Secure Group Head Communication in Wireless Mesh Networks

Developed by:

Lubna Zafar
445/FBAS/MSCS/S08

Supervised by:

Prof Dr. Muhammad Sher
Chairman
Department of Computer Sciences,
Faculty of Basic and Applied Sciences,
International Islamic University
Islamabad

Co-supervised by:

Mr. Fazl-e-Hadi
Lecturer
King Saud University
Saudi Arabia

Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad
(2010)

Department of Computer Science

International Islamic University Islamabad

Date: 04-12.10

Final Approval

It is certified that we have read the thesis report, titled **"Secure Group Head Communication in Wireless Mesh Networks"** submitted by **Lubna Zafar, 445/FBAS/MSCS/S08.** It is our judgment that this thesis is of sufficient standard to warrant its acceptance by International Islamic University, Islamabad for the degree of **MS in Computer Sciences.**

Committee

External Examiner
Prof Dr. Muhammad Arif
Chairman
Department of Computer Sciences,
Faculty of Basic and Applied Sciences,
Air University, E-9, Islamabad

Internal Examiner
Dr. Muhammad Zubair
Assistant Professor
Department of Computer Sciences,
Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad

Supervisor
Prof Dr. Muhammad Sher
Chairman
Department of Computer Sciences,
Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad

Co-Supervisor
Mr. Fazal-e-Hadi
Lecturer
King Saud University
Saudia Arabia

Dedication

Dedicated to The Holy Prophet Muhammad (Allah's grace and peace be upon Him). And also my beloved parents, teachers and my friends who support me a lot and their prayers pay the way to success in my life.

Lubna Zafar
445/ FBAS/MSCS/S08

Declaration

I hereby declare that this thesis **"Secure Group Head Communication in Wireless Mesh Networks"** either as a whole or as a part has been copied out from any source. It is further declared that I have done this research with the accompanied report entirely on the basis of my personal efforts, under the proficient guidance of my teachers especially my supervisors **Prof Dr. Muhammad Sher and Mr. Fazl-e-Hadi**. If any part of the system is proved to be copied out from any source or found to be reproduction of any project from any of the training institute or educational institutions, I shall stand by the consequences.

Lubna Zafar
445/FBAS/MSCS/S08

A dissertation Submitted To
Department of Computer Science,
Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad
As a Partial Fulfillment of the Requirement for the Award of the
Degree of MS in Computer Sciences.

Acknowledgement

All praises to be on Almighty Allah, the most "REHMAN" the most "RAHEEM", the provider of hope, guidance and knowledge. Without HIS remembrance surely could not have overcome our moments of despair.

It is said in the Holy Quran:

"Does man think that he will be left uncontrolled, (without purpose)? Was he not once a drop of ejected semen? Then he became a clot, so He created and fashioned him and made him into two sexes, male and female. Is He who does this not able to bring the dead to life?" [Surah alQiyama: 36-40]

I thank to **The Holy Prophet Muhammad** (Allah's grace and peace be upon him). Without His blessings, I was unable to complete the thesis. I am also indebted to every one whose efforts helped me to make this thesis possible and I express my cordial and humble thanks for their untiring help and cooperation in completing this thesis.

I cordially regard the inspiration, prays, encouragement, and financial support of our loving and affectionate parents and family for their motivation in every aspect of my life.

Lubna Zafar
445/FBAS/MSCS/S08

Project In Brief

Project Title:	Secure Group Head Communication in Wireless Mesh Networks
Undertaken By:	Lubna Zafar 445/FBAS/MSCS/S08
Supervised By:	Prof Dr. Muhammad Sher Chairman Department of Computer Sciences, Faculty of Basic and Applied Sciences, International Islamic University Islamabad
Start Date:	15 Aug.2009
Completion Date:	12 Aug.2010
Tools & Technologies:	OMNET++
Documentation Tools:	Microsoft office tools
Operating System:	Microsoft Windows XP Professional
System Used:	Pentium IV

Abstract

Wireless mesh networks (WMNs) is most researchable and emerging area. WMNs are hybrid in nature, have infrastructure based gateways on one hand and on the other hand having mobile or fixed clients. Group communication is an important paradigm to study for its variety of applications such as video conferencing, broadcasting, online games, distance learning. Security is a critical issue in group communication. Mostly, group communication relies on its head for communication, so securing the group head is vital. In this thesis, i propose reliable authenticated group head communication (RAGHC) architecture. This architecture is organized into three parts i.e., group head authentication, secure inter group communication via group heads and group head maintenance. Demonstrating the inter group communication is an additional contribution of this study. By extensive simulation we demonstrate that how group heads are created authenticated and how they communicate within the group and outside the group securely. Comparative results with previous techniques show that RAGHC is better in terms of packet delivery ratio and packet delay.

Table of Contents

List of Figures

Introduction

Wireless technology has been most recent and researchable field in the last few decades. Users get the desired information and use devices at any place at any time. Wireless networks connect the devices and people at any place. Wireless networks are divided into two major types; ad-hoc and infrastructure-based wireless networks. In infrastructure-based wireless network, base stations are placed in different areas where wireless devices are connected with each other. Examples are; wireless LANs and cellular networks. Wireless LAN provides good interportability within different operating systems. Wireless LAN major advantages are: mobility, ease of use, simple and flexible.

Ad-hoc wireless networks make the connection ad-hoc; it is not a permanent connection. Different nodes will automatically configure each other when they want to communicate with each other. So that's why ad-hoc wireless network is powerful and flexible. These properties of ad-hoc network make them suitable for many applications where central node is not reliable and where nodes can be deployed quick and fast and urgent communication can be done easily.

1.1.1 Mesh Network

A wireless mesh network (WMN) is a new emerging and challenging technology. 802.11 and 802.16 are the IEEE standards for this network. It offers low cost community services. Mesh network are organized in such a way that they create an ad-hoc network. Mesh network is very reliable. Every node is connected to several nodes. If any hardware fails in the network or any node crashes then remaining node can find its neighbor node or any other route for communication. Wireless mesh network often consists of gateways, mesh points, mesh stations, mesh routers, mesh portal points, mesh clients and mesh access points.

Mesh clients are often laptops, PDAs, cell phones and other cellular technology. These clients are connected to mesh routers through the gate ways. Mesh routers has the many locations and it chooses the best path for the communication. Mesh routers send the data through the gateways to the network. All communication is done on mesh point and this mesh point is connected with different mesh access points to access the network. Communication between different networks and mesh network is done on mesh portal point. Mesh stations are outside from the wireless LAN and they are connected to different mesh access points. All nodes are organized in such a way it makes a mesh cloud within a mesh topology.

1.1.2 Wireless Mesh Networks Types

Wireless mesh networks types are as below;

1.1.2.1 Flat Wireless Mesh Networks

Mesh routers make a network for mesh clients. Clients and routers are both nodes. These nodes are placed at the same area. Client nodes cooperate with each other for network configuration, routing and other client services. It makes a temporary ad-hoc and simple network.

1.1.2.2 Hierarchical Wireless Mesh Networks

This mesh network has many hierarchies and clients are at the lowest hierarchy. Client nodes communicate with the routers. Here router nodes are dedicated nodes to make a backbone network. Like clients backbone nodes may not source or final destination. Routers responsibility is to heal, organize and maintain backbone network and this network is connected to the internet and some servers in the wired network such nodes are called gateway nodes.

1.1.2.3 Hybrid Wireless Mesh Networks

WMNs uses WiMAX wireless networks and cellular wireless networks for communication. Hybrid WMNs uses multiple technologies for back haul and WMNs backbone. WMN growth depends on that how it works with other technologies.

1.1.3 Routing

The process of sending message to the destination following some routes is called routing. Routing is an essential component for a network. There are various issues a routing protocol must address, as have been discussed in [27], for example, ensuring the absence of loops, detecting node failure, minimizing the overhead network traffic and so on. As discussed in [27], Router makes a routing table and sends all the packets to the receiver end. There are various other features of ad hoc networks, as discussed in [20] that make the task of routing tough. Some of these are:

- Poor resource devices
- Limited bandwidths
- High error rates
- Continually changing topology
- Vulnerability to external attacks

Therefore, as the authors in [20] have discussed, important points for ad hoc network protocols are:

- Minimal control overhead
- Minimal processing overhead
- Multihop routing capability
- Dynamic topology maintenance
- Loop prevention

1.1.4 Routing approaches in mobile ad hoc networks

There are mainly two types of routing approaches in MANETs: reactive and proactive [20]

1.1.4.1 Proactive approach

Each node in the network maintains a route to every other node in the network at all the times. Due to the instant availability of routes, there is not as much latency involved. However the storage of routes imposes a great amount of overhead on the nodes.

Two main classes of Proactive Routing Protocols are:

- Distance vector
- Link state

Every node know its neighbor nodes in link state routing, and this information is spread to each and every node in the network, then each node shall have enough information to complete the whole network [27]. The best route in the network is selected with the help of connectivity nodes.

This is different from the distance vector routing protocols, in which every node builds a one dimensional array and sends the vector value to the nearest nodes [27]. By having every node share its routing table with its neighbors, each node builds updated routing tables which make a decision for the next hop for any packet to be routed.

Information can be passed between different nodes through link state protocol. Link state protocol complexity is much less than the other protocols.

1.1.4.2 Reactive approach

In this approach the route discovery is through wide flooding of a request and routes are identified when they are used. This approach has an advantage over the proactive approach that the signaling overhead is greatly reduced relative to the proactive approach. Different protocols which have been proposed under this approach include AODV (Ad hoc On Demand Distance Vector Routing) [26] and DSR (Dynamic Source Routing) [27]. Geographical approach or the Hybrid approach has also been proposed [23] for wireless networks.

Several secure routing protocols have also been researched in ad hoc network. Some protocols have weaknesses that are exploitable by attacks [28].

1.1.5 Field Based Routing

The field theoretic approach has been studied in a number of different application scenarios. For instance, the approach has been used for any cast routing [19]. This is observed in the density based routing and the authors in [29] have proved that it shows its best performance in density and proximity and hence the applicability of field theoretic approach to this context. In mobile ad-hoc network field based routing has been studied for recovery [30]. The service providers or the destination nodes are modeled as positive charges and a field is established. In sensor networks, field based routing propose a routing scheme that monitor network and see that the live sensor nodes deliver data for a long period [31].

1.1 Motivation and challenges

The increasing demand for access to various resources even in areas where a centralized communications is absent or in case of mobility wireless ad-hoc networks are used. As discussed in [19], wireless ad hoc and autonomous networks that have been used in public vehicles, buildings, conferences or even in cities. As various fixed wireless infrastructures have served the purpose, ad hoc networks are still used where there are no centralized servers. There are many other factors that serve as motivation for ad hoc networks, as discussed in [19]:

- Autonomous systems
- Networks not reliable on fixed base station
- High cost incurred for fixed wireless infrastructure
- Utility as the means of communication during disaster
- Reduction in the energy consumption
- Usage in poor/discriminated areas

Mesh network is fairly applicable in city wide scenarios. In city wide network, musical groups and universities in which wireless mesh network is very suitable group communications can be unicast or broadcast.

1.2 Background

1.2.1 Networks

Exchange of information with a collection of interconnected independent nodes is done through a network. These independent nodes can be established through microwaves and fiber optics. It shares the resources and provides lots of entertainment and a powerful communication medium. Collection of interconnected nodes is known as the internet [21].

Network can be divided into core elements and its edge. Edge consists of devices and computers. These are called host systems. The host systems are mobile computers. The host systems have servers and clients. An end system is client that requests and the other one is server that receives the particular request.

The core network consists of routers and packet switches which send the packets to sender and receiver. Sender sends the message to the destination to follow the best path.

A protocol defines rules of communication between the sender and receiver. The Internet and computer networks use different types of protocols to fulfill the different tasks of communication.

1.3 Problem Statement

In wireless mesh networks group head applications security is a major concern. Secure inter group communication and group head authentication issues are not discussed in the literature. In wireless mesh networks group communication, group head authentication and communication between different group heads are still a researchable issue. In group communication applications, group heads are not registered, a node in the network may behave as a malicious node and wants to access the sensitive data that node may be any member node of any group or from outside, internal and external intruders. Any node can behave as a malicious node and show the highest heat value and can access all the sensitive information. Here, secure inter group communication is required to secure the data from these attacker nodes so that reliable, secure and efficient group communication can takes place.

1.4 Proposed Approach

An architecture is proposed named as; Reliable Authenticated Group Head Communication (RAGHC) architecture. The presentation of group communication is based upon the filed based routing [61]. To make the system reliable we introduced the concept of the certification authority (Local manager) which authenticates the group heads. These local managers are at various levels and share the information among them. The gateway at the top is the final certification authority.

Now as the network populates the local manger populates its list based upon the field value (As in field based routing entire routing depends upon this field value, in other words the group head which is nearer to the LM will be selected as the group head).

There are various nodes in the network sharing data with each other but the node which communicate on behalf of its group is the group head and if group "A" want to communicate with group "B" than the group "B" first confirm from the LM that is the group head "A" is a legal group head or not?? on the confirmation by local manager (because LM know who are the current group heads) the group head "B" will accept the data from the group head "A" and vice versa. Our authentication mechanism is very simple and it is in addition to our main contribution of introducing the group communication.

There are two possible problems if we are not using the local managers for authentication.

Internal selfish nodes and external intruders

As in the previous networks it is allowed that any node can communicate to any other node, so any node in the network can communicate on behalf of a group head as well. As in our authentication mechanism before accepting the data from any group head it is confirmed from the LM so the LM will detect the internal legal node as an internal intruder and the receiving group head will discard the data. Without LM any illegal node can communicate on behalf of the group head, first we introduced the group communication and by introducing the concept of the LM we made it secure.

"Any node "X" can advertise its field value as the highest value and receive by the LM, in this case the LM (as it comes to know about the field value from its neighbors) compares the value reported by the other neighbors of "X" (because they are also reporting the neighbors field value) if the difference is greater than a fixed threshold than the LM reject this request and considers that it is the internal intruder.

In case of crash the next group head is decided and it is based upon the distance from LM (field value of the next group head), so any attempt for becoming a group head wrongly is detected by the LM. All nodes send join request to the LM and LM decide that which one is new group head. Tie case is resolved by the node ID for example if two nodes are the same distance than the higher node ID wins.

By external intruder we mean that any node which resides inside the direct range of the deployed network but not the registered node. If LM are not installed than any node can send and receive the data and can interrupt the communication between the group heads and can launch active or passive attacks. LM concept is introduced to minimize the threats. Our LM concept has the list of legitimate nodes so the threat of external intruder intervention is also minimized.

Timestamps are maintained for each session. We assume that after every 5 min group head send the keep alive messages to the Local managers but if the messages did not come in time then node will be the group head that is closer to the Local manager and Local manager update its list and also send this updated list to the other Local managers as well.

1.5 Thesis Outline

The thesis comprises of 6 Chapters. Chapter 1 describes about the background, motivations and problem statement of the research. Chapter 2 contains the detailed study of related work. Chapter 3 discusses the problem scenarios in detail. Chapter 4 describe in detail the proposed solution and architecture. Chapter 5 shows the simulation results in detail. Finally, conclusion and future work are discussed in Chapter 6.

Literature Survey

2.1 Introduction

Now-a-days, group communication is among the most commonly researched areas. Multi-point to multi-point communication is done between different groups. Group oriented applications like web cast, internet gamming, video broadcasting, remote consultations and diagnosis systems for medical applications are the most common examples for group communication. These applications exchange and disseminate classified and sensitive information. In public places internet is used in real applications to convert that message in the form so that the group members can read it. For group communication security issues such as authorization, authentication, confidentiality and integrity is required.

In Wireless Mesh Networks, security is still a researchable issue in group oriented applications. An important security issue is to provide reliable and authentic data in group communication to different group heads in wireless mesh network. Authorization is an important issue in group head communication such that all the group heads are authenticated; no unauthorized node can send or share the data to any of the group heads. Authentication is the process in which only authenticated and authorized nodes can access and view the data and also this data is protected from the malicious nodes. A major security goal for group applications is providing node authenticity and reliability such that only authorized group heads can get the information. In our proposed scenario, all the group heads have a reliable communication within the network.

2.2 Related Research

In wireless mesh network group communication problems has been researched in a variety of ways. But, secure group head to group head communication is not considered in such a way. Lots of research has been done in wired an in wireless networks respectively.

In sensor networks CGR [1] schemes are used for secure group communication. The scheme is good in sensor networks as compared to other networks. Secure group head communication is not discussed. Attacks are also not considered.

SGL [2] in WAN environment provides data confidentiality. We can check the performance of SGL on inter group communication whether it deals with the intra group communication. Some features like efficiency and robustness are not discussed. Author does not show the work of SGL in inter group communication and also the group heads are not identified in SGL.

WAN distributed model [3] a scalable and reliable for group communication is developed for group communication but leave many security issues like authorization of group heads and their authenticity.

Secure intra and inter group communication consists of multiple nodes in a network and can share information. A mechanism developed [4] for sharing information. To study the impacts of group head authorization in mesh network more research is required and also checks communication overhead and performance with other networks.

The secure group communication main problem is to provide the keys in a decentralized manner. A common group key is established by Tree parity machines [5]. This is used where no server is present mostly in ad-hoc networks and where group communication is done. The proposed protocol must be compared with other protocols in future research.

Group communication in a decentralized manner with data confidentiality [6] is discussed but when the gateway sends the data to various groups and then their one head member then this head member should be secure, may be this is a malicious head member if it is not authenticated. So, group head authorization, group head communication and group head repairing is still a problem in mesh networks.

Broadcast encryption scenario [7] is also used in group communication. An issue in group communication is to provide confidential and authenticated communication between group members. Attacks are not considered in this scheme. In the case of unicasting and multicasting check the reliability and efficiency. Many group- oriented applications require a reliable and secure group head communication.

In wireless mesh network security is a big issue due to rapid access and less cost. An agreement protocol [8] is proposed. But group head communication and its member's events are not discussed. This protocol does not deal with the authenticity of the groups and scalability.

Group communication takes less time in accessing key entries and storing when nodes leave or join in a group where sliding window protocol [9] is proposed. The protocol has good performance in wireless networks but ignore many security issues. When a group head wants to join, the group manager checks whether group head is authentic or not. In group communication scalability is not addressed.

Mobile ad hoc networks (MANETs) are also designed that are also used in group communication and decreases bandwidth. Fixed routers give a more stable and decentralized structure than MANETs [10].

For more localized communication multiple clients can share the same access router. Localized mobility is used in mobile clients in WMNs unlike MANETs [10].

For wired networks these solutions are not suitable [11] and they assume reliable efficient and multicast delivery, in a multi-hop wireless environment which is much more expensive. Wireless sensor networks (WSNs) [11] and MANETs protocols are designed for mobility and scalability.

2.2.1 Secure Group Communication in Wired Networks

To encrypt the data a general method for group communication is the use of a shared key between different group nodes. Contributory key agreement and key distribution schemes depends on a protocol. A group manager generates a key for the group and distributes this key to all the group members.[12]

Tree-based key management protocols like LKH [12] and its variants are also used in wired networks [12]. These protocols communicate with the source node for joining and leaving of groups and maintain a global membership. Key delivery can be done with end-to-end unicast. The latency overhead and high bandwidth of these protocols for the multi-hop wireless environment is not suitable.

The group key is generated from all group members by using schemes such as n-party Diffie-Hellman key exchange in contributory key agreement schemes [13]. These schemes [13] perform a reliable communication between different group members depending on group dynamics. In multi-hop wireless networks this broadcast reliable communication is not good to achieve and also not good for WMNs.

Group communication in wired networks has also been worked for the overlay multicast networks [14]. Overlay networks do not have the properties of multiple clients that can share the same router, multi-hop and more bandwidth. These protocols are not suitable for WMNs.

2.2.2 Secure Group Communication in Wireless Networks

In wireless networks to achieve group communication with a protocol and a limited resource in wireless environment, to achieve efficiency and performance. We will discuss protocols for cellular networks and mobile ad hoc networks (MANETs).

Cellular network is basically two-tier architecture, low and high bandwidth links with base stations. A topology matching key management (TMKM) [39] scheme that takes the things from the traditional key tree (LKH) to compare with the other networks. TMKH connected with high-bandwidth wired links and distribute the keys between different base stations. A group communication protocol is designed in which mesh routers communicate with the other wireless links that are connected.

Group communication in MANETs include GKMPAN [23], CRTDH [37] and also in [24]. GKMPAN discusses about the member events and key distribution scheme for groups. A scheme is proposed for group members to encrypt the data between different groups by using pair-wise keys.

CRTDH [25] relies on the Diffie-Hellman group key agreement and Chinese Remainder Theorem for designing the keys for groups. For each time joining and leaving of groups, new key is assign of each group. In a wireless environment due to its limited bandwidth resources is not suitable.

Kaya et al [26] in MANETs for group dynamics is used to highlight the communication overhead for multi-hop communication. MANETs are of dynamic in nature and the proposed scheme is not successful for wireless communication for data delivery. In WMNs routers and clients share the same router.

An underlying multicast protocol [27] is also used for secure group communication. Against the data forwarding process they discuss the DOS attacks, thus they do not consider the problems of data authentication and achieving data confidentiality.

Wireless sensor networks [28], [29], [30] key pre-distribution schemes are also being researched. Instead of group communication these discusses about the pair-wise communication. Secure group communications has the ability to authenticate users it is a necessary condition. The protocols in [31].

2.2.3 Security Challenges in Wireless Mesh Networks

Some of the security challenges of Mesh networks are

1.External Attack

Launched by intruders who are not part of a WMN and try to gain illegitimate access to the network. Encryption and authentication.

2.Internal Attack

Launched by the nodes that are part of a WMN, such as the selfish nodes or the malicious nodes that have possibly been compromised by attackers. Have access to all the keying and authentication information. Cooperative mechanisms that help detect and isolate the misbehaving nodes need to be employed.

2.2.3.1 Corrupt node detection

- First Case

  There is a possibility of attack due to node replacement because there is no physical protection.
- Second Case:

  There would be the possibility of passive attack.
- Third Case:

  There would be chances attack on the routing algorithm by changing the internal state of the node.
- Fourth Case:

  The fourth case includes disrupting the routing mechanism by cloning the original device and installing the replicas at those locations from where false data can be sent and disabling the parts of nodes.

2.2.3.2 Multi-hop routing

The routing mechanisms in the WMN need to be secured by malicious attacks with the help of multi hop routing.

Fairness: Optimization of bandwidth utilization in the WMN by scheduling to ensure per-client fairness.

2.2.3.3 High level security issues

These are security requirements for a given communication system.

2.2.3.3.1 Availability

The basic concept of availability is the system is available to the authorized users and they can access the information without any interruption. The availability in WMN is compromised by the following crucial factors:

- Signal Jamming
- Denial of Service (DoS)
- Battery Exhaustion

2.2.3.3.2 Authenticity

Enables a node to ensure the identity of the communicating node. This may be possible through two ways:

- Secure Transient Association
- Imprinting

2.2.3.3.3 Integrity

This includes data tampering, impersonation, and packet modification and is especially hazardous if the intruder has malicious intent. Integrity includes

- Cryptography & Digital Signatures
- Pair-Wise key Sharing

2.2.3.3.4 Confidentiality

The delivery of sensitive data demands several degree of security. Therefore several authentication methods are needed in order to ensure that the authorized user can only access the sensitive data keeping the data confidentiality and privacy.

2.3 Limitations

According to the above literature we come to know that there are serious issues in group head communication and group head authentication. In wireless mesh network group communication, group head authentication is a crucial issue. In wireless mesh network group communication, group heads are not authenticated. In group head communication, a malicious node may try to be a group head and it wants to share and view the sensitive information from the authenticated groups. This intruder node may be a group member or the other group heads or its members. This malicious node may tries to access the sensitive data. Here, group head authentication is required to authenticate the data from these malicious nodes so that authentic, reliable and efficient communication between different group heads takes place.

In Wireless mesh networks security is a big and crucial issue as discussed above detail literature tells us. Group communication in a decentralized manner [6] with data confidentiality is discussed but cluster heads are not secured, node authentication is not done and lack of inter- group communication.

Wireless network makes an ad-hoc network with no central server. If nodes are not directly connected with each other and they want to communicate then it can only be possible when the hosts allow them to sends the packets from source to destination [41].

Field base routing (FBR) is discussed by Lenders et al. [42] and V. Park et al. [43]. FBR are robust expensive but good for security attacks.

For linear programming problem Tague et al. [54] presents a model and all nodes can deals with attacks.

In mesh network X.Wu et al. [55] tells the attacks are very common. “Onion” a routing algorithm is proposed it has all the routing information.

2.4 Summary

In this chapter the literature about mesh network, any cast routing, field based routing and all the security issues in mesh network is discussed in details. The literature discusses a lot about the group communication in the mesh network but group heads are not secured in mesh networks as well as other networks. We implement a scenario where all group heads are secured.

Requirement Analysis

3.1 Problem Domain

Wireless mesh networks (WMNs) is a challenging and emerging field in which group oriented applications has been researched a lot. Security is a big and crucial topic in wireless mesh network group head communication. Group applications require a reliable and authentic group head communication. A big issue is to provide reliable and authentic data in group communication to different group heads in wireless mesh network.

Group head to Group head communication is also an important issue. Data is authenticated always but node authenticity is still a problem. Earlier, data is unicast to a group or broadcast to all groups and gateway serve as a certification authority so it takes maximum time to gave a certificate. Here, group head authentication is required to authenticate the data from the intruder nodes so that reliable communication between different group heads takes place. In this thesis we focus on reliable communication and authentication of group heads. Authentication is an important issue in group head communication such that all the group heads are authorized; no unauthorized node can send or receive the data to any of the group heads. This reliable group head communication is done for both inter and intra-group communication. In this thesis, a reliable authenticated architecture is proposed for group head communication in WMNs. The proposed architecture is very reliable and efficient. In WMN, reliable group communication, group head authentication is an important issue. Group heads are not authenticated in WMNs group communication. A malicious node come and claims to be a group head. This research mainly focuses on "Group head authentication", "Secure inter group communication via their group heads" and "Group head repairing".

We propose Reliable Authenticated Group Head Communication (RAGHC) architecture for reliable group head communication in which all the above features are achieved securely and efficiently. A reliable authenticated architecture is proposed for group head communication in WMNs. The proposed architecture is very efficient and secure.

The architecture mainly focuses on;

- Group head authentication
- Secure inter group communication via their group heads
- Group head repairing

3.2 Problem Scenario

Secure Group Overlay Multicast (SeGrOM) [6] is designed to reduce the latency and communication overhead for maintaining the confidential data of a group. SeGrOM deals with the group dynamics and member mobility in a decentralized manner, and have the lower overhead, bandwidth and latency and also to avoid the cost of hop to hop communication. In a decentralized manner and WMN two tier architecture and its broadcast nature, SeGrOM consists of two protocols and uses a structure; a global data delivery protocol is used for backbone communication and a local data delivery protocol for all the members connecting with a same router for the delivery of data between groups. The global data delivery is done by an overlay protocol and it is designed for wireless multicast protocol and this communication is done on backbone routers. SeGrOM, for the global data delivery protocol it has following different types, security, trading, communication cost and complexity. All members connected with the same router uses the local data delivery protocol, and selected a head member with election. Joins and leaves are handled by the local delivery protocol. Local data delivery and global data delivery protocol connected with the same access router [6].

SeGrOM is an efficient protocol and takes the advantage of the localized mobility of clients. The message m; the source s sends the m to the local head member hs, hs receives m and sends it to all other members connected to the same access router with the local data delivery protocol, and then m reaches to the other head members through the global data delivery protocol. On receiving the m the head member hr, then again sends it to the members through a router with local data delivery protocol.

A group overlay over all the head members a framework is maintained for data delivery, on top of all the members and nodes. An authenticated key exchange protocols a link key is madc. Thcsc protocols know thc ncighboring mcmbcrs, and thcn thc ncxt hcad mcmbcr can also access the information. The head member handles the join and leaves of members and made a multicast tree. When head members are not changed then the join and leave of all the members are done by local head member [6].

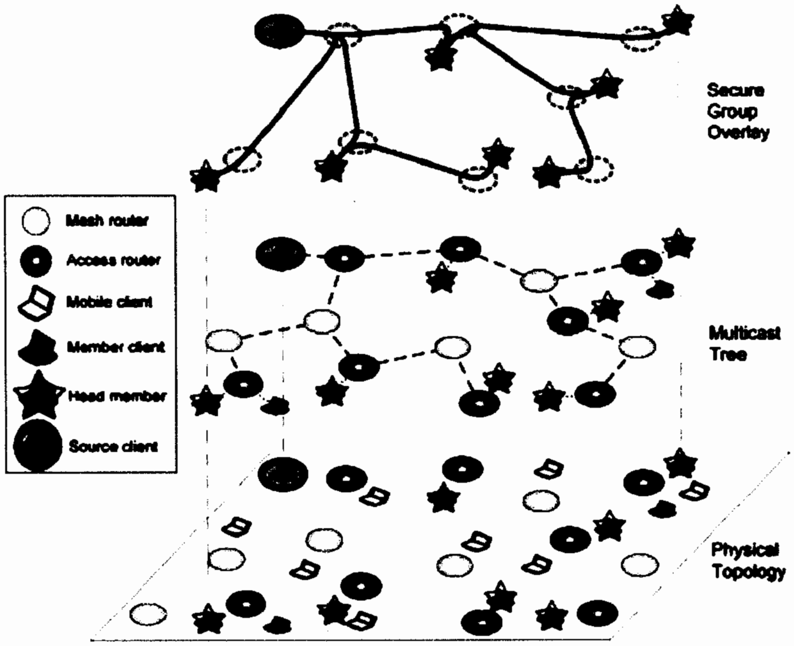


Fig. 3.1. A Group Ovcrlay [6]

3.3 Focus of Research

Group applications have been mostly researched nowadays. According to the above problem scenario, we identify that head members (group heads) are not secured. When there are no secure group heads then how confidential data can be transmitted. Security of group heads is a major issue in group communication scenario. We deal with the authentication of the group heads, node authenticity, and group head to group head communication. In group communication data confidentiality [6] is discussed but when the gateway sends the data to various group heads how can this group head is authentic and reliable, may be this is a malicious group head. So, group head authorization, secure inter group communication via their group heads and group head repairing is an important issue in wireless mesh networks.

3.4 Summary

This chapter focus on the problem domain that how we identify this problem from a particular scenario. Then we briefly discuss about that scenario from where we get our research point and what is the flaw in that scenario? We also describe focus of research.

System Design and Implementation

4.1 Introduction

WMNs is a temporary ad hoc network consists of many routers and clients and forms a network. Its transmission power is less. WMN is seen in Fig.4.1. [35].

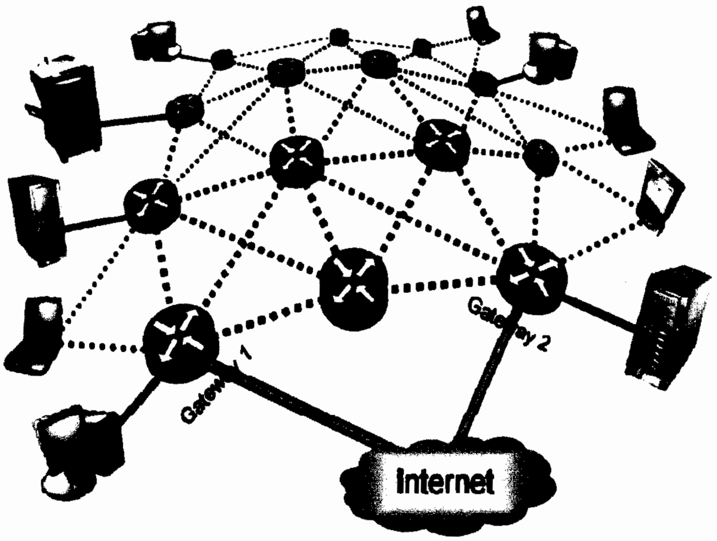


Fig.4.1. Basic Mesh Network Architecture

In wireless mesh network, mesh clients forward the packet to the different nodes but it is not the gateway [15]. In wireless mesh network infrastructure nodes can be fixed or can be static. There also may be some base stations, access stations, mesh points and mesh portal points and these all are used for connectivity.

4.1.1 Route Packet from Internet to Group

Route packet from internet to cluster head, the following steps is involved;

4.1.2 Gateway to Local Manager (Unicasting)

We route packet from gateway to Local manager in a unicast manner that is one to one communication. Using field based routing we find out the field value of the receiver node that is the Local manager and send the message to that Local manager. Local manager then issue the certificates to the different group heads for authentication if the group heads are authenticated then packet is send to the nearest group head.

4.1.3 Intra-group and Inter-group Communication (Broadcasting)

When a packet reached at group head then the next step is if we want to send packet to every node in a group, so we broadcast this packet from Head to all the group members. And group head can also communicate with the other group heads through the Local manager. Local manager verify the certificate of the other group head if it is authenticated then it send the packet to that other group head.

4.2 Design Requirements

4.2.1 Type of Nodes

In this scenario there four types of nodes exist on which all the traffic routes. The details of all these nodes are as under:

4.2.2 Gateway

Gateway is the first type of node and sends the packet to the network. Traffic flows may be of different types within a network. In our proposed scenario, gateway sends the message to the Local manager and LM forwards this message to the registered group heads.

4.2.3 Intermediate Nodes

Routers are the second type of nodes and route the message from the routers to the clients. The intermediate nodes are a router and have all the information about their neighbor's nodes and route the packet to the destination by using some hops.

4.2.4 Local Managers

Another node is called Local managers, this acts as the certification authority who give certificates to the group heads for reliable and authenticated communication.

4.2.7.3 Geocast traffic

The third types of packets are of geocasting they travel in a unicast manner from gateway to the Local manager, then cluster head and then broadcast to all the group members after arrival at any of the cluster head.

4.2.8 Routing Criteria for Secure Field Based (SFBR) Algorithm [61]

4.2.8.1 Field value

Field value is a value associated with every node in the network as the network routing criteria is field based so every node has to calculate some value on the basis of which routing took place. Field value is of type double and maximum value is one i.e. the node nearest to the destination [61].

4.2.8.2 Calculation of Field value

Every node in the network calculates its routing field value from its neighbors. The cluster head has the highest field value. Those nodes which are directly connected to the cluster head have the largest field value as compared to other nodes in the network. All the other nodes in the network calculate their field value from their directly connected neighbors consider cluster heads as source [61].

4.2.9 Group Head Authentication

All the group heads are registered in the Local manager. Local manager assign the keys to the group heads and reliable group head communication is done. Whenever a group head receive communication request from the other node then this group head confirms from the Local manager that is authenticated or not. Local managers share the list with the other Local manager in the network. Reliable and fast route is followed to reach the destination.

4.2.10 Group head to Group head Communication

Reliable communication between different group heads can be done with field based routing algorithm [61. Group head to Group head communication is done through the Local manager. When a group head wants to communicate with the other group head, Local manager check the authenticity of the other group head. If it is authentic then group head to group head communication takes place else packet is dropped.

4.2.11 Group Head Repairing

Whenever a new node wants to join, it sends a join request to the Local manager. Local manager assign the authentication keys and register this group head and update the list or a group head wants to leave it also update the list. Timestamps are maintained for each session. After every 5 min group head sends the keep alive messages to the Local managers but if the messages did not come then the node close to the Local manger will be the group head. Local manager assign the key to this new node and update its list and also send this updated list to the other Local managers as well. When intruder is identified Local manager show it to the network and replace it.

4.3 Reference Architecture

4.3.1 Network Model and Proposed Architecture

Our proposed architecture environment is WMNs, is consist of a fixed wireless mesh routers. We assume that the routing nodes (forwarding nodes will pass the request securely), the secure communication is done through the field based routing [61].

The authentication can be done when the network populates or at any time, as in the fixed scenario the Local manager know about its clients.

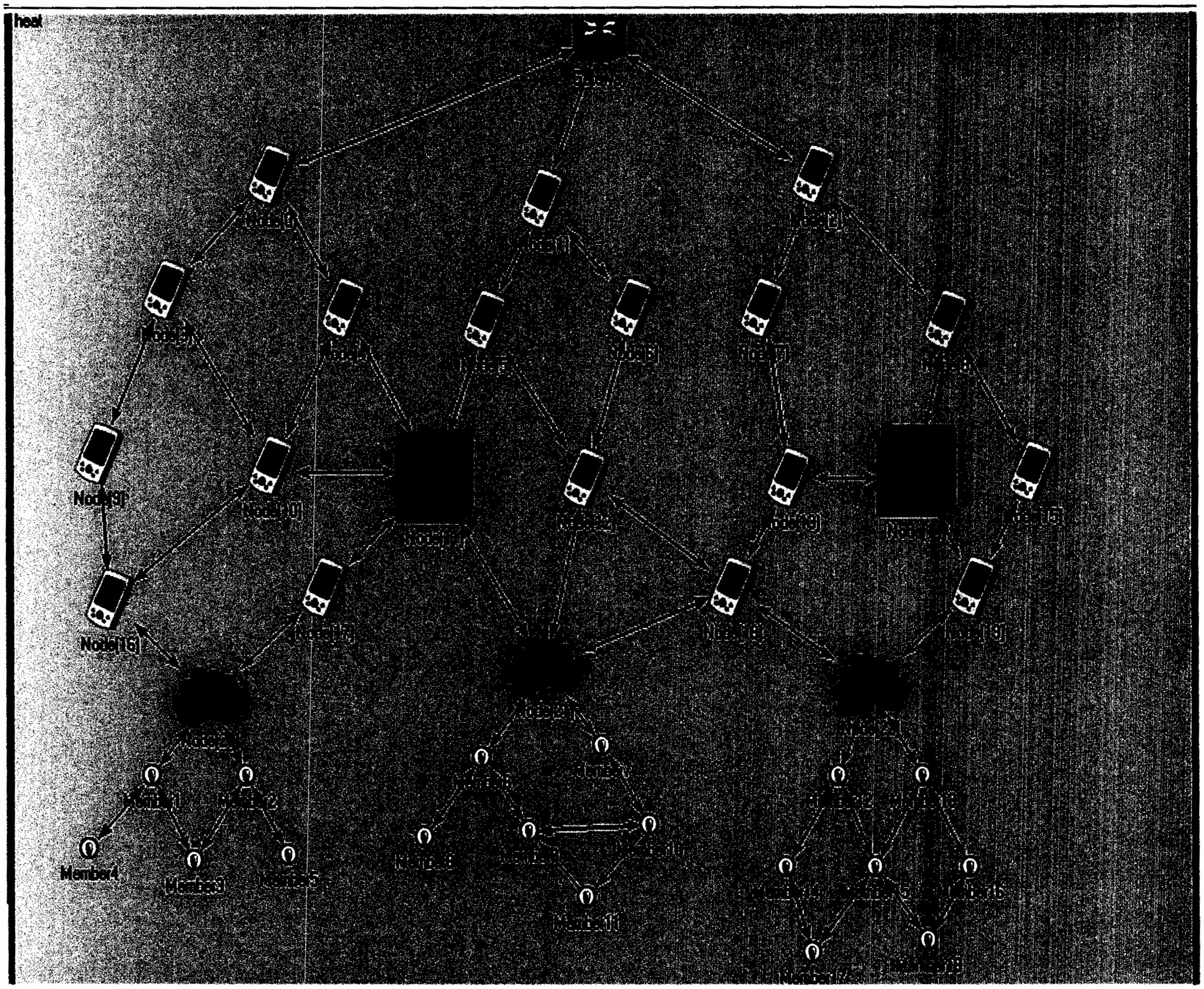


Fig.4.2. Proposed Architecture (RAGHC)

Group heads can share, distribute or access the data within a group or outside the group. All the group heads are registered in the Local manager. That node will be the group head that is close to the Local manager. Local manager assign the authentication keys to the group heads which is used for reliable and authentic communication. Whenever a group head receive communication request from the other node or the other group head it confirms its key from the Local manager. Local managers share the list with the other Local manager. Reliable and fast route is followed to reach the destination.

Reliable communication between group heads will be done through SFBR [61]. In field based routing a digital value is assigned to every node in the group. Destination node has the highest heat value. When data packet is sent from the gateway check the heat value and through the steepest gradient.

Field based routing [61] is very simple and robust, in this routing no routing table is maintained and routing is based on heat values of the nodes. When new group heads join it send the request to the Local manager. Local manager assign the keys to group head and register this group head and update the list or group head wants to leave then Local manager also update the list.

Timestamps are maintained for each session. After every 5 min group head send the keep alive messages to the Local managers if it is not done then the next nearest node will the group head and Local manager assign the key to this newly join group head and update its list and also send this updated list to the local managers as well. When an intruder or attacker node is detected then Local manager remove this node and key is not assigned to this node.

4.3.2 Authentication of Group Head

We assume that the authentication managers (Local manager) have the knowledge about the structure of the topology and they know that who the authenticated group head. The generalize form of authentication is this that the group head will send a request for the Local manager to authenticate, and the Local manager will send a key to the group head and will maintain a list and also share these information with the other Local managers and the gateway to update their list, the group head will use this key for the authenticated communication.

As in the fixed scenario, the Local managers know about its clients, if an intruder came in and want to communicate on the behalf of the group head it will be unaware of the source (group head) secret information which are known by the group head and the authentication authorities.

4.4. Algorithm

```
Gh – Group head
Lm– Local manager
m – message
L – List
 do
      checkgrouphead authenticity → gha
      if gha is NO, then
            Display "intruder"
      else
            if gha is YES
             Lm(m, Gh)
            update L
            end if
      End if
      Broadcast message
        stop
```

4.5 Flow chart

Fig.4.3. indicates that how secure group head communication takes place. Gateway sends a message to the local manager. Local manager check the group head authenticity if group head is authenticated then sends the message. Group head receive the message and broadcast it to the group members. On the other case if an intruder tries to become a group head, local manager did not send the data to that group head and drop the message.

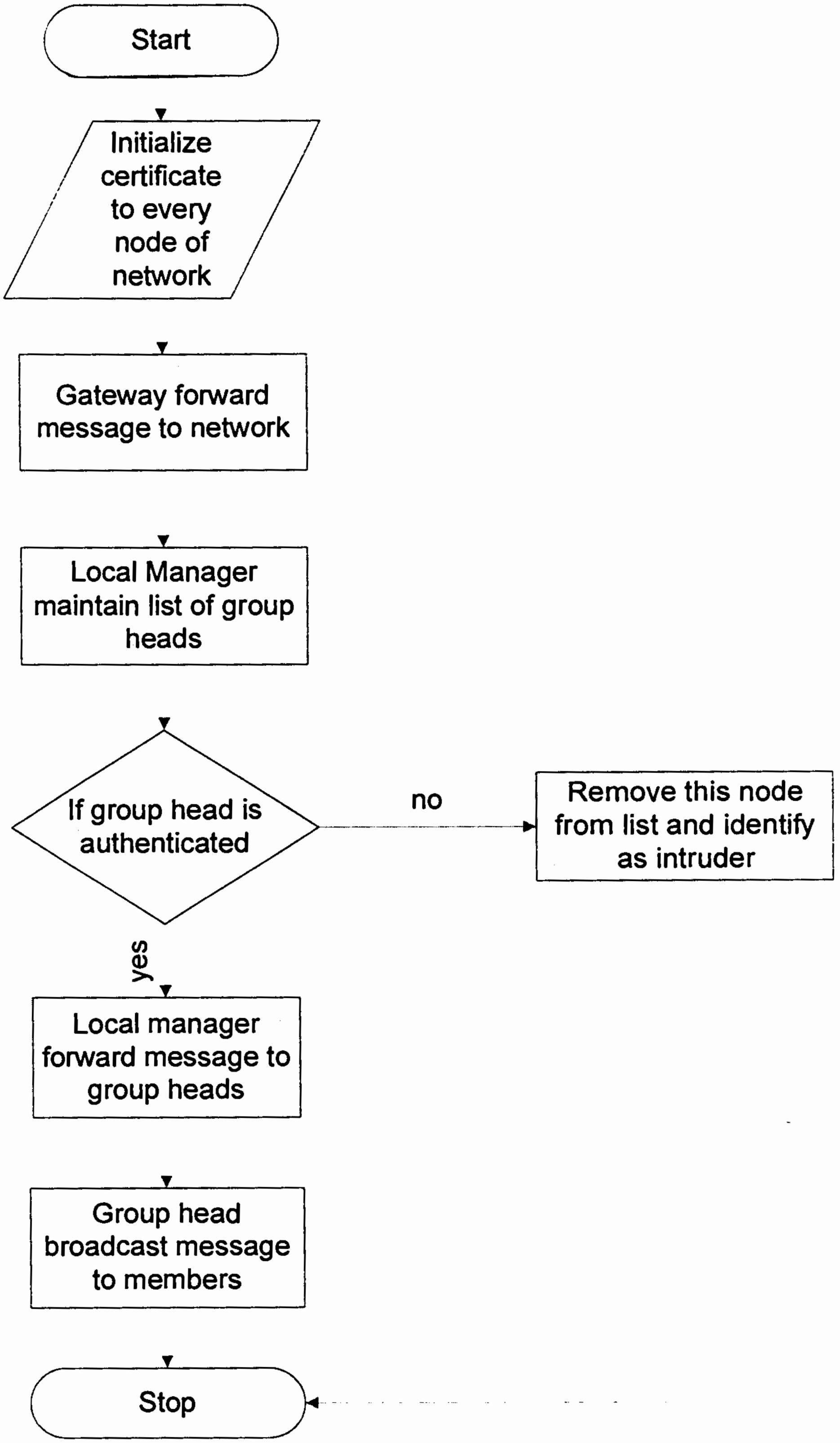

Start
Initialize certificate to every node of network
Gateway forward message to network
Local Manager maintain list of group heads
If group head is authenticated
no
Remove this node from list and identify as intruder
yes
Local manager forward message to group heads
Group head broadcast message to members
Stop

Fig.4.3. Flowchart of RAGHC Architecture

4.6 Summary

This chapter briefly discuss about the design of the architecture and traffic patterns. We also discuss about the design requirements, type of nodes. We also discuss field based routing in detail. Then, we propose an algorithm and at the end a flowchart of the proposed scenario.

Testing and Performance Evaluation

5.1 Introduction

Simulation is developed using OMNeT++ and is executed with different type of scenarios. To analyze the results, we consider different scenarios. OMNET++ is a discrete event modular and object-oriented simulator. It is being used in development since 1992. Primary use of OMNET++ is to simulate communication networks, distributed systems and parallel systems. Students at Technical University of Budapest, Hungry, started OMNET. Andrås Varga, one of the pioneer students maintains this open source simulation package. Several people contributed to this package. The first public release was in 1997 and animation was added in 1998, which made the package even more usable for education.

5.1.1 Simulation Model

To simulate the model OMNet++ is used. A network having routing nodes are placed the details of the scenario is discussed below.

5.1.2 Proposed Model

A proposed model is shown in the figure, having gateway, intermediate nodes, Local manager, group head and group members.

These nodes are randomly placed but for this simulation they are fixed and not change their positions, the top most is called gateway, below gateway there are many intermediate nodes having routing capacity between these nodes there are two group managers that serve as the certification authority the third type of nodes are called group heads that act as the group head of the group and the traffic is always route towards these heads. The last types of nodes are called group members having capability of routing the traffic to their group members.

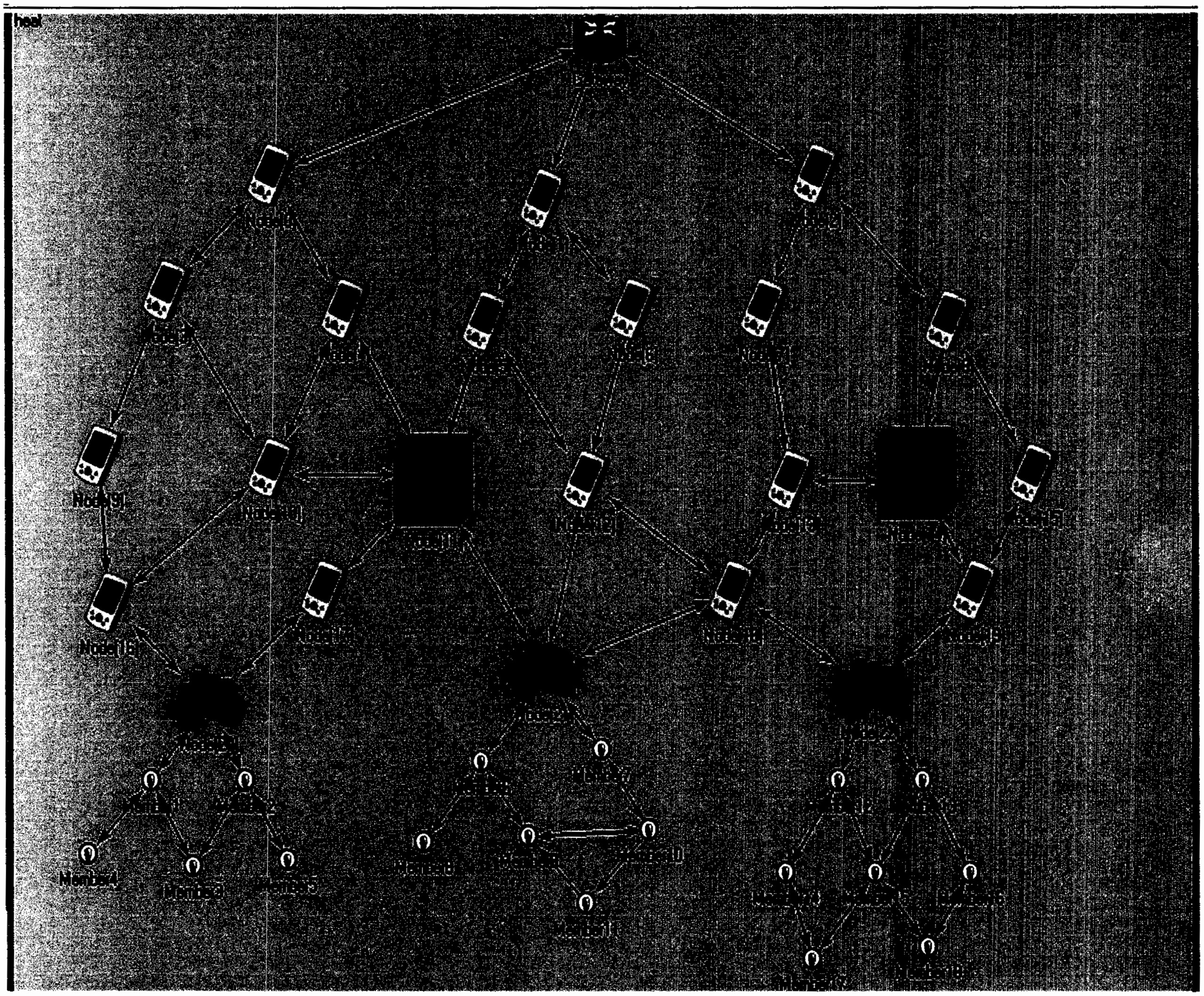


Fig.5.1. RAGHC (Reliable Authenticated Group Head Communication)

5.1.3 Traffic analysis

To analyze the traffic in the network, as the existing literature discusses that how to route the packet from Mesh network to the gateway using anycasting but routing from gateway to the mesh network is not done using anycasting.

There are three types of traffic coming from gateway, i.e. anycast, unicast and geocast. First gateway analyzes the type of traffic and then sends it to the group manager and issues a certificate and then forwards it to the particular cluster head. Similarly, group head can also communicate with the other group head via local manager. On receiving the packet group head broadcast it to its group member.

5.2 Test scenarios

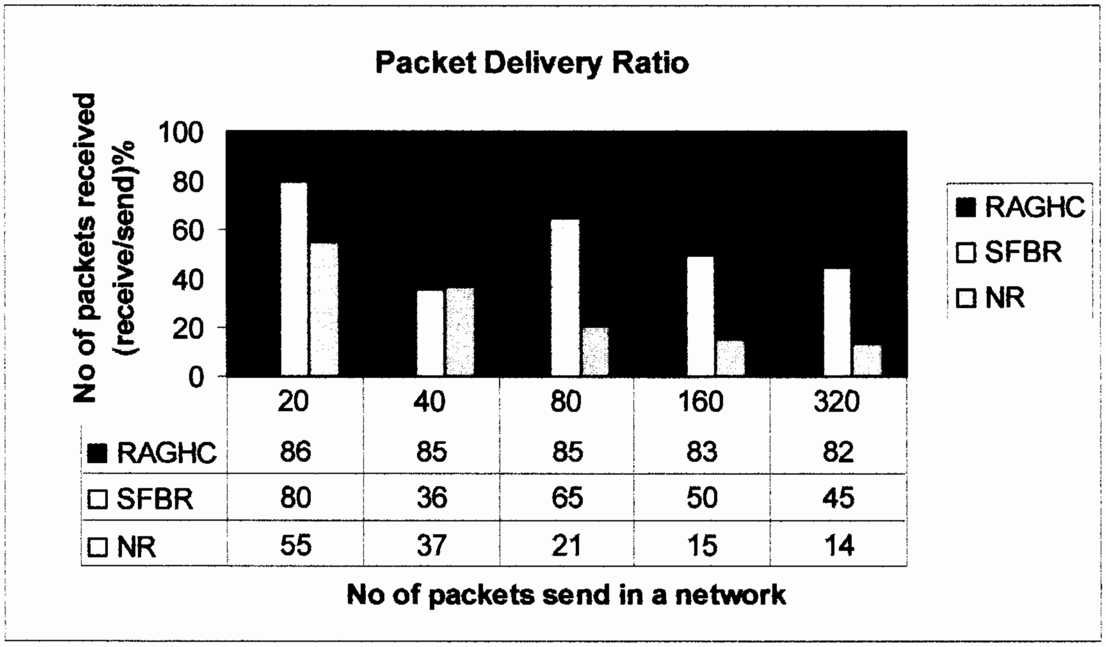
5.2.1 Packet Delivery Ratio

Fig.5.2. It shows that in RAGHC (Reliable Authenticated Group Head Communication) 86% of the packets are delivered and remaining is lost while in SFBR (Secure Field Based Routing) also 80% are delivered and rest is lost. In NR (Normal Routing) just 55% of packets are delivered and rest is lost if the no of packets is 20. But when the no of packets are increased then RAGHC performance is good than the other two techniques and RAGHC delivered more no of packets and it is good for heavy traffic because it delivered more packets. So, RAGHC delivery ratio is high than the normal techniques.

Packet Delivery Ratio Values:

No. of Packets	RAGHC	SFBR	NR
20	86	80	55
40	85	36	37
80	85	65	21
160	83	50	15
320	82	45	14

Table 1. Packet Delivery Ratio



	20	40	80	160	320
■ RAGHC	86	85	85	83	82
□ SFBR	80	36	65	50	45
□ NR	55	37	21	15	14

Fig.5.2. Packet Delivery Ratio

5.2.2 Secure Inter Group Communication

The graph below shows the secure inter group communication between different group heads via their local manager levels. There may be many local managers within the network. Each local manager may b 1 or more than 1 group heads. When local manager is 1 level away (in hierarchy) from the groups then the time delay will be 7.8 on packet 160. When it is 2 level away then delay will be 11.7 and up to so on.

Secure Inter Group Communication Values:

Local Manager levels	On packet 160
1	7.8
2	11.7
3	15.4
4	19.7
	22.8

Table 2.Secure Inter Group Communication

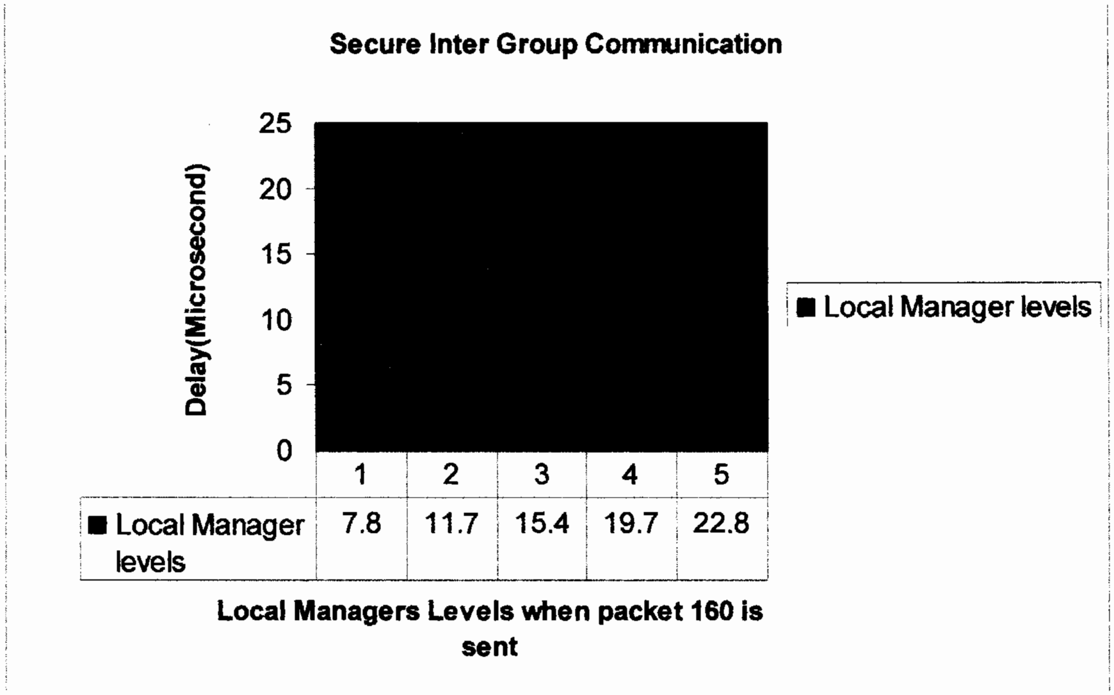
Packet Delivery Ratio Values:

No. of Packets	RAGHC	SFBR	NR
20	86	80	55
40	85	36	37
80	85	65	21
160	83	50	15
320	82	45	14

Table 1. Packet Delivery Ratio

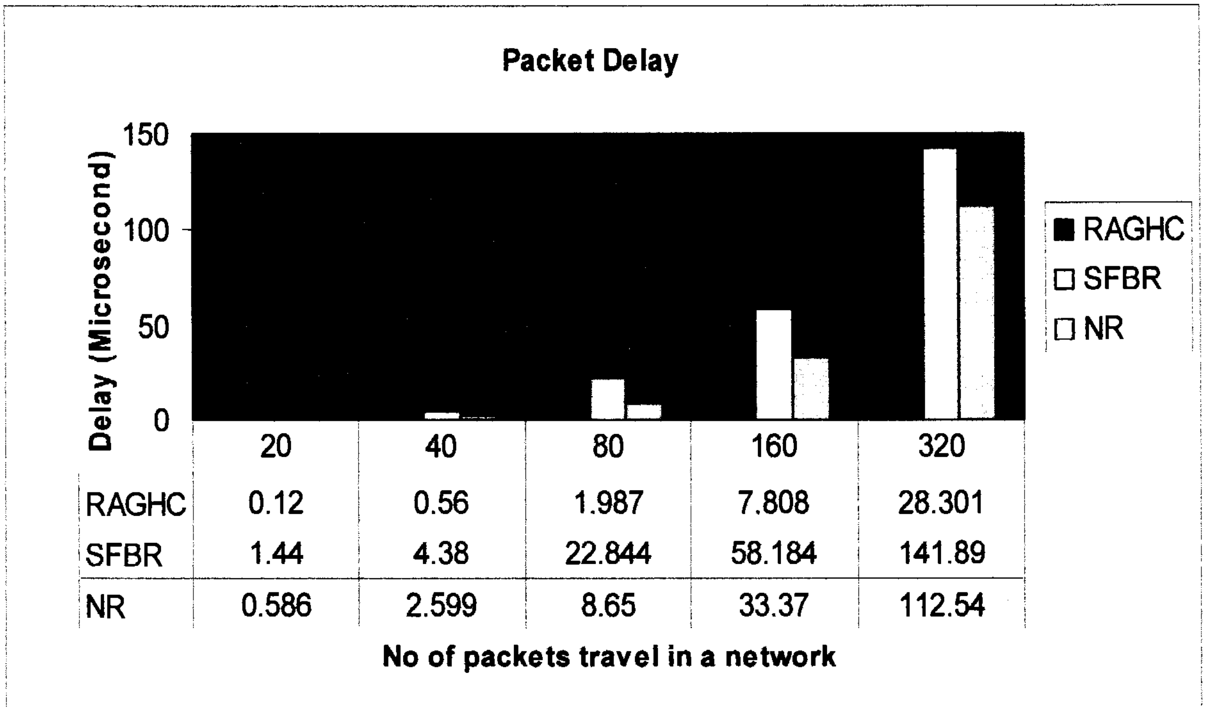
5.2.2 Secure Inter Group Communication

This graph below shows the secure inter group communication between different group heads via their local manager levels. There may be many local managers within the network. Each local manager may b 1 or more than 1 group heads. When local manager is 1 level away (in hierarchy) from the groups then the time delay will be 7.8 on packet 160. When it is 2 level away then delay will be 11.7 and up to so on.



	1	2	3	4	5
■ Local Manager levels	7.8	11.7	15.4	19.7	22.8

Fig.1.6. Secure Inter Group Communication



	20	40	80	160	320
RAGHC	0.12	0.56	1.987	7.808	28.301
SFBR	1.44	4.38	22.844	58.184	141.89
NR	0.586	2.599	8.65	33.37	112.54

Fig.1.7. Packet Delay

Packet Delay Values:

No of Packets	RAGHC	SFBR	NR
20	0.12	1.44	0.586
40	0.56	4.38	2.599
80	1.987	22.844	8.65
160	7.808	58.184	33.37
320	28.301	141.89	112.54

Fig.1.5. Packet Delay

5.3 Performance and evaluation

All the above results show that the performance of the RAGHC performance is good and reliable than the SFBR and NR. RAGHC packet delivery ratio is high and packet loss is much less than the other two techniques. RAGHC is reliable, secure and efficient for the group head communication. Secure inter group communication can now easily be done through our proposed architecture.

5.4 Summary

This Chapter focuses on the test scenarios and their results. We analyze and compare RAGHC with SFBR and NR. Test results show that RAGHC is reliable and secure than the other two and is good for heavy traffic.

Conclusion and Future Work

6.1 Conclusion

Wireless Mesh Networks (WMNs) are static or mobile multihop nodes. Mesh network is mostly used in cities. In cities group exists like musical groups and universities etc, where wireless mesh network is mostly used. It is not easy to provide security in Wireless Mesh Network due to robustness, scalability, and with more coverage area. Security is a big and crucial problem in Wireless network. A major problem in the design of these networks is their openness so that attackers can easily attack.

The primary contribution of our thesis is to authenticate the group heads in wireless mesh network. Group communication take place in mesh network but ignore the group head security. Gateway sends the data in unicast and broad cast manner to different groups but the group heads are not registered in the network. When group heads are not registered then how secure, authentic and reliable data is send to the group members. A malicious node come and claims to be a group head. After identify this problem, we propose an architecture in which group heads are registered and local manager issue a key to the group heads and only authenticated group heads have that key for the authentic communication in the group and with the other other heads. We follow the field based routing algorithm for secure communication. In the case of join or leave we update the list which is maintained by the local managers. We do simulation in OMNET++ and hence proved that the RAGHC is good in results as compared to the SFBR and NR.

6.2 Achievements

Group heads are secured, group heads can communicate directly to each other and share large no of messages within a small time period. RAGHC is more efficient and reliable. It has less communication cost. RAGHC has also less communication cost and less delay.

6.3 Future work

Proposed scenario can be test with mobile scenario in future. RAGHC does not deal with data authenticity. Route different types of traffic in this network and check the simulation results; this all can also be done in future.

References

[1] Yong Wang and Byrav Ramamurthy: "Group Rekeying Schemes for Secure Group Communication in Wireless Sensor Networks", Proceedings of International Conference of IEEE, 2007.

[2] S.Kalaiselvi, II M.E (CSE) Prof.S.JabeenBegum, M.E., (PhD): "A Secure Group Communication Using Non-interactive key Computation in Multiparty Key Agreement", Proceedings of the International Conference on Computing, Communication and Networking, 2008.

[3] D. A. Agarwal, O. Chevassuty, M. R. Thompson G. Tsudik: "An Integrated Solution for Secure Group Communication in Wide-Area Networks", In Proceedings. of 6th IEEE Symposium on Computers and Communications, 2008.

[4] Weichao Wang Yu Wang: "Secure Group- Based Information Sharing in Mobile Ad Hoc Networks", Publication in the ICC proceedings,2008.

[5] Zhen-Ai Jin; Geum-Dal Park; Kee-Young Yoo, "An improved Secure Authenticated Group Key Agreement Protocol for WMNs", IEEE-ALPIT, 2008.

[6] Jing Dong, Kurt Ackermann, Cristina Nita-Rotaru: "Secure Group Communication in Wireless Mesh Networks", ICST-MeshNets, 2009.

[7] Bjorn Saballus1, Markus Volkmer, and Sebastian Wallner2: "Secure Group Communication in Ad-Hoc Networks using Tree Parity Machines" Kommunikation in Verteilten Systemen, KiVS Bern, Switzerland, 2007.

[8] V.Vijayaraghavan R.S.D.Wahida Banu, AP/CSE Department Professor/ECE Department Sona college of Tech. A.C. College of Engg and Tech.Salem.5, TamilNadu. Karaikudi: "Efficient Key Management Architecture With Copyright Protection For Dynamic Groups", Computing Conference of IEEE, 2007.

[9] Yair Amir, Member, IEEE, Cristina Nita-Rotaru, Member, IEEE, Jonathan Stanton, Member, IEEE, and Gene Tsudik, Member, IEEE: Secure Spread: "An Integrated Architecture for Secure Group Communication", Proceedings on networking in IEEE, 2008.

[10] In Joe Khor (Oklahoma State University Tulsa, USA) Johnson Thomas (Oklahoma State University Tulsa, USA jpt@cs.okstate.edu) Istvan Jonyer (Oklahoma State University Tulsa: "Sliding Window Protocol for Secure Group Communication in Ad-Hoc Networks", ICST-MeshNets, 2009.

[11] CS Division, Korea Advanced Institute of Science and Technology: "A Distributed Model for Secure and Scalable Group Communication"6th IEEE Symposium on Computers, 2008.

[12] Rainer Baumann, Simon Heimlicher, Vincent Lenders, Martin May: "Routing packets into Wireless Mesh Networks"Conference of IEEE,2008.

[13] Rainer Baumann, Simon Heimlicher, Vincent Lenders, Martin May: "HEAT: Scalable Routing in Wireless Mesh Networks Using Temperature Fields", Computing of ICCN,2008.

[14] V. Lenders, M. May, and B. Plattner, "Density-based vs. Proximity-based Anycast Routing for Mobile Networks," in IEEE INFOCOM, Barcelona, Spain, April 2006.

[15] I. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, March

2005 vol. 47, no. 4, pp. 445–487.

[16] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: Commodity multihop ad hoc network,", Commun Magazine, IEEE,March 2005, pp. 123–131.

[17] Yaling Yang , Jun Wang , Robin Kravets, "Designing Routing Metrics for Mesh Networks", Workshop on Wireless Mesh Networks (WiMesh),IEEE, 2005.

[18] V. Lenders, M. May, and B. Plattner, "Density-based vs. Proximity-based Anycast Routing for Mobile Networks," in IEEE INFOCOM, Barcelona, Spain, April 2006.

[19] Vincent Lenders, PhD thesis. "Field-based Routing and its Application to Wireless Ad Hoc Networks" Shaker Verlag, 2006.

[20] Muhammad Shoaib Siddiqui, Choong Seon Hong "Security issues in Wireless Mesh Networks", International Conference on Multimedia and Ubiquitous Engineering,IEEE,2007.

[21] A. S. Tanenbaum. Computer Networks. Prentice Hall, third edition.

[22] J. F. Kurose and K. W. Ross. Computer Networking: A Top-Down Approach Featuring the Internet. Addison-Wesley, second edition, 2002.

[23] Elizabeth M. Belding Royer. Routing Approaches in Mobile ad hoc Networks. In Mobile Ad Hoc Networking, edited by Stefano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, IEEE, 2004.

[24] Larry L. Peterson and Bruce S. Davie. Computer Networks-A Systems Approach, 3rd edition, Morgan Kaufmann Publishers, 2003.

[25] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, a. Qayyum et L. Viennot. Optimized Link State Routing Protocol. In IEEE INMIC Pakistan, 2001.

[26] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA '1999.

[27] D. Johnson and D. Maltz. Dynamic source routing in ad hoc wireless networks. In Mobile Computing (ed. T. Imielinski and H. Korth), Kluwer Academic Publishers, Dordrecht, The Netherlands, 1996.

[28] Yih-Chun Hu and Adrian Perrig. A Survey of Secure Wireless Ad Hoc Routing. In IEEE Security & Privacy, special issue on Making Wireless Work, 2(3). May/June 2004.

[29] Vincent Lenders, Martin May, Bernhard Plattner. Density-based Anycast. A Robust Routing Strategy for Wireless Ad Hoc Networks. In Proceedings of IEEE/ACM Transactions on Networking, IEEE, 2007.

[30] Vincent Lenders, Martin May, Bernhard Plattner. Service Discovery in Mobile Ad Hoc Networks. A Field Theoretic Approach. Elsevier Journal on Pervasive and Mobile Computing, Elsevier, Vol. 1, No. 3, pages 343-370, September, 2005.

[31] Praveen Kumar, Joy Kuri, Pavan Nuggehalli, Mario Strasser, Martin May, Bernhard Plattner. Connectivity-aware Routing in Sensor Networks. In Proceedings of Sensorcomm 2007, IEEE, September, 2007.

[32] http://www.webopedia.com/TERM/A/anycast.html.

[33] Rainer Baumann and Vincent Lenders and Simon Heimlicher and Martin May, "HEAT: Scalable

Routing in Wireless Mesh Networks using Temperature Fields," in Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2007 submitted.

[34] M. Mosko and J. J. Garcia-Luna-Aceves, "Ad hoc routing with distributed ordered sequences," in IEEE INFOCOM 2006, Barcelona, Spain, April 2006.

[35] B.-N. Cheng, M. Yuksel, and S. Kalyanaraman, "Orthogonal rendezvous routing protocol for wireless mesh networks," in Proc. of ICNP. Santa Barbara, California: IEEE, Nov. 2006.

[36] M. Mosko and J. J. Garcia-Luna-Aceves, "Ad hoc routing with distributed ordered sequences," in IEEE INFOCOM 2006, Barcelona, Spain, April 2006.

[38] S. Bhattachargee, M. Ammar, E. Zegura, N. Shah, and Z. Fei. Application Layer Anycasting. In Proceedings of the IEEE INFOCOM'97, 1997.

[39] D. Katabi and J. Wroclawski. "A Framework for Scalable Global IPAnycast (GIA)". Proceeding Applications, Technologies, Architectures, and Protocols for Computer Communication, Stockholm, Sweden, 2000.

[40] V. D. Park and J. P. Macher. "Anycast Routing for Mobile Networking". Proc. of the IEEE Military Communications Conference, volume I, pages 1–5, 1999

[41] Zheng Xie, Jianxin Wang, Yuan Zheng and Songqiao hen, "A Novel Anycast Routing Algorithm in MANET", PACRIM IEEE, 2003.

[42] Jianxin Wang, Yuan zheiig, Weijia Jia, "An AODV Based Anycast Protocol in Mobile Ad Hoc Network", PACRIM IEEE, 2003.

[43] Mihail L. Sichitiu, "Wireless Mesh Networks Challenges and Opportunities", ACM Computer Communications, 2008, Volume 31, Issue 7, Pages 1413-1435.

[44] V. Lenders, M. May, and B. Plattner, "Density-based vs. Proximity-based Anycast Routing for Mobile Networks," in IEEE INFOCOM, Barcelona, Spain, April 2006.

[45] V. Park and S. Corson, "Temporally-Ordered Routing Algorithm (TORA)", IETF Internet Draft, July 2001.

[46] Rainer Baumann and Vincent Lenders and Simon Heimlicher and Martin May, "HEAT: Scalable Routing in Wireless Mesh Networks using Temperature Fields," IEEE WoWMoM, 2007.

[47] Muhammad Ali Khan, Syed Muhammad Reza, Hamed Moradi: A Brief Overview Of Wireless Mesh Networks with Focus on Routing", IEEE-ICC, 2007

[48] Naouel Ben Salem Jean-Pierre Hubaux: "Securing Wireless Mesh Networks", IEEE Wireless Communications, 2006, vol. 13, no 2.

[49] Yong Wang and Byrav Ramamurthy: Group Rekeying Schemes for Secure Group Communication in Wireless Sensor Networks", IEEE-ICC, 2007

[50] Kalaiselvi, S Begum, S.J.,"a secure group communication using non-interactive key computation in multiparty key agreement", IEEE-ICCC, 2008.

[51] S.Roy, V.Addada, S. Setia, S. Jajodia, Securing MAODV: attacks and counter measures, in:

proceedings of SECON'05, 2005.

[52] R. Curtmola, C. Nita-Rotaru, BSMR: "Byzantine-resilent secure multicast routing in multi-hop wireless networks", in: IEEE SECON 2007.

[53] Guangsong Li, "An Identity-Based Security Architecture for Wireless Mesh Networks", IEEE-IFIP. 2007.

[54] H. Chun-Yih and H.J.Wang, "A framework for location privacy in Wireless Networks," in proc of ACM SIGCOMM Asia Workshop,2005.

[55] P. Tague, R.Poovendran "Modeling node capture attacks in multi-hop wireless networks," Ad Hoc Networks, August 2007, vol. 5 issue 6,. pp. 801- 814

[56] X.Wu , N. Li, "Achieving privacy in Mesh Networks," in proceedings if SASN'06, 2006, pp- 13-22. October 30.

[57] Muhammad Shoaib Siddiqui, Chong Seon Hong: "Security Issues in Wireless Mesh Networks", 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07).

[58] Muhammad Ali Khan, Syed Muhammad Reza, Hamed Moradi: "A Brief Overview Of Wireless Mesh Networks with Focus on Routing".

[59] Naouel Ben Salem Jean-Pierre Hubaux: "Securing Wireless Mesh Networks".

[60] B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, S. Vasudevan, C. Zhang: "Secure Group Communications For Wireless Networks", 2001 IEEE.

[61] Atif Naseer, Fazl-e-Hadi,M. Younus Javed: "SFBR: A Secure Field Based Routing Protocol for Wireless Mesh Network",2009

Acronyms

WAN	Wide Area Network
LAN	Local Area Network
WMN	Wireless Mesh Network
AODV	Ad-hoc on Demand Distance Vector
DSR	Dynamic Source Routing
SGL	Secure Group Layer
MANET	Mobile Ad-hoc Network
BSs	Base Stations
TMKM	Topology Matching Key Management
CRTDH	Chinese Remainder Theorem & the Diffie-Hellman
DoS	Denial of Service
HWMP	Hybrid Wireless Mesh Protocol
TAPs	Transit Access Points
PKI	Public Key Infrastructure
SeGrOM	Secure Group Overlay Multicast
SFBR	Secure Field Based Routing
RAGHC	Reliable Authenticated Group Head Communication
OMNET++	A Network Simulator