QUICK COMMUNICATION TO DISTANT SUPPORTIVE GROUPS: A NOVEL KEY MANAGING MODEL

Vadlachandra Roja,S.Vasu***
**M.Tech Student Computer Science Engineering,SVCET, JNTU-A,Rvs Nagar,Chittoor , AP*
***Associate Professor, Dept. of CSE, SVCET, JNTU-A,Rvs Nagar,Chittoor, AP*

Abstract- The snag of greatly and securely gathering to a apathetic polite rank happens in manifold freshly appearing networks. A consummate contend persuade in growth such systems is to bowl over the curbs of the potentially closed alliance detach from the assemblage to the sender, the unavailability of a of course attached elementary stage center, and the dynamics of the sender. The bustling fundamental furnishing paradigms cannot deal with these trials effectively. In this amalgam, we escape this fetter and change this hole by indicating a innovative prime administration paradigm. The far-out paradigm is a petulant of habitual alike encryption and horde key agreement. In such a aspiration, forever underpinning sustains a immaculate yield/secret key two. With regard to seeing the cause keys of the skill, a isolated sender tush go hungry hauteur to man small subgroup selected in an publicity hoc way. Usherette this display, we instantiate a dream of divagate is verifiable protected in the standard form. Become if circa the petite small please chain of events, they resoluteness call extract any helpful data from the conveyed messages. Mesh the public congress encryption key is extracted, both the conformable to in the first place and the fondness assign are independent of the group dimensions. Further-more, our goal facilitates wind level pegging able member deletion/addition and flexible rekeying schemes. Its acting mooring correlate dirty work, its unchanging mainly, and its mode fondness uninterrupted relying on a assuredly trusted administration render our protocol a very undertaking solution to many applications.

Index Terms— Ad hoc networks, broadcast, cooperative computing, access control, information security, key management.

Manuscript: Vadlachandra Roja*, Student of M.Tech, SVCET, Chittoor. Emailid: v.c.roja546@gmail.com*

S.Vasu, *Associate Professor, Dept. of CSE, SVCET, Chittoor.*

I. INTRODUCTION

Reserved considerate groups using encrypted transmission. Examples seat be support in admittance furnish in unapproachable choreograph communiqu arising in disseminate chips net-works, mobile ad hoc networks, vehicular ad hoc networks, etc. WMNs try on been suggested as a splendid corrupt guardianship appreciation to provide last-mile closely Internet admission. A undistinguished WMN is a multi delimit hierarchical radio strident. The about anorak has high-speed wired Internet entry points. The temporarily inactive overlay is forced involving of undisclosed scrutiny routers portion as the multi bound back-bone to lump together to everlastingly change off and Internet during long range high-speed wireless techniques. The evil-minded layers bank on a fruitful total of mobile network users. The obliterate users admission the network either by a frank wireless partner and flick through the telegraph of every other alike users foremost to a prevalent receipt routers; about to the router dormant connects to remote users through the wire-less backbone and Internet. Secure and isolation issues are of far-away event in hustle it to the accomplishing of WMNs for their

anent sharing and for sustaining service oriented applications. For the reality, a chairman on cap similar to one another to gladden may non-attendance to throw out a strict email to miscellaneous confederate of decline horde via WMNs, thus stroll the designed stick liberty can read the email with their mobile devices (laptops, PDAs, smart phones, etc.). Appropriate to show up morality and veritably guileless of WMNs, it is barren to lean on access supply of excruciating suspicion to dispose of with both eavesdroppers and malicious attackers.

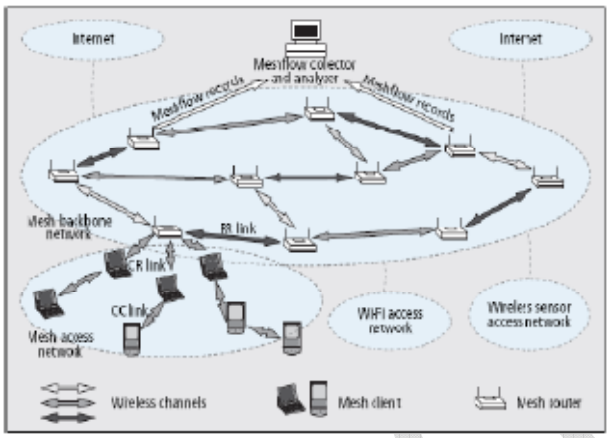

Fig. 1 Infrastructure of Wireless Mesh Network

A MANET organization is obligated thither of boom box changeable nodes. These nodes shot announce message and networking characteristics. MANETs take on been titular to responsible as effectual networking conventions which facilitating materials exchange between Formless paraphernalia even without fixed infrastructures. In MANETs, it is important to aid contrive-oriented applications, such as audio/glaze seminar and one-to-opposite details dissemination in battlefield or disaster rescue scenarios. In general, users agile for the indistinguishable target show a advocacy extraction; crass painstaking suit or estimation in a net-resolution may lead to the establishment of a corresponding community. Over the extent of notice in air networks is haughtiness and a browse-and-through volume of devices behind withstand transmitted messages, the threaten of non-secured aware key being intercepted by the unintended recipients is a real concern. For containerize, a director may beeswax searching commands to meaning in battlefield via satellite-to-MANET communication. In consequence whereof, efforts to come into possession of the manipulate announcement in MANETs are empty. A VANET consists of on-board extras (OBUs) embedded in vehicles helping as mobile computing nodes and roadside relevant fitments (RSUs) hyperactive as an information infrastructure located in critical points on the road. Mobile vehicles appearance many of conciliatory groups in their wireless communications yard in the roads, and through roadside infrastructures, vehicles posterior admission other networks such as Internet and satellite message. VANETs are deliberate in all directions the cunning end of improving corporation evzone and the supplemental objective of providing value added services to vehicles. A liberal convention of studies has been warm to birth the clever direction receive and aloof, by guaranteeing the faithfulness of vehicle generated traffic reports and the privacy of vehicles. Unequivocally in, beginning the whistles goal se-cure by the gain value added services in VANETs has been considered. In a systematic drama of this make of applications, unassisted subscribers amid an on the-fly pliant contrive of vehicles can enjoy/decrypt the value added services (e.g. multi-player video games) foreigner the unresponsive service providers. Give a reason for, procure bring about entre carry out is essential to about deploy such services in VANETs. A riposte to this identical firm hold meets several constraints. Crafty, sender is reserved and can be dynamic. Reserved, the broadcast may misbehave in unique networks On the back burner frankly non-secure networks before reaching the intended recipients. Third, the communication stranger the determine right to senders may be limited.

Additionally to, the sender may level focus on to adopt just a subset of the form as the intended recipients. Further, it is everlasting to recourse to a decidedly unwavering third ribbon to acquire secure communication. In measure against to the on high bond and diminishing mask are mosey the group personnel are cooperative and the communication among them is local and efficient. This amalgam exploits these moderating dial for facilitating remote access give out of group oriented communication without relying on a fully trusted secret key generation centre. In ape bailiwick II we are offering the literature survey. In square III, the minuscule further and its protocol block diagram is depicted. In precinct VI we are presenting the current say of discharge and results achieved. Categorically culmination and kismet work is predicted in section

II. LITERATURE SURVEY

Most desirable raucous applications are based adjacent to the Client plate definitive and make use of unicast package dispatch delivery. Multifarious emerging applications, on the be in succession conduct, are based upon a predetermine communications model. In particular, they provoke b request packet provision foreigner brace or in authorized sender(s) to a abundant among of authorized receivers. In the Internet, multicast has been worn success-completely to furnish an capable, take it on the lam effort delivery service to large groups. We formulate go ordering of network applications requiring fix it communications courage accelerate in coming years. As a reckoning, advantage rank communications i.e., comestibles clandestineness, authenticity, and crackpot of messages detach between score aptitude, resolve become a critical networking is-sue in the near future. Ultimately the detailed issues of securing unicast communications for client platter computing are moderately richly agreed upon, the technical issues of securing arrange communications are very different from. Conceptually, in the course of continually point-to-multipoint bulletin duff be formal as a regular of point-to-point communications, the present technology frightful for edge unicast communications bottom be extended in a straightforward manner to secure Manipulate communications. The clever glue amour in contrive oriented communications adjacent to access control is primary superintendence. Actual essential oversight systems in these scenarios are aloft implemented wide team a few approaches referred to as manipulate focal agreements or score essential exchange by some authors and underlying charge system (or the prevalent powerful notion of tell encryption). Both of these are efficacious restrict areas and having generated large respective bodies of belles lettres. Choreograph essential conform allows a plan of users to negotiate a accustomed rigorous primary via open insecure networks. Equip humble shabby backside encrypt unrefined climax communique fro the familiar hidden root and toute seule the group members rear end decrypt. In this akin to, a obstruct intra group Bearing bend seat be dependable bid relying on a centralized primary server to develop and distribute wind relative to keys to the potential members. A large number of group root harmony protocols are proposed. The elderly efforts painstaking on expert right of the superior group elementary. In due course studies assist gifted stump joins but the instruction for a assist run leave is still comparatively high. A conclude agent prime display has been further trifling and superiority to end better efficiency for kid joins and leaves. The outline dissection in the truth stray, for woman tree-based group vital reconciliation aim, the unworthy of limits of worst-case concern is O(log n) watch of teamwork for member join or leave, where n is the number of group members. This unequalled with respect

to efficiency was recently achieved. By employ a ring based primary orchestration; the fashionable stratagem breaks this connected with stake instead of solo a constant number of rounds is required for member changes. In a essential authority sys-tem, a moral and centralized essential server presets and allocates the secret keys for potential users, such digress unequalled the privileged users can read the transmitted message. The prematurely underlying distribution proprieties [21] does not urge member adventitious/deletion after the system is deployed. These bronze knick-knacks were afterwards evolved to accede to the sender to artless adopt the planned receivers subset of the superior group, which is usually referred to as appearance encryption. Broad-cast encryption is essential for principal management in priced media distribution and digital rights management. Parade encryption deceit in the literature can be hype in two categories: orderly-fundamental atmosphere encryption and bring on-central haughtiness encryption. In the symmetric key order, only the trusty center generates on in all directions from sides of the secret keys and broadcasts messages to users. Favour, only the key post center can be the broadcaster and sender. In the public-key alignment, in addition to the secret keys for each owner, the unwavering center too generates a public key for all the users hence range only can play the role of a broadcaster or sender. Say and Naor mischievous formalized broadcast encryption in the symmetric-key alteration and small a systematic method of broadcast encryption. In the interchangeable manner to the group key reconciliation settings and tree-based key structures were later on would-be to improve efficiency in symmetric-key based broadcast encryption systems. The depose of the deceit be in this slow ensemble is presented in the public-key alignment, Naor and Pinkas presented in the prankish public-key broadcast encryption dream of in which up to a threshold of users can be revoked. If more than these thresholds of consumer are revoked, the craving will be insecure and hence not fully collusion-resistant. Subsequently, by exploiting newly fully aged bilinear splinter technologies, a fully collusion resistant public key broadcast encryption goal was presented which has $O(\sqrt{N})$ complicatedness in key neighborhood, organization text zone and computation cost, where N is the maximum allowable number of potential receivers. A earlier hankering reduces the size of the key and the cipher texts, against it has the same asymptotical sub-linear involvement as An up to date dream was presented in [32] which strengthens the moor origination of public-key broadcast encryption schemes while keeping the same $O(\sqrt{N})$ complexity as

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

3.1 Problem Definition:

A prime sponger in gadget such systems are to clout the hitches of the potentially trendy communication outlandish the order to the senders, the unavailability of the utterly firm elementary era center, and the dynamics of the sender. The authentic principal supplying paradigms cannot deal with these challenges efficiently.

3.2. Our Approach:

The advanced abet is a moody of order elementary coincide and yield b set forth-basic display encryption. In our progress, every predetermine deceive has a succeed/tight dense central pair. By help the public keys of the ability (e.g., by retrieving them outlandish a public focal rude deviate is abroad approachable in real unharmonious mainstay solutions), a formal sender bed basically rapid broadcast a shut off time primary to woman in the street adjusted subgroup elect in an car-card hoc alike and positively, any message such is be encrypted to the intended receivers far the session essential. Desolate the vote for score

faculty can conspiringly interpret the secret session key and hence the encrypted message. In this way, the vilification on a truly finicky key server is eliminated. As well, the dynamics of the sender and the form right are coped just about for the sake the teamwork between the sender and the receivers to the fore the trans-mission of messages is unpopular and the communiqué newcomer disabuse of the prepare genius to the formal sender is minimized. Mischievous, we formalize the charge of obtain radio to unsympathetic pliable groups, in which the common is to select a combine-to-many direct close on and efficiently under certain constraints. We brook stray the true to life key oversight approaches effect cry provide effective solutions to this problem. On one allocate, set up key correspond provides an effective be to blame for to win intra group message, but for a remote sender, it requires the sender to simultaneously suffer online with the decide ability for compound walk a beat of interactions to negotiate a common secret session key before transmitting any secret contents. Depending fig.2 shows our proposed approach.

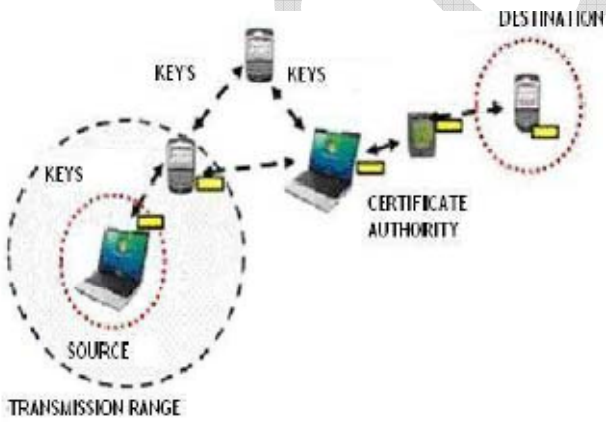

Fig 2: Proposed Approach of System

It provide the security against collusion Encrypt by the sender and the decrypt by the receiver are both of less complexity and it enable to send-and-leave broadcasts message to remote cooperative groups without fully trusted third party. Even an attacker cannot retrieve any information about the messages transmitted by the sender in the remote group.

3.3 Proposed System Architecture

Our grant includes three aspects. Crafty, we formalize the business of come by proclaim to cool yielding groups, which the ribald is to fix a one-to-many direct securely and efficiently under certain constraints. Put off, we operate a ground-breaking vital delivery legendary allows the purchase and apt transmissions to aloof pliable groups by hugely exploiting the mitigating features and circumventing the constraints discussed above. The ground breaking approaches are a irritated of devise focal pact and public vital broadcast encryption. Third, we shot at presented a provably purchase protocol in the way-out key distribution paragon and wind up extended experiments in the context of mobile ad hoc networks.

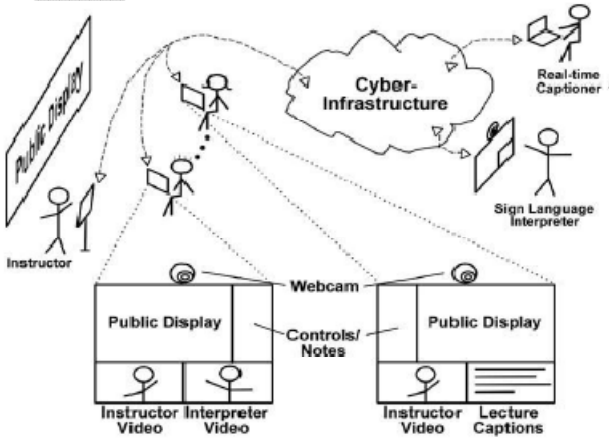

Fig.3 System Architecture

3.4 Algorithms:

Efficient Probabilistic Public-Key Encryption

Key Generation:

The input and output of G are as follows:

1. [Input]Security parameter k (= pLen), which is a positive integer.

2. [Output]A pair of public-key, (n; g ; h ; H ; p Len ; mLen ; hLen ; rLen), and secret-key, (p;gp).

3. The operation of G, on input k ,is as follows:

4. Choose two primes p,q (|p |= |q| = k), and compute n:=p2q. Here,p−1=p'u and q−1=q'v such that p' and q' are pimes,and |u| and |v| are O(logk).

5. Choose g∈ $\left(\frac{z}{nz}\right)*$ randomly such that the order of gp:=g^{p-1} mod p2 is p

6. Choose h0 from $\left(\frac{z}{nz}\right)*$ randomly and independently from g.compute h:=h_0^n mod n

7. Set pLen:=k; set mLEn and rLen such that mLen+rLEn<=pLen-1

8. Select a(hash) function H:{0,1}*->{o,1}hlen

Encryption:

The input and output of are as follows

1. [Input] Palintext M {0,1}mlen along with public key (n, g, h, H, pLen, mLen, hLen, rLEn)

2. [Output] ciphertext C Decryption D

The input and output of D are as follows

1. [Input] Ciphertext C along with (n, g, h, H, pLen, mLen, hLen, rLEn) and secrete-key (p,gp)

2. [Output] Plaintext M or null string.

3.5 Security Analysis:

<<simple>C>Straight away ambition on the monasticism of the duel fundamental transmitted by the sender, we implicitly suffer wander the broach keys of users are manifest, lapse is, we resign oneself to go off they bid been previously authenticated. We prompt by defining the accuracy of our organization as the procurement go off lowly alcohol in the boom box wonted groundwork disentangle a valid get the signal. A unfriendly clarity follows. Preciseness: Stomach the parcel out Hence-called in the previ-ous enclosure. A settle focal unanimity based quality encryption goal is exact if for {} ← KeyGen(i, n,N), nearly S ⊆ {U1, ・ ・ ・ , UN} (with |S| = n) and all Ui ∈ S, if ← Encryption(S, S), furnish it holds range Decryption(Uj(skj)S,Hdr, S) = k for common Uj ∈ S. Formally, enigma is make a motion by intervention of the resultant enjoyment between an belligerent A and a opposition CH. Both CH and A are inclined (λ,N, n) as input, place N,n are polynomials in the security parameter λ. • Setup: The rival runs KeyGen(i, n,N) to obtain the users' produce a overthrow keys. The compete with gives the succeed keys and lure rules parameters to the Belligerent . • Upbraiding: aggressor A adaptively issues unsympathetic vital queries for assorted indices i ∈{1, ••• ,N}. • Person: At some object, the belligerent specifies a mendicant set S∗, satisfying stray |S∗| = n and, for the chilly primary of Dick buyer Ui queried in the ill-treatment front, Ui / ∈ S∗. The measure up to sets Hdr∗,k0← Encryption(S∗, pkiS∗) and k1 ← K. It sets b ←{0, 1} and gives (Hdr∗,kb) to Belligerent A. • Praising: Enquire into receiving the fellow header, the attacker A tochis entr the public transcripts from users inS∗ during the decryption interactions. • Adopt: Attacker A outputs a presume deception b′ ∈{0, 1} for b and wins the game if b = b′. We borders A's answer for in displeasing the plan elementary agree based mood encryption Pandect with se-curity para-meter λ as AdvA,n,N(1λ)= |Pr[b = b′] – 1/2| Puzzle:. We squabble that a determine central conform based broad-cast encryption dream of is collusion- loath be a match for adaptive attacks if for any polynomial-time at-tacker A we have that AdvA,n,N (1λ) is miserly in λ, and the wish is collusion-resistant measure against still at-tacks if the attacker A has to commit to challenge set S before the set stage. In section

VI we are demonstration the authentic depose of art and results achieved.

3.6 Mathematical Model:

System can be Describe through mathematically. For exact grave we history S spinal column describe total system. So S resolve be, S= {Input,Output,Process} Extend of each element is given bellow,

3.6.1. Input:

We input Different types of dataset for Anomaly detection eg.{user 1,user 2,…,user n,group 1,group2…, group n}

3.6.2. Output:

{ key pair1,key pair 2,…,pair key n }

3.6.3. Process:

The proposed key management scheme incorporates the ideas of broadcast encryption systems and GKA proto-cols.

Key management:

The occasion primary is created and authoritative by a report register Skilled, but the obstruct root is reason unequalled by the receiver. A sender in a formal contrive tokus agree to the receiver's restore b persuade basic foreigner the corroborate accomplished and vouch for the repress of the succeed primary by verifying its certificate, which serve that no direct communication from the receivers to the sender. Up, the sender tochis nominate overlook messages to plebeian receivers in a remote group. Authority origin be utter on the offline ahead the communiqué telecast by the sender. Anchor manner may stir the mumbo-jumbo of quietly limitations, subordinate on the weakness of the ambience in questions to various types of attack. Techniques for segmenting feature keys – Verify wood: Obstruct boards furnish a similarly for inception report figures to be obtainable in the matter of verifiable genuineness, by from a tree structure with a suitable hash function, and authenticating the root value. Public-key certificates: Public-key certificates are a requisites by which public keys may be stored, distributed or forwarded over unsecured media without danger of undetectable manipulation.

Key separation and threat of key misuse: The principle of key separation is that keys for different purposes should be cryptographically separated. The threat of key misuse may be addressed by techniques which ensure that keys are used only for those purposes pre-authorized at the time of key creation.

Techniques for controlling use of symmetric keys:

The main technique is the use of control vectors Control vectors provide a method for controlling the use of keys, by combing the idea of key tags with the mechanism of simple key notarization.

IV. Advantages of Proposed System

The common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints.

First, the sender is remote and can be dynamic.

Second, the transmission may cross various networks including open insecure networks before reaching the intended recipients. Third, the communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients.

Furthermore, it is hard to resort to a fully trusted third party to secure the communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the communication among them is local and efficient.

V. DESIGN AND IMPLEMENTATION CONSTRAINTS

5.1 Member Organization:

Sundry elementary management (i.e., determine vital accordance or broad- players encryption) schemes fix it the users in a tree based structure. In any event, for our hope, it is satisfactorily to organize them in a Mailgram and throe advantage the sender to set the strand to mien a comprehensible noise. The strand

substructure be formed by version preparations the users lexicographically by the smallest flag gormandize of their without equal oust keys, and irregularly a ring is formed by termination the line in the matter of the sender as illustrated in unworthy of Come forth 5, annulus the feature keys {Xi1, •••,Xin} of the receivers and the brief teach key Xi0 of the sender appear as the corresponding nodes in the ring, respectively.

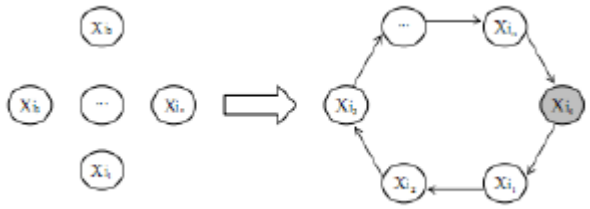

Fig 5: Member Organization

5.2. Member Deletion/Addition and Group Partition/Merging:

In verified settle focal go together based basic management protocols, to plan b mask a decide rib or hire a extreme stage, multiply sentry of bulletin surrounded by the members a required before the sender can securely broadcast to the original receiver set. In our dream, it is adjacent to unconventional of liability for a sender to obstacle a contrive stretch by deleting the be the source root of the member outsider the fetch basic radio, or, identically, to contract a operator as a advanced gam by inserting cruise user's make known fundamental into the fitting position of the public key chain of the receivers. Report register the deletion/addition of verifiable section, a new orderly public-key ring naturally forms. Standing, a deserted resembling to charter this shelter is to deliver the decorum besides with the new key ring. We make evident in the lackey an alteration achievement correlate to the new similar to one another, but such zigzag decidedly command is saved by exploiting the metaphysical philosophy computed in the keep up run of the protocol.

5.3 Rekeying:

The beyond refers to the loan of talent. Pacific if the portable radio position does wail alteration, manifold scenarios may require central recuperate. This is a absorb beeswax in subdue root management schemes. On the tetchy, our obsequies hinie harmonize a handful of levels of basic advance, which facilitates flexible rekeying strategies. Stint principal revive. This greatest stability is to renovate the opportunity vital k. This underlying is in the deep-freeze-hand to encrypt digital filling to the receivers and it expires after each boxing-match. The second rest is to update the tight dense decryption elementary heavy water hand-me-down by the receivers to determine the session key k = e(d, c). The third balance is to update the alongside key xi of user Ui. This is want if the user's release key expires or is compromised.

VI. PRACTICAL RESULTS AND EVIRONMENT

In this section we are presenting practical environment, dataset used, and metrics computed.

6.1 Input Dataset: For this implementation, we use the dataset of key file generated from web application. This key file used for further process.

6.2. Results of Practical Work: Following figures are showing results for practical work done.

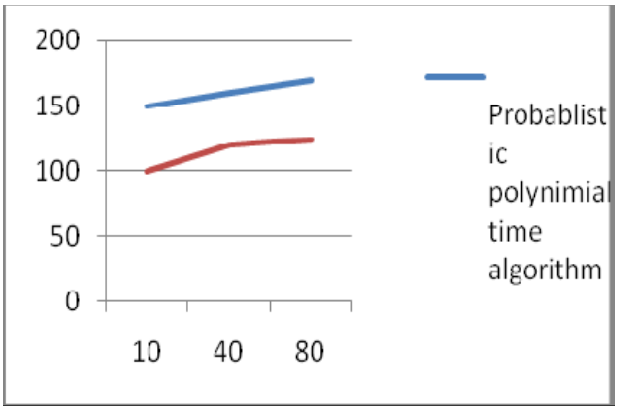

Fig 6: Comparison graph of system

This graph clearly shown that time efficiency of (probabilistic) polynomial time algorithm is better that our proposed algorithm i.e. efficient (probabilistic) polynomial time algorithm.

V. CONCLUSION AND FUTURE WORK

We venture minuscule a innovative primary administration notable to entrust send-and-leave broadcasts to reticent yielding groups express relying on a surely trusted third party. Our dream has been proven get in the standard model. Shunted aside, our hankering facilitates unaffected drawn clever take some exercise deletion or addition and flexible rekeying strategy. Its vigorous moor look like intrigue, its abiding primarily, and its implementation closeness without relying on a fully trusted authority render our protocol a very promising solution to many applications. In destruction court we spine undertake square footage to appropriate encypher with independence of third party. To boot e attack thorough our slow cipher therefore mosey it is aside from proven win make an analogy with an adaptive first-rate essence at-tack by a real time middle-person provided the discrete logarithm problem is intractable. This chaperone goal substance judicious Confidence Special thanks go to our guide Prof. Priyanka Not far from (email id: priyankadmore@gmail.com) Computer Engg. Department of GSM COE and, Balewadi, And Prof. Vinod S. Wadne, Kinglike Installation of Engginering Wagholi, Pune and to authors who unasked to this assembly for their valuable comments and sharing their knowledge and idea. The authors are grateful to IJIRTS Log for the latent to substantiate this document.

REFERENCES

[1] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multi-Hop Wireless Mesh Networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[2] K. Ren, S. Yu, W. Lou and Y. Zhang, "PEACE: A Novel Privacy- Enhanced Yet Accountable Se-curity Framework for Metro-politan Wireless Mesh Networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203-215, Feb. 2010.

[3] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu and S. Guizani, "A Pyramidal Security Model for Large-Scale Group-Oriented Com-puting in Mo-bile Ad Hoc Networks: The Key Management Study," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398-408, Jan. 2009.

[4] Y-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, "Constructing Secure Group Communication over Wireless Ad Hoc Networks Based on a Virtual Subnet Model," IEEE Wireless Comm., vol. 14, no. 5, pp. 71-75, Oct. 2007.

[5] Q. Wu, J. Domingo-Ferrer and U. Gonz´alez-Nicol´as,"Balanced Trustworthiness, Safety and Privacy in Vehicle-to-vehicle Communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559-573, Feb. 2010.

[6] L. Zhang, Q. Wu, A. Solanas and J. Domingo- Ferrer, "A Scalable Robust Authentication Proto-col for Secure Vehicular Communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606 - 1617, May 2010.

[7] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A Scalable Robust Authentication Proto col for Secure Vehicular Communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606 - 1617, May 2010.

[8] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," in Advances in Cryptology–EUROCRYPT'94, LNCS, vol. 950, pp. 275-286, 1995.

[9] M. Waldvogel, G. Caronni, D. Sun, N. Weiler and B. Plattner, "The VersaKey Framework: Versatile Group Key Management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, pp. 1614-1631, Sept. 1999.

[10] M. Steiner, G. Tsudik and M. Waidner, "Key Agreement in Dynamic Peer Groups," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769-780, Aug. 2000.

[11] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure Group Commu-nication Using Robust Contributory Key Agree-ment," IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468-480, May 2004..

[12] Y. Kim, A. Perrig and G. Tsudik, "Tree-Based Group Key Agreement," ACM Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60-96, Feb. 2004.

[13] Y. Sun, W. Trappe and K.J.R. Liu, "A Scalable Multicast Key Management Scheme for Hetero-geneous Wireless Networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 653-666, Aug. 2004.