Secure and fast transmission to isolated cooperative assemblies framework

Sujata Asabe[1] , Prof. Priyanka More[2]

[1] Research PG Scholar, Department of CSE, GSMIT,Balewadi-411045,Pune,India.
sujata.asabe@87gmail.com
[2] Professor, Department of IT Engineering, G.S. Moze College of Engineering, Balewadi -411045, Pune, India.
morepriyankad@gmail.com

I. ABSTRACT

Recently in several new rising networks the matter of expeditiously and firmly broadcasting to a foreign cooperative cluster. the prevailing key management paradigms cannot influence these challenges effectively. to beat the obstacles of the doubtless restricted communication from the cluster to the sender ar major challenge in production such systems, the inconvenience of a totally trusty key generation center and therefore the dynamics of the sender. during this paper, every member maintains one public/secret key try. For proposing a unique key management paradigm, we tend to circumvent these obstacles and shut this gap. Remote sender use public keys of the members for broadcasting to any meant subgroup chosen in an advert hoc means. By resolution this theme we tend to prove secure model. conjointly economical member deletion/addition and versatile rekeying methods extended by this paper. any we tend to extend out cryptography algorithmic rule to enhance security level to manager all communication in secure thanks to attain higher application.

Index Terms - *Ad hoc networks, broadcast, cooperative computing, access control, information security, group key management, session key.*

II. INTRODUCTION

In several recently rising networks, there\'s got to broadcast to remote cooperative teams mistreatment encrypted transmission. Wireless mesh networks are recently recommended as a promising low price approach to supply last-mile high-speed net access. the highest layer consists of high-speed wired all net entry points and also the second layer is created of stationary mesh routers serving as a multi-hop backbone to attach to every different and net via long-range with high speed wireless techniques. Here bottom layer includes an outsized variety of mobile network users. Security and privacy problems of utmost concern in pushing the success of WMNs for his or her wide readying and for supporting service orienting applications. the tip users access the network either by an on the spot wireless link or through a sequence of different peer users resulting in a close-by mesh router. Attributable to the as such open and distributed nature of the WMNs and it's essential to enforce access management of sensitive data to deal with each overhang droppers and malicious attackers.

MANETs are projected to function an efficient networking system facilitating information exchange between mobile devices even while not mounted infrastructures. Wherever just in case of MANETs, it's vital to support group-oriented applications, Likewise audio or video conference and one-to-many information dissemination in piece of ground or disaster rescue eventualities. Since communication in wireless networks is broadcast and an exact quantity of those devices will receive the transmitted messages and also the risk of unsecured sensitive data being intercepted by inadvertent recipients could be a real concern. A VANET consists of on-board units (OBUs) embedded in vehicles serving as mobile computing nodes and road-side units (RSUs) operating because the data infrastructure situated within the vital points on the road. Mobile vehicles kind several cooperative teams in their wireless communication target the roads, and thru margin infrastructures, vehicles will access different networks like net and satellite communication. VANETs are designed with the first goal of rising traffic safety and also the secondary goal of providing added services to vehicles.

The major security concern in group-oriented communications with access management is vital management. Existing key management systems in

these eventualities are in the main enforced with 2 approaches mentioned as cluster key agreement (or cluster key exchange by some authors) and key distribution systems (or the additional powerful notion of broadcast encryption). Each is active analysis areas having generated giant various bodies of literature. Cluster key agreement permits a gaggle of users to barter a typical secret key via open insecure networks. Then any member will code any confidential message with the shared secret key and solely the cluster members will decipher. during this manner, a confidential intra cluster broadcast channel will be established while not counting on a centralized key server to get and distribute secret keys to the potential members. A tree key structure has been additional planned and improved to realize higher potency for member joins and leaves [11]. The theoretical analysis in [20] proves that, for any tree-based cluster key agreement theme, the boundary of the worst-case value is O(log n) rounds of interaction for member be part of or leave, wherever n is that the range of cluster members. This optimum spherical potency was recently achieved in [18]. By employing a ring-based key structure, the up-to-date proposal in [19] breaks this spherical barrier as a result of solely a relentless range of rounds are needed for member changes.

III. LITERATURE REVIEW

Previously in literature survey we are going to discuss all recent methods over the Double Guard: Detecting Intrusions in Multitier Web Applications.

Text mining is data mining applied to textual data. Text is "unstructured, amorphous, and difficult to deal with" but also "the most common vehicle for formal exchange of information." Therefore, the "motivation for trying to extract information from it is compelling even if success is only partial . Whereas data mining belongs in the corporate world because that's where most databases are, text mining promises to move machine learning technology out of the companies and into the home" as an increasingly necessary Internet adjunct (Witten & Frank, 2000) – i.e., as "web data mining" (Hearst, 1997). Laender, Ribeiro-Neto, da Silva, and Teixeira (2001) provide a current review of web data extraction tools.

In Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multi-Hop Wireless Mesh Networks," [1] As Multi-hop wireless mesh networks as WMNs are finding ever-growing acceptance as a viable and effective solution to ubiquitous broadband Internet access. In this paper they have addresses the security of WMNs, which is a key impediment to use wide-scale deployment of the WMNs, thus far receives a little attention. Here we first thoroughly identify the unique security requirements of the WMNs for a first time in the literature. Then we propose ARSA and attack-resilient security architecture for WMNs. In the contrast to conventional cellular as like solution, ARSA designed the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. With ARSA in case, all users are no longer bound to most specific network operator, as he or she ought to do the current cellular networks. Instead, he or she acquires a universal pass from a third-party broker whereby to realize seamless roaming across WMN domains administrated by different operators.

In B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu , S. Guizani, "[2] The Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks:- Key Management Study" In case of mobile ad-hoc networks (MANETs), many applications require group-oriented computing among a large number of nodes in an adversarial environment. To deploy the large-scale cooperative applications and secure multicast service that must be provided to efficiently and safely exchange data among all the nodes. The existing literature has extensively studied security protection for a single multicast group, in which all the nodes are assumed to have the same security level. However, such assumption cannot valid in practice because, for many applications, different number of users can play different roles and thus naturally be classified into multiple security levels.

In Y-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, "Constructing Secure Group Communication over Wireless Ad Hoc Networks Based on the Virtual Subnet (MANET) Models," [3] previously, Number of peoples have begun using mobile devices as like PDAs and notebooks or iPod. Now days it has been profoundly affected by such devices. A mobile ad-hoc network is an effective networking system facilitating an exchange data between the mobile devices, without support of wireless access points and base stations. A MANET is not restricted to the uncast or multicast communication, but can also provide "many-to-many" device transmission, which can be treated as the node in group communication. Until nowadays, however, the way in which such groups are formed had not drawn more attention. Because of communication in wireless networks is broadcast and a certain amount of devices can receive the transmitted messages, and risk

of unsecured sensitive information being intercepted by unintended recipients is the real concern.

In Q. Wu, J. Domingo-Ferrer and U. Gonzalez-Nicol´as, "Balanced Trustworthiness, and Safety and Privacy in Vehicle-to-vehicle Communication"-[4] The Vehicular ad hoc networks VANETs) are being designed to improve traffic safety and efficiency. To meet this entire goal, the messages disseminated in VANETs must be trustworthy. We propose a privacy-reserving system which guarantees message trustworthiness in vehicle-to-vehicle V2V) communications. Vehicle privacy is provided as a vehicle does not attempt to endorse the same message more than once. In case of spite of a message having been aridly endorsed, if it is later found to be false, System offers a possibility of a posteriori tracing the message generator.

In M. Vijaya Kumar, V. Priya Dharshini, and Dr. C. Selvan, "New Key Management Paradigm for Fast Transmission in the Remote Co-operative Groups.-[5] In case of Emerging technology as Mobile ad-hoc network (MANET) is widely used many areas and successfully to achieve the fast transmission and communication. Here it not possible achieve fast transmission /broadcasting in all Remote Area. To overcome such problem new key management paradigm techniques are used. In the proposed method a new advance key management paradigm form some group. In that select group any one of the node or system based on that priority to send the secret version of key distribution between the users as sender and receiver to improve fast data transmission rate in remote Area. Each and every data transmission, secret key will be generated and also should be updated.

IV. PRAPOSED SYSTEM

4.1 System Architecture:

In terms of pattern discovery, the data mining techniques can be used for pattern discovery.

As seen in design fig.1 we tend to targeted higher than drawback by formalizing the new advance key management paradigm referred because the cluster key agreement based mostly broadcast encoding. System design is illustrated within the Fig. 1. The potential receiver's square measure connected at the side of associate degree economical native reference to communication infrastructures; they will be connecting to heterogeneous networks. a distant sender will retrieve the receiver's public key from a certificate authority and validate the believability of the general public key by checking its certificate, which suggests that there\'s no direct communication from use World Health Organization is receivers to the sender is required. every and each receiver incorporates a public key/secret key try. Public secret\'s certified by the certificate authority however secret secret\'s unbroken solely by receiver. and therefore the sender will send secret messages to any chosen set of the receivers. we tend to next formally outline the model of cluster key agreement based mostly broadcast encoding. The definition incorporates the up-to-date definitions of cluster key agreement and public-key broadcast encoding. Since the core of key management theme is to firmly distribute a session key to the meant receivers, it\'s comfortable to outline the system because the session key encapsulation theme. Then sender will at the same time cipher every message beneath the session key and solely the meant receivers will decode.

We the formally outline a model of cluster key agreement based mostly broadcast secret writing. The theme incorporates the up-to-date definitions of the cluster key agreement and public-key broadcast secret writing. Since core of key management is to firmly distribute a session key to the meant receivers, it's not enough to outline the system as a session key encapsulation mechanism. Then sender can at the same time write in code any message underneath the session key and solely the meant receivers will decipher.

In a ancient broadcast secret writing theme, Third party must be totally sure, and third party is aware of the key keys of all cluster members and may scan any transmission to any subgroup of the members. this type of totally sure third party is tough to implement in open networks. In distinction, the third party in our key management model is just partly sure. In different words, the third party solely is aware of and certifies the general public key of every member. this type of partly sure third party has been enforced and is understood as public key technique (PKI) in open networks. Then the new key management paradigm seemingly needs a sender to grasp the keys of the receivers, which can want communications from the receivers to sender as in ancient cluster key agreement protocols. And, some subtleties should be discovered here.

In an exceedingly ancient cluster key agreement protocols, sender user must at the same time keep on-line with the receivers and direct communications from the receivers to the sender ar

required. this can be troublesome for a far off sender. On the contrary, in our key management paradigm, the sender solely has to acquire the receivers' public keys from a 3rd party and no direct communication from the receivers to the sender is needed, that is implementable with precisely the existing PKIs in open networks. Hence, this can be possible for a far off sender. moreover, a sender doesn't have to be compelled to often contact the third party or keep an oversized variety of keys since a sender typically communicates to a comparatively mounted cluster in follow. as an example, a department manager typically communicates along with her subordinates, superiors and different department managers, however seldom has to send secret messages to any or all employees members.

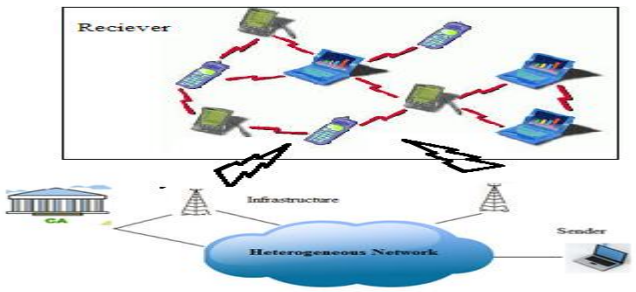

Figure 1: - Proposed System Block Diagram

Overall discussions show that our key management scheme paradigm addresses the first two constraints of the secure transmission to the remote cooperative groups. Then we show that other constraints are also addressed. By the definition, only sender and the intended receivers are involved in the Encryption and Decryption content procedures. Hence, the complexity of the system doesn't depend on the size *N* of the full group but on the size of the receiver subset. Here same analysis applies to the dynamics for the sender and receivers. This implies that our approach is particularly efficient in the case when the full group is very large but the actual receiver set is small. Indeed, proposed protocol enjoys almost constant complexity while coping with the change of the sender or the receivers. This is especially attractive for mobile networks.

4.2 Algorithm Used:

Secrete key management scheme consists of the following polynomial time algorithms:

- Key Generation (*i, n,N*): This key generation algorithm executed by each user $Ui \in \{U1, \ldots\ldots, UN\}$ to generate his/her public or private secrete key pair. An user takes as the input the system parameters *n, N* and her index $i \in \{1, \cdot\ \cdot\ \cdot, N\}$, and outputs *_pki, ski_* as her public/secret key pair. Denote $\{\_pki, ski\_ | Ui \in S \subseteq \{U1, \ldots\ldots, UN\}\}$ by *_pki, ski_*S and similarly, $\{\_pki\_ | Ui \in S \subseteq \{U1, \ldots\ldots, UN\}\}$ by *_pki_*S. Here, we implicitly omit the input security parameter as λ: actually, *n,N* are polynomials in the λ.

We considered that each user's public key is certified by a publicly accessible certificate authority so that anybody can retrieve the public keys and then he/she can verify their authenticity. This is plausible as a public key infrastructure has been a standard component in many systems supporting security services. The key generation and the registration to the certificate authority can be done offline before the online message transmission by sender in the system.

- Encryption(S, *_pki_*S): It is executed by any sender who may or may not be in $\{U1, \cdot, UN\}$, provided that sender knows the public keys of the potential receivers. It takes as input a recipient set $S \subseteq \{U1, \cdot\ \cdot\ \cdot, UN\}$ and the public key *pki* for $Ui \in S$. If $|S| = n$, it outputs a pair *_Hdr, k_* where *Hdr* is called the header and *k* is the message encryption key. (S,*Hdr*) is sent to the receivers. This algorithm incorporates the functionality of the encryption procedure in traditional broadcast encryption systems.
- Decryption (*Uj*(*skj*)S, *Hdr*, *_pki_*S): This algorithm is jointly execute by the intended receivers to extract secret session key *k* hidden in header. Each receiver *Uj* privately inputs her secret key *skj* . The common inputs are the header *Hdr* and the public keys of receivers in the recipient set S. If $|S| = n$, each receiver in S outputs the same session key *k*. This procedure incorporates a traditional group key agreement protocol. It exploits the cooperation of the receivers with efficient local connections.

We then justify the assumptions on trusted authorities and limited communication from the receivers to the sender in our key management paradigm. At a first

look, the new paradigm seems to require a trusted third party as its counterpart in traditional broadcast encryption systems. A closer look shows there is a difference.

4.3 Mathematical Model:

The proposed key management mechanism shows the ideas of broadcast encryption systems and GKA protocols.

Key Gen. Assuming the above bilinear group setting, each user i for $i = 1,\ldots, N$ randomly chooses $xi \in Z * p$ and computes $Xi = gxi \in G$. User i keeps xi secret as her secret key, and registers Xi to the certificate authority as her public key. The registered public keys are supposed to be organized in a certain order. Encryption Assume that a sender wishes to broadcast to users indexed by $\{i1,\ldots, in\} \subseteq \{1, \ldots, N\}$. The sender runs the following algorithm.

1. Randomly select $r, xi0 \in Z * p$ and compute:
   $Xi0 = gxi0$, $Yi0 = (Xi1/Xin)\, xi0$, $c = gr$.
2. Extract the public group encryption key for S:
   $K = e(Xi1, Xi2)\, e(Xi2, Xi3) \ldots e(Xin-1, Xin)$
   Note that $K = e(g, g)\, xi1xi2+xi2xi3+\cdots+xin-1xin$.
3. Compute
$S=Ke(Xin,Xi0)e(Xi0,Xi1)=e(gg)xi1xi2+xi2xi3+\cdots+xinxi0+xi0xi1$
4. Compute the secret session key
   $k = Sr = e(g, g)xr$.
5. Broadcast the header
   $Hdr = (Xi0, Yi0, c)$

As well as the receiver set S to the receivers.

Using the session key k, the sender can encrypt any message to the receivers with any secure symmetric encryption algorithm,

e.g. AES. The encrypted message can be simultaneously sent to the receivers with the header.

Decryption The intended receivers run this algorithm as follows.

1. For $j = 1, \ldots, n$, each receiver $Uij \in S$ publishes
   $Yij = (Xij+1/Xij-1)\, xij = g(xij+1 - xij-1)\, xij \in G$
   Where the subscript j of ij is computed modulo $n + 1$. That is, $n + 1 \equiv 0 \bmod (n + 1)$.
2. Each receiver indexed by ij can compute the secret decryption key $d = X$
   $(n+1)xij\, ij-1\ Y\, n\, ij\, Y\, n-1\, ij+1 \ldots Yij-2$
Similarly, the subscript j of ij is also computed modulo $n + 1$ here.
3. Using d, each receiver extracts the session key k from c by computing $k = e(d, c)$. Finally, the receiver can read messages encrypted with this session key.

The correctness of the scheme follows from the following direct verification:

$d = X(n+1)xij\, ij-1Y\, nij\, Y\, n-1ij+1 \ldots Yij-2$
$= g(n+1)xij-1xij\ gn(xij+1-xij-1)xij \times g(n-1)(xij+2-xij)xij+1 \ldots g(xij-1-xij-3)xij-2$
$= g(n+1)xij-1xij\ gnxij\ xij+1\ -nxij-1xij \times g(n-1)xij+1xij+2\ -(n-1)xij\ xij+1 \ldots gxij-2xij--xij-3xij-2$
$= gxij-1xij\ gxij\ xij+1\ gxij+1xij+2 \ldots gxij-2xij-1$
$= gxi0xi1+xi1xi2+xi2xi3+\cdots+xinxi0$
$= gx$

Hence, $k = e(d, c) = e(g, g)xr$. This completes the correctness proof of the scheme. The security of our scheme relies on the (P,Q)-DDH assumption. Bresson *et al.* formalized a family of assumptions which can be instantiated by setting the polynomial sets P and Q. For our proposal, one can set

$P = \{\alpha i | i = 0, \ldots, n\} \cup \{\alpha i\alpha i+1 - \alpha i-1\alpha i | i = 0, \ldots, n\}$ and $Q = \{ \_\ n\ i=0\ \alpha i\alpha i+1\}$,

Where the subscripts i are computed modulo $n + 1$. Based on the instantiated (P, Q)-DDH assumption, we have the following claim.

4.4 Proposed Algorithm:

Encryption steps using Hybrid Crypto System

1.Encrypt plain data block (PDB) using secrete key (SK)to get encrypt data (ED)

2.Encrypt secrete key (ESK) using destinations public key to get encrypted secrete key (ESK)

3.Concatenate encrypted data (ED) with its correspondent encrypted secrete key (ESK) to get encrypted data block (ED) which is sent to the receiver EDB = {ESK, ED}

Decryption steps

1.Decrypt Encryption Secret Key(ESK) using Private Key(PRK) to retrieve SK (Note: This should be done using same public key algorithm which is use at source)

2.Use the retrieve SK as Decryption Key to Decrypt ED to get PDB possible "noises."

V. EXPERIMENTAL ANALYSIS

Results of Practical Work:-

In section, we evaluate the proposed Hybrid group key generation algorithm and compare its performance to the existing key algorithm. The below graph clearly

shown that time efficiency of (probabilistic) polynomial time algorithm is better that our proposed algorithm , cost of the fist run ,cost of member deletion and addition and cost of group decryption key update

Graph of Time comparison

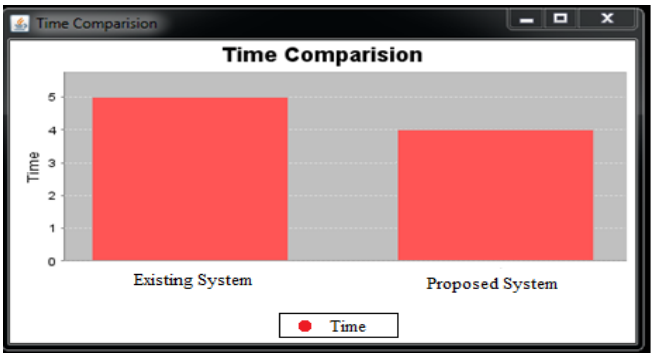

Fig.2 Time Comparison between proposed and existing system

Proposed Encryption and decryption:

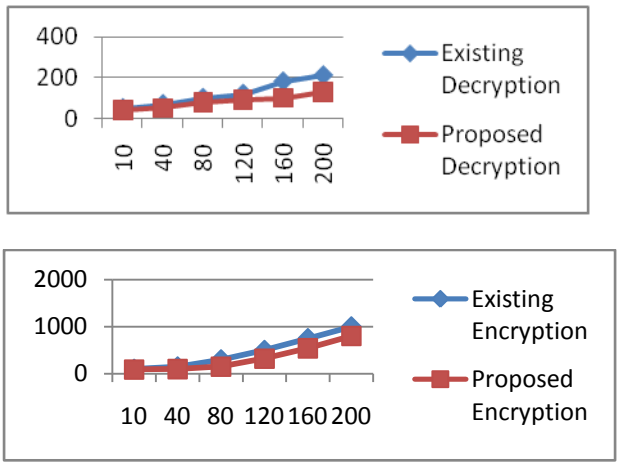

Fig 3: Cost of the first run of the protocol

In Figure 3, the time delay introduced by group decryption (excluding the interactions for decryption)is really low. The cost of the encryption to the group grows linearly with the number of the receivers due to the linear number of bilinear map operations. The network delay grows faster than the delay incurred by encryption and decryption when there are more than 100 members. However, even for a remote group with 240 members, the total delay is about only five seconds. This is bearable for a sender to transmit to a remote group organized and connected in an *ad hoc*dy. Note that the greatest delay is caused by the network; this result highlights the importance of reducing the number of communication rounds to cope with member changes in key management protocols designed for MANETs, as we have done in this work.

Cost of member Deletion and member Addition:

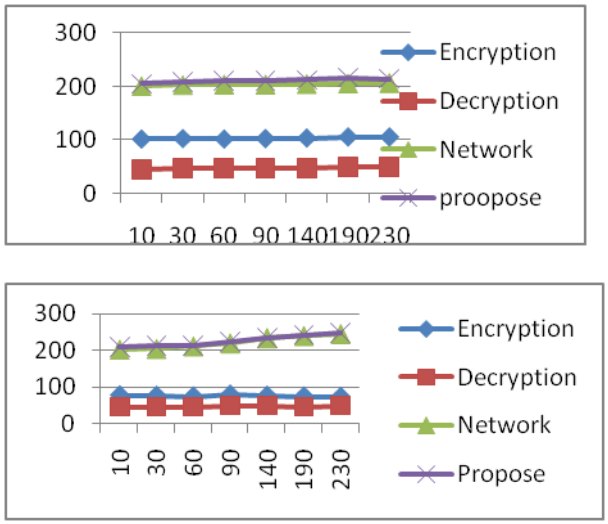

Fig.4 a) Cost of member deletion b)Cost of member addition

In Figures 4, member deletion and addition have very similar cost, much smaller than the cost of the basic protocol. This feature is desirable in practice, since members may leave and join a MANET.

Cost of group decryption key update:

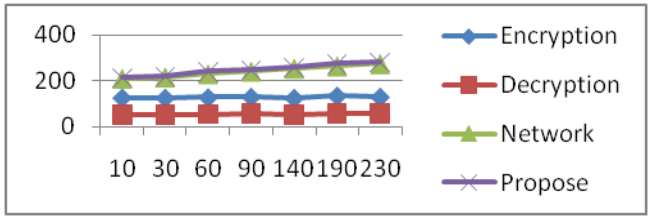

Fig.5 Cost of group decryption key update

From Figures 5, updating a group decryption key or the long-term key of a member has a similar cost as deleting or adding a member. Among these two update operations; group decryption key update is slightly More efficient due to less time spent in group encryption and decryption. The network time of these two operations is similar and accounts for the most substantial delay.

VI. CONCLUSION AND FUTURE WORK

Our proposed system is capable to send-and-leave broadcasts to remote cooperative groups without relying on the fully trusted third party. Our new key management scheme has been proven that it is secure in the standard model. Our proposal is also more efficient in terms of computation and communication. These features render our scheme a promising solution to group-oriented communication with access control in various types of ad hoc networks. Also proposed systems efficiently add delete members and flexible rekeying strategies extended. Also we have proven encryption decryption algorithm to improve security level to manager all communication in secure way to achieve better application

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

VII. REFERENCE

[1] Y. Zhang Y. Fang- "ARSA: An Attack-Resilient Security Architecture for the Multi Hop Wireless Mesh Networks," IEEE J. Sel. Areas Common. vol. 24, no. 11, pp. 1916-1928, Oct. 2006.

[2] K. Ren, S. Yu, and W. Lou and D. Zhang, "PEACE:- The Novel Privacy- Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks," IEEE Trans with Parallel Disturber. Syst., vol. 21 and 22, no. 3, and Feb. 2010.

[3] B. Rong, H.-H. Chen, - Y. Qian, K. Lu, R. Q. Hu, S. Guizani, "A Pyramidal Security Model for Large-Scale Group Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study," IEEE Trans. Veh. tech., vol-58, number-1, pp. 345-408, Jan. 2009.

[4] Y-M. Huang, C.-H. Yeh, T.-I. Wang, H.C. Chao, "Constructing Secure Group Communication over Ad Hoc Networks Based on a Virtual Subnet mythology model," IEEE Wireless Commn., vol-54, no-5, pp. 67-88, Oct. 2007.

[5] Q.-Wu,J-. Doming. -Ferret and U. Gonz´alez, Nicol´as, "Balanced Trustworthiness, -Safety with Privacy in the Vehicle ad-hoc Communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559-576, Feb. 2010.

[6] S. Fiona Abishag, and Dr. P. Deepalakshmi,- "Secure groups communication over MANET using hybrid secrete Key Management ", International Journal and Engineering Research, v-5, Issue 5, May-2014

[7] L. Zhang, Q. and Wu, A. Solanas, and J. Domingo Ferret,"A Scalable Robust Authentication Protocol for Secure Vehicular Communications," IEEE Trans. Veicalh. Technol., volume. 59, no. 4, pp. 1601,-May 2010.

[8] K.Sampigethaya, M.Li, L. Huang and R.Poovendran, "AMOEBA Advanced Robust Location Privacy Scheme for the VANET scheme," IEEE J. Sel. Arae Common. Volome-25, pp. 1569-1589, Oct-2007.

[9] M. Burmester, Y. Desmedt, "A Secure and Efficient Conference secrete Key Distribution System" in Advances in Cryptology EUROCRYPT'94, LNCS, vol-950, pp-212 286.

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

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

[12] A.Sherman and D. McGrew, "Key Establishment in Large Dynamic Groups with One-way Function Trees," IEEE Trans. Software Eng., vol. 29, no. 5, pp. 444, May 2003.

[13] 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 Distributed System vol. 15, no. 5, pp. 468- 480, May 2004.

[14] 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.

[15] Y. Sun, W. Trappe and K.J.R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless ad-hoc Networks," IEEE-ACM Trans. Net., vol.12, no. 4, pp. 653-666, Aug. 2004.

[16] W. Trappe, Y. Wang and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous scheme network," IEEE/ACM Trans Netw, volume-13, no 3, pp.134, Feb. 2005.

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

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

[19] W. Yu, Y. Sun and K. J. R. Liu, "Optimizing Rekeying Cost for Contributory Group Key Agreement mechnism," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 3, pp. 121 - 242, July-Sep. 2007.

[20] R. Dutta and R. Barua, "Provably more secure constant round contributory group secure key agreement in dynamic setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007-2021, May 2008.