© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Asymmetric Group Key Agreement Protocol for Secure Group Communication Using FIFO Routing Technique for Wireless Networks

M.Thamarai Selvan[1], Dr.N.Pasupathy[2]

[1]Research Scholar, Department of Electronics, Erode Arts and Science College, Erode, India

[2]Associate Professor, Department of Electronics, Erode Arts and Science College, Erode, India

ABSTRACT

At present scenario a popular approach to secure group communications is to utilize group key agreement (GKA) and asymmetric secret key generated by asymmetric Group key agreement (AGKA) algorithm based on strongly indefensible and identity-based batch multi-signatures (IBBMS) is widely employed for secure group communications in contemporary mutual and group-oriented applications in wireless networks. AGKA is identify-based cryptosystems with an emphasis on round-efficient, the sender has to be unlimited and the member is vibrant. It allows a more then members dynamically in to the network communication and establish a public group encryption key, and each member has a different secret decryption key in an identify-based cryptosystem. Any node of the network is to be encrypting the message using group secret key and decrypt the message using unique private key in the target node This paper examines a set key settlement trouble where a person is simplest privacy to his associates at the same time as the connectivity graph is arbitrary. In our hassle, there is not any centralized initialization for users. A group key settlement with those functions could be very appropriate for social networks. The results show that the proposed Identity-based authenticated asymmetric group key agreement (IBAAGKA) protocol with First in First Out (FIFO) routing technique establish a common encryption key which does not need certificates and is free from key escrow, extra efforts are required to address user dynamicity and provable security. This protocol acquires lower bounds at the round complexity with passive protection and actively relaxed protocol is constructed from a passively at ease one.

Keywords: Group key agreement, asymmetric group key, lower bound, authentication, protocol.

I. INTRODUCTION

KEY agreement is a mechanism that lets in or extra events to safely share a mystery key (referred to as a session key). Starting from Diffie-Hellman for the 2-birthday party case, this topic has been substantially studied within the literature. However, nearly all of the protocols assume a complete connectivity graph: any users can talk without delay. In the actual world, this isn't always actual. For example, in social networks consisting of Face book, Skype, We chat and Google+, a user is most effective linked together with his pals. For a group of customers (e.g., the school union in a university) who desire to set up a consultation key, it isn't always important that any two of them are pals. But they could nevertheless be related not directly via the pal network. Of the direction, we will nonetheless regard them as without delay linked via regard-in the intermediate users as routers. However, that is quite exclusive from an instantaneous connection. First, in a roundabout way linked users won't have the public records of every different (e.g., public-key certificate). Second, circuitously related customers won't recognize the life of every other (e.g., in our school union instance, one professor in one branch might not understand another professor in a one-of-a-kind department). Third, a message between not directly linked customers travels an extended time than that between immediately connected users.

The observe the group key settlement with an arbitrary connectivity graph, where every consumer is only privacy to his acquaintances and has no information about the lifestyles of different users. Further, he has no information about the community topology. Under this placing, a consumer does not want to trust a person who is not his neighbor. Thus, if one is initialized the usage of PKI, then he want no longer trust or consider public-keys of users beyond his pals. A comprehensive literature survey is performed in the support of the group key agreement problem. In literature, several techniques have been presented for allowing two or more parties to securely share a secret key called as session key. In network security field, the group key agreement problem is considered to be the challenging task that tries to address the issue of securely sharing a secret key between two or more parties. The group key agreement with an arbitrary graph is the main difficulty for securely sharing the secret key among multiple parties. Several methods have been proposed to solve the complexity observed in the group key agreement. Group key agreement still remains difficult task. [1] This paper considers the problem of key agreement in dynamic peer groups. (Key agreement, especially in a group setting, is the stepping stone for all other security services.) Dynamic peer groups require not only initial key agreement (IKA) but also auxiliary key agreement (AKA) operations, such as member addition, member deletion, and group fusion. In this research Author specifically focus on the requirements of Dynamic Peer Groups (DPGs). DPGs are common in many layers of the network protocol stack and many application areas of modern computing. Examples of DPGs include replicated servers (such as database, web, time), audio and video conferencing, and more generally, collaborative applications of all kinds.In contrast to large multicast groups, DPGs tend to be relatively small in size, on the order of a hundred members. (Larger groups are harder to control on a peer basis and are typically organized in a hierarchy of some sort.) DPGs typically assume a many-to-many communication pattern rather than one-to-many commonly found in larger, hierarchical groups. The second difference is due to group dynamics. Two-party communication can be viewed as a discrete phenomenon: it starts, lasts for a while, and ends.[2]In this paper the public key distribution system is generalized to a conference key distribution system (CKDS) which admits any group of stations to share the same encryption and decryption keys. The analysis reveals two important aspects of any conference key distribution system. One is the multi tap resistance, which is a measure of the information security in the communication system. The drawback is the choice of a suitable symmetric function of the private keys and the choice of a suitable one-way mapping thereof is not validated in proper. [3]In this research author establish a key with a rate as large as possible under the constraint that the observations at Eve do not provide any information about the generated key. There are two lines of previous work relating to key agreement over fading channels: that concerned with the channel model and the new randomly generated key with a different rate leads to higher latency in transmitting information over the channel. [4] To ensure the authenticity, integrity, and confidentiality of bundles, the in-transit Protocol Data Units of bundle protocol (BP) in space delay/disruption tolerant networks (DTNs), the Consultative Committee for Space Data Systems bundle security protocol (BSP) specification suggests four Internet Protocol Security (IPSec) style security headers to provide four aspects of security services. However, this specification leaves key management as an open problem.[5]In a public key broadcast encryption [6], the key size problem can be waived. But one nonetheless has to set the edge for the quantity of horrific users. Also the cipher text size depends on the range of users and subsequently can be massive (e.g., it is O (√n) in [6] for n users). Further, customers are initialized through a government which is not desired in our putting. Traitor tracing is a unique broadcast encryption, in which except the same old broadcast functionality, it could hint a pirate user: if a user allows build an unlawful decryption tool, where the person could be diagnosed. This primitive inherits the drawbacks of a printed encryption. Then the rest of the paper is organized as follows. Section 2 analyses the problem statement of the existing algorithms where as section 3 briefs about network model IBBMS based IBAAGKA protocol Section 4 & 5 gives the overview of IBBMS SECURITY MODEL and section 6 gives the complete explanation about IBAAGKA PROTOCOL with FIFO routing technique and section 7 discussing the efficiency of the proposed and section 8 concludes the paper with future work.

II. PROBLEM STATEMENT

We take into account the situation of a sender who wants to securely transmit messages to a collection of receivers. The problem is how the sender can try this in an environment with the subsequent constraints:

1) A fully trusted provider to generate keys for the organization members isn't available;
2) It is tough to estimate who will ship encrypted messages to the organization individuals; three) the machine is fundamental escrow loose;
3) The organization is dynamic, this is, a consumer can also be part of or leave the group. It is really worth noticing that broadcast encryption can also carry out a comparable characteristic to AGKA. However, in a broadcast encryption system, a depended on dealer is commonly required to keep the group. Even though some broadcast encryption systems are unfastened from depended on dealers, they cannot provide ahead secrecy and/or key escrow freeness. The above mentioned problems are addressed with the help of proposed solutions.

III. NETWORK MODEL IBBMS BASED IBAAGKA PROTOCOL

The key generation center (KGC) is a trusted authority. It issues private keys for the protocol participants. The protocol participants run our Identity-based Authenticated Asymmetric Group Key Agreement (IBAAGKA) protocol to establish a group encryption key and respective secret decryption keys for each participant. At any time, a protocol participant may leave the group. A user may also join the group if the number of the protocol participants is smaller than the maximum allowable group size. A sender can be a protocol participant or any user not in the group.The security of our constructions is based on the assumptions that the computational Diffie-Hellman (CDH) and k-bilinear Diffie-Hellman exponent (BDHE) problems are hard.

CDH Problem: Given g, gα, gβ for unknown α, β ∈ Zq , compute gαβ.

k-BDHE Problem: Given g, h and gi = gαi in G1 for i = 1, 2, . . . , k, k+2, . . . , 2k as input, compute ˆe(g, h)αk+1.

IV. OUTLINE OF THE SECURITY MODEL AND NOTATIONS

A. NOTATIONS

Let P be a polynomial-size set of participants. Any subset U = {*U*1. . . *Un*} ⊆ P may launch an IBAAGKA protocol.

We define the following notations which will be used in our security model:

• _*π Ui* represents instance *π* of participant *Ui* .

• *I DπU I* is the current identity associated with _*π Ui* . If the protocol is static, *I DπU*

I is always equal to the real identity *I Di* of *Ui* . In our dynamic protocol, each articipant will obtain several private keys along with different indices from the KGC. Thus, in the dynamic case, *I DπU I* contains *I Di* and the current index of *Ui* 's private key.

• pid*π Ui* is the *partner ID* of _*π Ui* . It contains the current identities of the participants in the group with whom _*π Ui* intends to establish a session key, including *Ui* itself.

• sid*π Ui* is the unique *session ID* of instance _*π Ui* . All members taking part in a given execution of a protocol have the same session ID. In our protocol, we will set the session ID to be the concatenation of pid*π Ui* , a time interval (for example, one day specified as a date) and a counter of the number of sessions executed by the participants with *partner ID* pid*π Ui* in the time interval.

• isid*π Ui* is the initial *session ID* of instance _*π Ui* . In a static IBAAGKA protocol, isid*π*
Ui is equal to sid*π Ui* . However, in the ynamic case, isid*π Ui* is set to be the *session ID* of the protocol when it is first initiated.

• ms*π Ui* is the concatenation of all messages sent and received by _*π Ui* during its execution, where the messages are ordered by the indices of the protocol participants.

• ek*π Ui* is the group encryption key held by _*π Ui* .

• dk*π Ui* is the group decryption key held by _*π Ui*

.• state*π Ui* represents the current (internal) state of instance _*π Ui* . _*π Ui* is *terminated*, if it stops sending; and it is *accepted* if _*π Ui* is *terminated* and no incorrect behavior has been detected, i.e., it possesses ek*π Ui (_= null)*, dk*π Ui (_= null)*, ms*π Ui* , pid*π Ui* and sid*π Ui Definition 1 (Partnering):* Two instances _*π Ui* and _*π _ Uj* (with *i _= j*) are partnered if and only if (1) they are accepted; (2) pid*π Ui* = pid*π _ Uj* ; and (3) sid*π Ui* = sid*π _ Uj*..

B. THE MODEL

IBBMS scheme as a building block of our IBAAGKA protocol.The security model for dynamic IBAAGKA protocols is described by a game, that's run between a challenger C and an adversary A. In the sport, C generates the grasp-mystery, initializes the system parameters and answers diverse queries from A, who controls the community communications. This game has the subsequent levels:

• Send*(_π Ui ,_)*: It sends a message _ to instance _*π Ui* , and outputs the reply generated by this instance. In particular, if _ = *(*sid*,* pid*)*, this query prompts *Ui* to initiate the protocol using session ID sid and artner ID pid. If _ is of incorrect format, it returns *null*.

• Send*L(_π Ui ,_)*: It sends a message _ to instance _*π Ui* and is triggered when a participant leaves the group. In particular, if _ = ⊥, this query prompts *Ui* to leave the group.

Definition three: An IBAAGKA protocol is stated to be semantically indistinguishable against selected identity and plaintext assaults (Ind-ID-CPA) if is negligible for any probabilistic polynomial-time (PPT) active adversary within the above version.

Similar to, we most effective outline chosen plaintext attacks (CPA) of dynamic IBAAGKA protocols.

A more potent definition is safety towards chosen-cipher text assaults (CCA). To obtain CCA safety, a few well-known buildings were proposed to transform a CPA comfy encryption scheme right into a CCA at ease one, such as the Fujisaki-Okamoto conversion . Hence, in this paper we will cognizance on CPA protection of dynamic IBAAGKA protocols.

V. OVERVIEW AND BUILDING BLOCK OF IBBMS SECURITY MODEL

An IBBMS scheme lets in multiple signers to sign more than one message beneath a bit of kingdom statistics, so one can generate in an efficient manner a batch multi-signature. Later, the unmarried batch multi-signature can be separated intercom

Multi-signatures. The state statistics may be instanced by way of concatenating the identities of all of the signers, a time c program language period and a counter of the wide variety of signatures issued by using those signers inside the time interval. An IBBMS scheme has the following 5 algorithms

BM. Setup: On enter a security parameter; it generates a master-secret and a list of gadget parameters. For brevity, the device parameters are disregarded as part of the inputs for the relaxation of algorithms.

BM. Extract: On inputs an entity's identity I Di and the master-secret, it outputs the personal key of the entity.

Sign: It takes as inputs a chunk of kingdom facts in f o, t messages, a signer's identification I Di and private key, and it outputs a batch signature on t messages.

Aggregate: It takes as enter a set of x batch signatures via x signers at the equal t messages beneath the identical kingdom facts in f o, and it outputs a batch multi-signature.

BM. Verify: It takes as input a batch multi-signature on t messages generated by way of x signers, beneath the equal kingdom facts in f o, and it outputs both "all valid" if the batch multi-signature is valid, or a set which contains the indices of the valid multi-signatures on the corresponding messages.

Roughly speaking, a IBBMS scheme is strongly unforgettable if an adversary cannot output a one-of-a-kind multi-signature on a message m underneath any kingdom facts and x signers' identities although he can achieve the signature(s) on m below the identical kingdom information and identities. The formal definition makes use of the subsequent game between a challenger C and an adversary A.

• BM.Extract: The input of this query is an identity *I Di* of an entity. On receiving such a query, *C* outputs the private key corresponding to *I Di* .

• Sign: *A* may request a batch signature on Messages {*m*1, . . . ,*mti* } under an identity *I Di* and a piece of state information *in f oi* . On input *(I Di , in f oi ,m*1, . . . *,mti)*, *C* generates a valid batch signature. If *A* requests a batch signature with a previously used state information but a different message set as input, *C* returns *null*.

Forgery: Eventually, *A* outputs a multi-signature $\sigma*$ on a message *m*∗ under *x* identities *(I D*∗ 1, . . . , *I D*∗ *x)* and a piece of state information *in f o*∗. *A* wins the above game if the following conditions are satisfied:

1) *I D*∗ *I* ∈ {*I D*∗ 1, . . . , *I D*∗ *x* } has never been submitted to BM. Extract.

2) $\sigma*$ is not obtained by using the batch signatures output by submitting *(I D*∗ *i , in f o*∗*,m*1, . . . *,mI,* . . . *,mt)* to the Sign queries, for *I D*∗ *I* ∈ {*I D*∗ 1, . . . , *I D*∗ *x* }, where *mI* = *m*∗ and *I* defines the index of the message.

VI. THE PROPOSED FIFO TECHNIQUE ON DYNAMIC IBAAGKA PROTOCOL

In this segment, we endorse our one-spherical dynamic IBAAGKA protocol. In this protocol, we need to set manager to keep the institution. We notice that the institution supervisor may be any of the protocol contributors and might also go away the organization. This isn't like a relied on supplier. However, for better overall performance, we require the organization manager to be surprisingly static.

A. THE PROTOCOL

• Setup: The same as the BM.Setup in Section 6-C, except that an additional cryptographic hash function *H*5 : G2 −→ {0, 1}*l*0 is chosen, where *l*0 defines the bit-length of plaintexts. The system's parameter list is *Υ* = *(q,*G1,G2, ˆ *e, g, gpub, H*1 ∼ *H*5, *l*0*)*.

- Extract: Each entity may request at most N private keys. Suppose the identity of an entity is I Di . The KGC computes idi, j,0 = H1(I Di , j, 0), idi, j,1 = H1(I Di , j, 1) for 1 ≤ j ≤ N, and outputs N private keys {si, j,0 =
Idκ i, j,0, si, j,1 = idκ i, j,1 } j∈{1,...,n}. in our protocol, when a user joins the group with the same isid, he has to usea new private key. generally, a user will not join and leave the group with the same isid frequently. therefore, n does not need to be large in most cases.
- Agreement: Assume the group size is n and the group manager is the t-th participant in the group. This protocol runs as follows:

1) Choose ηi, θi ∈ Z ∗q , compute ri = gηi , ui = gθi .
2) Compute v = H2(isid),_i = H4(isid, I Di , ιi
ri , ui), where ιi is initially set to be 1.
3) For 1 ≤ j ≤ n, compute f j = H3(isid, j).
4) For 1 ≤ j ≤ n, compute zi, j = si,ιi ,0s_i
i,ιi ,1 vθi f ηi j .
5) Publish σi = (I Di , ιi , ri , ui , {zi, j } j∈{1,...,n}, j
_=i).

Each participant Ui , i _= t maintains a table like

The safety of our scheme is primarily based on the hardness of the CDH hassle. The following declare verified in the Appendix relates the safety of the IBBMS primitive to the difficulty of solving the CDH hassle. Theorem 1: If an adversary A can win the sport in Section IV-B with advantage in time τ after making at most qHi queries to Hi for 1 ≤ i ≤ 3, qE Extract queries, and qσ Sign queries with maximal message size N, then there exists an algorithm to resolve the CDH problem with gain (x+2 qE+qH3 +x+1)x+2 qH3 ex+2 in time O(τ), wherein x is the most wide variety of customers in a solid IBBMS and e is Euler's wide variety.

Further the above discussed protocol is analyzed with Runtime Contention and Bandwidth-Aware Adaptive Routing Selection Strategies for Networks-on-Chip. This method helps to increase reliability of Network-on-chip by avoiding errors and crosstalk between the routers. Whereas this method presents the design of a NoC router based on turn model. A swapping router is used to avoid deadlock conflicts. Also the router integrates a dynamic arbiter to increase the Quality of Service of network.

Table 1. Comparison Table of All the methods.

Parameters	Methods	Methods	Methods
Router Parameters	2D router	2D router	2D router
Buffer Depth	4	4	4
Flit size (bit)	32	32	32
Switching	wormhole	Wormhole	wormhole
Flow control Scheduling	Credit based Dynamic arbiter	Credit based Dynamic arbiter	Credit based Dynamic arbiter
Routing	Reconfigurable router	Swapping router	FIFO router
Target device	Virtex5 XC5VFX70T	Virtex5 XC5VFX70T	Virtex5 XC5VFX70T

The arbiter module of the switch allocator uses a round-robin and a priority scheduler schemes to assign the highest priority packet to the adequate output port in the existing methods where FIFO is used in the proposed method as shown in the Table.1.

The turn model which is a deadlock-free swapping router for mesh NoC.In wormhole switching, the deadlock situation occurs when packets are waiting for each other in cyclic dependencies. In 2D mesh network, routers may forward packets in four directions: North, East, South and West. As shown in figure 3.b, packets may take eight turns for each direction. A turn in this context refers to a change of 90-degree of the travelling direction of the packet. The swapping router is chosen due to its scalability and simplicity. The reconfigurable transfer lets the proposed FIFO method is integrated with DYNAMIC IBAAGKA PROTOCOL outperforms existing reconfigurable router design in terms of area overhead and timing constrain. A detailed performance analysis of the five notable group key agreement methods with respect to communication and computation costs is analysed with the help of the simulation tool NS allinone 2.34 and routing architecture are analyzed using Field Programmable Gate Array (FPGA) as shown in the results and discussion section. An in-depth experimental evaluation obtained from live experiments with various types of group membership changes over both local- and wide-area networks are discussed below.

VII. RESULTS AND DISCUSSION

These results provide valuable insights into the protocols' scalability and practicality Figure 2 explains about if the network creation in a particular area that will considered as a node and there is a node1 and node2 communication between the neighborhood nodes. In this scheme, those w transmission opportunities are the only times a node may ever send any packets. A node that has 73 generated a new packet to send records the ID and position of the destination in the packet header, along with its own ID as the source and a sequence number. Informally, key independence means that a passive adversary who knows any proper subset of group keys cannot discover any other (future or previous) group key.

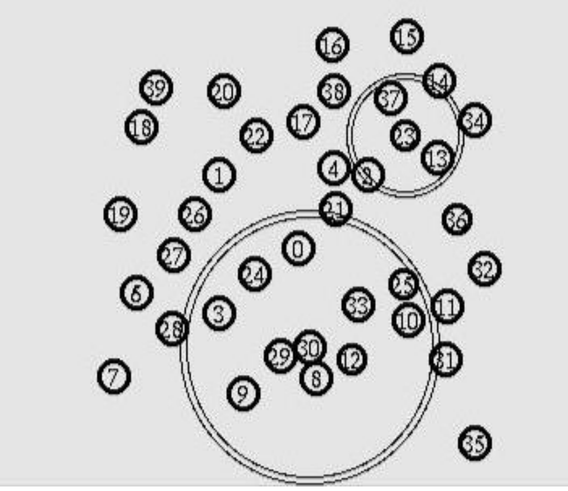


Figure 1. Represents the Formation of Nodes

Figure 1 represents the multi hop network which has more nodes to place in a particular location and that are ready to communicate with each other. The reliable protocol for multi-hop communication. Where Figure 2

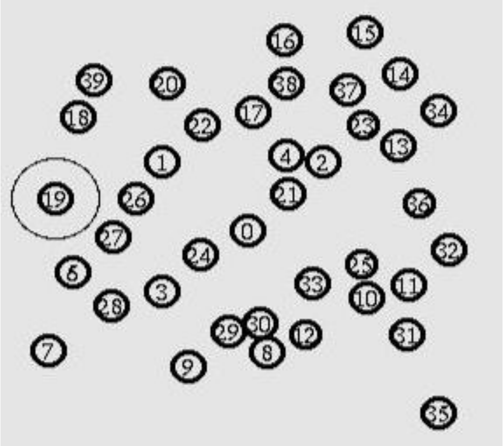


Figure 2. Creation of Cluster Head

Figure 2 explains about Clustering is one of the important methods for prolonging the network lifetime in wireless sensor networks (WSNs). It involves grouping of sensor nodes into clusters and electing cluster heads (CHs) for all the cluster and represents the multi hop network which has more nodes to place in a particular location was created.

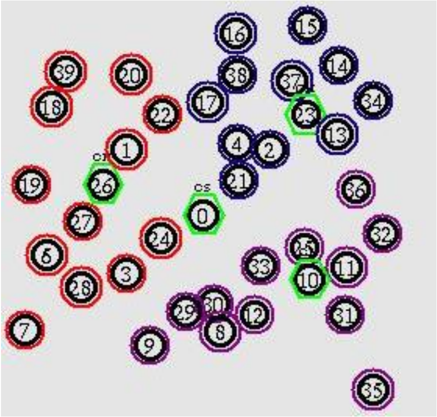


Figure 3. Group formation in the network

Figure 3 explains about if they choose in cluster head selection and creating group formation. The group formation selects the one cluster head. The cluster head based data transfer.

Figure 4 explains about the group key is introduced based on the nodes capability within two hops. In this scheme, direct trust and indirect trust is computed to identify Cluster Heads (CH) and the concept of auxiliary cluster head is introduced for effective key management.

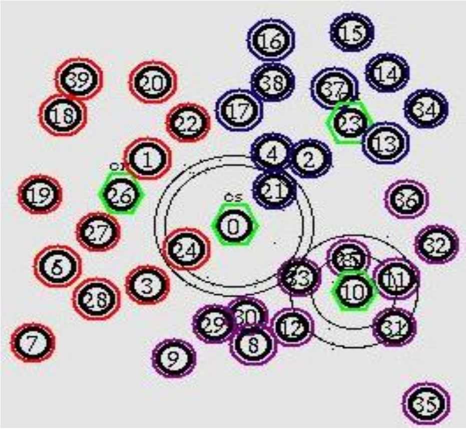


Figure 4. Key Send Cluster

Figure 5 explains about the process of transferring messages from a member to another member securely within a network is known as secure group communication. Key management is an important primitive to ensure this, as it provides a secure method for cryptographic keys creation, distribution and management. Group key establishment/management methods are key management's two sides. Group members use group key (GK) for encryption/decryption of messages in group communication. Communication needs quality and security for better performance and for acceptance of users and client companies.

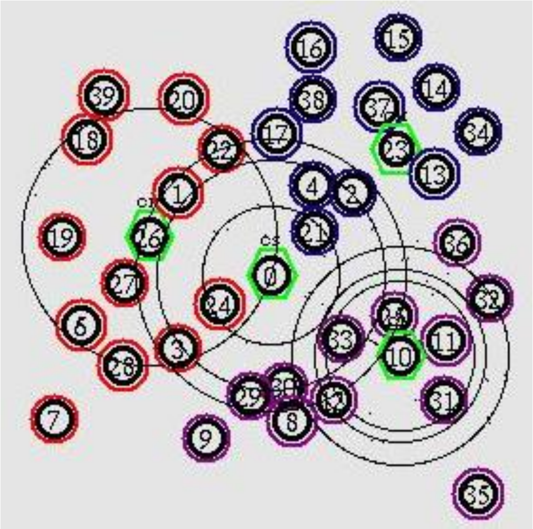


Figure 5. Key Send Cluster Head2

Figure 6 Explains about the In traditional group key transfer protocol, the key generation center randomly selects a session key and then transports it that has been encrypted by another secret key. Afterwards, scholars construct authenticated key transfer protocols based on secret sharing instead of encryption algorithm.

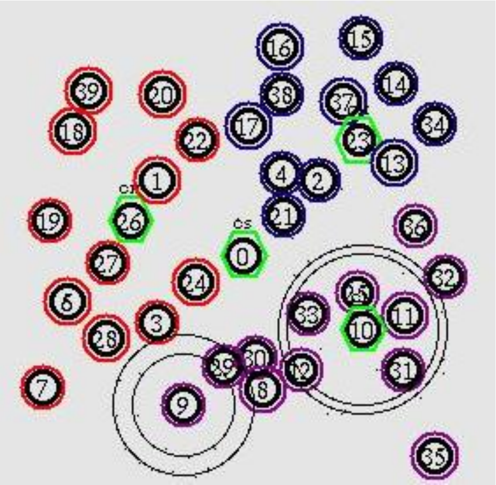


Figure 6. Key Share To Group 1

Figure 7 Explains about an authenticated key transfer protocol based on secret sharing scheme that KGC can broadcast group key information to all group members

at once and only authorized group members can recover the group key; but unauthorized users cannot recover the group key. The confidentiality of this transformation is information theoretically secure. We also provide authentication for transporting this group key.

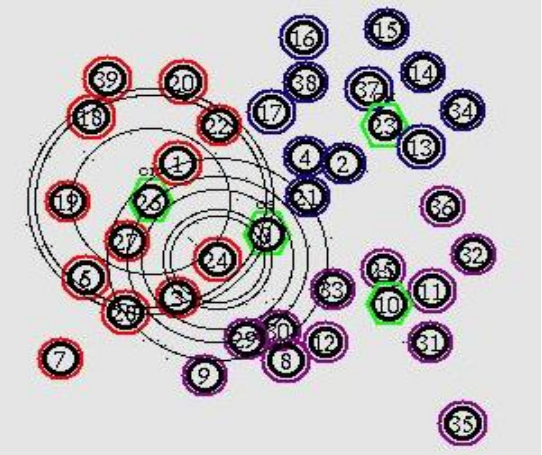


Figure 7. Key Share To Group 2

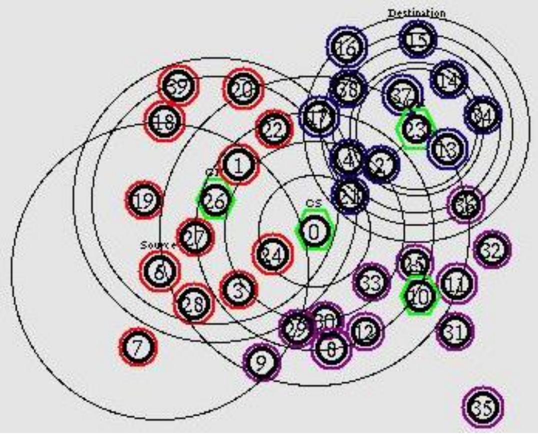


Figure 8. Key Based Data Transfer

Cryptography and Steganography are two important areas of research that involve a number of applications. Fig 8 shows key based data transfer, these two areas of research are important especially when reliable and secure information exchange is required. The below figure (9, 10) shows the comparison of throughput and end to end delay

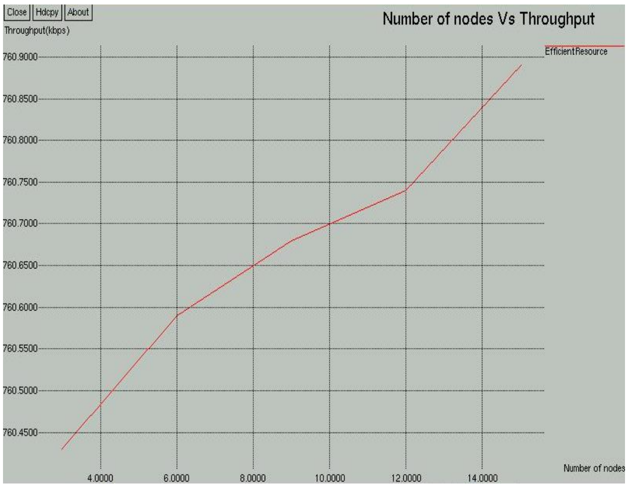


Figure 9. Number of nodes vs Throughput

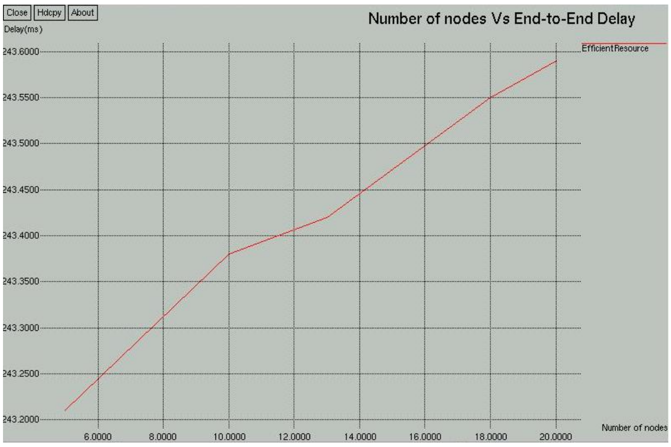


Figure 10. Number of nodes vs End to End delay

Specifically, we designed a robust contributory key agreement protocol resilient to any sequence of (possibly cascaded) events and proved that the resulting protocol preserved group communication membership semantics and ordering guarantees. Further the implementation of FIFO based structure in the nodes are given here.

All the methods are tabulated Table 2. where the Proposed FIFO approach improves the logic circuit's throughput while reducing some of the overheads in the existing nodes. In this architecture the cycle time overhead of traditional reconfigurable switches avoided as there are no internal buffer. Cycle time is obtained by the variation in the signal propagation delay from the logic and delays from the register of input and output. Latency from the pipeline avoids the traditional method overhead because the signals do not propagate from end to end of internal buffer. Overhead due to partitioning is reduced as the pipeline is not divided into stages separated by buffer.

Table 2. Logic utilization of nodes while transmitting data

	Reconfigurable Router	Swapping Router	FIFO Router
Slice LUTs	787	725	526
Slice Flip Flops	344	248	571
Delay	13.14ns	11.608ns	3.141ns
Frequency	732.224MHz	86.149MHz	318.400MHz

It explores the idea of pipelining approach which in turn reduces the Delay with High operating Frequency and High Throughput of the device in future as shown in the Figure 11. Redundancy has reduced through this reconfigurable swapping architecture through parallel pipeline approach. The optimized results are shown in table.2.In the above result the total composition of look up table has been given in detail, in turn helps to analyze the utilization of bit in the memory of the particular device which has selected for implementation. In case partitioning makes registers of considerably bigger width to be essential then the decline in the combinational delay per stage will be offset by the rise in the completion delay so that the throughput of the system may not essentially rise; then in order to reduce the delay and to improve throughput parallel pipeline stage approach is taken.

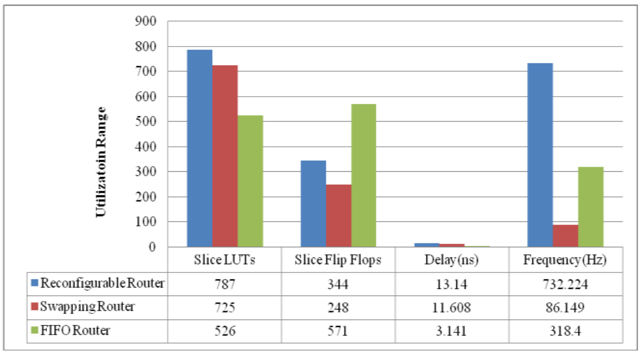
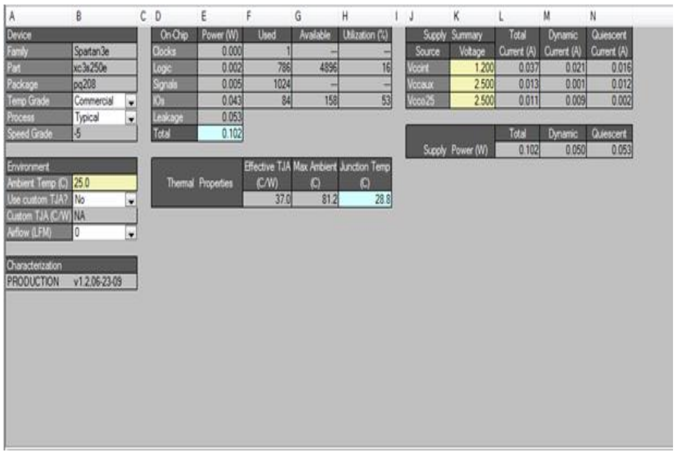


Figure 11. Comparison of area overhead constrains

Area report has analyzed for all the methods which includes (As shown in Table 4.1).An n-bit LUT can code any Boolean function of n-input by designing of functions as truth tables. This is a best way of Boolean logic functions encoding, and LUTs with 4-6 bits of input are in fact the important constituent of modern FPGAs. Storage caches (such as processor caches for either data or code or disk caches for files) work also like a lookup table. As shown in the Figure 11. and the power report the proposed FIFO routing architecture is shown in the Figure 12.



Device	
Family	Spartan3e
Part	xc3s250e
Package	pq208
Temp Grade	Commercial
Process	Typical
Speed Grade	-5

Environment	
Ambient Temp (C)	25.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	0

Characterization	
PRODUCTION	v1.2,06-23-09

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.000	1	--	--
Logic	0.002	786	4896	16
Signals	0.005	1024	--	--
IOs	0.043	84	158	53
Leakage	0.053			
Total	0.102			

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	37.0	81.2	28.8

Supply Source	Summary Voltage	Total Current (A)	Dynamic Current (A)	Quiescent Current (A)
Vccint	1.200	0.037	0.021	0.016
Vccaux	2.500	0.013	0.001	0.012
Vcco25	2.500	0.011	0.009	0.002

	Total	Dynamic	Quiescent
Supply Power (W)	0.102	0.050	0.053

Figure 12. Power analysis report of FIFO architecture.

VIII. CONCLUSION AND FUTURE WORK

In this paper the security model for dynamic IBAAGKA protocols, in which an attacker is allowed to learn the master secret of the KGC. A one-round dynamic IBAAGKA protocol with FIFO technique is proposed and proven secure in our Model under the k-BDHE assumption. It offers secrecy and known-key security, and it does not suffer from the key escrow problem. Therefore, not even the KGC can decrypt the cipher texts sent to a group. A group key agreement problem, where a user is only aware of his neighbors while the connectivity graph is arbitrary. In addition, users are initialized completely independent of each other. A group key agreement in this setting is very suitable for applications such as social networks. The constructed two passively secure protocols with contributiveness and proved lower bounds on a round complexity, demonstrating that our protocols are round efficient. Finally, constructed proposed model actively secure protocol from a passively secure one. In this work, we did not consider how to update the group key more efficiently than just running the protocol again, when user memberships are changing. We are not clear how to do this. One can either propose algorithms to our current protocols (as Data and Buru did) or construct a completely new key agreement with these features.

IX. REFERENCES

[1]. Pourpouneh, Mohsen, Rasoul Ramezanian, and Afshin Zarei. "A Note on Group Authentication Schemes." International Journal of Computer Network and Information Security 8, no. 5 (2016): 1

[2]. X. Lv, H. Li, and B. Wang, "Authenticated asymmetric group key agreement based on certificateless cryptosystem," Int. J. Comput. Math., vol. 91, no. 3, pp. 447-460, 2014.

[3]. Zou, Shaofeng, Yingbin Liang, Lifeng Lai, H. Vincent Poor, and Shlomo Shamai. "Broadcast networks with layered decoding and layered secrecy: Theory and applications." Proceedings of the IEEE 103, no. 10 (2015): 1841-1856.

[4]. Lv, Xixiang, Yi Mu, and Hui Li. "Key management for Smart Grid based on asymmetric key-wrapping." International Journal of Computer Mathematics92, no. 3 (2015): 498-512.

[5]. Garg, Sanjam, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. "Candidate indistinguishability obfuscation and functional encryption for all circuits." SIAM Journal on Computing 45, no. 3 (2016): 882-929.

[6]. L. Zhang, Q. Wu, B. Qin, H. Deng, J. Liu, and W. Shi, "Provably secure certificateless authenticated asymmetric group key agreement," in Proc. 10th Int. Conf. Inf. Security Pract. Exper. (ISPEC), vol. 8434. 2014, pp. 496-510.

[7]. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, S. S. M. Chow, and W. Shi, "Secure one-to-group communications escrow-free ID-based asymmetric group key agreement," in Proc. 9th Chin. Int. Conf. Inf. Security Cryptol. (INSCRYPT), vol. 8567. 2014, pp. 239-254.

[8]. X. Lv, H. Li, and B. Wang, "Authenticated asymmetric group key agreement based on certificateless cryptosystem," Int. J. Comput. Math., vol. 91, no. 3, pp. 447-460, 2014.

[9]. M. H. Au, J. K. Liu,W. Susilo, and J. Zhou, "Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1909-1922, Dec. 2013.

[10]. S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices and applications," in Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT), 2013, pp. 1-17.

[11]. V.R. Sarma Dhulipala, G. R. Kanagachidambaresan, and R. M. Chandrasekaran. "Lack of Power Avoidance: A Fault Classification Based Fault Tolerant Framework Solution for Lifetime Enhancement and Reliable Communication in Wireless Sensor Networks." Information Technology Journal 11 (2012): 719-724.

[12]. V.R. Sarma Dhulipala, R. M. Chandrasekaran, and R. Prabakaran. "Timing Analysis and Repeatability Issues of Mobile Adhoc Networking Application Traffics in Large Scale Scenarios." International Journal on Recent Trends in Engineering (IJRTE), Academy Publishers 1.1 (2009).

[13]. Baskar S, Pavithra S, Vanitha T. [2015] Optimized placement and routing algorithm for ISCAS-85 circuit",Electronics and Communication Systems (ICECS),2015 2nd International Conference on 2015/2/26,IEEE, 958-96

[14]. Baskar S. [2012] ERROR DETECTION AND CORRECTION ENHANCED DECODING OF DIFFERENCE SET CODES FOR MEMORY APPLICATION, International Journal of Advanced Research in Computer and Communication Engineering, IJARCCE. (10):816-820.

[15]. Baskar S. [2014] Error recognition and correction enhanced decoding of hybrid codes for memory application at Devices, Circuits and Systems (ICDCS),2nd IEEE Conference. 1-6.

[16]. Baskar S. Reliability Oriented Placement And Routing Analysis In Design Of Low Power Multiplier For Wireless Sensor Networks" at International Journal of Applied Engineering Research. 10(44):31384-31390.

[17]. Baskar S, Sarma Dhulipala VR. Comparative Analysis on Fault Tolerant Techniques for Memory Cells in Wireless Sensor Devices, Asian Journal of Research in Social Sciences and Humanities. 6 (cs1):519-528.

[18]. VoBa, Son, and Octavian T. Ureche. "Distribution control and tracking mechanism of virtual machine appliances." U.S. Patent 9,703,586, issued July 11, 2017.

[19]. Ali, Mazhar, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. "SeDaSC: secure data sharing in clouds." IEEE Systems Journal 11, no. 2 (2017): 395-404.

[20]. Dowlin, Nathan, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. "Manual for using homomorphic encryption for bioinformatics." Proceedings of the IEEE 105, no. 3 (2017): 552-567.