ISSN:0975-9646

Multicast Security Using RSA for Inter Cluster Communication with Rekeying in MANET

G. Sankara Rao [1], E. Jagadeswara Rao [2], K. Suneeta [3], H. Vanajarani [4]
[1]*Asst.Professor, Dept. of CSE, GVP College of Engg for Women, kommadi, Visakhapatnam, AP.*
[2]*Asst. Professor, Dept of CSE, CMR College of Engg & Technology, Hyderabad, Telangana.*
[3,4]*Student -GVP College of engineering, kommadi, Visakhapatnam, AP.*

Abstract-In 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 a MANET, message delivery can speed up by means of group communication. In an adversarial ad hoc environment such as in military or public emergency network applications, it is necessary to provide secure multicast or group communication. For the secure group communication, there is a process of generating, distributing and updating keys to the network 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 (NS2).

Key Words- Ad Hoc, MANET, DSDV, DSR, AODV, AOMDV, QoS, NS2

1. INTRODUCTION

Since the communication in wireless technology is growing, folks predict to be proficient to employ the terminals of the network any place and any time. Samples of that type of terminals are unit Personal Digital Assistance (PDA), Automatic Data Acquisitions (ADA) and laptops. Users want to maneuver concerning whereas the network assets are using (i.e., Internet), and wireless technology provides them with this possibility. Wireless assets to the network providers the liberty of pressure group they need. The majority of the wireless networks nowadays needs associate in nursing underlying architecture of fixed position routers, and is so needed on offering communications. Characteristically, the nodes moving in such networks are in touch in a straight line with questionable access points (APs) that successive relays the traffic to the consequent nodes. These days, an additional sort of wireless technology is rising, specifically impromptu wireless network areas. These network areas include moving nodes and the infrastructure less networks those themselves provides, underlying design to commune in the wireless technology. Owing to this feature, no already offered routers area unit required.

The model of Open Systems Interconnection (ISO)

The Internet Standard Organization (OSI) model was urbanized by the alliance for standardization (ISO) so as to normalize the network protocols employed in numerous network layers. IEEE802.11 may be a folks of provision for wireless areas, native space areas of the networks (WLANs) like all IEEE802.11 principles, the 802.11works on the 2 lower levels of the OSI model. Even if wireless networks aren't restricted to any special hardware, nodes in such networks area unit seems to work in step with the IEEE802.11. Figure 1.1 shows the IEEE802.11 values mapped to the OSI reference model. As well, the figure depicts, however the accomplishment of a distinctive UNIX router corresponds to those models. In wireless networks, moving nodes usually employ frequency channels as their substantial standard. This represents to rock bottom layer within the OSI model. Since the nodes need not be physically associated, the network offers information assets at the side of user excellence. The IEEE802.11MAC layer corresponds to the information link layer within the OSI model. The most aim of the OSI link layer is to create error-free broadcast of information across a physical link. IEEE802.11 protocols' version of this theme consists of 2 sub layers: Logical Link management (LLC) and Medium Access management (MAC). The (possibly) most very important services that the LLC offers are error and flow management. The MAC layer directly interfaces with the physical layer, and provides services like address, framing, and media access management.

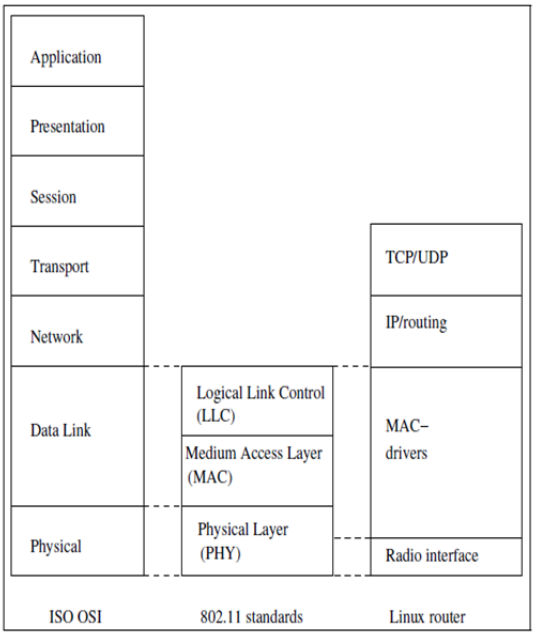


Fig.1.1. IEEE 802.11 standards mapped to the OSI reference model

Wireless Networks:

Many absolutely different wireless networks subsist, variables within the method the nodes interconnect. One will approximately classify them in 2 types:

- Infrastructure dependent
- Ad hoc wireless networks

Present cellular networks area unit divided because the infrastructure dependent networks. What is archetypal for these networks is they make use of, access points, or base stations. Additionally to proceed as a router in the network, associate in nursing entry purpose may also act sort of an overpass linking, for instance, the wireless network and a wire network. GSM, and its 3G equivalent 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. Therefore, the nodes have to be compelled to be a lot of intelligent in order that they'll perform as routers similarly as regular hosts. Federal routing. Associate at simplifying resource management with an Access Point implies less guilt than the spread 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 Microwaves (MW) is unit 2 different broadcasting technologies, of that IEEE802.11 supports the previous one additionally to radio. Wireless LANs use the magnetic attraction airwaves to speak. The air waves propagate during house (even in an exceedingly vacuum). Completely dissimilar frequencies have different qualities: the upper the magnetic attraction frequency, a lot of data will be transmitted per second. Nevertheless, lower frequencies area unit straightforward to get, will trek long distances, and might infiltrate buildings simply. Radio waves operate poorer frequencies than infrared waves, creating it a lot of appropriate for many wireless networks. Frequency hopping spread spectrum FHSS) and direct sequence unfolded spectrum DSSS) area unit the 2 radio transmission schemes supported in IEEE802.11. The concept in the rear FIHSS 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 unlike receivers not awake to the pattern, the broadcast is difficult to notice. DSSAS, on the other hand, does not hop from one frequency to a dissimilar, however distributes the signal over the complete wave band hurriedly.

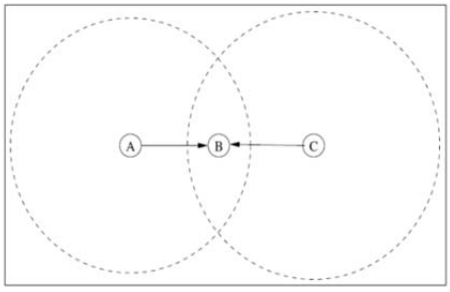


Fig1.2.The hidden terminal problem

Issues in wireless networks

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

Hidden terminals

As illustrated in Figure1.2, node A and node C area unit in varying from human activity with node B, however not with one another. Each could attempt to stay in touch with node B at the same time, and may not notice any interference on the wireless medium. Thus, the signals crash at node B, which will not be able to obtain the transmissions from either node. The standard resolution for this is known as Hidden terminal. The drawback is that the nodes coordinate transmissions themselves by asking and conceding permission to send and receive packets. This theme universally known as RTS/CTS (Request to send/Clear to send).The elementary plan is to capture the channel by notifying unlike nodes regarding Associate in nursing impending transmission. This will be often done by stimulating the receiving node to outputting a brief frame in order that seal nodes can notice that a transmission goes to require place. The lock nodes area unit then predictable to avoid transmission for the length of the approaching (large) information frame.

Exposed terminals

Consider a topology just like that of Figure1.2, however extra a node D solely accessible from node C. Furthermore, suppose node B communicates with node A, and node C needed to transmit packet to node D. Throughout the transmission between node B and node A, node C senses the channel as busy. Node C incorrectly concludes 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 seats. 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 swap topological data, flooding is that the solely thanks to get information to a particular destination.

Mobile Ad Hoc Wireless Networks:

In ad-hoc networks, as mentioned on top of, the nodes themselves area unit liable for steering and forwarding of packets. If the wireless node area unit inside varies of every different, no routing is critical. But, on the opposite hand, if the nodes have got rid of varing from one another, and so aren't able to communicate directly, the intermediate node 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 exists 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 are unit quite few problems that require being throughout on cent 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 move 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, since, for Associate in nursing example, reducing the transmission power at a node because a decrease in interference at neighboring nodes, and increase frequency utilize.

Routing in ad hoc wireless networks

As the nodes in a wireless ad hoc network can be connected in a dynamic and arbitrary manner, the nodes themselves must behave as routers and take part in finding and preservation of routes to other nodes in the network. The goal of routing algorithms to devise a scheme to transfer a packet from one node to another. One challenge is to define/choose which criteria to base the routing decisions on. Examples of such criteria include hop length, latency, and bandwidth and transmission power.

Resource Constraints:

Nodes in a wireless network typically have limited battery and processing power, and the resources must be managed optically by the routing protocol.

Error-prone channel state:

The characteristics of the links in a wireless in network typically vary, and this call for an interaction between the routing protocol and the MAAC protocol to, if necessary, find alternate routes.

Hidden and exposed terminal dilemma

This is described in below section. MANET routing protocols are typically subdivided into two main categories: proactive routing protocols, and reactive on-demand routing protocols.

Proactive protocols

In networks utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to each other node. To uphold the fresh routing information, topology information needs to be interred changed between the nodes on a regular basis, leading to pretty high slide on the network. One the other offer, routes\will always is available on request. Many proactive protocols stem from conventional link state routing, as well as the Optimized Link State Routing protocol (OLR).

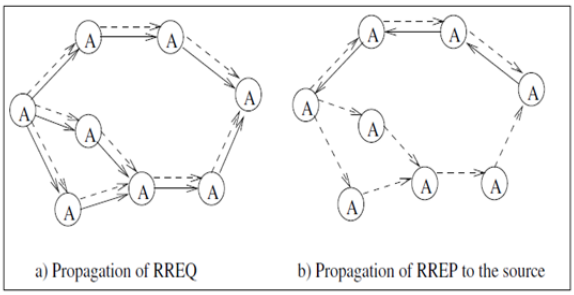


Fig.1.3.AODV Route Discovery

Hybrid protocols

These types of protocols mingle proactive and reactive protocols to try and exploit their strengths. One comes contained by reach of is to divide the network into zones, and use one protocol within the zone, and another between them.

1.2 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 be discussed in key management is distribution of keys in a secure manner. In general, no security techniques make use of traffic encryption keys for encryption and key encryption keys for decryption. When a multicast data (MD) are transmitted, the keys are used by mobile nodes for encrypting and decrypting the data to be transmitted.

1.3 Problem Statement

A substantial amount of energy consumed in the key management process.

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

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

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

When the threshold number of the shareholders compromised, then the security of the network is ruined.

1.4 Re-keying

In multicast proclamation, group key is essential when manifold nodes wish for to broadcast statistics firmly by via far run of the mill secret key. Two nodes preserve make a secret key by using Diffie-Hellman protocol without the support of any centralized trusted party. This rule preserves also be extended for n nodes. The progression of assembly keyboard has to take in hand the concern of security when the regard of the nodes changes. During link changes, the group key has to be rejuvenated to aid security. Grouping key stimulant can also be performed either every so often or after each involvement change. Thus, the processes of key stimulant assure forwards and backwards security.

1.5 Issues of rekeying

A downside of the Rekeying scheme is that it cuts down the level l of security and performance of the network. Since the rekeying machinery requires a number of communications to be transmitted for key making and delivery; it noticeably degrades the concert of the system. Furthermore, for real-time group statement, it requires advance bandwidth and before the keys are encrypted every node requires a significant amount of reminiscence to keep track of the dynamic rekey communication and the rate of amplifying in node join and leave requests.

In our first job we focused on civilizing sanctuary aspects along with the Quality of Service (QoS) for multicast security in MANET. In this practice the nodes with most existing bandwidth and residual energy are chosen as cluster heads (CHs) which acts as multicast group leaders (GL). Each CH compute the trust value of its members using the accomplishment or failure ratio of the data and the control packets. Based on the trust value, the CH decides whether a node is allowed to join the multicast group or not. When the multicast source wants to pass on the data packet, it utilizes the secret-key based packet forwarding technique. In our second work we focused on group key organization technique for multicast security in MANET. This technique works in a hierarchical model such that CHs are prioritized over the cluster members. The Secure Keys are generated using one way function chain (OFC). In calculation to secure key management, the issue of mobility is also handled.

On examining our preceding two facilities, we find that the purpose of a rekeying and cosseted inter cluster communication mechanism is essential to reduce the cost and transparency and to recover the effectiveness of the set of connections. Thus, in this paper, we propose to deploy an inter cluster announcement and re-keying (ICICR) skill for multicast security in MANET.

2. METHODOLOGY OF THE WORK CARRIED OUT

Existing system:

In this paper, we propose an ICcR technique for multicast security in MANET. As soon as the nodes deploy in the network, they form clusters and a CH is chosen. For facilitating, inter cluster communication, we assume centralized key manager (CKM) to produce and share out private key shares. The generated keys are scattered through a secure communication medium, each node is provided with a single private key share using t-polynomial degree function.

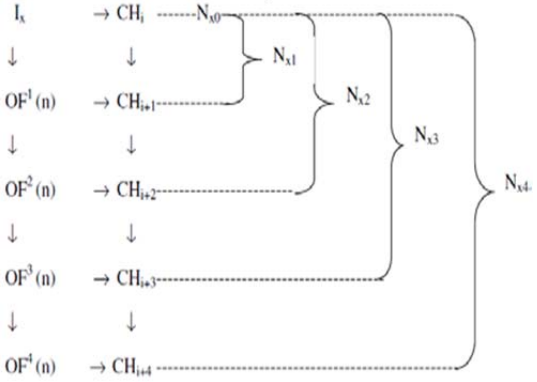
By fiddle proofing the data using private key share, secure inter cluster communication is accomplished. When a node joins the cluster group it forwards a CH_J_REQ (CH join Request to the CH. By in receipt of the request message, the CH invokes the rekeying mechanism. The CH selects pre-distributed keys and generates secret keys using OFC. The generated keys distributed to the nodes through shuffle algorithm.

2.1.1 Generating keys using one way function chain

Step1:Consider a function OF is recursively applied times to an argument n, that is OFj(n),then it can derive OFi(n) where j<I.

Step2: Let $K_{x0} = I_x$ be the x^{th} initial key element to originate a set of secret keys.

A secret key is denoted by, $K_{xy} = f(OF^j(I_x))$



2.2 Proposed Algorithm:

Algorithm -1:

The Key generation algorithm for generating keys when a node joins in clusters or leaving from the cluster.

Step1: Node joins into a cluster or leaves from a cluster else go to 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 key is (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 $P \neq q$

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, $d= e^{-1} \bmod Ø (n)$

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).

3. RESULTS:

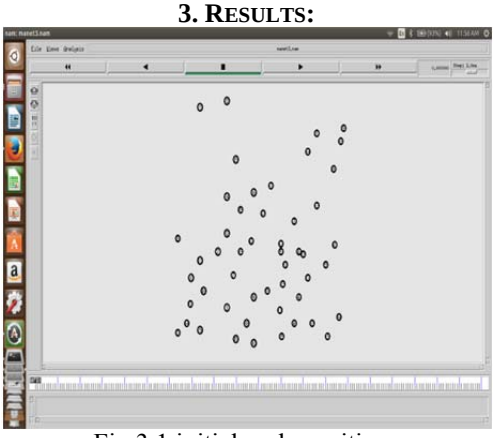


Fig.3.1 initial node positions

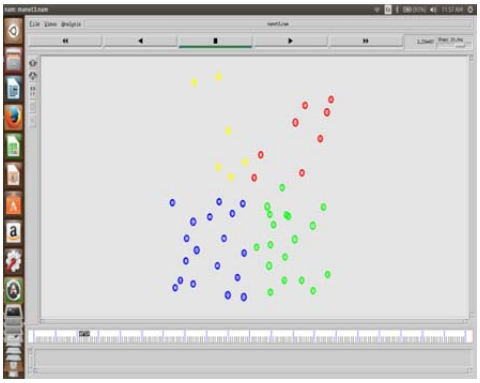


Fig.3.2 Nodes form into clusters

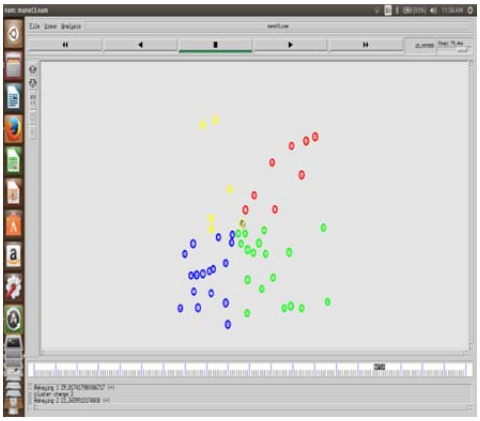


Fig.3.3 Nodes Crossing cluster Boundaries

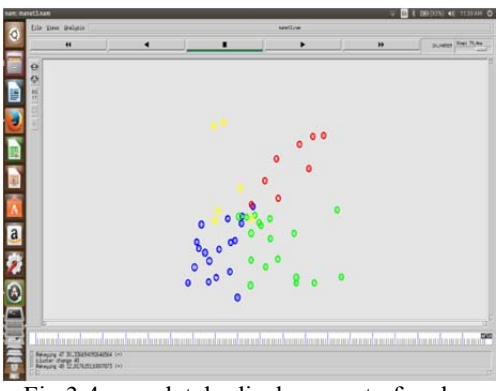


Fig.3.4 completely displacement of nodes

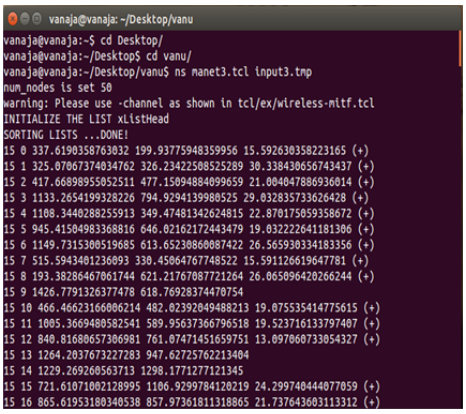


Fig.3.5 keys generated

3.1 Table) **Rekeying**

Simulation Time	Nodes	X-position	Y-position	Key
15	0	337.619	199.9378	18.92226064
15	1	325.0707	326.2342	26.4345868753 (+)
15	2	417.669	477.151	13.1016138904 (+)
15	3	1133.265	794.9294	16.8246564063 (+)
15	4	1108.344	349.4748	10.0002212864 (+)
15	5	945.4151	646.0216	13.7191611094 (+)
15	6	1149.732	613.6523	21.9407657259 (+)
15	7	515.5943	330.4507	22.4495549795 (+)
15	8	193.3829	621.2177	26.6705412104 (+)
15	9	1426.779	618.7693	
15	10	466.4662	482.0239	30.7861233995 (+)
15	11	1005.367	589.9564	27.3759757855 (+)
15	12	840.8168	761.0747	22.0250266697 (+)
15	13	1264.204	947.6273	
15	14	1229.269	1298.177	
15	15	721.6107	1106.93	10.623238277 (+)
15	16	865.6195	857.9736	26.7657212106 (+)
15	17	916.0072	953.5366	13.4763871448 (+)
15	18	1620.488	1452.272	
15	19	1445.025	209.5671	
15	20	1443.467	1423.897	
15	21	402.0173	1583.885	15.6387418786 (+)
15	22	558.1941	1618.083	28.3347540406 (+)
15	23	946.685	419.2293	29.2111607111 (+)
15	24	511.6267	887.5002	16.9780716444 (+)
15	25	941.6522	160.1202	26.4501278738(+)
15	26	1566.733	1202.866	
15	27	1238.736	436.1322	
15	28	1720.048	1488.711	
15	29	275.6157	423.9168	22.2991746093 (+)
15	30	691.1747	228.933	19.2276579622 (+)
15	31	920.4964	747.9358	14.2473712132 (+)
15	32	590	728	16.5679795828 (+)
15	33	1083.781	686.8676	22.0328489579 (+)
15	34	1850	250	
15	35	527.2092	808.2208	16.09243612 (+)
15	36	740	688	30.573868119 (+)
15	37	506.9314	483.1112	30.0014753509 (+)
15	38	683.9337	515.6739	27.7962231137 (+)
15	39	863.734	665.7081	29.1218716885 (+)
15	40	1800	800	
15	41	300	680	28.2974679462 (+)
15	42	870	830	11.543772009 (+)
15	43	1550	200	
15	44	150	200	21.1761550764 (+)
15	45	700	80	23.638369798 (+)
15	46	1350	200	
15	47	1000	1040	15.0811954267 (+)
15	48	340	450	23.65153616 (+)

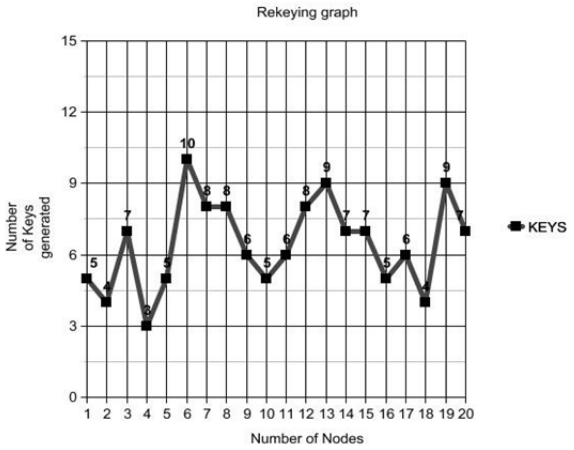


Fig.3.6 Key Generation Graph

4. CONCLUSION:

Conclusion & Future Enhancement

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 and decrypting the generated keys using RSA. The above results shows bit improvement in key generation.This paper can further extend by applying various key management algorithms like GKMP, Logical Key Hierarchy (LKH) and so on, to calculate the effectiveness of those algorithms and to make a comparative study.

REFERENCES:

[**1**] Vennila Rajamanickam, Duraisamy Veerappan 'Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks', IET Inf. Secure., 2014, Vol. 8, Is. 4, pp. 234-239 doi: 10. 1049/iet-ifs.2013.2017n

[**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 for multicast security 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 for pervasive computing'. IEEE Int. Conf. on Info-tech and Info-net, (ICII2001), 2001

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

[**6**] Seetha, R., Saravanan, and R.: 'Multicast security issues in mobile Ad hoc networks', Int. J. Emerge. Trends Eng. Dev., 2013, 1, (3), pp. 189–194

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

[**8**] Singh, U.P., Rathore, R.S.: 'An efficient Distributed group key management using Hierarchical approach with ECDH and Symmetric algorithm', J. Compute. Eng. Intel. Syst., 2012, 3, (7), pp. 32–41

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

[**10**] Xiong, W.A., Gong, Y.H.: 'Secure and Highly efficient three level key management Scheme for MANET', WSEAS Trans. Comput. 2011, 10, (1), pp. 6–15

[**11**] Bouassida, M.-S., Chrisment, I., Festor, O.: 'Group key management in Mantes', Int. J. Netw. Secure. 2008, 6, (1), pp. 67–7920 Chauhan, K.K., Sanger, A.K.S.: 'Securing mobile Ad hoc networks: Key management and routing', Int. J. Ad Hoc Netw. Syst., 2012, 2, (2), pp. 65–75

[**12**] Computer Networks, Prentice Hall Professional, 2003, Andrew S. Tanenbaum.

[**13**] Computer Networking by William Stallings.

[**14**] Introduction to Network simulator by Ekram Hossain.

[**15**] Network Security and Cryptography by Forouzan.

[**16**] An Overview of Mobile Ad Hoc Networks: Applications and Challenges by Piet.

[**17**] D.Suganya Devi "Secure Multicast Key Distribution for Mobile Adhoc Networks" (IJCSIS) Vol. 7, No. 2, 2010

[**18**] Network Simulator:http://www.isi.edu/nsnam/ns