol is proposed, which satisfies most of the security requirements like mutual authentication, confidentiality, integrity for one hop communication in MANET. In the proposed work, there is no pre key distribution and key storage for making protected data transmission in vulnerable wireless link. Common secret key is generated only between the communicating peers on the fly to provide secure communication simultaneously, while performing authentication.

There are three scenarios in the proposed work, which are given below:

Case 1 : Time Triggered Protocol (TTP) is completely reachable by every node of the MANET.

Case 2 : TTP is not reachable by some of the nodes of the MANET.

Case 3 : TTP is not reachable by any of the node of the MANET.

This authentication and key agreement protocol is based on authority based MANET. Every node gets a certified token from the TTP after successful verification of its credentials. All nodes are properly set up with certified tokens before network formation. TTP can be a mobile node in the MANET or it can be a separate entity, apart from MANET and its presence is not compulsory in the active phase of the network. Each node is hard coded, which is unique in nature and immutable.

There are two phases involved in the proposed work, which are 1) Bootstrap phase, 2) Authentication and key management phase. The bootstrap phase is a pre-authentication phase. TTP verifies the credential information of the particular node to examine its genuineness. On successful verification TTP generates and distributes token to that particular node.

The authentication and key management phase is executed when a node in MANET needs to communicate with other nodes which are one hop distance. This approach is scalable, requires reasonable computational complexity and less communicational overhead.This authentication and key management (agreement) protocol is scalable, which requires reasonable computational complexity and less communicational overhead.

5.5.1 *Secured Group Key Management Scheme*

This Secured Group Key Management Scheme generates and distributes group key, thus reducing the burden of generating and verifying blinded key for each group members. In addition, it performs periodic rekeying and periodic group leader changes. The proposed Key Management technique is propagation of speeds of request and statistical profiling; they do not require network-wide synchronized clocks, do not impose any additional control packet overhead, and need only simple computations by the group leader and group member of connections.

The technique is based on reducing the computational burden and memory requirement of the node acting as a group leader. It implements the techniques in a widely studied secured group key management system and evaluated their effectiveness. Once the group is formed, a group leader is elected and it generates and distributes group key for that group and intimates its group members to generate private keys.

The methodology implemented for Rekey on Member Join is shown below:

- Node n broadcast a “Hi” message to all its neighbouring nodes. Send_msg(“Hi”).

- If the message received by a neighbour node which is not the Group Leader (GL) then: Forward the message to its neighbour node.

- If the message is received by a neighbour node which is the present group leader then:

  a) GL request for some basic confidential information to the new node.

  b) Verify the information and authenticate the new node.

  c) Provide the group_id and let permission to the new node to generate private key_id.

  d) Broadcast information about the new member to the group members.

The methodology for Re-key on Member Leave is described below:

- The node that leaves the group has to send a leave notice to the group leader.
- Send leave ("Leaving!!"). If the group leader wants to leave the network then it must have to perform handoff.
- If the message received by a neighbour node which is not the GL then forward the message to its neighbour node.
- If the message is received by a neighbour node which is the present group leader then:

  a) Broadcast the node leaving information to all the member of the group (i.e.,) if node A leave then group leader will broadcast the message as "Node A doesn't belongs to the group anymore".

  b) Generates a new group key for the group and notifies the group member to rekey their private keys.

The methodology for the Periodic rekeying is explained in the below: It assumes n-party DH algorithm for key generation. It uses the algorithm to generate key.

$$k = m^e \bmod n \qquad (5.1)$$

Where, k is the key, n is a prime number, m is a random number chosen by the node and e is primitive root of the prime number.

The methodology for the Periodic Group Leader Change is briefed below:

It is assumed that the node that acts as the GL should maintain a timer for certain sec/min/hrs.

- When the timer reaches the grace period then: GL will broadcast a message leadership change(“request for leadership change”);

- The node that is a valid member of the group and which provides a fast response to the request will be the new group leader.

- Perform handoff.

- Broadcast message about the new GL to the group member.

- Performs rekeying operation.

Every time the group leader verifies the request sent by the member of the group for group leader change request, the group leader verifies the information of each of the node. The node that doesn’t send any response is considered as the non-existing node and the group leader will broadcast the non-existing node information to its group members.

5.5.2 *System Architecture of DGKMS*

The responsibilities of the system are partitioned in such a way that each subsystem performs its own functions and when they are integrated together, they represent the complete functionality of the system. The first module takes the responsibility group formation and selecting the Group Leader.

The next immediate module is responsible for generating the Group key. It deals with DH algorithm implementation and in turn makes use of Message Digest 5 (MD5) for key generation. Whenever a Group leader is chosen the information has to be broadcast along with the group key. The next module deals with interval-based rekeying among the group members. It also performs rekeying on ever membership change. When a new node tries to join in a network the intermediate nodes are responsible for forwarding the packets from the new node to the Group Leader of the existing group.

Each node generates its join request; the requests are verified to ensure security. If the request is appropriate, new node is authenticated and included in the group. Then the group leader will generate a broadcast message that includes: information about new node, new group key and rekeying notice for all the group members. Node leaving operation works in the same way as like the operations that involves when a node joins except that the node must have to generate a leaving notice to the group leader.

The system performs interval-based Group Leader change operation to share the work burden of all the nodes among the network. This is done to maintain the security of the network. It is hard to predict the mobility of a wireless node. So a node can act as a group leader only for a certain period of time.

When a group leader change operation is performed the node performs handoff. The new node that has been selected as a new group leader performs rekeying to protect the information about the group. Once the hand off and rekeying is done new group leader ID is passed to all the nodes in the network.

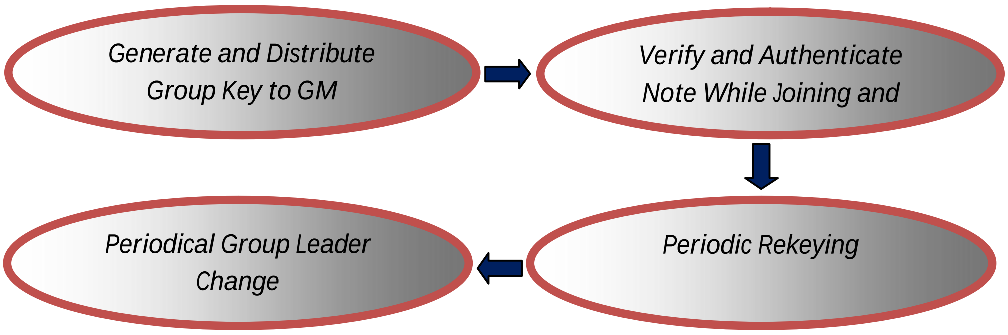

Generate and Distribute Group Key to GM
Verify and Authenticate Note While Joining and
Periodic Rekeying
Periodical Group Leader Change

Figure 5.1 Basic Information Flow in GKMS

The basic information flow diagram is shown above. It describes the functionality of the starting of modules. It contains four states namely: Generate and distribution of group by GL, verify and authenticate node while joining and leaving, periodic rekeying and periodic group leader change.

5.5.3 *Algorithms*

Algorithm-A:node_join()

- Create a node, n.

- Node n broadcast a “Hi” message to all its neighboring nodes. Send_msg(“Hi”)

- if the message is received by a neighbor node which is the present group leader then:

  a. GL request for some basic confidential information to the new node.

  b. Verify the information and authenticate the new node.

  c. Provide the group_id and let permission to the new node to generate private key_id.

- If the message received by a neighbor node which is not the GL, then Forward the message to its neighbor node.

Algorithm-B: **node_ leave()**

- The node that leaves the group has to send a leave notice to the group leader. Send leave (“Leavind!!”). If the GL wants to leave the network it has to elect new leader and performs handoff.

- if the message is received by a neighbour node which is the present group leader then:

a. Broadcast the node leaving information to all the member of the group (i.e.,) if node A leave then GL will broadcast the message as “Node A doesn’t belongs to the group anymore”.

b. Invoke group_rekey() algorithm.

- If the message received by a neighbour node which is not the group leader (GL) then: Forward the message to its neighbour node.

Algorithm-C: GL_Change()

Assumption: The node that acts as the GL must have to maintain a timer for certain sec/min/hrs.

- When the timer reaches the grace period then: Group Leader will broadcast a message leadership_change(“request for leadership change”);

- Group Leader verifies which node have send response and which node doesn’t send any response. Nodes which dint respond are considered as the non-member node and is identified.

- The node that is a valid member of the group and which provides a fast response to the request will be the new group leader.

a) Perform handoff.

b) Broadcast message about the new GL to the group member.

- Invoke group_rekey().

Algorithm-D: rekey()

Assumption: either can use MD5/ data encryption standard algorithm.

- Invoke n-party DH (MD5) algorithm.
- Broadcast the new key generated to the group. Broadcast(groupke, ki).
- Along with the key, send intimation to the group member to generate a new key.
- Return.

5.6 Result and Performance Analysis

The proposed DGKMS in this thesis is compared with the traditional Target Authority (TA) Model and Recent Mobile Agent (MA) model. The Reliability and scalability are major research issues in the design of networking protocol.

Hence, the proposed work has analysed the reliability and scalability of proposed work and compared with TA and MA. The reliability is computed based on the simulation data and result. The number of nodes is varied and number of attacker node also varied for performance comparison.

The simulation data is shown in Table 5.1. The reliability when 10% of attacker node, 20% of attacker node, and 30% of attacker node are shown in Figure 5.1, 5.2 and 5.3.

Table 5.1 Simulation Environment

Parameters	**Values**
Simulation Time	10 unit time
No of Nodes	100, 200, 300, 500 and 1000
Attacker Nodes	10%, 20% and 30% on total number of nodes
Reliability	In term of Packet Delivery Ratio (PDR)
Scalability	Model supports > 75% PDR

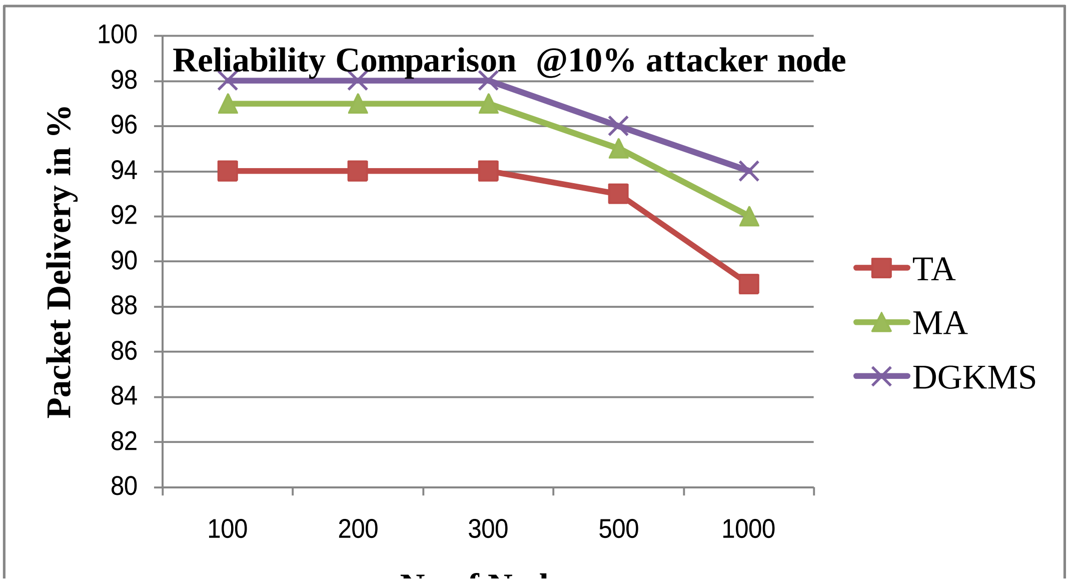


Figure 5.2 Reliability When 10% of Attacker Node

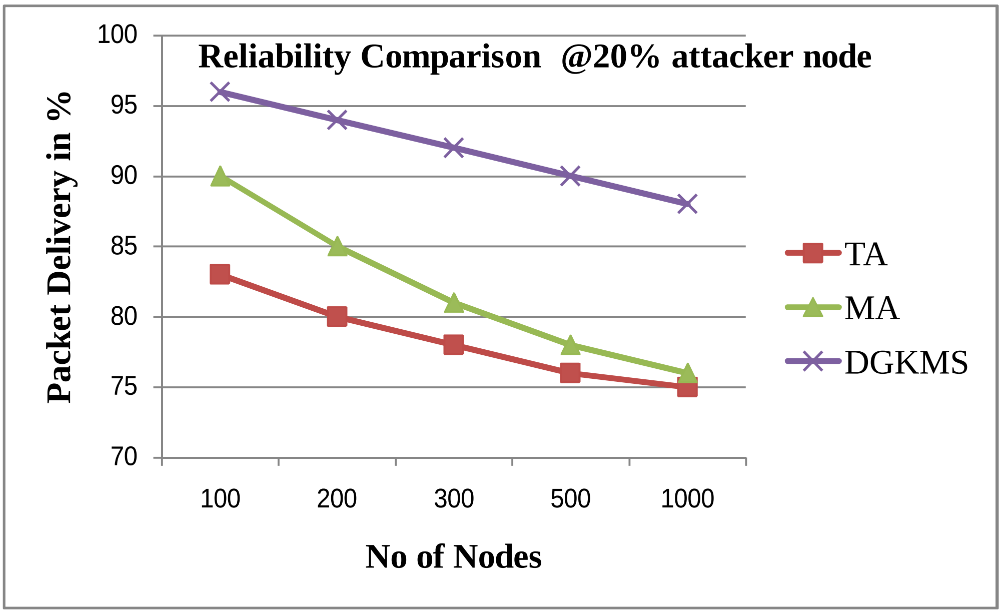


Figure 5.3 Reliability When 20% of Attacker Node

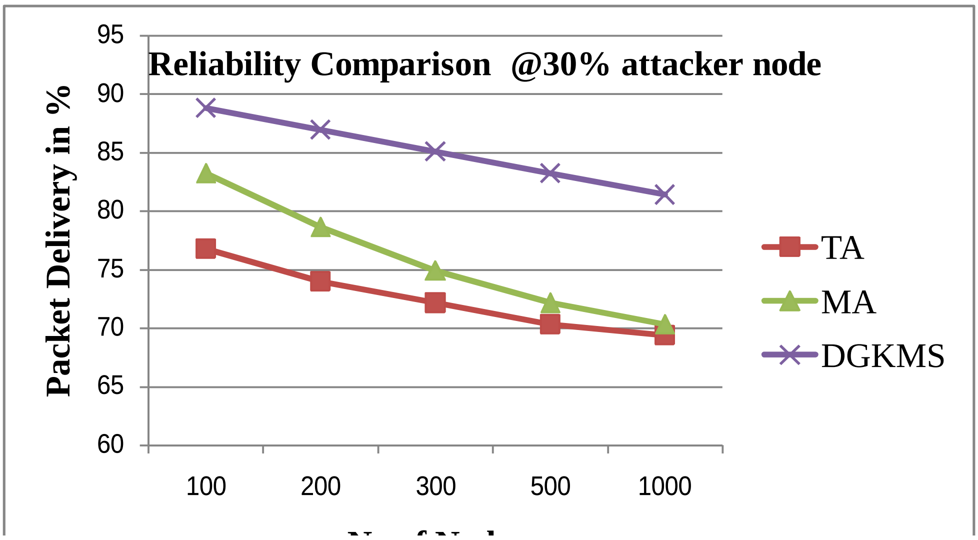


Figure 5.4 Reliability When 30% of Attacker Node

The reliability of the methodologies is computed based on packet delivery ratio. The packet delivery ratio is total number of effectively delivered packets and total number of data packets transmitted. The packet delivery ratio is computed by increasing number of nodes and increasing number of attacker nodes. The numbers of attacker node are defined as 10%, 20% and 30% of the total number of nodes. The number of nodes are varies from 100 nodes, 200 nodes, 300 nodes, 500 nodes and 1000 nodes.

5.7 Conclusion

The scalability is observed from the above data, in which the system has 70% and above packet delivery ratio only accepted as scalable system. Hence, when 10% attacker nodes are inserted the TA supports up to 300 Nodes, whereas MA supports up to 500 Nodes and proposed DGKMS support 1000Nodes.

When attacker nodes are increases to 20% of number of nodes, the TA supports up to 300 Nodes only, whereas MA supports up to 500 Nodes and proposed DGKMS support even for 1000Nodes. Similarly, the TA supports only 100 Nodes, the MA supports up to 200 Nodes when 30% of attacker nodes are inserted. The proposed system always supports above 80% packet delivery ratio. Hence, the proposed system proves better scalability than the existing systems.

CHAPTER 6

SECURED AND SCALABLE VIRTUAL INFRA STRUCTURE (SASVIS)

6.1 Proposed SASVIS

This research work proposes three methodologies which are 1) Scalable EE-ABC Clustering, 2) Node Authentication using SGKMS and 3) Secured Model against Black hole attack (SMB).

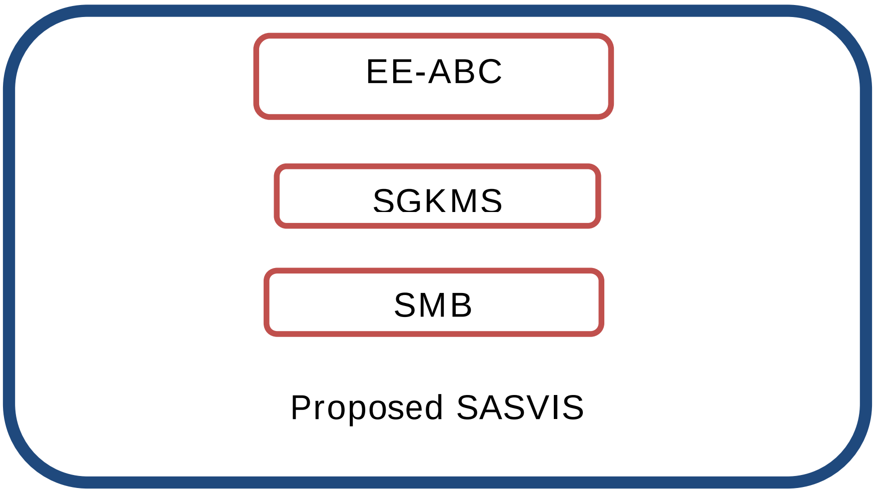


Figure 6.1 Proposed SASVIS System Diagram

6.1.1 *Proposed Energy Efficient and Scalable ABC Clustering*

The design and working nature of the proposed ABC is redefined in order to provide optimality. The existing ABC has a few pitfalls such as the improper number of scout bee will lead local optimal problem, slow convergence and as a result is non-feasible especially for computer network routing.

The bees search for food sources in a way that maximizes the ratio

$$\forall (E, H) \Leftrightarrow F(\theta_i) = \frac{E}{H} \tag{6.1}$$

Where, E is the energy obtained, H is the hop count, number of Inter Mediate Peer between hive to the food source. Here E is proportional to the nectar amount of food sources discovered by bees and it works to maximize the honey being stored inside the hive. In a maximization problem, the goal is to find the maximum of the objective function, F(θ). F(θ) is the nectar ratio, shown in equation (6.1), $\theta \in R^P$. R^P represents the region of the search area.

Assume that θ_i is the position of the ith food source; $F(\theta_i)$ represents the nectar ratio of the food source located at θ_i and it is proportional to the energy $E(\theta_i)$.

If the nectar ratio, F (θ), of the food source is higher than the minimum threshold, then the scout bee initialises the waggling dance with rhythm above the food source (which is called as dance floor). This waggling dance is a visualization technique that can transfer information to the insight worker bees. If the worker bees are beyond insight, the rhythm of scout bee may reach the worker bee. Based on the visual and or audio information from the scout bee, the worker bee from one hive or more hive will reach the dance floor (food source) for collecting the nectar.

$$T(\theta_i) = \begin{cases} \alpha \bullet F(\theta_i) & F(\theta_i) > F_{th} \\ 0 & otherwise \end{cases} \qquad (6.2)$$

$$R(\theta_i) = \begin{cases} \beta \bullet F(\theta_i) & F(\theta_i) > F_{th} \\ 0 & otherwise \end{cases} \qquad (6.3)$$

Where the $T(\theta_i)$ is the duration of waggling dance, $R(\theta_i)$ is the volume of rhythm, $F_{th}$is the minimum threshold of the nectar value and α, β are the constant which is termed as time scale factor and volume scale factor.

$$0 < \alpha < 1 \qquad (6.4)$$

$$0 < \beta < 1 \qquad (6.5)$$

If the value of α and β are small, then convergence becomes fast. If the value of the same is high, more precise result will occur.

The bees search for food sources and collect the nectar (E). This process initiates the waggling dance on the floor for T time units (based on the equation 2) with an R volume of the rhythm (based on the equation 6.3).

If the dancing time of the bee has elapsed, it will search the neighbouring dancing bee and goes to the dance floor of neighbouring bee to watch the dance as guest bee. It more than one dancing bee is found near the bee chooses the one with higher rhythm (Rhythm of bee proportional to nectar).

The energy level of the ad hoc nodes or sensory nodes is mapped as the rhythm of the ABC. When a guest bee enters the dancing floor, the data from this guest bee is stored in the nectar (routing) table of dancing bee. The mapping of biological terms with the networking terms for the proposed ABC clustering methodology are described in table 6.1.

6.1.2 *Proposed secured key Node Authentication*

The system architecture of the proposed secured key node authentication is shown in figure 6.2.

The responsibilities of the system are partitioned in such a way that each subsystem performs its own functions and when they are integrated together, they represent the complete functionality of the system. The next stage of the system is responsible for generating the Group key. It deals with DH algorithm implementation and in turn makes use of MD5 for key generation. Whenever a Group leader is chosen, the information has to be broadcasted along with the group key.

Next step deals with interval-based rekeying among the group members. It also performs rekeying on ever membership change. When a new node tries to join in a network the intermediate nodes are responsible for forwarding the packets from the new node to the Group Leader of the existing group.

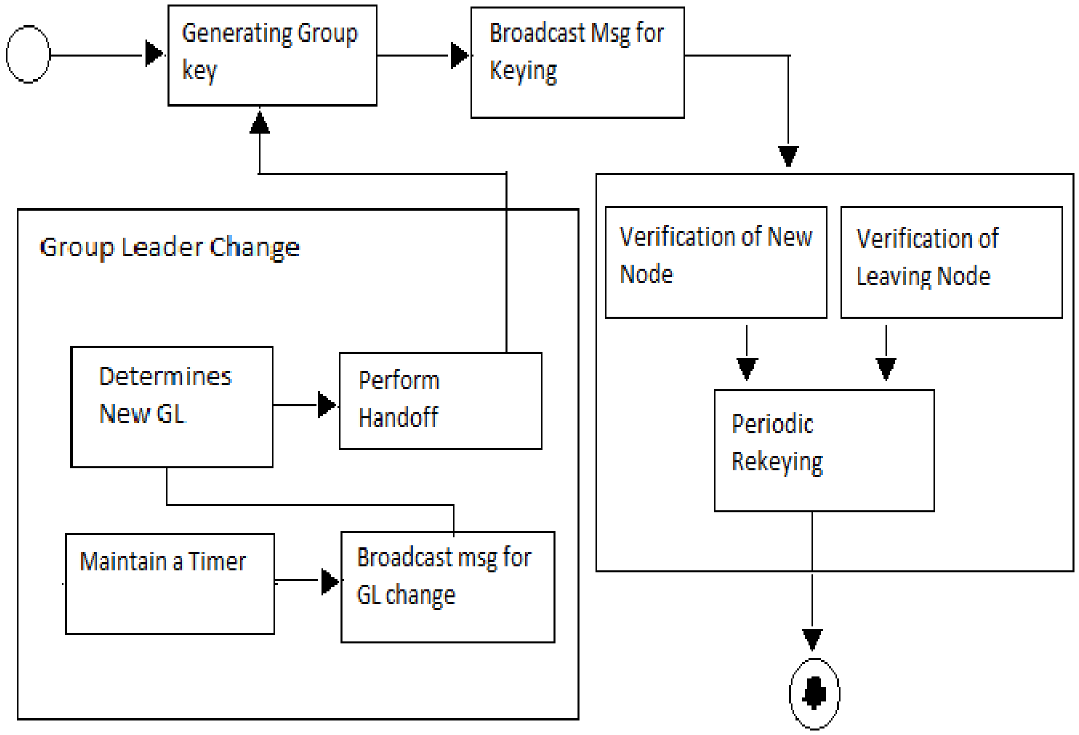


Figure 6.2 System Architecture of Secured Key Node Authentication

Each node generates its join request; the requests are verified to ensure security. If the request is appropriate, a new node is authenticated and included in the group. Then the group leader generates a broadcast message that includes: information about new node, new group key and rekeying notice for all the group members. The Node leaving operation works in the same way as the operations that involves when a node joins except that the node must have to generate a leaving notice to the group leader.

The system performs interval-based Group Leader change operation to share the work burden of all the nodes among the network. This is done in order to maintain the security of the network. It is hard to predict the mobility of a wireless node. So a node can act as a group leader only for a certain period of time. When a group leader change operation is performed the node performs handoff. The new node that has been selected as a new group leader performs rekeying to protect the information about the group. Once the hand off and rekeying is done, the new group leader ID is passed to all the nodes in the network.

The basic information flow diagram is shown in figure 6.1. It describes the functionality of the starting of the modules. It contains four states namely: Generate and distribution of group by GL, verify and authenticate node while joining and leaving, periodic rekeying and periodic group leader change.

6.2 Proposed Secured Model Against Black Hole Attack

The proposed mechanism for defending against a cooperative black hole attack modifies the AODV protocol by introducing two concepts, viz., (i) Data Routing Information (DRI) table and (ii) Cross Checking. In the proposed scheme, two bits of additional information are sent by the nodes that respond to the Route Request (RREQ) message of a source node during the route discovery process. Each node maintains an additional DRI table.

In the DRI table, bit 1 stands for ‘true’ and bit 0 stands for ‘false’. The first bit ‘From’ stands for the information on the routing data packet from the node (in the Node filed), while the second bit ‘Through’ stands for information on routing data packet through the node (in the Node field). The algorithm for proposed secured model is given below:

A. Algorithm for Detection of Grouped Malicious Node to Avoid Black Hole Attack

```
SN broadcasts RREQ
SN receives Route Reply
IF (RREP is from DN or a reliable node) {
    Route data packets (Secure Route)
}
ELSE {
    Do {
        Send FRq and ID of IN to NHN
        Receive FRp, NHN of current NHN, DRI entry for NHN's next hop,
            DRI entry for current IN
        IF (NHN is a reliable node) {
            Check IN for black hole using DRI entry
            IF (IN is not a black hole)
                Route data packets (Secure Route)
            ELSE {
                Insecure Route
```

```
                    IN is a black hole
        All the nodes along the reverse path from IN to the node that
                        generated RREP are black holes
              }
          } ELSE
        Current IN = NHN
        } While (IN is NOT a reliable node)
  }
```

Where, SN denotes Source Node, IN denotes Intermediate Node, FRq is Further Request, DN is Destination Node, NHN is Next Hop Node, FRp is Further Reply and ID is Identity of the node.

6.3 Results and Discussion

The proposed work is simulated in Network Simulator 2 (NS2) and the performance of proposed work is compared with existing well known protocols. The simulation environment is shown in Table 6.1.

Table 6.1 Simulation Environment

Parameter	Value
Number of sensors	50,100, 200, 300, 400, 500, 1000
Total Time of Simulation	10 Sec
Protocols Compared	LEACH, CGSR

Table 6.2 Latency of Data Transmission

No of Nodes	CGSR	LEACH	Proposed SASVIS
50	65	63	61
100	81	77	75
200	100	95	93
300	123	117	116
500	152	146	144
1000	188	179	176

Table 6.3 Throughput of Data Transmission

No of Nodes	CGSR	LEACH	Proposed SASVIS
50	164	179	199
100	186	211	234
200	206	233	258
300	218	247	274
500	229	259	288
1000	239	271	301

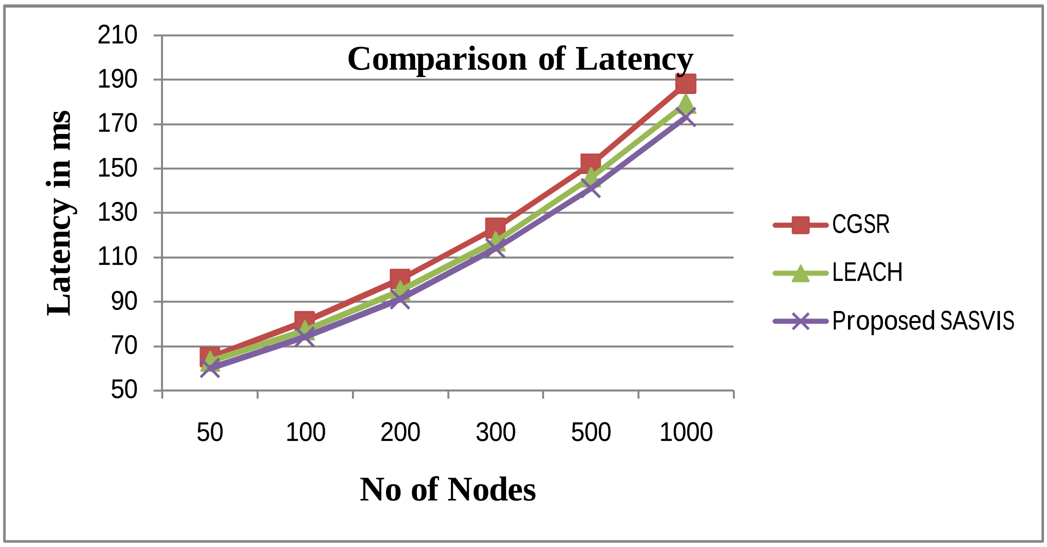


Figure 6.3 Comparison of Latency

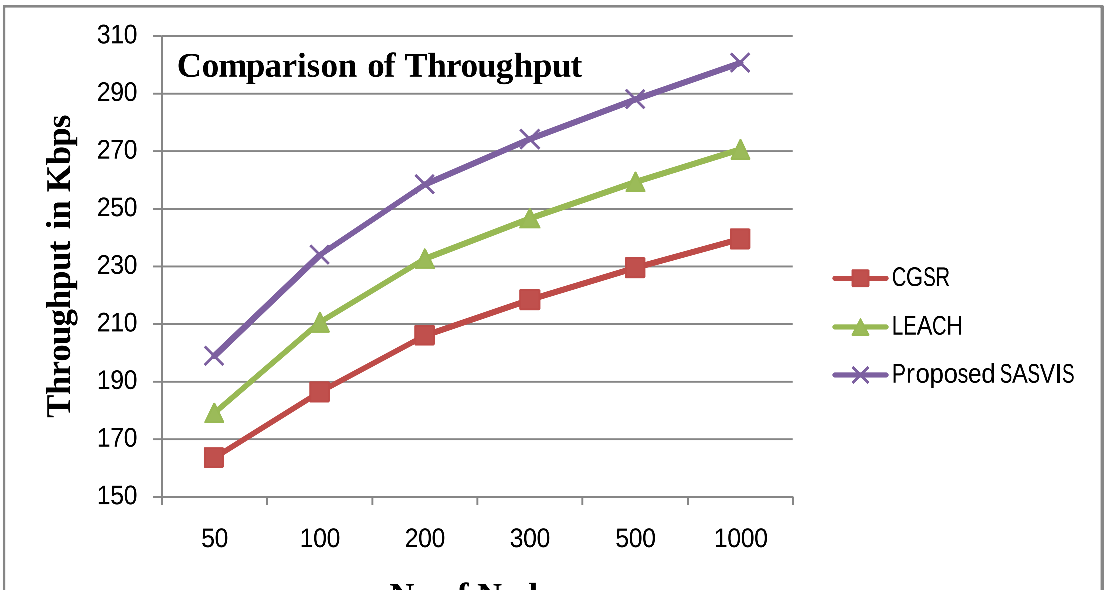


Figure 6.4 Comparison of Throughput

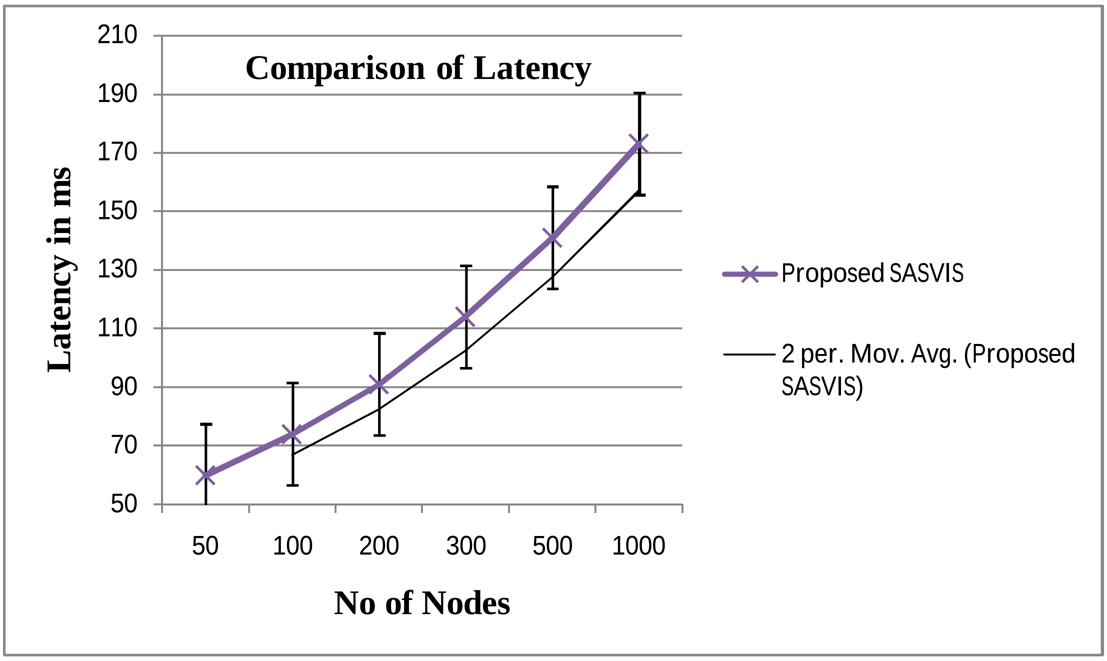


Figure 6.5 Performance of Proposed Work in Latency with Trend Line and Moving Average

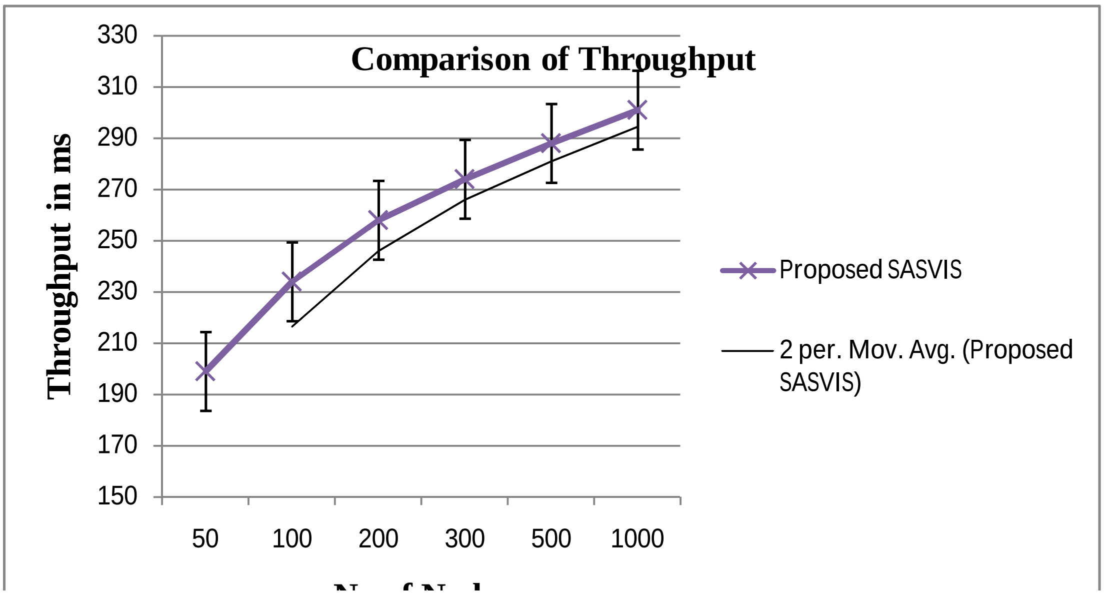


Figure 6.6 Performance of Proposed Work in Throughput with Trend Line and Moving Average

The performance in terms of latency and throughput on various numbers of nodes are recorded in Table 6.2 and 6.3.

The proposed work compared with CGSR and LEACH. The performance of proposed work with trend line and two point average also represented in Figure 6.2 and 6.3.

6.4 Conclusion

From the result and performance analysis, it is concluded that the proposed SASVIS improves the performance of virtual infrastructure. The latency of the proposed work is reduced around 6% than CGSR and around 3% than LEACH.

The throughput of the proposed work is improved by around 25% than CGSR and around 11% than LEACH. Hence, it is concluded that the proposed work will outperform than the existing methodologies.

CHAPTER 7

CONCLUSION AND FUTURE DIRECTION

7.1 Summary

In this research work, security and clustering are focused for effective virtualization of MANET. In clustering, energy efficient clustering with effective node deployment is proposed. In security, dynamic group key management based security model is proposed.

The proposed node deployment model is explained in chapter 3. From the result, it is obvious that the proposed node deployment architecture provides effective utilization of power, minimum wastage of bandwidth and stable clustering structure, minimized overhead, effective maintenance phase and maximized lifespan of mobile nodes in the system.

The proposed EE-ABC based clustering model is described in chapter 4. From the result and performance analysis, it is proved that the Latency of the proposed work is improved around 5% more than LEACH and around 8% more than CGSR. Similarly the throughput of the proposed work is improved around 15% more than LEACH and around 10% more than CGSR. The packet loss of the proposed work is shown always above 95%. Hence, it is concluded that the proposed work outperforms than the existing methodologies.

The proposed DGKMS is shown in chapter 5. In the result and performance analysis, scalability and reliability are computed. The scalability is observed from the above data, in which the system has 70% and above packet delivery ratio only accepted as scalable system. Hence, when 10% attacker nodes are inserted, the TA supports up to 300 Nodes, whereas the MA supports up to 500 Nodes and proposed DGKMS support 1000Nodes. When attacker nodes are increases to 20% of number of nodes, the TA supports up to 300 Nodes only, whereas the MA supports up to 500 Nodes and proposes DGKMS support even for 1000Nodes.

Similarly, the TA supports only 100 Nodes, the MA supports up to 200 Nodes when 30% of attacker nodes are inserted. The proposed system always supports above 80% packet delivery ratio. Hence, the proposed system proves better scalability than the existing systems.

From the above results and performance analysis, it is concluded that the proposed work will perform optimal than the existing works.

7.2 Future Scope

The proposed methodologies for clustering, security are implemented in the simulation environment using NS2. The result of real time implementation of these methodologies may differ from the simulation result. This may lead to a study of the performance degradation factors which affect the proposed methodologies. Hence, the real time implementation may provide additional research problems to the active researchers.

The security model of the proposed work concentrates on MANET. Cellular communication is one among the important resource of everyone’s life time and which is growing rapidly over the past few decades. Hence, the proposed secured model can be implemented to the upcoming 5G and beyond cellular networks.

REFERENCES

1. Abbas, S., Merabti, M., Llewellyn-Jones, D., and Kifayat, K., “Lightweight Sybil Attack Detection in MANETs”, IEEE Systems Journal, Vol. 7, No. 2, pp. 236-248, 2013
2. Ahmed, M.A., Haidar, Azah Mohamed, AiniHussain, and Norazila Jaalam “Artificial Intelligence application to Malaysian electrical power system”, Journal of Expert Systems with Applications (Elsevier), Vol. 37, pp. 5023-5031, 2010.
3. Ali M. and Babak, A. “A new clustering algorithm based on hybrid global optimization based on a dynamical systems approach algorithm”, Expert Systems with Applications (Elsevier), Vol. 37, pp. 5645-5652, 2010.
4. Alok, S., “An artificial bee colony algorithm for the leaf-constrained minimum spanning tree problem”, Applied Soft Computing (Elsevier), Vol. 9, pp. 625-631, 2009.
5. Andrew, K. and Wenyan, L. “Short-term prediction of wind power with a clustering approach”, Renewable Energy (Elsevier), Vol. 35, pp. 2362-2369, 2010.
6. Berenbrink, P., Cooper, C., and Hu, Z., “Energy efficient randomised communication in unknown AdHoc networks Original Research Article”, Theoretical Computer Science, Vol. 410, No. 27–29, pp. 2549-2561, 2009.
7. Bhagavathula, R; Thanthry, N., and Pendse, R,, “Mobile IP and virtual private networks”, Proceedings on Vehicular Technology , pp. 2414 – 2418, 2002

8. Bin-Xie, Kumar, A. and Agrawal, D.P. “Enabling multiservice on 3G and beyond: challenges and future directions”, IEEE Wireless Communications, Vol. 15, No. 3, pp. 66 - 72, 2008 .

9. Boukerche, A. F.; Zarrad, A; and Araujo, R. E., “A Cross-Layer Approach-Based Gnutella for Collaborative Virtual Environments over Mobile Ad Hoc Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 21 , No. 7, pp.911 – 924, 2010

10. Bravo-Torres, J.F., Lopez-Nores, M., and Blanco-Fernandez, Y., “Experiences with virtual mobile nodes that do move in vehicular ad hoc networks”, Proceedings of Third International Conference on Network of the Future (NOF), 2012.

11. Budyal, Manvi and Hiremath, “Agent driven multi-constrained quality of service any cast routing in mobile ad hoc networks”, Proceedings of International Conference on Information Networking, pp. 391 - 396, 2013

12. Chan, A.C.-F., “Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks”, IEEE Wireless Communications Letters, Vol. 1 , No. 1, pp. 46-48, 2012.

13. Chandramohan B. and Baskaran R., “Survey on Recent Research and Implementation of Ant Colony Optimization in Various Engineering Applications”, International Journal in Computational Intelligent Systems, Vol. 4, No. 4, pp. 556 – 582, 2011(f)

14. Chandramohan, B. and Baskaran, R., “Improving network performance by optimal load balancing using ACO based Redundant Link Avoidance algorithm”, International Journal of Computer Science Issues, Vol. 7, Issue. 3, No. 6, pp. 27 – 35, 2010

15. Chandramohan, B. and Baskaran, R., “Energy Aware and Energy Efficient Routing Protocol for Adhoc Network using Restructured

Artificial Bee Colony System”, HPAGC 2011, Vol.169, pp. 480 – 491, 2011(a)

16. Chandramohan, B. and Baskaran, R., “Priority and Compound Rule Based Routing using Ant Colony Optimization”, International Journal of Hybrid Intelligent System, Vol. 8, No. 2, pp.93 – 97 , 2011(b)

17. Chandramohan, B. and Baskaran, R., “Survey on Recent Research and Implementation of Ant Colony Optimization in Various Engineering Applications”, International Journal in Computational Intelligent Systems, Atlandis Press, Vol. 7, Issue 4, 2011(d)

18. Chandra, R., “A Virtualization Architecture for Wireless Network Cards”, Published by Cornell University, 2006.

19. Changsheng, Z., Dantong, O. and Jiaxu, N. “An artificial bee colony approach for clustering”, Expert Systems with Applications (Elsevier), Vol. 37, pp.4761-4767, 2010.

20. Chowdhury, N.M.M.K. and Boutaba, R. “Network virtualization: state of the art and research challenges”, IEEE Communications Magazine, Vol. 47, No. 7, pp. 20-26, 2009

21. CvZhu, T., Zhang, Y., Wang, F., and Lv, W., “ A location-based push service architecture with clustering method “, Proceedings of Sixth IEEE International Conference on Network Computing and Advanced Information Management (NCM), pp. 107-112, 2010.

22. David, V., Julio, C., Francisco, J. and Nicolas, R. “A Honey Bee Foraging approach for optimal location of a biomass power plant”, Applied Energy (Elsevier), Vol. 87, pp. 2119-2127, 2010.

23. Derr, K., and Manic, M., “Extended Virtual Spring Mesh (EVSM): The Distributed Self-Organizing Mobile Ad Hoc Network for Area

Exploration", IEEE Transactions on Industrial Electronics, Vol. 58, No. 12, pp. 5424-5437, 2011.

24. Dervis, K. and Bahriye, A. "A comparative study of Artificial Bee Colony algorithm", Applied Mathematics and Computation (Elsevier), Vol. 214, pp. 108-132, 2009.

25. Dervis, K. and Celal, O. "A novel clustering approach: Artificial Bee Colony (ABC) algorithm", Applied Soft Computing (Elsevier), Vol. 11, pp.652-657, 2011.

26. Dey, B., Nandi, S., Das, G., "Mobility Assisted Efficient Coverage Control in Cluster Based Sensor Networks ", Proceedings of Second International Conference on Emerging Applications of Information Technology(EAIT), pp. 243-246, 2011.

27. Dey, H., Datta, R., "Transmission-efficient group-key generation in large dynamic MANET environments", Third International Conference on Emerging Applications of Information Technology (EAIT), pp. 355-360, 2012.

28. Di and Mouftah, "Performance evaluation of per-hop forwarding behavior in the Diffserv Internet", Proceedings of Fifth IEEE Symposium on Computers and Communications, pp. 334 - 339, 2000

29. Dissanayakeand Armstrong, "Comparison of ACO-OFDM, DCO-OFDM and ADO-OFDM in IM/DD Systems",Journal of Lightwave Technology, Vol. 31, No. 7, pp. 1063 - 1072, 2013

30. Dorigo and Stutzle, "Ant colony optimization", MIT Press, Cambrige, 2004

31. Dorigo, M. and Luca, M.G. "Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem," IEEE Transactions on Evolutionary Computation, Vol. 1, No. 1, pp. 53 – 66, 1997

32. Dorigo, M., Maniezzo, V. and Colorni, A., “Ant System: Optimization by a colony of cooperating agents,” IEEE Transactions on Systems, Man, and Cybernetics—Part B, Vol. 26, No. 1, pp. 29 – 41, 1996

33. Gazdar, T., Benslimane, A., and Belghith, A., “Secure Clustering Scheme Based Keys Management in VANETs “, Proceeding of 73rd IEEE Vehicular Technology Conference(VTC Spring), pp. 1-5, 2011.

34. Gazis, V., Alonistioti, N. and Merakos, L. “Toward a generic always best connected capability in integrated WLAN/UMTS cellular mobile networks(and beyond)”, IEEE Wireless Communications, Vol. 12, No. 3, pp. 20-29, 2005.

35. Gomathi, K., Gandhi, M., “ Weight based clustered key management scheme using RSA for wireless mobile Ad hoc networks “, Proceeding of Third International Conference on Advanced Computing(ICoAC), pp. 359-364, 2011.

36. Hai-tao, X., “A Cluster-Based Key Management Scheme for MANET “, Third IEEE International Workshop on Intelligent Systems and Applications(ISA), pp.1-4, 2011.

37. Hongnian, Z., Shujun, Z. and Kevin, H. “A Review of Nature-Inspired Algorithms”, Journal of Bionic Engineering, Vol. 7, pp. S232–S237, 2010

38. Huang , Wu and Hao, “A Pheromone-Rate-Based Analysis on the Convergence Time of ACO Algorithm”,IEEE Transactions on Systems, Man, and Cybernetics, Vol. 39, No. 4, pp.910 - 923, 2009

39. Jha, Khetarpal and Sharma, “A survey of nature inspired routing algorithms for MANETs”, Proceedings of 3rd International Conference on Electronics Computer Technology, Vol. 6, pp. 16 - 24, 2011

40. J iejin, C., Xiaoqian, M., Qiong, L., Lixiang, L. and Haipeng, P. “A multi-objective chaotic ant swarm optimization for environmental/

economic dispatch", Electrical Power and Energy Systems (Elsevier), Vol. 32, pp. 337-344, 2010

41. John, S.P., Samuel, P., "A distributed hierarchical key management scheme for mobile Ad hoc networks", Proceedings of IEEE International Conference on Information Networking and Automation(ICINA), Vol. 1, pp. VI-308 – VI-414, 2010.

42. JongpilJeong, "Hashing-Based Lookup Service with Multiple Anchor Cluster Distribution System in MANETs", Lecture Notes in Computer Science, Volume 6785, Computational Science and Its Applications - ICCSA 2011, Pages 235-247, 2011

43. Jun Zhao, Quanli, L., Wei, W., Zhuoqun, W. and Peng, S. "A parallel immune algorithm for traveling salesman problem and its application on cold rolling scheduling", Information Sciences (Elsevier), Vol.181, pp. 1212-1223, 2011.

44. Karmouch, E., Nayak, A., "A Distributed Constraint Satisfaction Problem Approach to Virtual Device Composition", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 11, pp. 1997 – 2009, 2012.

45. Katranaras, E., Imran, M.A., and Hoshyar, R., " Energy Aware Transmission in Cellular Uplink with Clustered Base Station Cooperation", Proceedings of 73rd IEEE Conference on Vehicular Technology, pp. 1-5, 2011.

46. Kaur, B., "Security Architecture for MANET and Its Application in M-Governance", Proceedings of International Conference on Communication Systems and Network Technologies (CSNT), 2013.

47. Khan, F., Bashir, F., and Nakagawa, K., "Dual head clustering scheme in wireless sensor networks ", International Conference on Emerging Technologies(ICET), pp.1-5, 2012.

48. Kokku, R., Mahindra, R., Zhang, H., and Rangarajan, S., “NVS: A Substrate for Virtualizing Wireless Resources in Cellular Networks”, IEEE/ACM Transactions on Networking, Vol. 20, No. 5, pp. 1333-1346, 2012.

49. Kush, A. K., Gupta, P., and Rishiwal, V., “A New Protocol for Mobile Ad hoc Networks With Virtual Backbone Nodes”, IEEE International Advance Computing Conference, pp. 822 – 826, 2009

50. Larry, L.P. and Bruce, S.D. “Computer Networks – A Systems approach”, Morgan Kaufmann, San Fransisco, Second Edition, 2000.

51. Lee, J; Moon, I, “Research on Virtual Network for Virtual Mobile Network”, International Conference on Computer and Network Technology (ICCNT), pp. 98 – 101, 2010

52. Li and Xiang-Gen “A Fast Robust Chinese Remainder Theorem Based Phase Unwrapping Algorithm”,IEEE Signal Processing Letters, Vol.15, pp. 665-668, 2008

53. Li, L., Liu, R., “Securing Cluster-Based Ad Hoc Networks with Distributed Authorities”, IEEE Transactions on Wireless Communications, Vol. 9, No. 10, pp. 3072-3081, 2010.

54. Liang ,Zhang and Jia,“A generalized”, Proceedings of IEEE International Conference on Signal Processing, Communications and Computing. pp. 1 - 4, 2011

55. Liang, J., Yu, J., “A mobility management scheme based routing for hierarchical ad hoc networks”, Proceedings of IEEE 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol. 3, pp. V3-360-V3-463, 2010.

56. Liu, W., Nishiyama, H., Ansari, N., Yang, J., and Kato, N., “Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 2, pp. 239- 249, 2013.

57. Ma and Tsai, “Formal Modeling and Analysis of a Secure Mobile-Agent System”, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, Vol. 38, No. 1, pp.180 - 196, 2008

58. Maier, S., Herrscher, D., and Rothermel, K., “Experiences with node virtualization for scalable network emulation”, Computer Communications, Vol. 30, No. 5, pp. 943-956, 2007

59. Michael, M., Vasileios, P. and Lixia, Z. “A taxonomy of biologically inspired research in computer networking”, Computer Networks (Elsevier), Vol. 54, pp. 901-916, 2010.

60. Michelle, M.E. and Stephen, P.R. “Honey bees as a model for understanding mechanisms of life history transitions”, Comparative Biochemistry and Physiology (Elsevier), Part A, Vol. 141, pp. 362 – 371, 2005.

61. Mohite, V., Ragha, L., “Cooperative Security Agents for MANET”, World Congress on Information and Communication Technologies (WICT), pp. 549-554, 2012.

62. Nestinger, Chen and Cheng, “A Mobile Agent-Based Framework for Flexible Automation Systems”, IEEE/ASME Transactions on Mechatronics, Vol.15, No. 6 ,pp. 942 - 951 , 2010

63. Ni M., Zhong, Z., and Zhao D, “MPBC: A Mobility Prediction-Based Clustering Scheme for Ad Hoc Networks “, IEEE Transactions on Vehicular Technology, Vol. 60, No. 9, pp. 4549-4559, 2011.

64. Nicanor, Q. and Kevin, M.P. “Honey bee social foraging algorithms for resource allocation: Theory and application”, Engineering Applications of Artificial Intelligence (Elsevier), Vol. 23, pp. 845-861, 2010.

65. NS2, available online at: www.isi.edu/nsnam/ns/

66. Papadogiannis, A., Alexandropoulos, G.C., “The value of dynamic clustering of base stations for future wireless networks”, IEEE International Conference on Fuzzy Systems(FUZZ), pp.1-6, 2010

67. Park, C; Choi, N ; Eunkyoung P; Kwon, T; Choi, Y, “Multiple Interface/Prefix Selection for Virtual Mobile Networks”, International Conference on Advanced Communication Technology, Vol. 1, pp.187 – 190, 2008

68. Pattanavichai, S; Jongsawat, N; Premchaiswadi, W, “ Real options analysis for valuing strategic investments and decisions of the Mobile Virtual Network Operator's investment in E-UMTS”, International Conference on ICT and Knowledge Engineering (ICT & Knowledge Engineering), pp.138 – 144, 2012

69. Peibo, X. and Huaxi, G. “Intelligent Bees for QoS Routing in Networks-on-Chip”, Second Pacific-Asia Conference on Circuits, Communications and System (PACCS), pp. 311-315, 2010.

70. Peter Kacsuk, Thomas Fahringer, and Zsolt Nemeth, “Distributed and Parallel Systems”, Springer Science, 1st Edition, 2007

71. Pin, Lv., Cai, Z., Xu, J., and Xu, M., “Multicast Service-Oriented Virtual Network Embedding in Wireless Mesh Networks”, IEEE Communications Letters, Vol. 16, No. 3, pp. 375-377, 2012.

72. Pin, X., Li, H., “Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks”, IET Information Security, Vol. 7, No. 2, 2013.

73. Porkodiand and Arumuganathan, “Group-oriented signature schemes based on Chinese remainder theorem”,Nature & Biologically Inspired Computing, pp.1661 - 1664, 2009

74. PushpaLakshmi, R., Kumar, A.V.A., and Rahul, R., “ Mobile agent based composite key management scheme for MANET “, International

Conference on Emerging Trends in Electrical and Computer Technology, pp. 964-969, 2011.

75. Qayyum, M., Subhash, P., and Husamuddin, M., “Security issues of data query processing and location monitoring in MANETS”, Proceedings of International Conference on Communication, Information & Computing Technology(ICCICT), 2012.

76. Rajesh, K., Devendra, S. and Abhinav, S. “A hybrid multi-agent based particle swarm optimization algorithm for economic power dispatch”, Electrical Power and Energy Systems (Elsevier), Vol. 33, pp. 115-123, 2011.

77. Raji and Ladani, “Anonymity and security for autonomous mobile agents”IET Information Security,Vol.4 , No.4 ,pp.397 - 410, 2010.

78. Rivera, B., Gopaul, R., and Lu, B., “A scalable testbed for emulating wireless Mobile Ad-hoc Networks”, Proceeding of IEEE Military Communications Conference, 2008.

79. Rong, B., Chen, H., Qian, Y., Lu, K., Hu, R.Q., and Guizani, S ., “A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study", IEEE Transactions on Vehicular Technology, Vol. 58 , No. 1, pp. 398- 408, 2009.

80. Sabari and Duraiswamy, “Ant Based Multicast Routing Algorithm with Multiple Constraints for Mobile Adhoc Networks”, IEEE International Conference on Security Technology, pp. 35 - 40 , 2008

81. Saini, N.K., trivedi, A., “Refined Cluster Based Mobility Prediction with Weighted Algorithm “, Proceedings of IEEE International Conference on Computational Intelligence and Communication Networks(CICN), pp.350-354, 2010.

82. Santhishree, K., and Damodaran, A., “CLIQUE: Clustering based on density on web usage data: Experiments and test results”, Proceedings

of IEEE 3rd International Conference on Electronics Computer Technology (ICECT), Vol. 4, pp. 233-236, 2011.

83. Salmanian, M., Pan, L., Hu, J., and Li, M., "On the efficiency of establishing and maintaining security associations in tactical MANETs in group formation", Conference Proceedings on Military Communications conference, MILCOM 2011.

84. Sedaghat, S., Adibniya, F., and Derhami, V., "A mechanism-based QoS and security requirements consideration for MANETs QoS routing", Sixth International Symposium on Telecommunications (IST), 2012.

85. Sharony J, "A mobile radio network architecture with dynamically changing topology using virtual subnets", IEEE International Conference on Communications, Converging Technologies for Tomorrow's Applications, pp.807 – 812, 1996

86. Siva R.M.C. and Manoj, B.S. "Adhoc Wireless Network", Pearson Education, Second Edition, Delhi, 2000.

87. Surachai, C., Ekram, H. and Jeffrey, D. "Channel Assignment Schemes for Infrastructure-Based 802.11 WLANs: A Survey", IEEE Communications Surveys & Tutorials, Vol. 12, No. 1, pp. 124-136, 2010.

88. Taher, N., Hamed, Z., Meymand, and Majid, N. "A practical algorithm for optimal operation management of distribution network including fuel cell power plants", Renewable Energy (Elsevier), Vol. 35, pp. 1696-1714, 2010.

89. Tanenbaum, S.A., "Computer Networks", Prentice Hall of India, 3rd Edition, New Delhi, 1998.

90. Toh, C.K., "Ad Hoc Mobile Wireless Networks: Protocols And Systems", Published by Dorling Kindersley (India) Pvt. Ltd, Pearson Education, 2009.

91. Umamaheswari, Radhamani, G., “Clustering schemes for mobile adhoc networks: A review “, Proceedings of IEEE International Conference on Computer Communication and Informatics (ICCCI), pp. 1- 6, 2012.

92. Xiaohua, T., Yu, C. and Xuemin, S. “DOM: A Scalable Multicast Protocol for Next-Generation Internet”, IEEE Network, pp. 45-51, 2010.

93. Xin-Li., Chan, Z. and Min-Rui, F. “Wired/Wirless Heterogeneous Network Performance Comprehensive Evaluation”, WRI Global Congress on Intelligent Systems (GCIS '09), Vol. 1, pp. 399-403, 2009.

94. Xu, K., Yang, K., and Stokmenovic, I., “Wired and wireless network virtualization [Guest Editorial]”, IEEE Network, Vol. 26, No. 5, pp. 6-7, 2012.

95. Yannis, M. and Magdalene, M. “A hybrid genetic – Particle Swarm Optimization Algorithm for the vehicle routing problem”, Expert Systems with Applications (Elsevier), Vol. 37, pp. 1446-1455, 2010.

96. Yu, F.R., Tang, H., Mason, P.C., and Wang, F., “A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks”, IEEE Transactions on Network and Service Management, Vol. 7, No. 4, pp. 258- 267, 2010.

97. Zafar, B., Gherekhloo, S., Asgharzadeh, A., Garrosi, M.T., and Haardt, M., “Self-Organizing Network with Intelligent Relaying (SONIR) “, Proceedings of IEEE 7th International Conference on Mobile Adhoc and Sensor Systems(MASS), pp. 756-767, 2010.

98. Zahidi, S.Z.H., Aloul, F., Sagahyroon, A., and El-Hajj, W., “Optimizing Complex Cluster Formation in MANETs Using SAT/ILP Techniques”, IEEE Sensors Journal, Vol. 13, No. 6, pp. 2400- 2412, 2013.

99. Zaman and Karray, “Lightweight IDS Based on Features Selection and IDS Classification Scheme”, Proceedings of International

Conference on Computational Science and Engineering, Vol.3, pp. 365 - 370, 2009

100. Zheng, X., Wang, H., Chen, Y., Liu, H., and Liu, R., “ A decentralized key management scheme via neighborhood prediction in mobile wireless networks “IEEE 7th International Conference on Mobile Adhoc and Sensor Systems(MASS), pp. 51-60, 2010.

List of Publications

1. **Kesavan R**., and ThulasiBai V., “Avoidance of Black Hole Attack in Virtual Infrastructure for MANET”, International Journal of Computer Applications, Vol. 50, No.3,2012.
2. **Kesavan R**., and ThulasiBai V., “Quality of Service In Mobile Adhoc Network Infrastructure Using Secured Group Key Management Scheme”, European Journal of Scientific Research, Vol. 96, No. 3, pp.467-475 , 2013.
3. **Kesavan R**., and Thulasibai V., “Efficient Energy Consumption Mechanism for Wireless Networks”, CIIT International Journal of Networking and Communication Engineering, Vol.5, No.6, pp.300-304,2013