ISSN:2321-1156
International Journal of Innovative Research in Technology & Science(IJIRTS)

A Key Framework For Fast And Secure Transmission To Issolated Co-operative Group

Sujata Asabe , ME Student of Computer Engg. Department , GSM COE College of Engg.,Balewadi, Pune.
Balasaheb Jadhav, Student of M.E (CSE) Imperial College of Engineering and Research, Wagholi pune.

Abstract : The difficulty of effectively and securely broadcasting to a remote cooperative group happens in many freshly appearing networks. A foremost dispute in developing such systems is to overwhelm the obstacles of the potentially restricted connection from the assembly to the sender, the unavailability of a completely trusted key generation center, and the dynamics of the sender. The living key administration paradigms cannot deal with these trials effectively. In this paper, we circumvent these obstacles and close this gap by suggesting a innovative key administration paradigm. The new paradigm is a hybrid of customary broadcast encryption and assembly key agreement. In such a scheme, each constituent sustains a single public/secret key two. Upon seeing the public keys of the members, a isolated sender can securely broadcast to any proposed subgroup selected in an publicity hoc way. Following this form, we instantiate a scheme that is verified protected in the standard form. Even if all the no proposed constituents collude, they will not extract any helpful data from the conveyed messages. After the public assembly encryption key is extracted, both the computation overhead and the connection cost are independent of the group dimensions. Furthermore, our scheme facilitates easy yet efficient member deletion/addition and flexible rekeying schemes. Its powerful security against collusion, its unchanging overhead, and its implementation friendliness without relying on a fully 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.

1. INTRODUCTION

Remote cooperative groups using encrypted transmission. Examples can be found in access control in remote group communication arising in wireless mesh networks, mobile *ad hoc* networks, vehicular *ad hoc* networks, etc. WMNs have been suggested as a promising low cost approach to provide last-mile high-speed Internet access. A typical WMN is a multi hop hierarchical wireless network. The top layer has high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as the multi-hop backbone to connect to each other and Internet via long-range high-speed wireless techniques.

The bottom layers include a large number of mobile network users. The end users access the network either by a direct wireless link and through the chain of other peer users leading to a nearby mesh routers; then the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing it to the success of WMNs for their wide deployment and for supporting service oriented applications. For instance, a manager on his way to holiday may want to send a confidential email to some staff of her company via WMNs, so that the intended staff members can read the email with their mobile devices (laptops, PDAs, smart phones, etc.). Due to distributed nature and intrinsically open of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers.

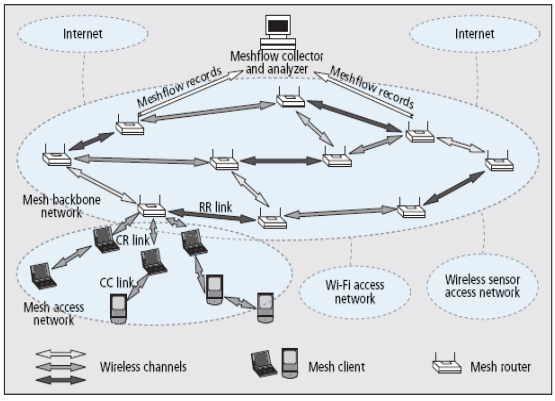

Fig. 1 Infrastructure of Wireless Mesh Network

A MANET system is made up of wireless mobile nodes.These nodes have wireless communication and networking characteristics. MANETs have been pro-

posed to serve as an effective networking system which facilitating data exchange between mobile devices even without fixed infrastructures. In MANETs, it is important to support group-oriented applications, such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. In general, users working for the same goal form a cooperation domain; any particular application or interest in a network may lead to the establishment of a corresponding community. Since communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of non-secured sensitive information being intercepted by the unintended recipients is a real concern. For instance, a commander may issue secret commands to soldiers in battlefield via satellite-to-MANET communication. Consequently, efforts to secure the group communication in MANETs are essential.

A VANET consists of on-board units (OBUs) embedded in vehicles serving as mobile computing nodes and road-side units (RSUs) working as an information infrastructure lo-cated in critical points on the road. Mobile vehicles form many of cooperative groups in their wireless communications range in the roads, and through roadside infrastruc-tures, vehicles can access other networks such as Internet and satellite communication. VANETs are designed with the primary goal of improving traffic safety and the secondary goal of providing value-added services to vehicles. A substantial body of studies has been devoted to making the primary goal secure and private, by guaranteeing the trustworthiness of vehicle-generated traffic reports and the privacy of vehicles. Very recently, making the secondary goal secure by the securing value-added services in VANETs has been considered. In a particular scenario of this type of applications, only subscribers among an on the-fly cooperative group of vehicles can enjoy/decrypt the value-added services (e.g. multi-player video games) from the remote service providers. Hence, secure group access control is essential to extensively deploy such services in VANETs.

A solution to this same problem must meet several constraints. First, sender is remote and can be dynamic. Second, the transmission may cross in various networks including open non-secure networks before reaching the intended re-cipients. Third, the communication from the group members to senders may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients. Further, it is hard to resort to a fully trusted third party to get secure communication. In contrast to the above constraints and mitigating features are that the group members are co-operative and the communication among them is local and efficient. This paper exploits these mitigating features for facilitating remote access control of group-oriented communication without relying on a fully trusted secret key generation centre.

In next section II we are presenting the literature survey. In section III, the proposed approach and its system block diagram is depicted. In section VI we are presenting the cur-rent state of implementation and results achieved. Finally conclusion and future work is predicted in section .

2. LITERATURE SURVEY

MOST network applications are based upon the Client–server paradigm and make use of unicast Packet delivery. Many emerging applications, on the other hand, are based upon a Group communications model. In particular, they require packet delivery from one or more authorized sender(s) to a large number of authorized receivers. In the Internet, multicast has been used successfully to provide an efficient, best effort delivery service to large groups. We envision that deployment of network applications requiring group communications will accelerate in coming years. As a result, securing group communications i.e., providing confidentiality, authenticity, and integrity of messages delivered between group members, will become a critical net-working issue in the near future. While the technical issues of securing unicast communications for client–server computing are fairly well understood, the technical issues of se-curing group communications are not. Conceptually, since every point-to-multipoint communication can be represented as a set of point-to-point communications, the current technology base for securing unicast communications can be extended in a straightforward manner to secure group communications.

The major security concern in group-oriented communications with access control is key management. Existing key management systems in these scenarios are mainly implemented with two approaches referred to as group key agreements or group key exchange by some authors and key distribution system (or the more powerful notion of broadcast encryption). Both of these are active research areas and having generated large respective bodies of literature.

Group key agreement allows a group of users to negotiate a common secret key via open insecure networks. Then any member can encrypt any confidential message with the shared secret key and only the group members can decrypt. In this way, a confidential intra-group broadcast channel can be established without relying on a centralized key server to generate and distribute secret keys to the potential members. A large number of group

key agreement protocols are pro-posed.

The earlier efforts focused on efficient establishment of the initial group key. Later studies enable efficient member joins but the cost for a member leave is still comparatively high. A tree key structure has been further proposed and improved to achieve better efficiency for member joins and leaves. The theoretical analysis in proves that, for any tree-based group key agreement scheme, the lower bound of worst-case cost is O(log n) rounds of interaction for member join or leave, where n is the number of group members. This optimal round efficiency was recently achieved. By using a ring-based key structure, the up-to-date proposal breaks this round barrier because only a constant number of rounds is required for member changes. In a key distribution system, a trusted and centralized key server presets and allocates the secret keys for potential users, such that only the privileged users can read the transmitted message. The early key distribution protocol [21] does not support member addition/deletion after the system is deployed. These notions were subsequently evolved to allow the sender to freely choose the intended receivers subset of the initial group, which is usually referred to as broadcast encryption. Broad-cast encryption is essential for key management in priced media distribution and digital rights management. Broadcast encryption schemes in the literature can be classified in two categories: symmetric-key broadcast encryption and public-key broadcast encryption. In the symmetric key setting, only the trusted center generates all the secret keys and broadcasts messages to users. Therefore, only the key generation center can be the broadcaster and sender. In the public-key setting, in addition to the secret keys for each user, the trusted center also generates a public key for all the users so that anyone can play the role of a broadcaster or sender.

Fiat and Naor first formalized broadcast encryption in the symmetric-key setting and proposed a systematic method of broadcast encryption. Similarly to the group key agreement settings and tree-based key structures were subsequently proposed to improve efficiency in symmetric-key based broadcast encryption systems. The state of the art along this research line is presented in the public-key setting, Naor and Pinkas presented in the first public-key broadcast encryption scheme in which up to a threshold of users can be revoked. If more than these thresholds of user are revoked, the scheme will be insecure and hence not fully collusion-resistant. Subsequently, by exploiting newly developed bilinear paring technologies, a fully collusion-resistant public-key broadcast encryption scheme was presented which has $O(\sqrt{N})$ complexity in key size, cipher text size and computation cost, where N is the maximum allowable number of potential receivers. A recent scheme reduces the size of the key and the cipher texts, although it has the same asymptotical sub-linear complexity as An up to date scheme was presented in [32] which strengthens the security concept of public-key broadcast encryption schemes while keeping the same $O(\sqrt{N})$ complexity as .

3. PROPOSED APPROACH FRAMEWORK AND DESIGN

3.1 Problem Definition

A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the senders, the unavailability of the fully trusted key generation center, and the dynamics of the sender. The existing key management paradigms cannot deal with these challenges efficiently.

3.2 OUR APPROACH

The new approach is a hybrid of group key agreement and public-key broadcast encryption. In our approach, each group member has a public/secret key pair. By knowing the public keys of the members (e.g., by retrieving them from a public key infrastructure that is widely available in existing network security solutions), a remote sender can securely broadcast a secret session key to any intended subgroup chosen in an ad hoc way and simultaneously, any message can be encrypted to the intended receivers with the session key. Only the selected group members can jointly decrypt the secret session key and hence the encrypted message . In this way, the dependence on a fully trusted key server is eliminated. Also, the dynamics of the sender and the group members are coped with because the interaction between the sender and the receivers before the transmission of messages is avoided and the communication from the group members to the remote sender is minimized.

First, we formalize the problem of secure transmission to remote cooperative groups, in which the core is to establish a one-to-many channel securely and efficiently under certain constraints. We observe that the existing key management approaches do not provide effective solutions to this problem. On one hand, group key agreement provides an efficient solution to secure intragroup communication, but for a remote sender, it requires the sender to simultaneously stay online with the group members for multiple rounds of interactions to negotiate a common secret session key before trans-

mitting any secret contents. Following fig.2 shows our proposed approach.

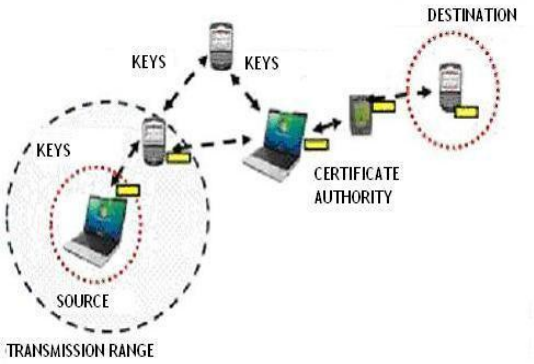

Fig 2: Proposed Approach of System

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 contribution includes three aspects. First, we formalize the problem of secure transmission to remote cooperative groups, which the core is to establish a one-to-many channel securely and efficiently under certain constraints.

Second, we propose a new key management paradigm allows the secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints discussed above. The new approaches are a hybrid of group key agreement and public key broadcast encryption. Third, we have presented a provably secure protocol in the new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks.

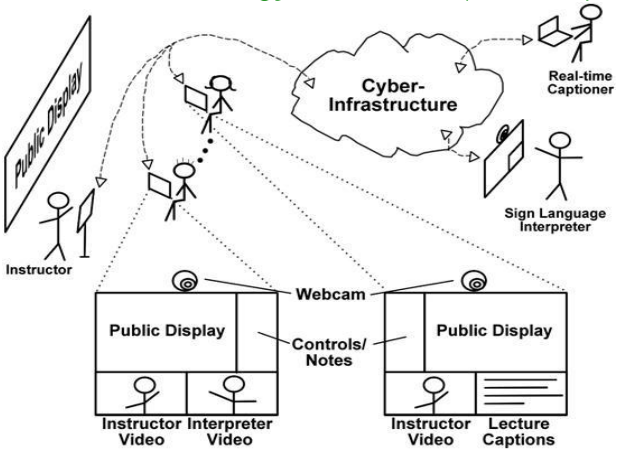

Fig.3 System Architecture

In the proposed protocol after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexities, even in case of member changes or system updates for rekeying.

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:

When focusing on the confidentiality of the session key transmitted by the sender, we implicitly assume that the public keys of users are authentic, that is, we assume that they have been previously authenticated.

We start by defining the correctness of our system as the property that any user in the receiver set can decrypt a valid header. A formal definition follows.

Correctness: Assume the model described in the previous section. A group key agreement based broadcast encryption scheme is correct if for

{<pki, ski>} ← KeyGen(i, n,N),

all S ⊆ {U1, ・ ・ ・ , UN} (with |S| = n) and

all Ui ∈ S, if <Hdr, k> ← Encryption(S, <pki>S),

then it holds that Decryption(Uj(skj)S,Hdr, <pki>S) = k for any Uj ∈ S.

Formally, secrecy is defined by means of the following game between an attacker A and a challenger CH. Both CH and A are given (λ,N, n) as input, where N,n are polynomials in the security parameter λ.

• **Setup**: The challenger runs KeyGen(i, n,N) to obtain the users' public keys. The challenger gives the public keys and public system parameters to the attacker.

• **Corruption:** Attacker A adaptively issues private key queries for some indices i ∈{1, ••• ,N}.

• **Challenge**: At some point, the attacker specifies a challenge set S∗, satisfying that |S∗| = n and, for the private key of any user Ui queried in the corruption step, Ui / ∈ S∗. The challenger sets Hdr∗,k0← Encryption(S∗, pkiS∗) and k1 ← K. It sets b ←{0, 1} and gives (Hdr∗,kb) to attacker A.

• **Observation**: After receiving the challenge header, the attacker A can access the public transcripts from users inS∗ during the decryption interactions.

• **Guess**: Attacker A outputs a guess bit b′ ∈{0, 1} for b and wins the game if b = b′.

We define A's advantage in attacking the group key agreement based broadcast encryption system with security para-meter λ as

AdvA,n,N(1λ)= |Pr[b = b′] – 1/2|

Secrecy:. We say that a group key agreement based broad-cast encryption scheme is collusion- resistant against adaptive attacks if for any polynomial-time attacker A we have that AdvA,n,N (1λ) is negligible in λ, and the scheme is collusion-resistant against static attacks if the attacker A has tocommit to challenge set S before the set stage. In section VI we are presenting the current state of implementation and results achieved.

3.6 Mathematical Model

System can be Describe through mathematically. For mathematical model we consider S will describe total system. So S will be,

S= {Input,Output,Process}

Detail 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 protocols.

Key management

The public key is created and certified by a certificate Authority, but the secret key is hold only by the receiver. A sender in a remote group can receive the receiver's public key from the certificate authority and validate the authentication of the public key by verifying its certificate, which provide that no direct communication from the receivers to the sender. Then, the sender can send secret messages to any receivers in a remote group. Authority can be done on the offline before the message transmission by the sender . Security policy may affect the stringency of cryptographic requirements, depending on the susceptibility of the environment in questions to various types of attack.

Techniques for distributing public keys –

Authentication trees: Authentication trees provide a way for making public data to be available with verifiable authenticity, by using a tree structure with a suitable hash function, and authenticating the root value.

Public-key certificates: Public-key certificates are a device 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.

Optimizations

The pairing is providing some optimizations. These may involve precomputation, and in some storage availability may introduce a problem. We can consider these optimizations in some other ways. If both left-hand and right-hand arguments are, pairing itself can be pre calculated and stored. If the left-hand parameter, its multiples that rise in its multiplication by the variable can be precalculated and it must store in coordinates. We consider no advantage can be taken on right-hand parameter, but only for a Type-1 pairing, symmetry can be move it to the left-hand side and precalculate as before. The protocol on a Type-3 pairing it may be useful for reversing the roles of the left-hand and right-hand parameters in the protocol. Note that if storage is not problem and the left-hand parameter the size of din E (Fpd) is not matter, and so it is no need to use a pairing-friendly curve . It will be advantage to use the pairing which provides the loop reduction, and limited storage need for precomputation by the degree of loop reduction can be achieve. scheme with constant-size cipher texts is a modified version of BGW by the same authors (dubbed BGW2 from now on), which has cipher texts that are double the size of our scheme (i.e., four group elements vs. ourtwo). BGW2 is proved selective CCA secure under BDHE, plus the assumption that a signature scheme used in the construction is strongly unforgivable, which is an assumption of comparable strength as UOWHF.

Broadcast Encryption

The basic tree scheme requires only log2 n keys to be stored in each receiver. Therefore it is reasonable to consider schemes with slightly more keys: for populations of several millions, we can afford to keep twice or four times as many keys in a receiver. In order to generate the extra key sets, we start with a "level-degree" profile, which specifies how many keys each user should hold at each level [9]. For a level with set size, a degree of d implies that each user should belong to extra sets(d-1), in addition to the one basic tree set it belongs to at this level. Thus we need to be able to generate nd/k sets of size , such that each user belongs to exactly d of them. We Achieve this by randomly permuting the N users times (D-1), and for each random permutation we add the users in positions (i-1)k+1,…….,ik as a set ,for i=1,…….,n/k.

Key Establishment Algorithm

Input: Target set K,
establishment key allocation $\mathcal{S} = \{S_1, \ldots, S_m\}$.

0. $R \leftarrow \emptyset$; $\mathcal{C} \leftarrow \emptyset$
1. **Repeat**
2. $\mathcal{A} \leftarrow \{S_i : \frac{|S_i \setminus R|}{|(K \cap S_i) \setminus R|} \leq f\}$.
3. $A \leftarrow S_i \in \mathcal{A}$ which maximizes $|(K \cap S_i) \setminus R|$.
4. $R \leftarrow R \cup A$; $\mathcal{C} \leftarrow \mathcal{C} \cup \{A\}$.
5. **until** the candidate collection $\mathcal{A}$ is empty.
6. **return** $R, \mathcal{C}$.

To calculate the redundant establishment key allocation over a universe u of size n .

The required number of keys a receiver needs to store. As we said before, this is typically a small fixed value which we can reasonably model by [illegible] inverse lower bound, on the number of transmissions. Asymptotically we can obtain the following bound.

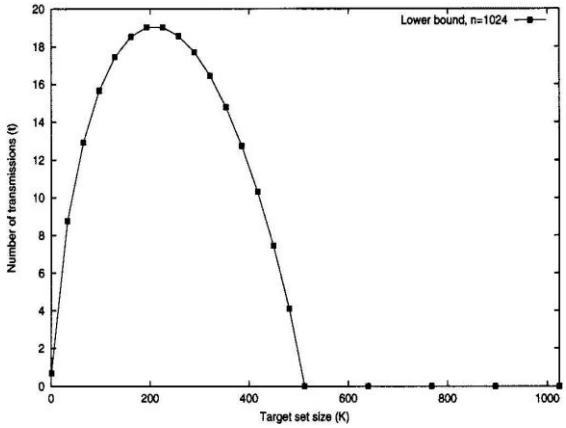

Fig.4. Number of transmission (t) as the function represent to the target set size (k).

4 .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.

5. Design and Implementation Constraints

5.1. Member Organization:

Many key management (i.e., group key agreement or broad- cast encryption) schemes organize the users in a tree-based structure. However, for our scheme, it is preferable to organize them in a chain and then use the sender to close the chain to form a logical ring. The chain can be formed by ordering the users lexicographically by the least important bits of their unique public keys, and then a ring is formed by closing the chain with the sender as illustrated in below Figure 5, where the public keys {Xi1 , ••• ,Xin} of the receivers and the temporary public key Xi0 of the sender appear as the corresponding nodes in the ring, respectively.

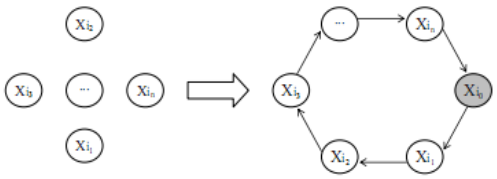

Fig 5 : Member Organization

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

In existing group key agreement based key management protocols, to exclude a group member or enroll a new member, multiple rounds of communication among the members a required before the sender can securely broadcast to the new receiver set. In our scheme, it is almost free of cost for a sender to exclude a group member by deleting the public key of the member from the public key chain, or, similarly, to enroll a user as a new member by inserting that user's public key into the proper position of the public key chain of the receivers. After the deletion/addition of certain member, a new logical public-key ring naturally forms. Hence, a trivial way to enable this change is to run the protocol independently with the new key ring. We illustrate in the following an alternative implementation equivalent to the trivial way, but such that much cost is saved by exploiting the values computed in the last run of the protocol.

5.3 Rekeying:

The above refers to the change of members. Even if the receiver group does not change, various scenarios may require key update. This is a complex issue in most key management schemes. On the contrary, our protocol can provide three levels of key update, which facilitates flexible rekeying strategies. Session key update. This first level is to update the session key k. This key is used to encrypt digital contents to the receivers and it expires after each session. The second level is to update the secret decryption key d used by the receivers to compute the session key k = e(d, c). The third level is to update the secret key xi of user Ui. This is needed if the user's public key expires or is compromised.

6. 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.

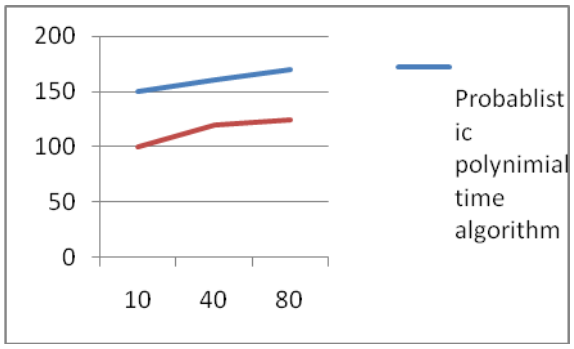

Fig 6: Comparison graph of system

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.

CONCLUSION AND FUTURE WORK

We have proposed a new key management paradigm to enable send-and-leave broadcasts to remote cooperative groups without relying on a fully trusted third party. Our scheme has been proven secure in the standard model. Further, our scheme facilitates simple yet efficient member deletion or addition and
flexible rekeying strategy. Its strong security against collusion, its constant overhead, and its im-plementation friendliness without relying on a fully trusted authority render our protocol a very promising solution to many applications. In future scope we will have scope to developed system with independence of third party. Also e have extended our authentication system so that it is also proven secure against an adaptive chosen text attack by a real time middle-person provided the discrete logarithm problem is intractable. This resulting scheme remains practical

ACKNOWLEDGMENT

Special thanks go to our guide Prof. **Priyanka More** (email id: priyankadmore@gmail.com) Computer Engg. Depart-ment of GSM COE and, Balewadi ,
And Prof. **Vinod S. Wadne**, Imperial College of Engginering Wagholi, Pune and to authors who contributed to this paper for their valuable comments and sharing their knowledge and idea. The authors are thankful to IJIRTS Journal for the support to develop 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 Security 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 Mobile 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 Trustwor-thiness, 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 Protocol 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 Communication Using Robust Contributory Key Agreement," 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 Heterogeneous Wireless Networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 653-666, Aug. 2004.

[14] W. Trappe, Y. Wang and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous Networks," IEEE/ACM Trans. Netw., vol 13, no 1, pp.134-146, Feb. 2005.

[15] P. P. C. Lee, J. C. S. Lui and D. K. Y. Yau, "Distributed Collaborative Key Agreement and Authentication Protocols for Dynamic Peer Groups," IEEE/ACM Trans. Netw., vol. 14, no. 2, pp. 263-276, April 2006.

[16] Y. Mao, Y. Sun, M. Wu and K. J. R. Liu, "JET: Dynamic Join-Exit- Tree Amortization and Scheduling for Contributory Key Management," IEEE/ACM Trans. Netw., vol 14, no 5, pp.1128-1140, Oct. 2006.

[17] W. Yu, Y. Sun and K. J. R. Liu, "Optimizing the Rekeying Cost for Contributory Group Key Agreement Schemes," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 3, pp. 228 - 242, July-Sep. 2007.

[18] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007-2025, May 2008..

[19] Ingemarsson, D.T. Tang and C.K. Wong, "A Conference on Key Distribution System," IEEE Trans. Inf. Theory, vol. 28, no. 5, pp. 714-720, Sep. 1982

[20] M. Abdalla, Y. Shavitt and A. Wool, "Key Management for Restricted Multicast Using Broadcast Encryption," IEEE/ACM Trans. Netw., vol. 8, no. 4, pp. 443-454, Aug. 2000.

[21] B. M. Macq and J.-J. Quisquater, "Cryptology for Digital TV Broad-casting," Proc. IEEE, vol. 83, no. 6, pp. 944-957, Jun. 1995.

[22] C. K. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Network., vol. 8, no. 1, pp. 16–30, Feb. 2000.

[23] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short cipher texts)," Adv. Crypto., vol. 5479, EUROCRYPT' 09, LNCS, pp. 171–188, 2009.

[24] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," Proc. IEEE, vol. 83, no. 6, pp. 944– 957, Jun. 1995.

[25] C. K. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16–30, Feb. 2000.

[26] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, no. 6, pp. 944– 957, Jun. 1995.

[27] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short cipher

texts)," *Adv. Crypto.*, vol. 5479, EUROCRYPT' 09, LNCS, pp. 171–188, 2009.

[28] A. Fiat and M. Naor, "Broadcast encryption," *Adv. Cryptol.*, vol. 773, CRYPTO'93, LNCS, pp. 480–491, 1993.

Biographies

Sujata H. Asabe received the BE degree in Computer Science from Solapur University, Solapur City, Maharashtra, India in 2010 and the currently pursuing the ME degree in Computer Engineering from the Ganeba Sopanrao Moze College of Engineering, Balewadi,Pune from Pune university, Pune City, Maharashtra,India.

Balasaheb B.Jadhav received the BE degree in Computer Science from Solapur University, Solapur City, Maharashtra, India in 2010 and the currently pursuing the ME degree in Computer Engineering from the J.S.P.M's Imperial College of Engineering and Research, Wagholi, Pune from Pune university,Pune city, and Currently working as Assistant Professor in JSPM Wagholi, Pune Maharashtra,India.