Each node acts as a base station and is responsible for dynamically discovering other nodes it can directly communicate with In MANET

K.Sowjanya Naidu- Assistant Professor, Rani Sesha Bhargavi- Assistant Professor,
V. Lokeshwari Vinya- Assistant Professor
Department of Computer Science Engineering and Technology
G. V. P. College of Engineering (A), Madhurawada, Visakhapatnam, Andhra Pradesh, India

Abstract: *In this paper, we utilize the Wireless networks, nodes can communicate through base stations. In this scenario, the communication process takes more time to complete. To reduce this delay time, a Mobile Ad hoc Network is introduced. A Mobile ad hoc Network (MANET) is an infrastructure less network. In this, each node acts as a base station and is responsible for dynamically discovering other nodes it can directly communicate with. In MANET, message delivery can be speeded up by means of group communication. For the secure group communication, there is a process of generating, distributing and updating keys to the nodes is called key management. One of the key management schemes is group key management scheme. In this scheme updating of keys for newly joining or leaving nodes in a group is done by rekeying technique. In the existing system, the authors have employed a technique using One-way Function Chain (OFC) for key generation. In the proposed research, the keys are generated randomly and encrypted the generated keys using RSA algorithm before the keys are assigned to the nodes in clusters. This technique is simulated in network simulator tool.*

keywords: *network of nodes, Data Sanitization, Access points, Radio technology, Denial of Service, Bayesian Belief Networks, data computation, Error Estimation, Discovering neighbors, Software metrics, empirical data..*

Date of Submission: 06-10-2017 Date of acceptance: 18-10-2017

I. Introduction

As wireless communication technology is increasing, folks predict to be able to use their network terminals anywhere and anytime. Samples of such terminals are unit PDAs and laptops. Users want to maneuver concerning whereas maintaining property to the network (i.e., Internet), and wireless networks offer them with this chance. Wireless property to the network provides users the liberty of movement they need. Most wireless networks nowadays needs associate in nursing underlying architectureof fixed positionrouters, and are therefore dependent on existing infrastructure. Typically, the mobile nodes in such networks communicate directly with questionable access points (APs), that successively routes the traffic to the corresponding nodes. Today, another sort of wireless networks is rising, specifically impromptu wireless networks. These networks include mobile nodes and networks that themselves creates the underlying design for communication. Owing to this, no pre-existing routers area unit required.

The OSI reference model: The open systems interconnection (OSI) reference model was developed by the alliance for Standardization (ISO) so as to standardize the protocols employed in numerous network layers. Also, the figure shows however the implementation of a typical UNIX router corresponds to those models. In wireless networks, nodes usually use frequencies channels as their physical medium. This corresponds to rock bottom layer within the OSI model. Since the nodes needn't be physically connected, the network offers information property at the side of user quality. MAC layer corresponds to the information link layer within the OSI model. the most objective of the OSI link layer is to produce error-free transmission of information across a physical link. protocols' version of this theme consists of 2sub layers: Logical Link management (LLC) and Medium Access management (MAC). The (possibly) most vital services that the LLC offers is error and flow management. The MAC layer directly interfaces with the physical layer, and provides services like addressing, framing, and medium access management.

Wireless networks: Numerous completely different wireless networks exist, varied within the method the nodes interconnect. One will roughly classify them in 2 types:

- Infrastructure dependent
- Ad hoc wireless networks

Current cellular networks area unit classified because the infrastructure dependent networks. What is typical for these networks is their use of access points, or base stations. Additionally to acting as a router inside the network, associate in nursing access purpose may also act sort of a bridge connecting, for instance, the wireless network and a wired network. GSM, and its 3G counterpart UMTS, are unit samples of well recognize cellular networks. In impromptu wireless networks, on the opposite hand, the nodes themselves are unit liable for routing and forwarding of packets. Hence, the nodes have to be compelled to be a lot of intelligent in order that they'll perform as routers similarly as regular hosts. Centralized routing Associate in simplified resource management by an AP implies less guiltiness than the distributed counterpart. An AP, as opposition individual nodes, sometimes has a lot of data concerning the network, and area unit so able to build intelligent selections once it involves routing.

Radio technology: As mentioned on top of, nodes in wireless networks usually utilize radio transmission. Infrared (IR) and Microwave (MW) are unit 2 different transmission technologies, of that IEEE 802.11 supports the previous one additionally to radio. Wireless LANs use magnetic attraction airwaves (radio or infrared) to speak. The airwaves propagate through house (even in an exceedingly vacuum). Completely different frequencies have different qualities: the upper the magnetic attraction frequency, a lot of data will be transmitted per second. However, lower frequencies area unit straightforward to get, will travel long distances, and might penetrate buildings simply. Radio waves operate lower frequencies than infrared waves, creating it a lot of appropriate for many wireless networks. Frequency hopping unfold spectrum (FHSS) and direct sequence unfold spectrum (DSSS) area unit the 2 radio transmission schemes supported in IEEE 802.11. The concept behind FHSS is that the transmitter hops from frequency to frequency many times per second. The hop pattern is understood to each the sender and receiver, and to different receivers not awake to the pattern, the transmission is difficult to notice. DSSS, on the opposite hand, doesn't hop from one frequency to a different, however distributes the signal over the complete waveband quickly.

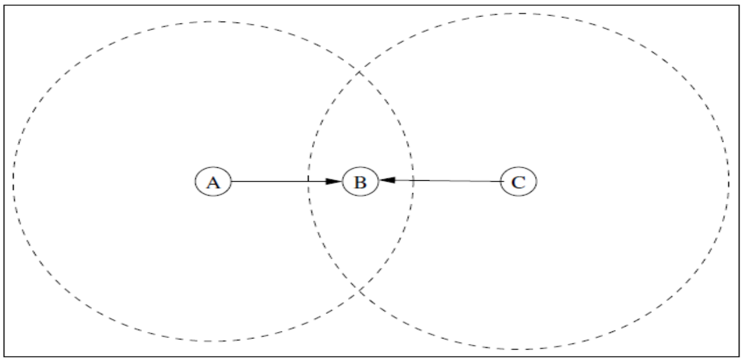


Figure1. The hidden terminal problem

Issues in wireless networks: There will be a variety of problems to contemplate once coming up with operations of wireless networks. Consecutive subsections describe a specific few of them.

Hidden terminals: As illustrated in Figure, node A and node C area unit in vary for human activity with node B, however not with one another. Each could attempt to communicate with node B at the same time, and may not notice any interference on the wireless medium. Thus, the signals collide at node B, which will not be able to receive the transmissions from either node. The standard resolution for thisisknown as Hidden terminal. Drawback is that the nodes coordinate transmissions themselves by asking and granting permission to send and receive packets. This theme commonly known as RTS/CTS (Request tosend/ Clear tosend).The fundamental plan is to capture the channel by notifying different nodes concerning Associate in nursing approaching transmission. This will be often done by stimulating the receiving node to outputting a brief frame in order that close nodes can notice that a transmission goes to require place. The close nodes area unit then expected to avoid transmission for the length of the approaching (large) information frame.

Exposed terminals: Consider a topology just like that of Figure, however extra a node D solely accessible from node C. Furthermore, suppose node B communicates with node A, and node C needs to transmit a packet to node D. throughout the transmission between node B and node A, node C senses the channel as busy. Node C incorrectly conclude that it's going to not send to node D, even supposing each the transmissions (i.e., between node B and node A, and between node C and node D) would succeed. Dangerous reception would solely occur within the zone between node B and node C, wherever neither of the receiver’s area unit situated. This drawback is commonly brought up as .the exposed terminal drawback. Both the hidden and also the exposed terminal drawback cause important scale back of network output once the traffic load is high.

Neighbor discovery: Discovering neighbors may be a central link layer operation in wireless networks. In some cases the node could be inquisitive about only 1 specific reasonably neighbor, or all neighbors. In either case, the node has to discover its neighbors and confirm their sorts. Since the topology of the network usually is incredibly dynamic, the neighborhood data ought to be updated sporadically. If the topology undergoes too fast changes in property for the nodes to exchange topological data, flooding is that the solely thanks to get information to a specific destination.

Mobile Ad Hoc Wireless Networks: In ad-hoc networks, as mentioned on top of, the nodes themselves area unit liable for routing and forwarding of packets. If the wireless nodes area unit inside vary of every different, no routing is critical. But, on the opposite hand, if the nodes have got rid of vary from one another, and so aren't able to communicate directly, intermediate nodes area unit required to form up the network during which the packets area unit to be transmitted. There are unit varieties of things during which impromptu networks area unit suited. Examples embrace emergency operations wherever there exist no fastened infrastructure, and military operations wherever the present infrastructure may not be sure.As for cellular networks, nodes in an ad hoc network area unit liable for dynamically discover that different nodes they will directly communicate with. There areunit quite few problems that required to be throughout once it involves impromptu networking. A short summary of a number of these follows.

Medium access scheme: The medium access protocol (MAC) has to be designed to permit surely characteristics of wireless networks. Typical for wireless networks the nodes moves concerning, and this ends up in hidden terminal drawback as antecedently delineate. Also, truthful access to the medium, and minimize collisions, should be taken into consideration. The MAC protocol ought to even be able to change the ability used for transmissions, because, for Associate in nursing example, reducing transmission power at a node cause a decrease in interference at neighboring nodes, and increase frequency utilize.

Routing : Traditional routing protocols are not designed for rapid changing environments such as ad hoc networks. Therefore, customized routing protocols are needed. Examples of such protocols are AODV[6] and OLSR[1]. Routing is further discussed below.

Security : Due to the fact that the nodes in a wireless ad hoc network communicate on a shared medium, security becomes an important issue. This, in combination with the lack of any central coordination, makes the network more vulnerable to attack than wired networks. There are different ways of compromising wireless networks, including:

- Denial of service. An attacker makes services unavailable to others by keeping the service provider busy.
- Resource consumption. Battery power of critical nodes is depleted because of unnecessary processing caused by an attacker, or the attacker causes buffer overflow which may lead to important data packets being dropped.
- Host impersonation. As the name suggests, a compromised node may impersonate a host, and thereby cause wrong route entries in routing tables elsewhere in the network.

Quality of service: Providing quality of service (QoS) in a wireless ad hoc network is a difficult task to overcome. Nodes in such a network usually act both as clients and service providers, making, contrary to most networks, the boundary between network and host less clear. Hence, to achieve QoS, a better coordination between the nodes is required. Furthermore, wireless communication usually implies limited resources, and this, in addition to the lack of central coordination, exacerbate the problem.

- Parameters. Different applications have different QoS parameter requirements. Whereas multimedia applications require high bandwidth and low delay, availability is the primary requirement for search-and-rescue operation applications. Routing. To make sure that applications are provided with the services they request, QoS parameters should be considered for route decisions. Throughput, packet loss rate, and reliability are examples of such parameters.

Routing in ad hoc wireless networks: As the nodes in a wireless ad hoc network can be connected in a dynamicand arbitrary manner, the nodes themselves must behave as routers and takepart in discovery and maintenance of routes to other nodes in the network. The goal of a routing algorithm is to devise a scheme for transferring apacket from one node to another. One challenge is to define/choose whichcriteria to base the routing decisions on. Examples of such criteria includehop length, latency, and bandwidth and transmission power. Literature lists some challenges in designing a routing protocol for ad hocwireless networks, and a brief overview of these is given below.

Mobility: The network needs to adapt to rapid changes in the topology due tothe movement of the nodes, or the network as a whole.

II. System Overview

Hidden terminals: As illustrated in Figure, node A and node C area unit in vary for human activity with node B, however not with one another. Each could attempt to communicate with node B at the same time, and may not notice any interference on the wireless medium. Thus, the signals collide at node B, which will not be able to receive the transmissions from either node. The standard resolution for thisisknown as Hidden terminal. Drawback is that the nodes coordinate transmissions themselves by asking and granting permission to send and receive packets. This theme commonly known as RTS/CTS (Request tosend/ Clear tosend).The fundamental plan is to capture the channel by notifying different nodes concerning Associate in nursing approaching transmission. This will be often done by stimulating the receiving node to outputting a brief frame in order that close nodes can notice that a transmission goes to require place. The close nodes area unit then expected to avoid transmission for the length of the approaching (large) information frame.

Exposed terminals: Consider a topology just like that of Figure, however extra a node D solely accessible from node C. Furthermore, suppose node B communicates with node A, and node C needs to transmit a packet to node D. throughout the transmission between node B and node A, node C senses the channel as busy. Node C incorrectly conclude that it's going to not send to node D, even supposing each the transmissions (i.e., between node B and node A, and between node C and node D) would succeed. Dangerous reception would solely occur within the zone between node B and node C, wherever neither of the receiver’s area unit situated. This drawback is commonly brought up as .the exposed terminal drawback. Both the hidden and also the exposed terminal drawback cause important scale back of network output once the traffic load is high.

Neighbor discovery: Discovering neighbors may be a central link layer operation in wireless networks. In some cases the node could be inquisitive about only 1 specific reasonably neighbor, or all neighbors. In either case, the node has to discover its neighbors and confirm their sorts. Since the topology of the network usually is incredibly dynamic, the neighborhood data ought to be updated sporadically. If the topology undergoes too fast changes in property for the nodes to exchange topological data, flooding is that the solely thanks to get information to a specific destination.

Mobile Ad Hoc Wireless Networks: In ad-hoc networks, as mentioned on top of, the nodes themselves area unit liable for routing and forwarding of packets. If the wireless nodes area unit inside vary of every different, no routing is critical. But, on the opposite hand, if the nodes have got rid of vary from one another, and so aren't able to communicate directly, intermediate nodes area unit required to form up the network during which the packets area unit to be transmitted. There are unit varieties of things during which impromptu networks area unit suited. Examples embrace emergency operations wherever there exist no fastened infrastructure, and military operations wherever the present infrastructure may not be sure.As for cellular networks, nodes in an ad hoc network area unit liable for dynamically discover that different nodes they will directly communicate with. There areunit quite few problems that required to be throughout once it involves impromptu networking. A short summary of a number of these follows:

Medium access scheme: The medium access protocol (MAC) has to be designed to permit surely characteristics of wireless networks. Typical for wireless networks the nodes moves concerning, and this ends up in hidden terminal drawback as antecedently delineate. Also, truthful access to the medium, and minimize collisions, should be taken into consideration. The MAC protocol ought to even be able to change the ability used for transmissions, because, for Associate in nursing example, reducing transmission power at a node cause a decrease in interference at neighboring nodes, and increase frequency utilize.

Routing: Traditional routing protocols are not designed for rapid changing environments such as ad hoc networks. Therefore, customized routing protocols are needed. Examples of such protocols are AODV[6] and OLSR[1]. Routing is further discussed below.

Security: Due to the fact that the nodes in a wireless ad hoc network communicate on a shared medium, security becomes an important issue. This, in combination with the lack of any central coordination, makes the network more vulnerable to attack than wired networks. There are different ways of compromising wireless networks, including:

- Denial of service. An attacker makes services unavailable to others by keeping the service provider busy.
- Resource consumption. Battery power of critical nodes is depleted because of unnecessary processing caused by an attacker, or the attacker causes buffer overflow which may lead to important data packets being dropped.
- Host impersonation. As the name suggests, a compromised node may impersonate a host, and thereby cause wrong route entries in routing tables elsewhere in the network.

Quality of service : Providing quality of service (QoS) in a wireless ad hoc network is a difficult task to overcome. Nodes in such a network usually act both as clients and service providers, making, contrary to most networks, the boundary between network and host less clear. Hence, to achieve QoS, a better coordination between the nodes is required. Furthermore, wireless communication usually implies limited resources, and this, in addition to the lack of central coordination, exacerbate the problem.

- Parameters. Different applications have different QoS parameter requirements. Whereas multimedia applications require high bandwidth and low delay, availability is the primary requirement for search-and-rescue operation applications.
- Routing. To make sure that applications are provided with the services they request, QoS parameters should be considered for route decisions. Throughput, packet loss rate, and reliability are examples of such parameters.

Routing in ad hoc wireless networks: As the nodes in a wireless ad hoc network can be connected in a dynamicand arbitrary manner, the nodes themselves must behave as routers and takepart in discovery and maintenance of routes to other nodes in the network.The goal of a routing algorithm is to devise a scheme for transferring apacket from one node to another. One challenge is to define/choose whichcriteria to base the routing decisions on. Examples of such criteria includehop length, latency, and bandwidth and transmission power. Literature lists some challenges in designing a routing protocol for ad hocwireless networks, and a brief overview of these is given below.

Mobility: The network needs to adapt to rapid changes in the topology due tothe movement of the nodes, or the network as a whole.

Resource constraints : Nodes in a wireless network typically have limitedbattery and processing power, and these resources must be managedoptimally by the routing protocol.

Error-prone channel state The characteristics of the links in a wireless network typically vary, and this call for an interaction between therouting protocol and the MAC protocol to, if necessary, find alternateroutes.

Hidden and exposed terminal problem : This is described in below section.MANET routing protocols are typically subdivided into two maincategories: proactive routing protocols and reactive on-demand routingprotocols.

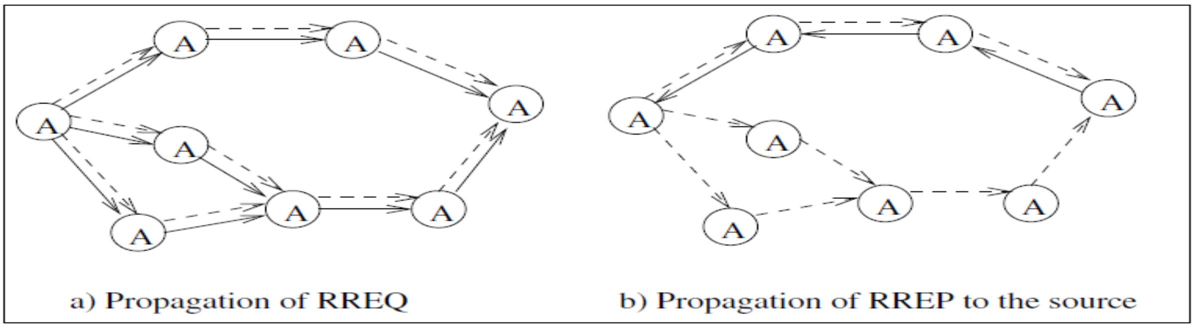


Figure2.AODV Route Discovery

Reactive protocols: Unlike proactive routing protocols, reactive routing protocols do not make the nodes initiate a route discovery process until a route to a destination is required. This leads to higher latency than with proactive protocols, but lower overhead. Ad Hoc On-Demand Distance-Vector routing protocol (AODV).

Hybrid protocols: These types of protocols combine proactive and reactive protocols to try and exploit their strengths. One approach is to divide the network into zones, and use one protocol withinthe zone, and another betweenthem.

Ad hoc On-demand Distance Vector (AODV): This section describes the AODV routing protocol. Some details on the route request mechanism and link sensing are provided, along with an example.

Introduction to AODV:AODV is an on-demand routing algorithm in that it determines a route to a destination only when a node wants to send a packet to that destination. It is a relative of the Bellman-Ford distant vector algorithm, but is adapted to work in a mobile environment. Routes are maintained as long as they are needed by the source. AODV is capable of both Unicast and Multicast routing.

In AODV, every node maintains a table, containing information about which neighbor to send the packets to in order to reach the destination. Sequence numbers, which is one of the key features of AODV, ensures the freshness of routes.

→Mobile ad hoc networks

A set of wireless communication nodes performing self-configuration in a dynamic mode for formation of network excluding fixed infrastructure or centralized supervision is termed as mobile ad hoc network (MANET). The nodes in MANET can act as hosts and routers for sending packets to each other . The network topology keeps changing quickly and randomly, whereas the terminal connectivity changes according to the time. MANET applications include military battlefields, emergency search and rescue locations and so on that requires quick deployment and active reconfiguration. It can also be utilized in a local scenario such as taxicab, sports, stadium, boat, small aircraft and conference hall .

Key management: The process of generating, distributing and updating keys to the nodes is called key management. This process plays a vital role in providing network security. An important point to be discussed in key management is distribution of keys in a secure manner . In general, more security techniques make use of traffic encryption keys for encryption and key encryption keys for decryption. When multicast data (MD) are transmitted, the keys are used by mobile nodes forencrypting and decrypting the data to be transmitted.

Moreover, the keys must be updated and refreshed when a node joins and leaves a group as essential metric in the key management process. This constraint has to be taken stringently in the key management process. Every node consumes a significant amount of energy during the key management process for generating, distributing and updating keys. Thus, key management processes in MANET require energy-efficient techniques.

In MANET, group communication can enhance the speed of message delivery. In addition, consumption of energy and bandwidth can be lessened through group communication. On the other hand, in group communication, as data are transmitted in the common communication channel, it brings in more security threats and attacks to the network that consequently reduces the network performance . In key management, apart from energy and bandwidth consumption issues, the characteristic of node mobility brings in more challenges on security that is, when a node moves from a group to another it gives rise to overhead and energy consumption cost

Problem Statement

† Substantial amount of energy consumed in the key management process .

† In hierarchal MANET (HMANET), a significant issue related to key management is mobility of nodes. This issue should address whether it permits the nodes to move from one group to another without requirement of much overhead and power consumption cost.

† While moving from one group to another, a node in HMANET endures high computation cost in key establishment time.

† In the key management process of HMANET, a critical problem is induced by roaming of nodes [9].

† When the threshold number of the shareholders compromised, then the security of the network is ruined [10].

Rekeying: In multicast communication, group key is necessary when multiple nodes desire to transmit data securely using a common secret key. Two nodes can create a secret key by using Diffie-Hellman protocol without the assistance of any centralized trusted party. This protocol can also be extended for n-nodes. The process of group key management has to address the issue of security when the membership of the nodes changes. During membership changes, the group key has to be refreshed to facilitate security. Group key refreshment can also be performed either periodically or after each membership change. Thus, the process of key refreshment assures forward and backward security [11].

Issues of rekeying:A downside of the Rekeying scheme is that it cuts down the level of security and performance of the network [12]. Since the rekeying mechanism requires a number of messages to be transmitted for key generation and distribution; it considerably degrades the performance of the system. Furthermore, for real-time group communication it requires more bandwidth and before the keys are encrypted every node requires a significant amount of memory to keep track of the dynamicrekey messages and rate of increase in node join and leave requests].

In our first work [14], we focused on improving security aspects along with quality of service (QoS) for multicast security in MANET. In this technique, the nodes with most available bandwidth and residual energy are elected as cluster heads (CHs) which act as multicast group leaders (GL). Each CH computes the trust value of its members using the success or failure ratio of the data and the control packets. Based on the trust value, the CH decides whether a node is authorized to join the multicast group or not. When the multicast source wants to transmit the data packet, it utilizesthe secret key-based packet forwarding technique. In our second work [15], we focused on a group key management technique for multicast security in MANET. This technique works in a hierarchical model such that the CHs are prioritized over the cluster members. The secure keys are generated using one-way function chain (OFC). In additiontosecure key management, the issue of mobility is also handled.

→FUNCTIONAL REQUIREMENTS: Functional Requirements refer to very important system requirements in a software engineering process (or at micro level, a sub part of requirement engineering) such as technical specifications, system design parameters and guidelines, data manipulation, data processing and calculation modules etc.

- Functional Requirements are in contrast to other software design requirements referred to as Non-Functional Requirements which are primarily based on parameters of system performance, software quality attributes, reliability and security, cost, constraints in design/implementation etc.
- The key goal of determining “functional requirements” in a software product design and implementation is to capture the required behavior of a software system in terms of functionality and the technology implementation of the business processes.
- The Functional Requirement document (also called Functional Specifications or Functional Requirement Specifications), defines the capabilities and functions that a System must be able to perform successfully.
- Functional Requirements should include:
- Descriptions of data to be entered into the system
- Descriptions of operations performed by each screen
- Descriptions of work-flows performed by the system
- Descriptions of system reports or other outputs
- Who can enter the data into the system?
- How the system meets applicable regulatory requirements
- The functional specification is designed to be read by a general audience. Readers should understand the system, but no particular technical knowledge should be required to understand the document.
- Functional requirements should include functions performed by specific screens, outlines of work-flows performed by the system and other business or compliance requirements the system must meet.
- Interface requirements
- Field accepts numeric data entry
- Field only accepts dates before the current date
- Screen can print on-screen data to the printer
- Business Requirements
- Data must be entered before a request can approved
- Clicking the Approve Button moves the request to the Approval Workflow
- All personnel using the system will be trained according to internal training strategies

→NON FUNCTIONAL REQUIREMENTS

- All the other requirements which do not form a part of the above specification are categorized as Non-Functional Requirements.
- A system may be required to present the user with a display of the number of records in a database. This is a functional requirement.
- How up-to-date this number needs to be is a non-functional requirement. If the number needs to be updated in real time, the system architects must ensure that the system is capable of updating the displayed record count within an acceptably short interval of the number of records changing.
- Sufficient network bandwidth may also be a non-functional requirement of a system.

III. Implementation Of System

Proposed Algorithm:

Algorithm 1:

Key generation algorithm for generating keys when a node joins in cluster or leavingfrom cluster.

```
Step1: Node joins into a cluster or leaves from a cluster else goto Step5
Step2: Call the Random function to generate a random number
Step3:Give the generated random number as an input to OFC
Step4: Call key distribution function keydis (Key, p, q)
Step5: End
```

Algorithm 2:

Encrypting the generated keys using RSA algorithm

/* checking function*/

```
Step1: get Ø(n), e
Step2: select ‘e’ such that 1 < e <Ø(n) and e is co-prime to Ø(n)
Step3: return ‘e’
```

```
/* encryption function*/
Step1:calculate  public key(e)
Step2: cipher text, C= exponentiation(P, e, n)
/*decryption function*/
Step1: calculate private key(d)
Step2: plain text, P= exponentiation(C, d, n)
/*get key function*/
Step1: select any two large prime numbers ‘p’ and ‘q’ such that
p ≠ q
Step2: calculate n = p x q
Step3: calculate Ø (n) = (p-1) x (q-1)
Step4: calculated numbers send to the “check ()” along with Ø (n)
Step5: generated public key pair (e, n) from step4
Step6: calculate private key pair (d, n) for decryption, d= $e^{-1}$ mod Ø (n)
Step7: call the encryption function to get the cipher text
       C= (P, e, n) where “P” is the generated key.
Step8: call the decryption function to get the plain text
       P= (C, d, n).
```

RSA.tcl

```
proc decrypt {c d n } {
set p1 [expr round([expr pow($c,$d)]) % $n]
set p1 [expr $p1 % $n]
puts "Plaintext:$p1"
}
#----------Deckey()------------------#
procdeckey { c e n phi} {
set d 1
set s [expr [expr $e*$d] % $phi]
while {$s!=1} {
set s [expr [expr $e*$d] % $phi]
          if {$s==1} {
puts "Decryption key: $d"
            #decrypt $c $d $n
     }
set d [expr $d+1]
}
puts "                 "
}
#---------Encrypt--------------------#
proc encrypt { p e n phi} {
set c [expr round([expr pow($p,$e)]) % $n]
set c [expr $c % $n]
#puts "plaintext:$p"
#puts "encryption key:$e"
puts "$c"
puts "    "
#deckey $c $e $n $phi
}
#---------check function-------------#
proc check { a b p } {
          globale,phi,count,n,p
          set n [expr $a * $b]
          set phi [expr [expr $a-1] * [expr $b-1]]

                    for {set e 2} {$e < $phi} {incr e} {
                    set count 0
                    for {set i 1} {$i< $phi} {incri} {
                              if {[expr $e % $i] == 0 && [expr $phi % $i] == 0} {
                              set count [expr $count + 1]
```

```
                                   }                              }
                                 if {$count == 1} {
                                 #Call Encrypt function by passing p,e,n
                                 encrypt $p $e $n $phi
                                 }  set p [lindex $argv 0]
set q [lindex $argv 1]
puts "$q"
set a 5
set b 11
check $a $b $p
```

IV. System Design

The Unified Modeling Language allows the software engineer to express an analysis model using the modeling notation that is governed by a set of syntactic semantic and pragmatic rules.A UML system is represented using five different views that describe the system from distinctly different perspective.

A Use Case Model describes the proposed functionality of a new system. A Use Case represents a discrete unit of interaction between a user (human or machine) and the system. This interaction is a single unit of meaningful work, such as Create Account or View Account Details.

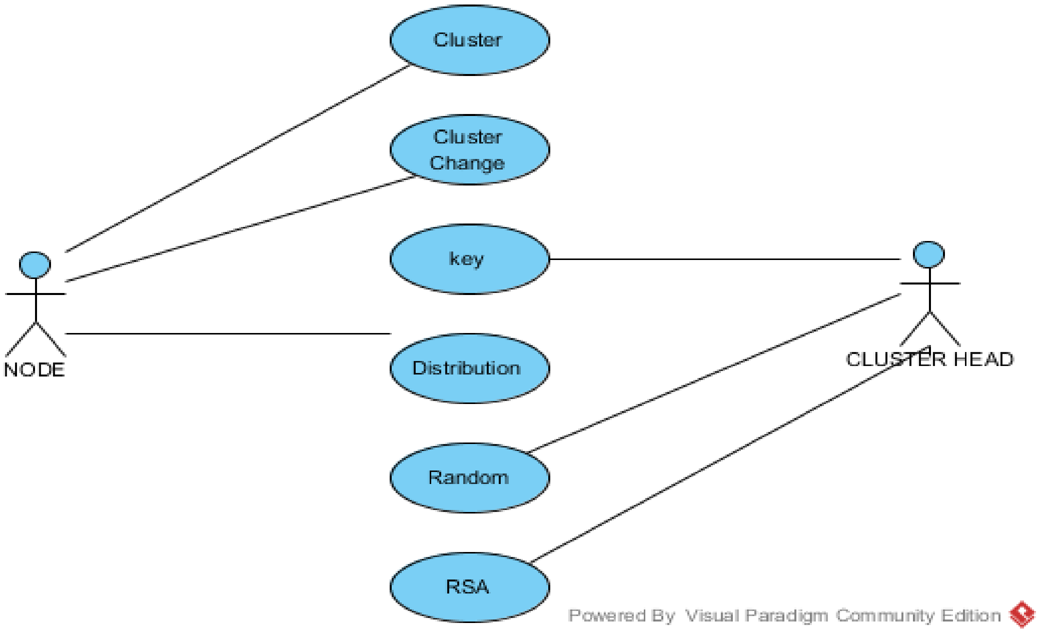
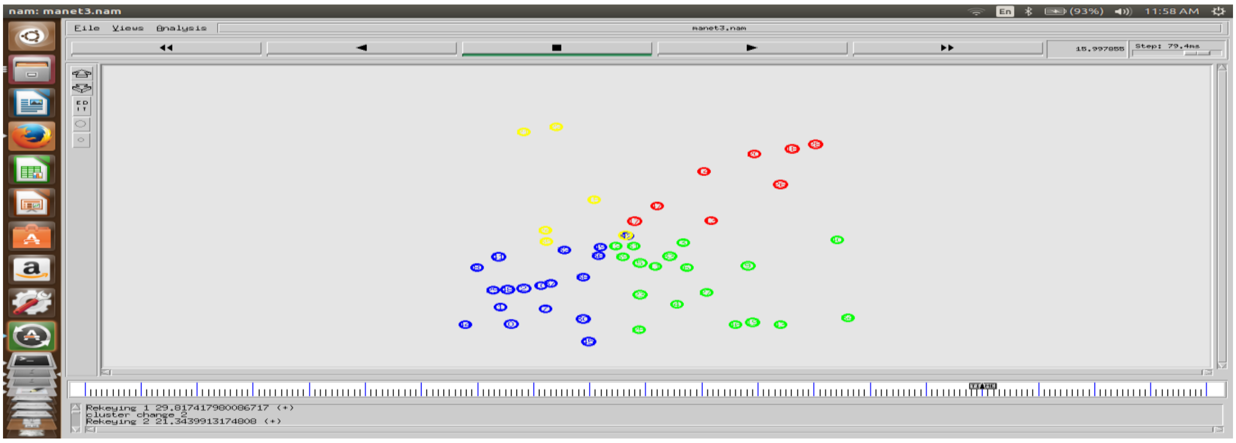


Figure3.2. Use-Case Diagram

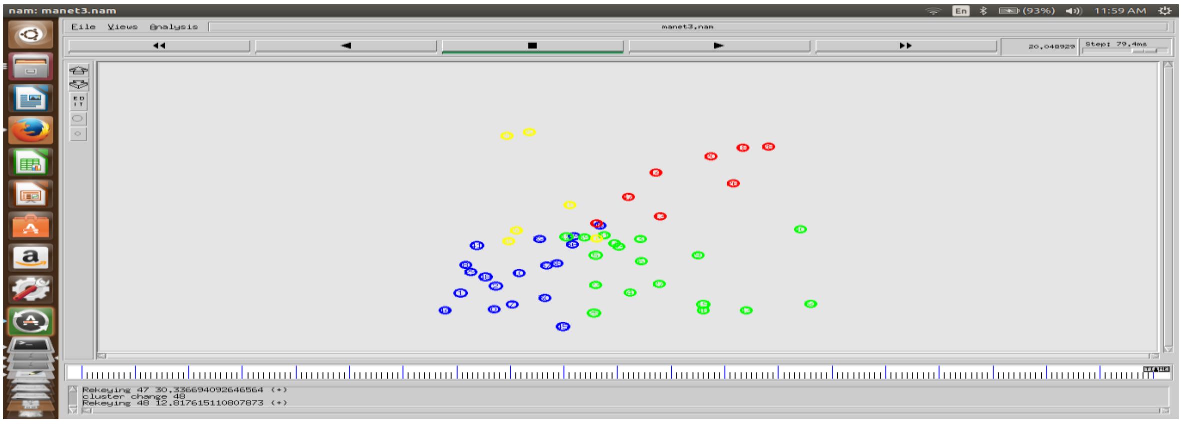
V. Experimental Results

Screenshots:



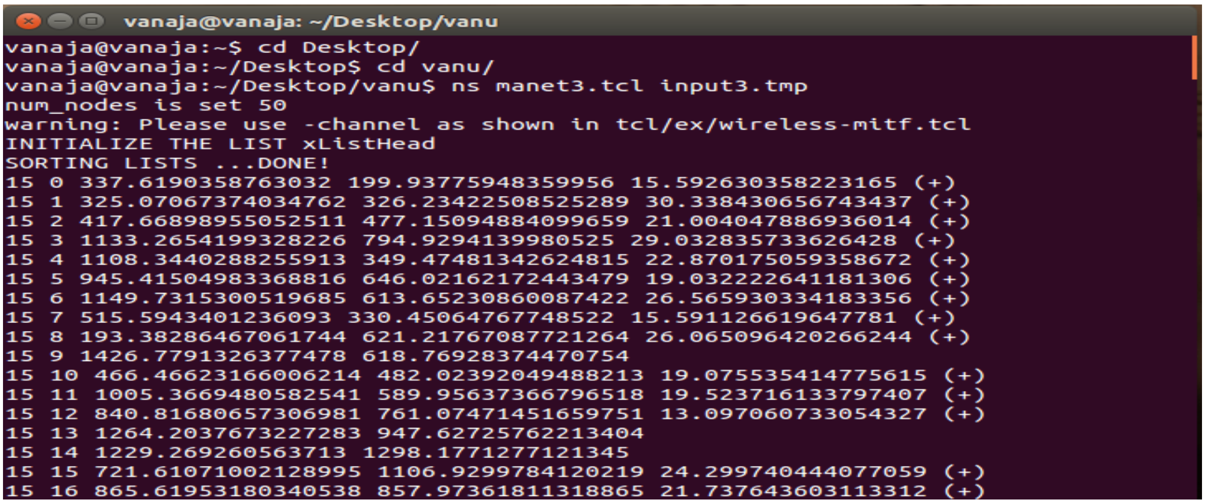
```
Rekeying 1 29.817417980086717 (+)
cluster change 2
Rekeying 2 21.3439913174808 (+)
```

Figure 5.1. Nodes Crossing cluster Boundaries



```
Rekeying 47 30.336694092646564 (+)
cluster change 48
Rekeying 48 12.817615110807873 (+)
```

Figure 5.2.completely displacement of nodes



```
vanaja@vanaja:~$ cd Desktop/
vanaja@vanaja:~/Desktop$ cd vanu/
vanaja@vanaja:~/Desktop/vanu$ ns manet3.tcl input3.tmp
num_nodes is set 50
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
SORTING LISTS ...DONE!
15 0 337.6190358763032 199.93775948359956 15.592630358223165 (+)
15 1 325.07067374034762 326.23422508525289 30.338430656743437 (+)
15 2 417.66898955052511 477.15094884099659 21.004047886936014 (+)
15 3 1133.2654199328226 794.9294139980525 29.032835733626428 (+)
15 4 1108.3440288255913 349.47481342624815 22.870175059358672 (+)
15 5 945.41504983368816 646.02162172443479 19.032222641181306 (+)
15 6 1149.7315300519685 613.65230860087422 26.565930334183356 (+)
15 7 515.5943401236093 330.45064767748522 15.591126619647781 (+)
15 8 193.38286467061744 621.21767087721264 26.065096420266244 (+)
15 9 1426.7791326377478 618.76928374470754
15 10 466.46623166006214 482.02392049488213 19.075535414775615 (+)
15 11 1005.3669480582541 589.95637366796518 19.523716133797407 (+)
15 12 840.81680657306981 761.07471451659751 13.097060733054327 (+)
15 13 1264.2037673227283 947.62725762213404
15 14 1229.269260563713 1298.1771277121345
15 15 721.61071002128995 1106.9299784120219 24.299740444077059 (+)
15 16 865.61953180340538 857.97361811318865 21.737643603113312 (+)
```

Figure 5.3. Keys

1) Graph Analysis

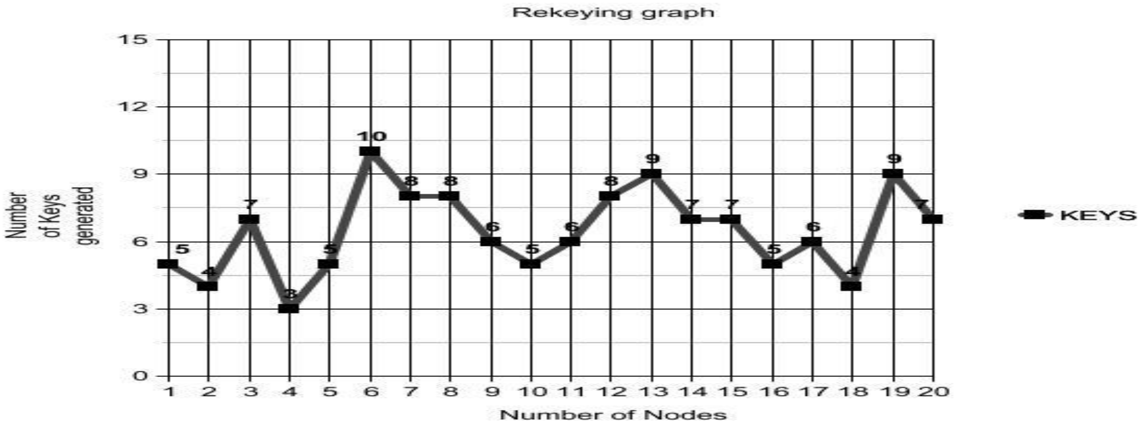


Figure 5.4 Key Generation Graph

VI. Conclusion

In this paper, we have proposed an Inter Cluster Communication and Rekeying (ICCR) technique for multicast security in MANETs. The technique facilitates inter cluster communication in a secure way by encrypting the generated keys using RSA.This thesis can further extended by applying various key management algorithms like GKMP, Logical Key Hierarchy and so on to calculate the effectiveness of those algorithms and to make a comparative study.

References

[1] VennilaRajamanickam, DuraisamyVeerappan .: 'Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks', IET Inf. Secur., 2014, Vol. 8, Iss. 4, pp. 234-239 doi: 10. 1049/iet-ifs.2013.2017

[2] Qin, F.: 'QoS topology control with energy efficiency for MANET',J. Converge.Inf. Technol., 2011, 6, (6), pp. 300–307

[3] Rajan, C., Shanthi, N.: 'Misbehaving attack mitigation technique formulticastsecurity in mobile ad hoc networks (MANET)', J. Theor.Appl. Inf. Technol., 2013, 48, pp. 1349–1357

[4] Sun, J.-Z.: 'Mobile Ad Hoc networking: an essential technology forpervasive computing'. IEEE Int. Conf. on Info-tech and Info-net, (ICII2001), 2001

[5] Wang, N.-C., Fang, S.-Z.: 'A hierarchical key management scheme forsecure group communications in mobile ad hoc networks', J. Syst.Softw., 2007, 80, pp. 1667–1677

[6] Loganathan, P., Purushothaman, T.: 'An energy efficient topology awarekey management scheme for multicasting in Ad-hoc networks',Int. J. Wisdom Based Comput., 2011, 1, (3), pp. 43–48

[7] Seetha, R., Saravanan, R.: 'Multicast security issues in mobile Ad hocnetworks', Int. J. Emerg. Trends Eng. Dev., 2013, 1, (3), pp. 189–194

[8] Francis, M., Sangeetha, M., Sabari, A.: 'A survey of key managementtechnique for secure and reliable data transmission in MANET',Int. J. Adv. Res. Comput. Sci. Softw. Eng., 2013, 3, (1), pp. 22–27

[9] Gunasekaran, S., Duraiswamy, K.: 'Energy efficient clusteringarchitecture for multicast security in mobile Ad hoc networks',Int. J. Adv. Eng. Res. Stud., 2012, 1, pp. 244–251

[10] Huang, D., Medhi, D.: 'A secure group key management scheme forhierarchical mobile ad hoc networks', Ad Hoc Netw., 2008, 1, pp. 560–577

[11] Singh, U.P., Rathore, R.S.: 'An efficient distributed group keymanagement using hierarchical approach with ECDH and symmetricalgorithm', J. Comput. Eng. Intel. Syst., 2012, 3, (7), pp. 32–41

[12] Renuka, A., Shet, K.C.: 'Hierarchical approach for key management inmobile Ad hoc networks', Int. J. Comput. Sci. Inf. Secur., 2009, 5, (1),pp. 87–95

[13] Zhu, S., Setia, S., Xu, S., Jajodia, S.: 'GKMPAN: an efficient grouprekeying scheme for secure multicast in Ad-hoc Networks'. IEEE FirstAnnu. Int. Conf. on Mobile and Ubiquitous Systems: Networking andServices, (MOBIQUITOUS), 2004

[14] Vennila, R., Duraisamy, V.: 'Multi-level group key managementtechnique for multicast security in MANET', J. Theor. Appl. Inf.Technol., 2013, 49, (2), pp. 472–480

Biography:

Mrs. K.Sowjanya Naidu. presently working as an assistant professor in computer science and engineering department, G. V. P. College of Engineering (A), Madhurawada, Visakhapatnam, India. She Received the Master of Technology degree in Andhra University,India. Received the bachelor of technology degree in Jawaharlal Nehru Technological University Kakinada,India. Research Interests Cyber Forensics , mobile ad-hoc networks , Data Mining, Information Security, Software Testing, Software Engineering, mobile communication and cloud computing. She Has 4+ Years Teaching Experience,

Mrs. Rani Sesha Bhargavi , presently working as an assistant professor in computer science and engineering department, G. V. P. College of Engineering (A), Madhurawada, Visakhapatnam, India. She Received the Master of Technology degree in G.V.P. College of Engineering (A), India. Received the bachelor of technology degree in GITAM University,India. Research Interests computer Networks, mobile ad-hoc networks , Data Mining, Information Security, Software Testing, Software Engineering, mobile communication and cloud computing. She Has 2+ Years Teaching Experience,

Mrs. V. Lokeshwari Vinya. presently working as an assistant professor in computer science and engineering department, G. V. P. College of Engineering (A), Madhurawada, Visakhapatnam, India. She Received the Master of Technology degree in GITAM University, India. Received the bachelor of technology degree in Jawaharlal Nehru Technological University Kakinada ,India. Research Interests Cognitive radio,mobile computing, Cyber Forensics , mobile ad-hoc networks , Data Mining, Information Security, Software Testing and cloud computing. She Has 4+ Years Teaching Experience.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

K.Sowjanya Naidu. "Each node acts as a base station and is responsible for dynamically discovering other nodes it can directly communicate with In MANET." International Journal of Engineering Science Invention(IJESI), vol. 6, no. 10, 2017, pp. 39–49.