International Journal of Engineering & Technology, 7 (4) (2018) 4930-4938

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.17987
Research paper

An Energy Efficient Cluster Based Group Key Management Scheme using Elliptical Curve Cryptography in Wireless Sensor Network

Usham Robinchandra Singh [1]*, Sudipta Roy [2]

[1] *Department of Computer Science & Engineering, Assam University, Silchar, Assam-788011, India.*
[2] *Department of Computer Science & Engineering, Assam University, Silchar, Assam-788011, India.*
**Corresponding author E-mail: robinchandra.u@gmail.com*

Abstract

Group communication with secure authentication in wireless sensor network can be attained by public key cryptography. Security is a measure concern in WSN. Deployment of many key during cluster formation is a important task for secure group communication. To realize this concept, we proposed an energy efficiency group key management using cluster head formation. In existing energy based cluster head selection, each node select cluster head to its neighbors. This paper presents fuzzy logic rules to select cluster head based on the energy cost, node mobility, received signal strength, residual energy model, number of neighbors, and distance of the nodes from the base station. Cluster head take the role of key manager. Moreover, selection of cluster head saves the energy of each node due to light-weight framework and easy authentication can be achieved. This group key is generated by the cluster head and communicated to other members through a secure channel that uses public key cryptography. Due to the resource constraints of wireless sensors, ECC based hierarchical cluster key management scheme is proposed for its small size of keys with same security level with compare to RSA. The technique proposed in this work uses digital signature scheme and encryption-decryption mechanisms using elliptic curve cryptography (ECC). The result shows that the proposed work is faster than other work.

Keywords: *Cluster Head; Energy Efficient; ECC; Fuzzy Logic; Group Key; Security; WSN.*

1. Introduction

The hierarchical clustering algorithm can improve the lifetime and the energy consumption significantly in the wireless sensor network. In hierarchical architecture, CHs are responsible for more complex tasks, e.g. they receive the collected data sent by sensor nodes, aggregate the sensor nodes packets into a single packet, and send it to the BS. At the same time, sensor nodes can turn off the radio after transmitting their packets, reducing energy consumption. In our proposed method, node to node authorization can realize a lot of security functions. In this new clustering scheme, clusters are formed dynamically and periodically. The proposed fuzzy based clustering key management scheme (FCKMS) using elliptical curve cryptography in wireless sensor networks can distribute the keys within a cluster and node capturing problem can be avoided at regular interval. Due to the resource constraints of wireless sensor network, Public-Key based Cryptographic algorithms like RSA and Diffie-Hellman are too complicated and energy-consuming for WSNs [1]. Therefore, we introduce ECC for its small size of keys with same security level with compare to RSA. As cluster head is responsible for processing of the data in cluster and transmission to BS, it has relatively large energy consumption and must be replaced periodically to balance the energy cost. In our scheme, we use similar approach to low-energy adaptive clustering hierarchy (LEACH) [2] to randomly choose CHs. LEACH is one of the most popular clustering algorithms. From an algorithmic point of view, LEACH is hierarchical, probabilistic, distributed and single hop protocol. In hierarchical routing entire network is divided into a number of clusters to achieve energy efficiency and stability [3]. The main idea behind LEACH is to form clusters based upon the signal strength of the sensors. Cluster heads (CHs) are chosen randomly amongst the nodes based upon the signal strength received that node from CH. CHs have to do a lot of work than sensors nodes. Hence they dissipate a lot more energy and may die quickly. CHs keep on rotating in every round to maintain a stable network. So a node which had become CH may not get an opportunity to become CH again before a set interval of time. A node can become the cluster head for the current round if its value is less than the threshold T (n). Generally, LEACH provides a good model for energy consumption while providing an equal opportunity for node to be elected CHs. Once chosen as a CH, sensor node cannot be reselected in subsequent round. Moreover, LEACH avoids unnecessary collisions between CHs because it uses the time division multiple access (TDMA) protocol. LEACH achieves 7 times more reduction in energy dissipation and about 4-8 times more reduction as compared to MTE routing protocol. Despite its general good performance, LEACH also has some clear limitations. It uses single hop communication which limits its scalability. In addition, the probabilistic election mechanism of CHs may lead to either high concentrations of CHs in one part of the network, or to orphan nodes (nodes without CHs in their neighborhood). Moreover, for a network of large regions, the dynamic clustering may become overhead since rotation of CH at every round and advertisements of CHs also dissipate energy. We use one way hash function, data encryption and message authentication code (HMAC) to authenticates the communicating nodes and update the pre-deployed network keys. Simulations show that security of newly proposed fuzzy based

Copyright © 2018 Aya Adnan Yaseen et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

cluster based elliptical cryptography has been improved, with less energy consumption not only lighter overhead but also reduces end to end delay compared to other centralized scheme. It is also more scalable, flexible, and resilient to node compromise attacks. However, recent improvement in the implementation of ECC has demonstrated the feasibility of applying PKC to WSNs.
The paper is organized as follows. Section 2 discusses related work, section 3 summarizes network architecture, section 4 discusses cluster formation and cluster head selection using fuzzy logic, section 5 discusses authentication using hash function, section 6 discusses dynamic nature of key generation amongst intra cluster and inter cluster secure communication, section 7 presents simulation scenario, section 8 provides the experimental results and performance evaluation of the proposed system, finally in section 9 presents conclusion.

2. Related Work

Group key management is a basic part for secure, robust and efficient key management system an important role in group communication. Group key has to be updated frequently whenever a member joins and leaves in order to provide forward and backward secrecy. To achieve a great advantage in terms of scalability for the key management in a multicast network, there is systematic approach called scalable and efficient group key management [4]. Pitipatana and Nirwanin [5] had presented an elliptic curve cryptosystem based group key management for secure group communications to provide security with a small key size. It uses a cluster structure for the network and provides methods to generate and establish the group key and the cluster key. Jabeen and Purusothaman in [6] proposed scalable and reliable cost effective key agreement protocol for secure group communication. M. Rahman and K. El-Khatib[7] proposed a novel key agreement protocol which is based on pairing-based cryptography over an elliptic curve. With the help this protocol, if any two nodes want to communicate independently can use the same secret key by using pairing and identity-based encryption properties. The proposed technique shows that it is robust against various attacks such as masquerade attacks, reply attacks, and message manipulation attacks. Jabeenbegum et al. in [8] proposed a cluster based cost effective contributory key agreement protocol for secure group communication. Paper describing secure group key agreement protocol using ECC (Elliptic Curve Cryptography) [9] is based on authenticated group key agreement protocol for wireless scenario. The protocol uses the concepts of elliptic curve cryptography to reduce the computation overheads and asymmetric encryption standards (AES) to maintain efficiency. It consists of a set of users and a trustworthy server, where both of them contribute to create the group key. The performance and security analysis shows that the proposed protocol is secure and performs better in terms of computation cost. For group communication , Wong et al. and Waller et al. has proposed a scheme 'logical key hierarchy (LKH) tree approach' [10-11] which provides an efficient and secure mechanism to maintain the keys. In addition, communication and computation cost increases logarithmically with the group size for a join or depart request. Communication cost in LKH is reduced from O(n) to O(logn) in the rekeying method, where n is the number of group members. One-way function (OFT) scheme was proposed by Sherman and McGrew [12] to reduce the communication cost from 2logn−1 to logn. These schemes need to rekeying message whenever member joins/leaves the group [10-14]. To overcome the above problem, Lin et al. [15] proposed the SBMK scheme using the star based architecture, in which there is no need for rekeying when a member joins and leaves the group. Key server calculates secret key using RSA algorithm [16] in SBMK and then is unicast to every group member separately. Therefore, it increases the burden on the server. Efficient star topology based multicast key management algorithm was proposed by Saravanan, K. and T. Purusothaman[17] which is based on the RSA algorithm [16] in which secret keys are calculated by the group members. This eliminates the need to unicast the secret keys to every member separately, henceforth, reducing the load on the server to great extent. In addition, our scheme does not need to maintain the key tree topology [10-14]and eliminates the rekeying process whenever member joins/leaves the group. In the aspect of security, our proposed scheme guarantees the group secrecy, forward secrecy, backward secrecy. A new cluster-based mobile key management scheme [18] shows less computational overheads and energy consumption. The new CH is selected based on its efficiency and trust ability by the moving CH for the cluster. This method can improve mobility management as well as network lifetime for an efficient network. The algorithm proposed in this research shows 20-23 percent improvements over existing algorithm. Blind factor is used to compute group key in this method [19] that ensures an attacker will not be able to get the group key when the cluster head broadcasts the group key. MAC is used along with the partial keys to guarantee authentication. Group key is generated by using partial keys in this research and use less energy consumption. Wang et al. [20] have proposed a pre-distribution policy considering hexagonal grids consisting of groups and keys. X. Zhang, J. He, and Q. Wei[21] proposed an energy-efficient distributed deterministic key management scheme (EDDK).With the help of this scheme pairwise keys and cluster keys of sensor nodes are well established as well as maintained securely and communication overhead is also less. They also made use of elliptic curve digital signature algorithm in EDDK, which provided the support for the establishment of pairwise keys and local cluster keys under the node mobility scenario. Naureen et al. in [22] proposed performance and security assessment of a PKC based key management scheme for hierarchical sensor networks. In the Diffie-Hellman (DH) scheme [23] the communication parties at both sides exchange some public information and generate a session key on both ends. Several enhanced DH schemes have been invented to counter man-in-the-middle attacks. The 2- party Diffie Hellman (DH) protocol can be extended to a generalized version of n-party DH. Furthermore, the security issue related to membership changes is a necessary address for group key management. The modification of membership requires refreshment of the group key. Tree Based Group Diffie Hellman (TGDH) [24] is a group key management scheme was proposed to combine the efficiency of the tree structure with the contributory feature of DH. The basic operation of this scheme is as follows. Each group member contributes its (equal) share to the group key, which is computed as a function of all the shares of current group members. As the group grows, new members' shares are factored into the group key but old members' shares remain unchanged. Departing members' shares are removed from the new key whenever the group shrinks, and at least one remaining member changes its share. All protocol messages are signed by the sender using RSA. In simple and efficient group key (SEGK) management scheme for WSNs proposed in [25] group members compute the group key in a distributed manner. The basic idea of the scheme is that a multicast tree is formed in WSNs for efficiency. Group members take turns to act as a group coordinator to compute and distribute the intermediate keying materials to all members through the active tree links. The author claims the architecture is secure one but there is possibility of snooping, modification, replay and masquerading attack. Forward secrecy ensures that an expelled member cannot gather information about future multicast communication and backward secrecy ensures that a joining member cannot gather information about past multicast communication [26]. For this reason, group key needs to be updated with each membership change and given away to the authenticated users. This process is known as group re-keying.

3. Network Architecture

In this section, hierarchical structure of sensor network is focus. Binary search tree like structure are most efficient when they have small height. In our architecture, grouping of sensor nodes into clusters hierarchically to achieve energy efficiently during key management process is better than distributed sensors network. Our network starts to select cluster head using some parameters based on fuzzy logic that is: i) energy cost ii) node mobility ii) received signal strength iv) residual energy model v) number of neighbors, and vi) distance from the base station of the nodes. Chance value obtained from above parameters is used to select threshold value during cluster head selection. The network is divided into base station, cluster head and sensor nodes. This architecture highlights the processing capacity of cluster heads among the sensor nodes and security measure taken by base station. Cluster head is responsible for processing of the data in cluster and transmission to base station. Therefore, it has relatively large energy consumption and must be replaced periodically to balance the energy cost. Here base station is the control center and play an important role amongst the cluster head by providing secure communication as well as reliability. In proposed architecture, node 0 is base station, source nodes are 46 and 23, and destination nodes are 29 and 21. Architecture of hierarchical wireless sensor network is shown in fig. 1.

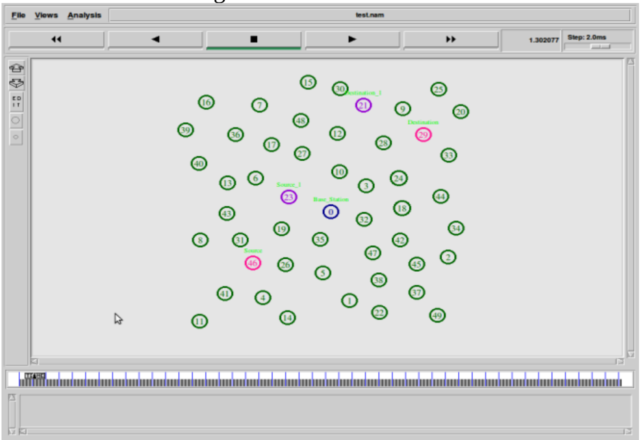

Fig.1: Hierarchical wireless sensor network architecture.

4. Cluster Formation and Cluster Head Selection Using Fuzzy Logic

In this paper, a new key management scheme called fuzzy based clustering key management scheme for wireless sensor network is proposed. This scheme involves the clustering of nodes and selection of cluster head (CH). Each node selects one of its neighbors as cluster head. After that cluster head send aggregated data to the Base station (BS). The selection of cluster heads is performed by using fuzzy logic based on Energy cost, node mobility, received signal strength, residual energy model, number of neighbors, and distance from the base station of the nodes and the data transmission process is performed by hashing techniques called HMAC using elliptical curve cryptography. Screenshot of cluster formation and cluster head selection is shown in fig. 2.

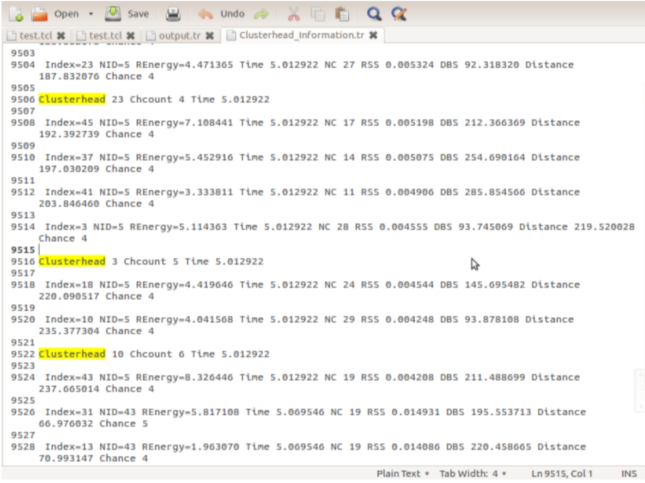

Fig.2: Snapshot code for Cluster Formation and Cluster Head Selection using Fuzzy Logic

Abbreviation used during cluster head selection is shown in table 1.In simulation node ID = 43, time = 5.069546, neighbor count =19, neighbor node =31, residual energy=5.817108, receive signal strength = 0.014931, distance from node 31 to base station (DBS) = 195.553713, distance from node 43 to node 31 = 66.976032, chance value for node (31) = 5,Chcount means cluster head count. Table 1 shows the abbreviations used during cluster head selection. Table 2 shows many input parameters used during cluster head selection process.

Table 1: Abbreviations used during cluster head selection

Terms	Description
INDEX	Current nodes
RENERGY	Residual energy
NC	Neighbor count
RSS	Received signal strength
DBS	Distance from node to base station
DISTANCE	Distance from node to neighbior node
CHANCE	Chance value for current node
CHCOUNT	Cluster head count

Table 2: Input parameters used during cluster head selection.

NID	INDEX	RENERGY	TIME	NC	RSS	DBS	DISTANCE	CHANCE
43	13	1.963070	5.069546	19	0.014086	220.458665	70.993147	4
43	8	8.883188	5.069546	13	0.012310	273.319459	81.231876	4
43	6	5.085267	5.069546	23	0.009967	171.506965	100.330409	4
43	19	6.066184	5.069546	26	0.008614	107.884254	116.089659	6
43	46	5.249531	5.069546	18	0.007968	197.421633	125.495642	5
43	40	9.744092	5.069546	14	0.007820	289.613973	127.872991	4
43	23	4.471357	5.069546	27	0.007613	92.318320	131.362746	6
43	26	6.549564	5.069546	23	0.005998	151.496489	166.717025	5
43	17	4.498674	5.069646	22	0.005494	195.658198	182.026129	4

43	36 262.122195	8.185089	5.069546 17 182.039852	0.05493 4
43	41 285.85466	3.333803	5.069546 11 184.208692	0.005429 5
43	35 67.556151	7.39549	5.069546 29 199.283364	0.005018 6
43	4 240.782558	7.158616	5.069546 17 206.176600	0.004850 5
43	27 146.020369	3.730492	5.069546 27 206.847980	0.004834 4
43	39 350.512761	2.593824	5.069546 10 210.348550	0.004754 4
43	0 0.000000	6.786351	5.069546 27 211.488699	0.004728 6
43	5 141.622910	8.292966	5.069546 22 237.665014	0.004208 4
43	10 93.878108	4.041560	5.069546 29 248.257791	0.004028 6

4.1 Algorithm for cluster Head selection

Step1: Find out the average threshold for all input parameters.
Step2. Decide Possible Threshold value to select cluster head that is chance value.
Step3. If (Threshold value is greater than or equal to chance value)
{
Selected as Cluster head
Else
Not Selected as Cluster head
}
Step4: End if

4.2 Existing Energy based cluster Head selection

In the scheme, each node selects the cluster head to its neighbors. The highest energy node selected as cluster head as done in the above process. A snapshoot of this architecture is shown in fig. 3.

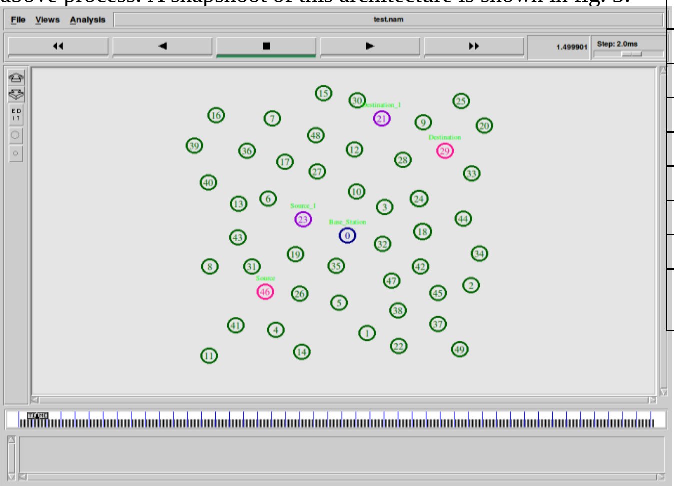

Fig. 3: Nam output showing existing energy based cluster head selection.

5. Authentication for Hash Tree Construction

Each member in the cluster generates hash value using its public key called Hpk. Cluster head concatenates the hash of each member and generates the root hash. The root hash value of each cluster head is known to all the cluster heads to perform authentication. The scenario of communication between sender and receiver is considered and both belong to different cluster. During the authentication, sender submits its hash value and transmits to the receiver. The cluster head corresponding to the sender attaches the hash of the remaining nodes. The cluster head corresponding to the receiver authenticates the sender by concatenating the hash value of the sender and the hash values produced by the cluster head and compress it with root hash value of the sender cluster head. In Hash tree construction, hashing algorithm called HMAC is applied. Table 3 shows all other notation used in our scheme.

5.1 Algorithm for Hash Tree Construction Key Management

Step 1: The cluster head broadcasts its public key to its members.
Step 2: The member broadcasts their public keys called Hash key say Hpk along with theirs ids to all the members in the cluster head.
Step 3: Cluster head concatenates the hash of each members and generate root hash.
Step 4: Root hash value of each cluster head is known to all the cluster heads to perform authentication.
Step 5: If authentication == true then
Verify digital signature.
Step 6: The leader of the cluster heads called Sink generates a new group key GKch which is then used for communication among the cluster heads
Step 7: Else exit (unsuccessful)
Step 8: Sensor node SN1 and Sensor node SN2 can communicate successfully.

Table 3: Notations

Notations	Description
BS	Base station
SN	Sensor node
CH	Cluster head
HPK	Public key of a sensor node
GKCH	
ID SNI	
ID SNJ	
IDCHI	
IDBS	
K	
H()	
HMAC	Hash message authentication code

Each member in the cluster generates hash value. During the selection of source node: 46, key =0, message = 46, HMAC Digest: c5c3a2d08f198038, HMAC Hash value: 0 as shown in the fig. 4.

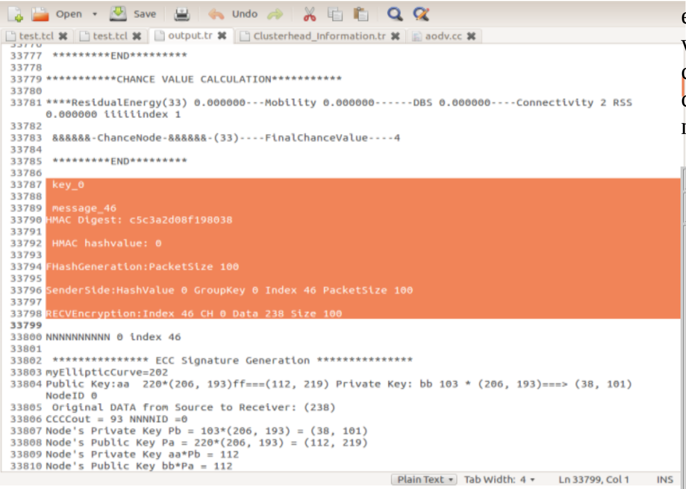

Fig.4: Snapshot code for authentication and signature generation of source node 46.

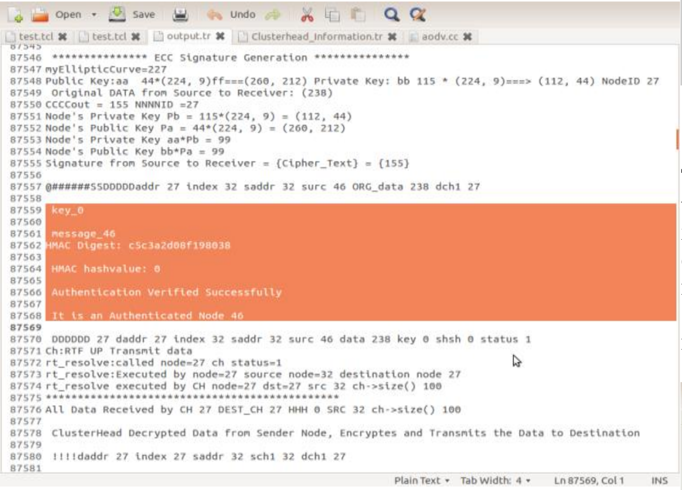

Fig. 5: Snapshot code for authentication of node 46 by cluster head node 27.

When destination (29) node received data from source (46), destination node recalculates the hash value. If the received hash value and recomputed hash value are equal that node is an authenticate node. It is confirmed that authentication of node 46 by cluster head node 27 is shown in fig. 5.

6 Network Dynamics

The number of nodes in the network is not necessarily fixed. New nodes may join the network or existing nodes may leave the network. Each node in WSNs may not be fixed in one position and may sometimes move frequently. In our scheme node addition and deletion can be done easily without any complexity. Rekeying is reduces here, because in the key generation process every SN gets the group key with separate communication with CH. Each node is having the location and ID of nearby CHs. When a SN wants to join another cluster by clustering algorithm it gets into it and gets public key of CH of that cluster. Now it can separately establish key with CH and finally gets GKch. When a SN leaves CH it first informs CH, delete the group key and then leaves.

6.1 Group Key Generation and Secure Inter cluster Communication Using ECC

Each CH generates the key for communicating with other CH. Whenever the data is transmitted by the sender to the receiver in other cluster; the data is encrypted by the sender using group key and transmitted. On receiving the data, CH corresponding to sender decrypts it and encrypts again using the key for communicating with other CH. On receiving the encrypted data the cluster head corresponding to the receiver decrypts it and transfer it to the receiver. Snapshot of group key generation in inter cluster Communication is shown in fig. 6.

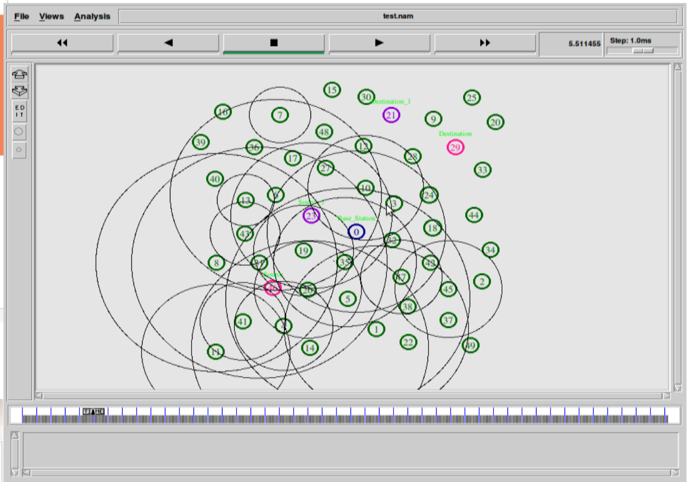

Fig. 6: Nam output showing group key generation in Inter Cluster Communication.

The data is transmitted by the sender to the receiver in other cluster. Some nodes are considered that is 46 - 32 - 27 – 29. Where 46 is the source node, 32 is the cluster head of source node, 27 is the cluster head of destination node, 29 is destination node. Sender node (46) encrypts the data and Transmits to cluster head (32). Snapshot code for ECC signature verification and generation by node ID 32 is shown in fig.7.

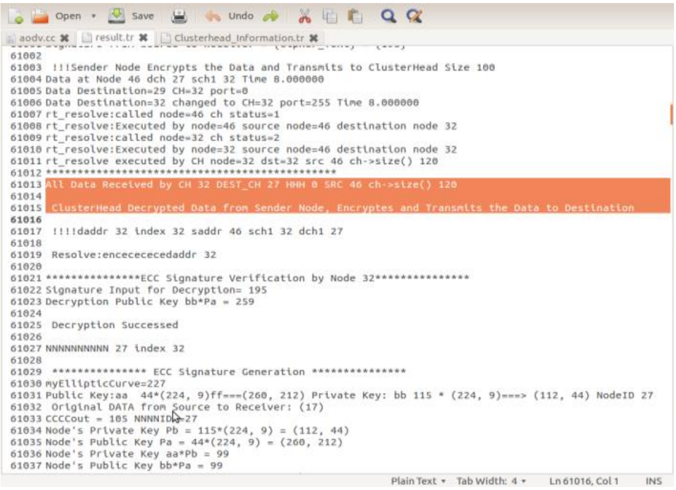

Fig. 7: Snapshot code for ECC signature verification and generation by node ID 32.

Source cluster head transfers the data to destination cluster head. All data received by node cluster head (32) transfers the data to destination cluster head (27). Cluster head decrypted data from sender Node, then encrypts and transmits to destination cluster head. Snapshot of Data encryption from source to destination as shown in fig.8. Snapshot code for ECC signature generation and successful decryption by node 32 is shown in fig. 9.

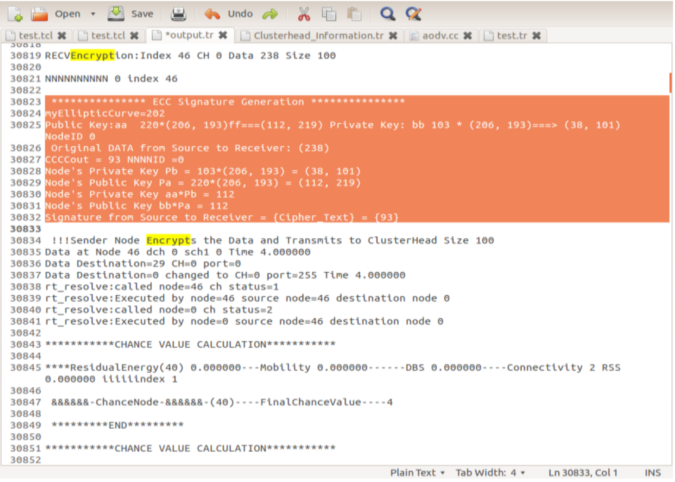

Fig. 8: Snapshot code for ECC signature generation by node 29.

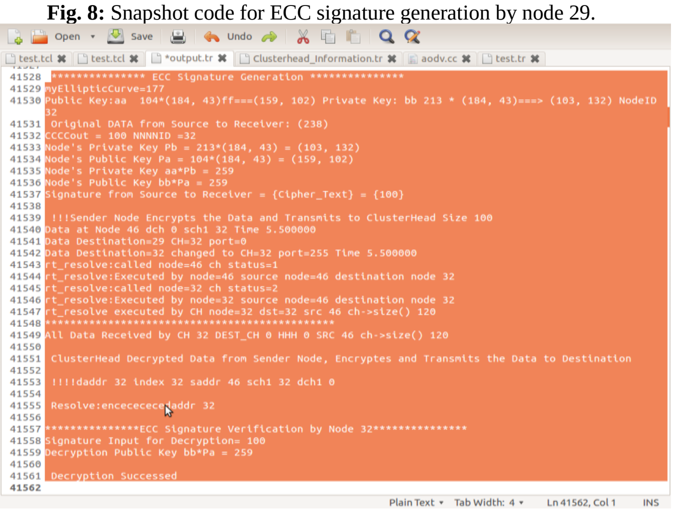

Fig. 9 Snapshot code for ECC signature generation and decryption by node 32.

On receiving the data, CH corresponding to sender decrypts it and encrypts again using the key for communicating with other CH. On receiving the encrypted data the cluster head corresponding to the receiver decrypts it and transfer it to the receiver.

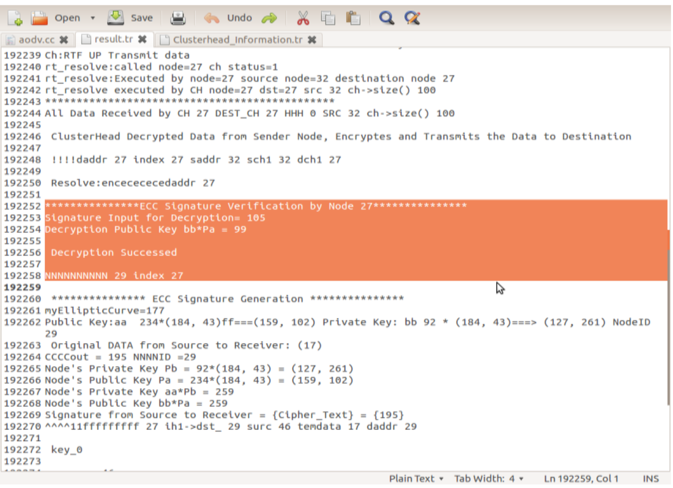

Fig. 10: Snapshot code for ECC signature generation and verification by node 27.

ECC signature generation and verification by node 27 is shown in the fig. 10. And received cluster head node receives the data from source node. This process will be continued till to reach the destination node and if the decrypted data is equal to original data, we can say that Decryption is successful. This process continued till to reach the destination node.

6.2 Group Key Generation and Secure Intra cluster Communication Using ECC

Each CH generates the key for the group and broadcast it to all its members. Whenever the data is transmitted to the member in same cluster, the data is encrypted using group key and transmitted. On receiving the data, it is decrypted by the member in the cluster. Snapshot of data transmission from source to destination node via intermediate routers (leaves) is shown in fig. 11.

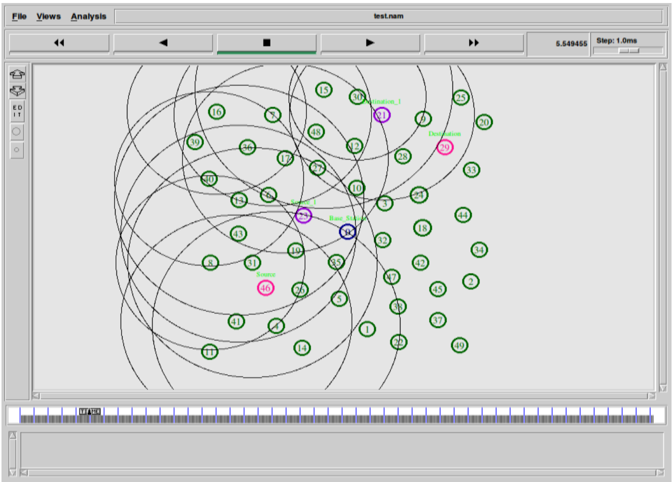

Fig. 11: Nam output showing data transmission from source to destination node via intermediate routers (leaves).

6.2.1 Key Exchange

Key exchange [27] can be done in the following manner. A large integer is picked and elliptic curve parameters a and b. This defines an elliptic curve group of points. Now, choose a base point $G=(x_1,y_1)$ in $E(a,b)$ whose order is a very large value n. The elliptic curve E and G are the parameters known to all participants. A key exchange between users A and B can be accomplished as follows:

1. A selects an integer n_A less than n. This is A's private key. A then generates a public key $P_A = n_A G$; the public key is a point on E.
2. B similarly selects a private key n_B and computes a public key $P_B = n_B G.$
3. A generates the secret key $K = n_A P_B$ and B generates the secret key $K = n_B P_A.$

The calculations in step 3 produce the same result. $K = n_A P_B = n_A(n_B G) = n_B(n_A G) = n_B P_A$. To break this scheme, an attacker would need to be able to compute k given G and kG, which is assumed to be hard.

6.2.2 Encryption using ECC

The plaintext message m is taken as input in the form of bits of varying length. This message m is encoded and is sent in the cryptographic system as x-y point P_m. This point is encrypted as cipher text and subsequently decrypted. As with the key exchange system, an encryption and decryption system requires a point G and an elliptic group $E(a,b)$ as parameters. User A selects a private key n_A and generates a public key $P_A = n_A G$. Similarly, user B selects a private key n_B and generates a public key. $P_B = n_B G$. To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the cipher text C_m consisting of pair of points $C_m = \{kG, P_m + kP_B\}$.

6.2.3 Decryption using ECC

To decrypt the cipher text, B multiples the first point in the pair by B's private key n_B and subtracts the result from the second point as shown by equation.

$$P_m + kP_B - n_B(kK) = P_m + k(n_B G) - n_B kG = P_m.$$

6.3 Group key generation and update: Cluster Member Leaves

Cluster members inform their cluster heads before leaving the cluster group and thereby cluster head permit the leaving members to leave. The cluster head automatically computes a new group key and distributes it to the members using unicast message encrypted with the public key of members. This is the reason that leaving members can not access the new group key. The cluster head reconstructs the hash tree without the leaving member and obtains the root hash value. These hash values are sent to the individual members encrypted with their respective public keys.

6.4 Group key generation and update: Cluster Head Leaves

It is the normal duty of the cluster head to sends a leave message to its own members and the other cluster heads before leaving the cluster. Upon receiving the leave message, the ordinary nodes and the cluster heads send a reply message to the leaving cluster heads. The cluster head delegates the role of the cluster head to the member that is having the smallest id and transfers all the information to this node. The new cluster head reconstructs the new hash tree for authentication among its members and also generates a new group key and sends it to members encrypted with their public keys. The cluster heads remove the leaving cluster heads entry and reconstruct the hash tree without the leaving cluster head and compute the new root value for authentication purpose. Consequently, cluster head with the lowest id regenerates the new group key and sends it the cluster heads encrypted with their respective public keys. If the cluster head is compromised and not leaving voluntarily, then the members in the cluster communicate with each other and elect the node having the smallest id as the cluster head and the whole process of initialization is repeated.
Source node 23 sends data to cluster head (32) which node forwards the data to destination node. Snapshot of sender node generates the hash value and forwards to destination node is show fig.12.

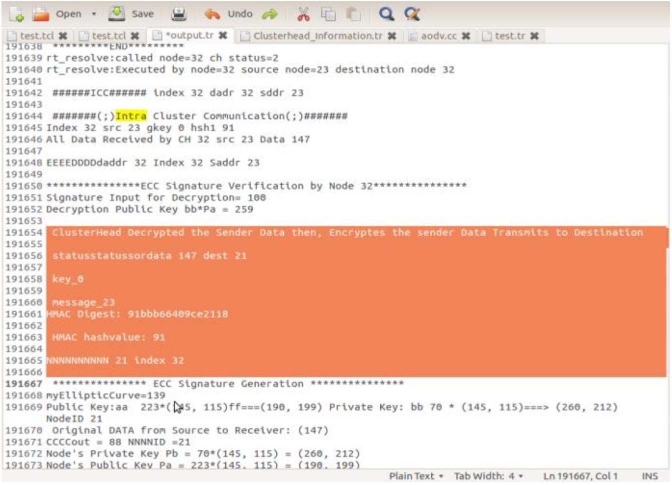

Fig.12: Snapshot code of for generation of hash value during intra cluster communication.

Cluster head received data from source node. Cluster head decrypted the sender data then, encrypts and transmits data to destination node. This process continued till to reach the destination node. Destination node (21) decrypted the received data from cluster head (32) via intermediate routers. Screenshot of ECC signature generation and Verification by node 23 is shown in fig. 13. And decryption is successful if decrypted data is similar with original data.

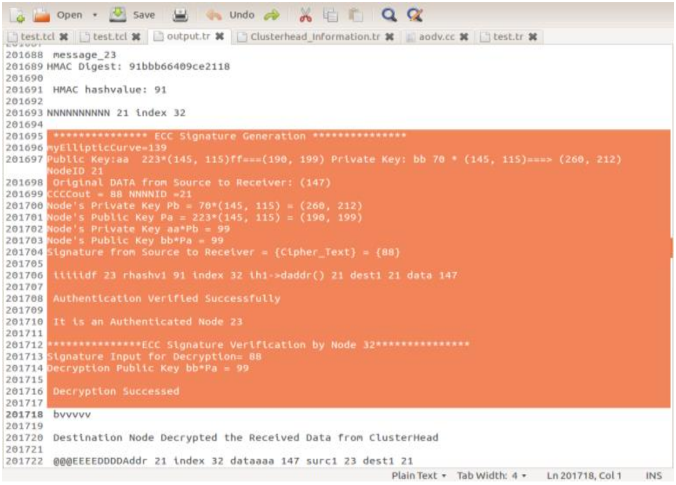

Fig.13: Snapshot code for ECC signature generation and verification by node 23.

7 Simulation Scenario

In this section, wireless network simulation scenario aimed at stimulating the network security through network average end to end delay, control overhead between the nodes within the scenario by using cryptography algorithms. In our simulation, we used HMAC algorithm to cipher package information that transfer between nodes. Existing energy based clustering key management (ECKMS) and fuzzy based clustering key management (FCKMS) scheme use elliptical curve cryptography in wireless sensor networks and methods are compared for the scenarios of varying number of flows. Totally 5simulation runs carried out for the 5 scenarios of varying number of flows as 1, 2, 3, 4, and 5. Simulation study has been made in order to realize the proposed approach for efficient key management. The simulation results show that new proposed scheme can save more energy during the computation of public key cryptography. The simulation environment is as given below. Table 4 shows the parameters list used in simulation scenario. Performances of existing energy based clustering key management scheme (ECKMS) and fuzzy based clustering key management scheme (FCKMS) are compared based on average end to end delay and control overhead. When the numbers of nodes are increased the delay is increased. The fuzzy based clustering scheme incurs decreased delay compared to existing energy based clustering scheme is shown in fig. 14.

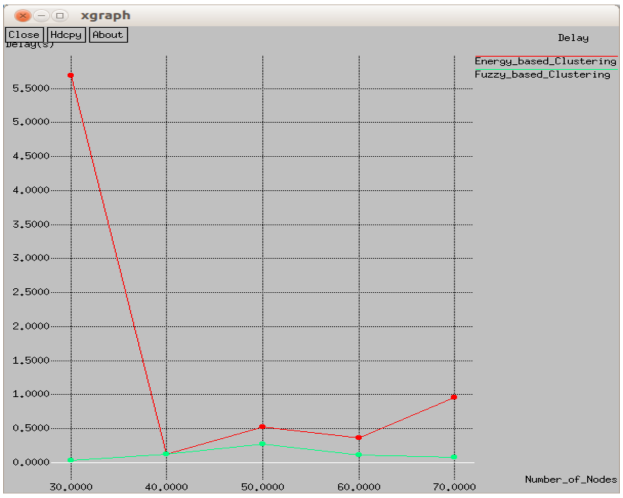

Fig.14: FCKMS achieves decreased delay when compared to ECKMS

When the numbers of nodes are increased, overhead is increased. The fuzzy based clustering scheme incurs decreased overhead compared to the existing energy based clustering scheme is shown in fig 15.

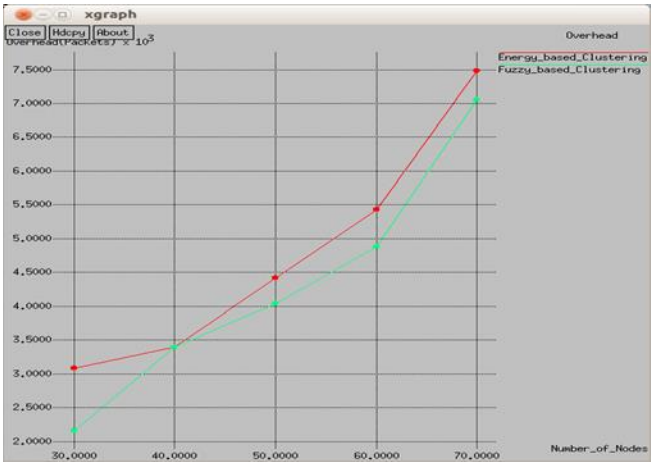

Fig. 15: FCKMS achieves reduced control overhead when compared to ECKMS.

8 Experimental Results and Performance Evaluation

Proposed technique is implemented by modifying AODV routing protocol files in NS2. Number of nodes can be varied as 30, 40, 50, 60 and 70. Performance is compared between proposed techniques with fuzzy based clustering technique with normal clustering. Ns2 is rebuilt with newly added protocol. Performance of the proposed FCKMS is evaluated for the simulation settings as per the following simulation model and compared with existing normal clustering. Metrics such end to end delay and control overhead computation are evaluated using awk script by analyzing trace file for the scenarios of varying number of nodes. Using the results obtained from awk script, graph is plotted for performance metrics using xgraph tool available in NS2.

Table 4: Simulation parameters

Parameter	Value
Simulation tool	Network Simulator 2
Number of Nodes	50
Area	600m x 600m
Communication Range	250m
Interface Type	Phy/WirelessPhy
Mac Type	IEEE 802.11
Queue Type	Droptail/Priority Queue
Queue Length	50 Packets
Antenna Type	Omni Antenna
Propagation Type	TwoRayGround
Routing Protocol	AODV
Transport Agent	UDP
Application Agent	CBR
Simulation Time	50seconds

8.1 Performance Metrics

In any network, secure communication is very important so there are possible chances of intruders, which may affect the network performance and security. To analyze the performance of implemented network, we consider the following two metrics:
i. Average end-to-end delay: It can be defined as the time taken by a packet to reach the appropriate destination from the source. It is difference between end time and start time.
ii. Control Overhead: It is the amount of control packets involved in routing process. i.e. Control overhead = Number of control packet.

8.2 Implementation Constraints

All nodes in single cluster will be in one hop and each cluster has number of members. Hence Clustering cannot be formed as binary tree. Hence the hashing for authentication can be followed by Hash tree construction. Therefore total number clusters will not be fixed as 2, 4, and 8. Numbers of clusters are decided based on topology dynamically. Hashing algorithm is applied for integrity verification (HMAC). ECC is applied for authentication with asymmetric.

9 Conclusion

This research work provides energy efficient clustering key management scheme using fuzzy logic. In the proposed architecture, there are two communication protocols for secure communication that is intra cluster communication and inter cluster communication. Hashing algorithm HMAC is use for authentication of nodes from source to destination through cluster head during data transfer. This scheme is based on logical key hierarchy because in this group members are arranged in hierarchical manner with cluster formation. Elliptic curve cryptography key agreement is introduced in asymmetric key management. Elliptic curve cryptography provides much stronger security with smaller key size than RSA. It is the elliptic curve cryptography that reduced the key size, thus reducing the re-keying process and re-distribution cost which further reduced the computation and communication costs respectively. Therefore elliptic curve digital signature algorithm (ECDSA) can be used for verification purpose. It can be ensured that, providing such an authentication and verification facility provide more secure system. It can be conclude that proposed system can provide individual authentication to the entire sensors node in the network.

References

[1] J. Zhang and V. Varadharajan. Wireless sensor network key management survey and taxonomy.Journal of network and Computer Applications,vol.33,no. 2,2010, pp.63-75.

[2] W.Heinzelman,A. Chandrakasan, and H. Balakrishnan. energy-efficeint communication protocol for WSN.In Proc. Of the 33rd Hawaii international Conference on System Sciences,Washington 2000.
[3] A.A. Aziz, Y.A. Sekercioglu, P. Fitzpartrick and M.Ivanovich.A Survey on Distributed Topology control techniques for Extending the Lifetime of Battery Powered wireless sensor Networks.Communications Surveys & Tutorials, IEEE, vol. 15, (2013),pp,121-144.
[4] N.M.Saravana Kumar and Dr T.Purusothaman. SEGKMS:Scalable and Efficient Group Key Management Scheme in Multicast Networks.European journal of 2012.
[5] Pitipatana, S., A. Nirwan. Elliptic Curve Cryptosystem-Based Group Key Management For secure Group Communications, IEEE Military Communications Conference doi: 10.1109/MILCOM. 2007.pp. 445-502.
[6] S.Jabeen Begum and Dr.T.Purosothaman. A New Scalable and Reliable Cost Effective Key Agreement Protocol for Secure Group Communication.Journal of Computer Science 7(3): 2011, pp.328-340.
[7] M. Rahman and K. El-Khatib. Private key agreement and secure communication for heterogeneous sensor networks.J. Parallel Distrib.Comput.,vol. 70, no. 8, pp. 858–870, 2010.
[8] S Jabeenbegum, T Purusothaman. A Cluster Based Cost Efective Contributory Key Agreement Protocol for Secure Group Communication.IEEE Second International conference on Computing, Communication and Networking, 2010,pp,1-12.
[9] Priyanka laiswal, Abhimanyu Kumar, Sachin Tripathi . Design of secure group key agreement protocol using elliptic curve cryptography.High Performance Computing and Applications (ICHPCA), International Conference,1 – 6. December 2014,pp. 22-24.
[10] D. Wallner, E. Harder and R. Agee.Key Management for Multicast: Issues and Architectures.Technical Report RFC 2627, Internet Engineering Task Force,1999.
[11] Wong, C.K., M.Gouda and S.S.Lam. Secure Group Communications Using Key Graphs.Proc. ACM SIGCOMM. Vancouver, Canada, September 1998, pp. 68–79.
[12] Sherman, A.T. and McGrew, D.A.Key establishment in large dynamic groups using one-way function trees,IEEE Trans. Softw. Eng.29, 2003,pp. 444–458.
[13] Heeyoul Kim, Seong-min Hong,H.Yoon and J.W.Cho.Secure Group Communication with Multiplicative One-way Functions. Proc IEEE International Conference on Information Technology:-Coding and Computing,2005, pp. 1-6.
[14] Yi-Ruei Chen and Wen-Guey Tzeng. Efficient and Provably- Secure Group Key Management Scheme Using Key Derivation.IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012,pp. 295-300.
[15] Lin, I.C., S.S. Tang and C.M. Wang . Multicast key management without rekeying processes.Comput. J., 53: 2010,pp. 940-950.
[16] R.L. Rivest,A.Shamir,and L. Adleman.A method for obtaining digital signatures and public-key cryptosystems,Commun. ACM, 21, 1978,pp.120–126.
[17] Saravanan, K. and T. Purusothaman. Efficient Star Topology based Multicast Key Management Algorithm.Journal of Computer Science 8 (6),2012,pp. 951-956.
[18] M.Shainika and Mrs.C.Hema.Cluster Based Mobile Key Management Scheme to Improve Scalability and Mobility in Wireless Sensor Networks.National Conference on Research Advances in Communication, Computation, Electrical Science and Structures (NCRACCESS-2015),pp.22-26.
[19] Jyothi Metan and K N Narasimha Murthy. Group Key Management Technique based on Logic- Key Tree in the Field of Wireless Sensor Network.International Journal ofComputer Applications,Volume 117 – No.12, May 2015,pp.0975 – 8887.
[20] X. Wanga, P. Lia, Y. Suia, and H. Yanga. A Hexagon-based Key Predistribution Scheme for Wireless Sensor Networks. Journal of Information & Computational Science,Vol. 11 (8), 2014,pp. 2479- 2491.
[21] X. Zhang, J. He, and Q. Wei. EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks.EURASIPJ Wireless Commun. Netw.,vol. 2011, Jan 2011,pp. 1–11.
[22] A Naureen, K Kim, F Ahmed. Performance and Security Assessment of a PKC Based Key Management Scheme for Hierarchical Sensor Networks.IEEE Commu-nication, 2008, pp.163-167.
[23] Burnett, S. and Paine, S., RSA Security’s Official Guide to Cryptography,RSA Press,2001.
[24] Y. Kim, A.Perrig and G.Tsudik. Simple and faulttolerant key agreement for dynamic collaborative groups.Proc. 7th ACM Conference on Computer and Communications Security, ACM Press, 2000, pp.235–244.
[25] Bing Wu, Jie Wuand Yuhong Dong. An efficient group key management scheme for mobile ad hoc networks.Int. J. Security and Networks,2008.
[26] V.Vasudevan and Joe Prathap ,P.M .Analysis of the various key management algorithms and new proposal in the secure multicast communications research paper,2009.
[27] Usham Robinchandra Singh, Sudipta Roy, Soram Ranbir Singh. A Brief Analysis on Key Management Schemes Using Elliptic Curve Cryptography in Wireless Sensor Network, International Journal of Engineering Science Invention,Volume 3 Issue 7, 2014, pp.57-70.