International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 11, Issue 3, March 2020, pp. 91-107, Article ID: IJARET_11_03_008
Available online at http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=3
Journal Impact Factor (2020): 10.9475 (Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

SIGNCRYPTION BASED HYPER ELLIPTICAL CUREVE CRYPTOGRAPHY FRAMEWORK FOR KEY ESCROW IN MANET

B. Vanathy
Research Scholar, School of Information Technology,
Madurai Kamaraj University, Madurai, Tamilnadu, India

M. Ramakrishnan
Professor and Head, School of Information Technology,
Madurai Kamaraj University, Madurai, Tamilnadu, India

ABSTRACT

Hyper elliptical curve cryptography is the prominent public key encrypto systems with practical approach to high level of security and shorter bit size of encryption. Public key encryption is a reliable cryptographic method for mobile adhoc networks. Still, some shortcomings of key management deter the reputation of its utilization in the real-time environment. One major disadvantage in the crucial necessity of elucidation is the key escrow problem. For secure group-based data transmission in the distributed environment, a secret key has to be shared among the users for the secured data transmission. For establishing efficient key distribution and management, a novel dynamic group secret key management is introduced. In this paper, we propose a signcryption based hyper elliptic curve cryptography framework for key escrow. Here the model of scheme is to divide a large group into several subgroups, each maintaining its subgroup secret keys to control the subgroup and managing many subgroups using Key Escrow Based Hyper Elliptic Curve Cryptography management algorithm. In the paper, a new methodology for collaborative key management using signcryption is implemented. The environment for mobile networks with the proposed algorithm named signcryption based Key Escrow HECC for Signcryption (KEHECCS) with a comparison of the conventional algorithms prevailing for MANETs is simulated. Compared to the existing approaches, KEHECCS demonstrates advanced key distribution features with better throughput efficiency without compromising on communication overhead and storage cost.

Keywords: Hyper Elliptic curve cryptography, Key escrow, MANET, Public key management, Short bit size, Signcryption, Security

Cite this Article: B. Vanathy and M. Ramakrishnan, Signcryption based Hyper Elliptical Cureve Cryptography Framework for Key Escrow in MANET, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 11 (3), 2020, pp 91-107.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=3

1. INTRODUCTION

With the progress and pervasiveness of wireless mobile networks, data communication and mobile computing technologies have frolicked a significant role in the day to day life. The communication has evolved from humans to machines, lead to the advancement of the Internet of Things (IoT). Yet, some probable security menaces such as information revelation, variation and distinctiveness impression always occur during effective communication. Conventionally, cryptographic measures are most generally exploited solutions.

Information and communication technology based real-time applications are growing at a very rapid phase. In such a network scenario, secured data communication over wireless channels becomes a task of paramount significance. Mobile Adhoc Networks is one, in which the dynamic number of nodes can join and withdraw during the data transfer mechanisms. Such topology is very much essential for the random environment with integrated internet and information domain. The typical mobile adhoc network with dynamic data transfer communication between source and destination is shown in Figure 1.

Figure 1 Mobile Adhoc Network Establishment

In wide range mobile adhoc network establishment, there are chances of various types of attacks. In such a scenario, cryptography is the concept to overcome untoward malicious activities and ensure the security of the nodes as well as the ongoing data communication. While encrypted data is hard to decipher, it is comparatively easy to detect. Physically powerful encryption algorithms and proper key management techniques for the systems will helps in achieving confidentiality, authentication and integrity of data. In this research work, various encryption (symmetric and asymmetric) algorithms have been evaluated. This describes cryptography by incorporating key management related to data encryption based on performance metrics such as Security and Time constraints.

The same key is used for both encryption and decryption of messages. Some symmetric key algorithms are DES, 3DES, AES, RC2, RC6. Data Encryption Standard (DES) divides the unique message into 64-bit blocks. Each block is then permutated to transform the order of its bits. Two 28-bit halves are divided by 56-bit key. Each half is than circular-shirted to the left, reconnected and enlarged to 48 bits and the half in right plaintext blocks is also extended to 48-bits.

Triple Data Encryption Standard (3DES) Triple DES takes 3 iterations of DES efficiently encrypting data with a 168-bit key which is very well-built for securing the sensitive message. The 56-bit DES key used for encrypting the data first, then another 56-bit DES key is for decrypting, and finally the original 56-bit DES key is used for encrypting again. 3 DES contains more levels of encryption and it can better protect against middle attacks.

Advanced Encryption Standard (AES) AES algorithm uses 128 bits block size. A key length is a dependent relative on a number of AES parameters. For example, if the key size used is 192, the number of rounds is 12 whereas it is 14 for 256 bits correspondingly. It is noted that, if there are longer keys, it is difficult to crack, but it will take more time for computation.

In Asymmetric Encryption there are two different keys are used for both encryption and decryption of the message. Some asymmetric algorithms are Rivest Shamir Adleman (RSA), Diffie- Hellman, and Digital Signature Algorithm (DSA). The two different keys are used for public cryptography namely, private key and public key. The public key is accessible but the private key is kept secret.

Diffie–Hellman Algorithm is one of the precise methods of exchanging cryptographic keys proposed in 1976. It transmits bits to sender and receiver that have no prior knowledge of each other to jointly establish a shared secret key over an unsecured communications channel.

RSA algorithm has two keys (public and private). Both private and public keys will be used for encryption and decryption process. The sender will encrypt the data using the receiver's public key and the receiver will decrypt the data using his own private key. It uses two prime numbers for generating a private key and public key. The security of RSA depends on the product of these two numbers which is represented by n.

Digital Signature Algorithm (DSA) is a public key cryptographic algorithm designed for authenticating the digital message. A data is signed by a secret key to produce a signature, and then this is verified against the message by a public key. Anyone in the network can check the signatures whereas the only one with the secret key can sign the messages.

The concept of Hyper Elliptical curve cryptography (HECC) was first suggested by Miller and Koblitz, way back in 1989. HECC is the extent of Elliptical curve cryptography. The retreat of hyper elliptic curve cryptography deceits on the distinct logarithm problem and solution in the jacobian of the curve. The implementation of signcryption mechanisms using HECC provides the secured encryption system with lesser unit of grouping band and shorter bit size when compared to traditional Elliptical curve cryptography.

2. LITERATURE REVIEW

A proficient key organization structure for fortified communication access mechanism in wireless broadcast networks is presented using the Key Tree Reuse scheme [1]. In order to deliver secure communication in wireless broadcast networks, symmetric key mechanisms are used, in which the authenticated users alone can decrypt the data. Key Tree Reuse scheme is efficient in handling complex key distribution structures and multiple user activities.

Provision of high-level security for the smart grid design in the data communication is effected by enhanced key identity oriented cryptography [2]. This scheme affords dual tenacity of not only preventing critical attacks but also reduces management overhead. The enhanced competence for key management is apprehended by intermittently invigorating all public and private key pairs as well as the key initiator entity.

The usage of public key procedures in power controlled Adhoc network environments is predominant for group communications. The protocol for deriving user session keys from

master keys for instituting a group key is presented [3]. Polynomial time computation to maximum possible approximation to optimum is achieved. Also, the computational necessities with respect to multi-party leeway of Diffie-Hellman key transfer are also compared.

Internet of Things (IoT) is a gigantic network that acquaintances various objects and empowers data communication in combination with the Internet. In several circumstances, the data information received from the IoT devices is diversely distributed. So, the classification of such data becomes essential for meaningful data processing. The transformation of original general approaches to point value classification based on sampling method is presented [4]. The distribution parameters are estimated using a Bayesian approach and standard benchmarks are established.

The overall introduction about sensitive information transmission through a public network and the establishment of authentication through key escrow mechanisms are presented [5]. The description of the escrowed encryption methodology and specific emphasis on secured data transfer is discussed.

Key Escrow mechanism for time-limited observation through one way communication is studied [6]. An innovative monitoring system is developed focusing on the communication type and other vital properties. A tool for non-interactive key renewal with threshold warrant bound is used for analysis key management scheme.

Public Key Encryption along with keyword search is an essential measure of searchable encryption. It is well practiced in data security and operability of encrypted data [7]. Certificateless cryptography is an efficient tool for removing inherent problems in public key management. Information retrieval domain data are extensively used to test adaptive keyword attacks. The measure provides a better solution for the key escrow problem and improves efficiency.

An arbitrated certificate less encryption mechanism without pairing processes for secretly distributing profound data in public cloud environments is presented [8]. The framework works on two schemes, first, the establishment of mediated certificate-less public key cryptography without pairing operations and then, constructing a feasible solution for sharing sensitive information over the cloud environment. The security and efficiency of the network found to improvise using the implementation of mediated certificate-less public key cryptography.

Public key infrastructures are offered to deliver numerous security measures. Some of the security measures including privacy need key escrow in certain situations, whereas in some other measures such as non-negation and confirmation normally proscribe key escrow [9]. A novel method using revocable identities to upkeep key escrow is proposed to assimilate the integral key escrow of encryption based on identity into public key infrastructures. This is an effective certificate based solution for public key management.

The explosion of large-scale disseminated file systems serving for various storage devices ranging from parallel access to multi-level storages leads to the problem of secure key establishment in data communication [10]. The process of network file systems which utilizes Kerberos for the establishment of keys in parallel session in between users and storage expedients. The workload of the metadata server and concomitantly supporting onward privacy is drastically reduced by the implementation of the authenticated key exchange protocols.

Attribute-based encryption upkeeps the precise distribution of encrypted data. In certain common strategies, these attribute-based aspects are accomplished by a responsible authority

[11]. The concept of attribute-based access mechanism scheme addresses key escrow problem and access encrypted data which enhances effectual user revocation.

Recently, Bitcoin has been marketed as decentralized crypto-currency by means of pseudonym to accomplish concealment. Inappropriately, a noted pivotal work has confirmed that Bitcoin only provides weak concealment [12]. A comprehensive decentralized mechanism for providing complete anonymity to bitcoin using secured escrow address is presented. The protocol is secured against probable malicious adversaries. The users can jointly accomplish the procedure and efficaciously realize the transaction without any trusted third party applications and additional charges.

Chipertext feature based encryption policy is one of the effective cryptographic practice for fine-tuned access control of external data in the cloud [13]. But, one of the major drawbacks is the need for the solution of the key escrow problem. A comprehensive key management mechanism which comprehends disseminated group, issue and storing of private keys without adding any additional infrastructure is presented. This method solves both key escrow problem and reduction of client overhead due to decryption [14].

The commonly embraced public key cryptography mechanism is Certificateless public key cryptography [15]. Certificateless implementation resolves issues related to key escrow and untrusted notifications. Some distinct deviations of digital signatures whose legitimacy can only be persuaded by a designated verifier are incorporated in the Certificateless implementation for achieving shorter lengths in signature and reduction in computational cost [16].

In mobile Adhoc environments, encryption based on signcryption measures is popularly considered as a proficient solution to one too many and many to many data communication [17]. This facilitates the source to securely transfer data to the multiple destinations in synchronization with the single logic operation. Only the accredited destinations can decrypt the data self-reliant. The concept of Certificateless cryptography with signcryption resolves key escrow problem [18]. The implementation also provides improvisation in system efficiency and receiver anonymity.

One of the primary operations of the Internet of Things is data aggregation. Effectively preserving the privacy of sensitive data during data aggregation in the fog environment is a critical issue [19]. Anonymous privacy-preserving scheme guarantees pseudonym and local certification authority. The implementation also pledges low computational complexity and overhead.

For achieving betterment in the security and privacy protection in the mobile networks, plentiful encryption mechanisms based on multi-receiver identity with bilinear pairing are proposed [20]. To avoid key escrow problems in such systems, Certificateless anonymous multi-receiver based encryption scheme is implemented. The runtime generation of ciphertext is much improved in the system and hence results in better confidentiality and receiver anonymity.

To establish the collaborative key management scheme based on key escrow and elliptical curve cryptography, the author has presented various strategic implementation combining the metric in Mobile Adhoc networks. The comparative assessment of identity based public key cryptography and public key infrastructure is presented. A novel approach for Certificateless cryptography using identity-based key management for secret key distribution is analyzed [21].

The enhancement of Certificateless Signature based on elliptical curve cryptography in IoT based mobile devices have gained principal attention in the dynamic wireless domain. The innovation principle of mystery division matching based Certificateless Signature without

the use of hash capacity and blending is implemented [22]. Performance valuation and association employing research exploration validate the improvisation of the certificateless measures when compared to traditional methods in the various system environments.

HECC is an innovative and speed based public key cryptosystem. It is much loftier in security parameters and solicitation competence. The concept of analysing blind signature using probabilistic encryption and blinding process is improvised using using HECC [23]. Hyper Elliptical Curve cryptography has advantages compared to the traditional public key encryption systems. The problematic solution of computational complexity theory is explained using HECC. With the shortened operating parameters, the same level of security level can be achieved. HECC with finite field of x bits is equivalent to traditional elliptical curve cryptography with finite field of 3x bits. Also the secure Jacobian group set with larger prime number order can be designed with a comparatively lesser basic field using HECC.

Multiple reserve proficient Signcryption Schemes with advancing secrecy based on HECC is proposed [24]. For any wireless mobile networks, the secrecy of the transmitted data is our prime concern. The concealment and the legitimacy of the network resources can be strengthened by the use of HECC based digital signcryption mechanisms. The concept of forward secrecy is implemented in two different signcryption mechanisms using HECC.

Hyper elliptic curve cryptography are best suited for resource controlled situations as it affords secrecy, remembrance, non-negation, forward privacy and public verifiability while employing low possessions, the foremost cause of non-acquisition of reputation is its probabilistic outcomes and double extension of information. Signcryption mechanisms can overwhelm the existing situation. It offers both the features of digital signature and encryption with a substantial resource handling than the existing techniques using signature algorithms and encryption mechanisms.

A proficient certification method implementing Hyper Elliptic Curve Cryptography (HECC) is proposed in [25]. A novel mechanism of message security using instant messaging with an effectual certification method to guarantee user validity is utilized. The certification user with key pair logic and communication mechanism is used for instant messaging to uplift the sanctuary level of data information. By using HECC algorithm, the system of encryption-decryption with the minimum short duration of group g=2 is achieved. The validation results shows that using this approach, the effective communication with secret instant messaging is realised.

Detailed review of various signcryption based hyper elliptical curve system is proposed in [26].Reduction of communication and computational overheads are achieved with the help of signcryption based HECC in this paper. The method is best suited for bandwidth restriction and low power computing.

3. PROPOSED METHODOLOGY

In cryptography, signcryption is a basic public-key entity which concurrently accomplishes the purposes of both digital signature and encryption. Encryption and digital signature are two essential cryptographic gears that can promise privacy, reliability, and non-negation. Signcryption is a fairly new cryptographic mechanism which establishes the system accomplishment in a unified logical expression. Signcryption meritoriously reduces storage costs and communication overheads when compared to conventional encryption and signature measures. Hyper Elliptical curve cryptography provides better security with shorter bit size and lesser computational cost. HECC based signcryption and the designcryption schematic is shown in figure 2.

A standard signcryption scheme entails of three phases, viz. key generation (KG), hyper elliptical curve signcryption (HSC) and designcryption (HDSC).

The HECC based signcryption scheme processes (hssp) can be defined from the following representation.

$$hssp=(KG, HSC, HDSC) \quad (1)$$

where the hyper elliptical curve is a unique type of non-singular curve expression with partial derivatives of non-vanishing equation for given group g>=1 satisfying the following criteria

$$H(X)=y^2+h(x)Y \quad (2)$$

- For the given user, the pair of keys are generated in the key generation phase, associated with security metric.
- For any message, signcryption is obtained by plain text message (tm), private signing key of the source (psk_s), public encryption key of the destination (pek_d). The signcrypted text (t) is given as follows:

$$t \leftarrow HSC(tm, psk_s, pek_d) \quad (3)$$

- Designcryption is the deterministic value representation with private signing key of the destination, (psk_s), public encryption key of the source (pek_d), given user (u), invalid result of designcryption (inv) and signcrypted text (t) is given as follows:

$$mU(inv) \leftarrow HDSC(t, psk_d, pek_s) \quad (4)$$

Thus, the entire Hyper Elliptical curve based Signcryption scheme can be consistently verified by giving two dissimilar mathematical functions, digital signature and encryption. The option of privacy and truthfulness would depend on the level of security anticipated by elliptical curve cryptography for key escrow in a MANET environment.

The usage of internet is very complex in information and communication technologies. Thus the use of Hyper Elliptic curve cryptography (HECC) for signcryption is the best method to provide authentication in key management scheme. This is a public key cryptosystem and it is used to create smaller, faster, and more efficient cryptographic keys. ECC authentication scheme is more suitable for wireless applications where the data is more confidentiality. It uses a smaller key size and low computational system requirements. The low processing power associated with ECC authentication scheme is to make suitable for use with secret key id (SECID) tags because they have consuming limited computing power

Signcryption based Hyper Elliptical curve cryptography (HECC) is a collaborative system with public key encryption technique. This is based on the elliptic curve concept in which more efficient Cryptographic keys are generated to provide a certification scheme to SECID system. Previous research describes that the security level that is provided by RSA and ECC, using HECC that same security can be provided but using smaller key size. Research proves that using RSA algorithm that same security level can be achieved using 1024 bits key size but using ECC require only 160 bits key size and for HECC it requires barest minimum of 52 bits. HECC algorithm can be implemented on the minimum size of SECID tags. So HECC authentication scheme is well suited for wireless applications. HECC point of a multiplication operation is more computationally effective than ECC and RSA using fast and efficient computational time. There are two types of attacks in cryptography in which we have to provide security to the system

Active Attack: Attacker can send previous manipulated messages or it can be deleted.

Passive Attack: In the case of passive attacks, the attacker can interrupt and make statistics about communication. The detection of these attacks is difficult, so the goal is to prevent them.

A SECID authentication scheme includes three main parts:

(1)The SECID tag

(2) The SECID reader

(3)The server

To implement certification already predefined between the tag and the reader when the system is firstly arranged. The interruption can easily occur in the wireless channel during data transmission. So to prevent data proper certification scheme is needed between SECID tag reader and SECID server.

Signcryption based Hyper Elliptic curve Cryptography certification scheme offers significantly better data security for a given key size. If the key size is smaller it is also feasible to implement for a given level of security so that it consumes less power and less heat construction. The less significant key size makes faster cryptographic operations, running on the smaller chip and on more compressed software in [6].

So for data security, HECC is the great choice for the following reasons:

1.HECC provides better security of given key size

2.By using smaller keys it makes more compressed implementation, high-speed cryptographic operations.

3.Less heat construction and less power consumption.

4. In HECC, there is efficient and compressed hardware implementation

5.It is almost impossible to find private key so it is not potential for the third party to obtain the secret.

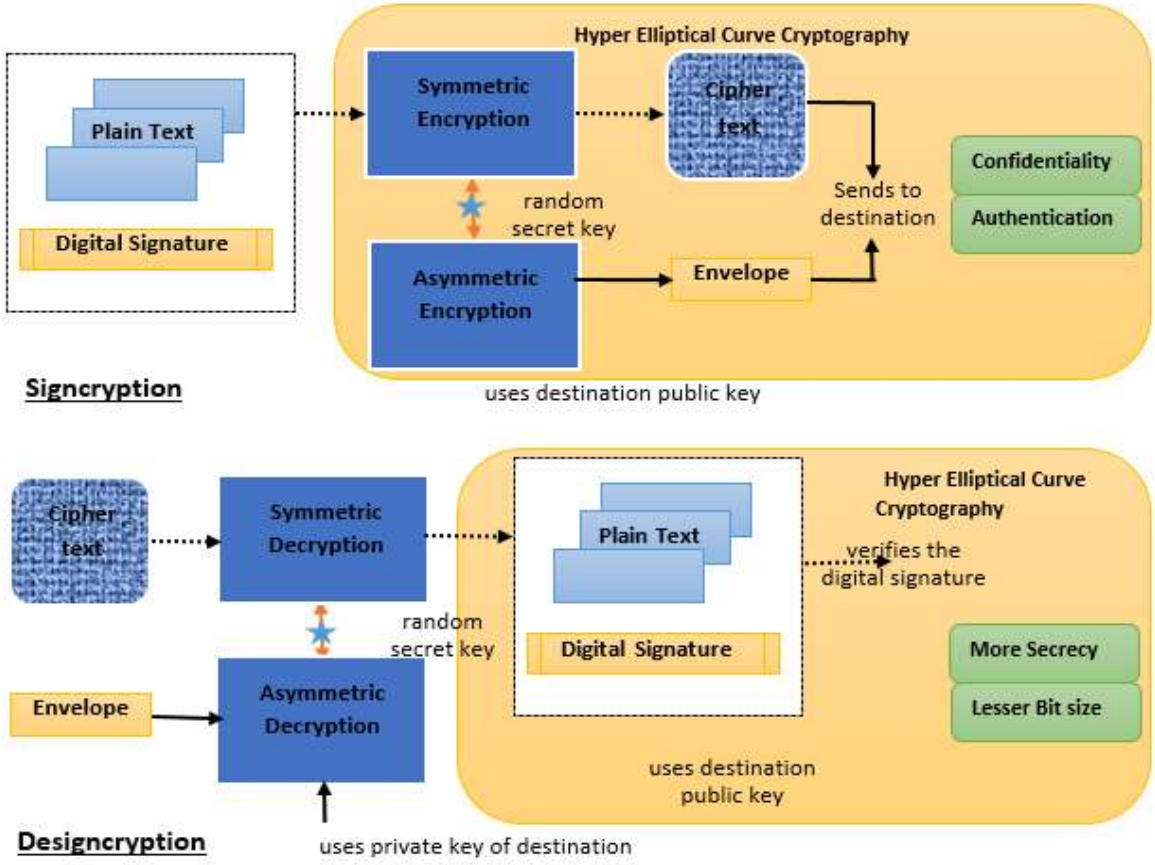

Figure 2 Signcryption and Designcyrption Schematic using Hyper Elliptical Curve Cryptography

Our proposed hyper elliptic curve distributed key management scheme achieves the correctness and secrecy requirements necessary to provide a distributed key generation protocol based on HECC. In this section, a security analysis of the proposed scheme is presented.

1) **Correctness**: The session secret key is uniformly distributed, and the corresponding session public secret key is uniformly distributed since the determination of whether the nodes participating in the node id key generation algorithm are honest or not depends on public broadcast information. All subset secret shares provided by any honest t +1nodes done the same secret key. All honest nodes have the same value as the node secret public key.

2) **Secrecy:** At least t +1server nodes need to cooperate in issuing a secret key certificate for a new ordinary node since only server nodes hold the shares of the CA secret key which is necessary to generate a partial CA signature for the certificate of the new ordinary node. No subset of less than t+1nodes can recover the session secret key. When a node receives its session secret key share, it can verify the received secret share by checking if it satisfies the algorithm in the session key generation algorithm. A new ordinary node cannot receive the previous keying information before joining the network. A new ordinary node can just send and receive secret information to any other node in the session after it joins the network which rejects the forward secrecy of the proposed scheme. When a mobile node leaves the session, a session key refreshing algorithm will be performed which prevent the leaving node to receive any keying information after it leaves the network which rejects the backward secrecy of the existing scheme.

4. SYSTEM MODEL

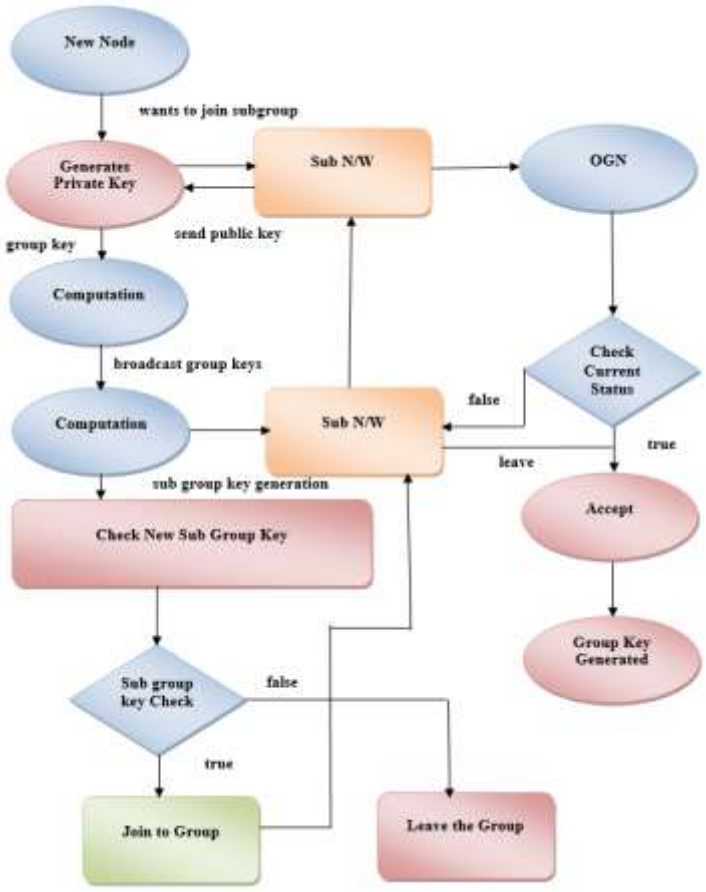

Figure 3 Algorithm for Signcryption based Hyper Elliptical Curve Cryptography Framework for MANET

In our scheme, there are two protocols namely, SSKG and GSKG. These two algorithms develop two secret keys which are used within the subgroup and in the external group respectively. These two algorithms are effective after finding the group secret key mobile node or checker for the subgroup and for the external group in the distributed environment. Using the power of the mobile node, the stability can be calculated in this scheme. This scheme is designed for the little authority mobile in the distributed network. The flowchart for the system model is presented in Figure 3.

In the present work, distributed key management protocol based on key escrow and hyper elliptic curve cryptography has been analyzed. From the results, our proposed scheme has moderate timings. It shows that timing does not vary significantly with changing the key size. It proves the suitability of the proposed scheme for applications where the devices are resource constrained such as in the mobile ad hoc environments. Simulations show that our proposed scheme is robust in the mobility environment of Mobile networks.

5. PERFORMANCE ANALYSIS

In the collaborative framework, two protocols namely, Subgroup Secret Key Generation (SSKG) and Group Secret Key Generation (GSKG) based on ECDH for subgroups and outer groups respectively are implemented. The keys belonging to the subgroup and other group keys have to be changed, whenever there is a change in membership (such as the occurrence of the current member leaving or the new member joining). The distributed key management protocol based on key escrow and hyper elliptic curve cryptography has been analyzed. When the gateway node of subgroups leave and new gateway node enters into the external group in the network, secured key management analysis is executed. In general, mobile nodes require smaller secret key sizes and smaller memory requirement for effective performance and throughput. With the implementation of the proposed signcryption based KEHECCS algorithm, the mobile network environment is simulated to measure the performances based on the metrics, Storage Cost, Communication Overhead and Throughput Efficiency.

Storage Cost: Storage cost is defined as the memory required for storing the data in the secured data transmission path in a distributed mobile environment. While sharing the secret key among the group nodes, the storage cost has to be less for the system. In the simulation analysis, the mobile network with Collaborative Key Management environment, the implementation of signcryption based KEHECCS is compared with the other traditional algorithms like AES and Elliptical Curve Cryptography (ECC). The simulation results prove that signcryption based KEHECCS has less storage cost when compared to AES and ECC. In our group key management protocol, the keys are stored by group nodes for that group only. But in other existing approaches, each node has to maintain the secret keys of its leaf nodes and so on. So our approach consumes very low memory storage cost than AES and ECC based approaches. Storage Cost is measured in terms of bits spent with respect to the simulation time. The graphical representation of the storage cost analysis is shown in Figure 4 and the tabulated values are charted in Table 1.

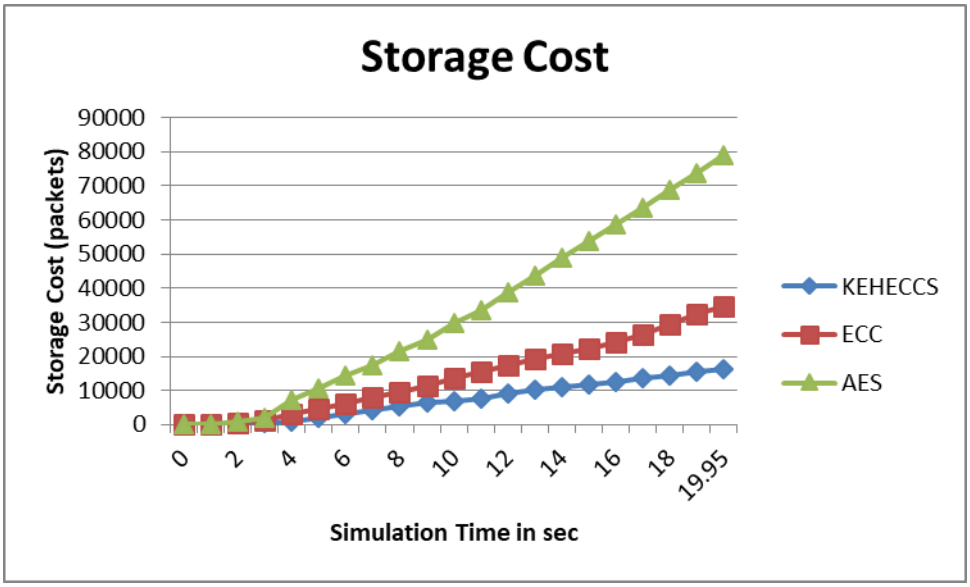

Figure 4 Storage cost

Table 1 Storage Cost

Time	KEHECCS	ECC	AES
0	0	0	0
1	0	0	0
2	171.4286	520	960
3	445.7143	1080	2080
4	1040	2940	7240
5	2091.429	4760	10800
6	3097.143	6160	14520
7	4285.714	7940	17200
8	5348.571	9560	21440
9	6342.857	11520	24960
10	6845.714	13520	29680
11	7748.571	15480	33600
12	9222.857	17400	38680
13	10182.86	19140	43600
14	11051.43	20680	49040
15	11817.14	22300	53760
16	12651.43	24200	58640
17	13542.86	26440	63680
18	14377.14	29260	68720
19	15314.29	32200	73720
19.95	16262.86	34740	78880

Communication Overhead: Under pragmatic data transfer and mobility circumstances, the secret key distribution procedures should minimize communication overhead to have better performance. The encumbrance occurred during the secret key sharing among the group nodes and between group and gateway nodes lead to communication overhead. In our proposed scheme, the communication overhead for the subgroup secret key members and for gateway nodes is very less when compared to the existing procedures like AES and ECC algorithms. There are two costs are involved: communication overhead for joining and communication cost for leaving. Communication overhead is determined by the number of

nodes join or leave from the subgroup. If there is a number of such users, the communication overhead is high. In our approach, we restrict the number of nodes in a subgroup and number of subgroups. We achieve better performance in our approach. The graphical representation of communication overhead comparison between various algorithms is presented in Figure 5 and tabulate values are shown in Table 2.

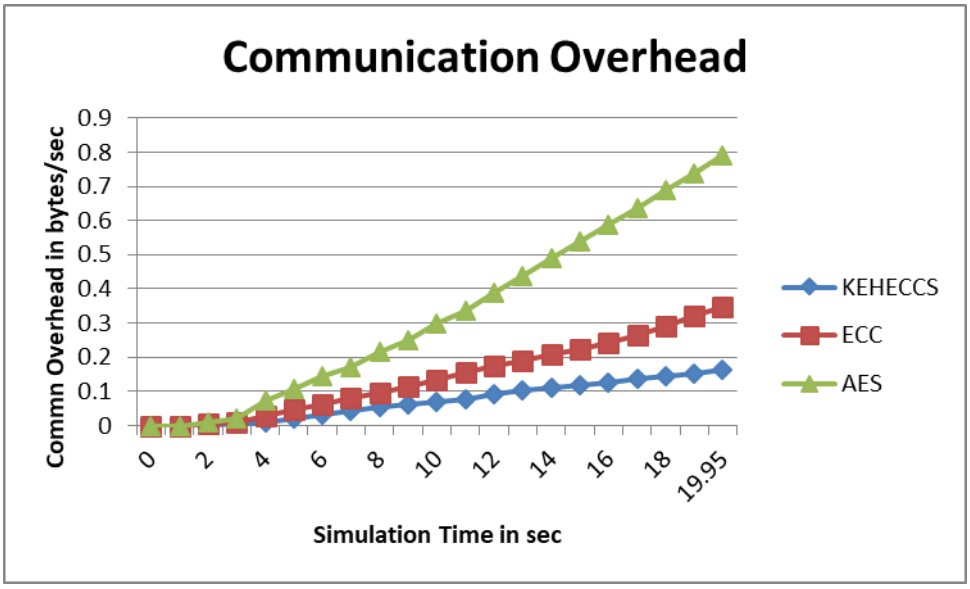

Figure 5 Communication Overhead

Table 2 Communication Overhead

Time	KEHECCS	ECC	AES
0	0	0	0
1	0	0	0
2	0.001714	0.0052	0.0096
3	0.004457	0.0108	0.0208
4	0.0104	0.0294	0.0724
5	0.020914	0.0476	0.108
6	0.030971	0.0616	0.1452
7	0.042857	0.0794	0.172
8	0.053486	0.0956	0.2144
9	0.063429	0.1152	0.2496
10	0.068457	0.1352	0.2968
11	0.077486	0.1548	0.336
12	0.092229	0.174	0.3868
13	0.101829	0.1914	0.436
14	0.110514	0.2068	0.4904
15	0.118171	0.223	0.5376
16	0.126514	0.242	0.5864
17	0.135429	0.2644	0.6368
18	0.143771	0.2926	0.6872
19	0.153143	0.322	0.7372
19.95	0.162629	0.3474	0.7888

Packet Delivery Ratio: The system performance is measured in terms of the number of successful packets transmitter over a period of time. Packet Delivery Ratio is defined as the packets transferred successfully in the mobile environment. It is measured in terms of bits per second. The simulation analysis shows that the collaborative key management scheme using signcryption based KEHECCS shows better packet delivery ratio when compared to the traditional algorithms like AES and ECC. The graphical representation of packet delivery ratio comparison between various algorithms is presented in Figure 6 and tabulate values are shown in Table 3

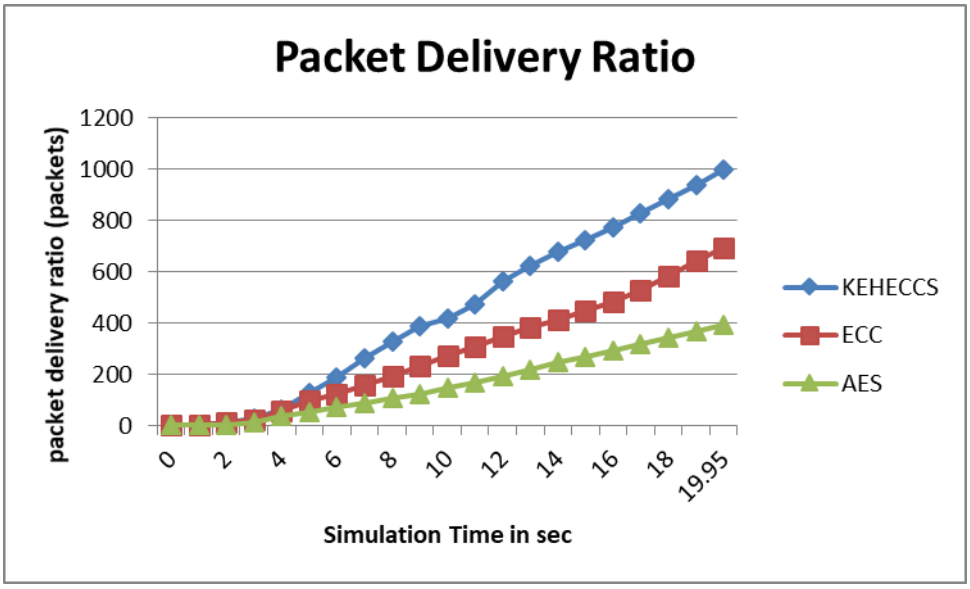

Figure 6 Packet Delivery Ratio

Table 3 Packet Delivery Ratio

Time	KEHECCS	ECC	AES
0	0	0	0
1	0	0	0
2	10.5	10.4	4.8
3	27.3	21.6	10.4
4	63.7	58.8	36.2
5	128.1	95.2	54
6	189.7	123.2	72.6
7	262.5	158.8	86
8	327.6	191.2	107.2
9	388.5	230.4	124.8
10	419.3	270.4	148.4
11	474.6	309.6	168
12	564.9	348	193.4
13	623.7	382.8	218
14	676.9	413.6	245.2
15	723.8	446	268.8
16	774.9	484	293.2
17	829.5	528.8	318.4
18	880.6	585.2	343.6
19	938	644	368.6
19.95	996.1	694.8	394.4

Throughput Efficiency: The overall system performance based on the packets transferred is analyzed in terms of Throughput efficiency. Throughput Efficiency is measured in terms of Percentage. In our scheme, there are many groups of mobile nodes communicating with each other using the group key agreement. Whenever a mobile node joins or leaves the subgroup, the GN wants to update the secret keys with all mobile nodes. The simulation analysis shows that the collaborative key management scheme using signcryption based KEHECCS shows better throughput efficiency when compared to the traditional algorithms like AES and ECC. The graphical representation of throughput efficiency comparison between various algorithms is presented in Figure 7 and tabulate values are shown in Table 4.

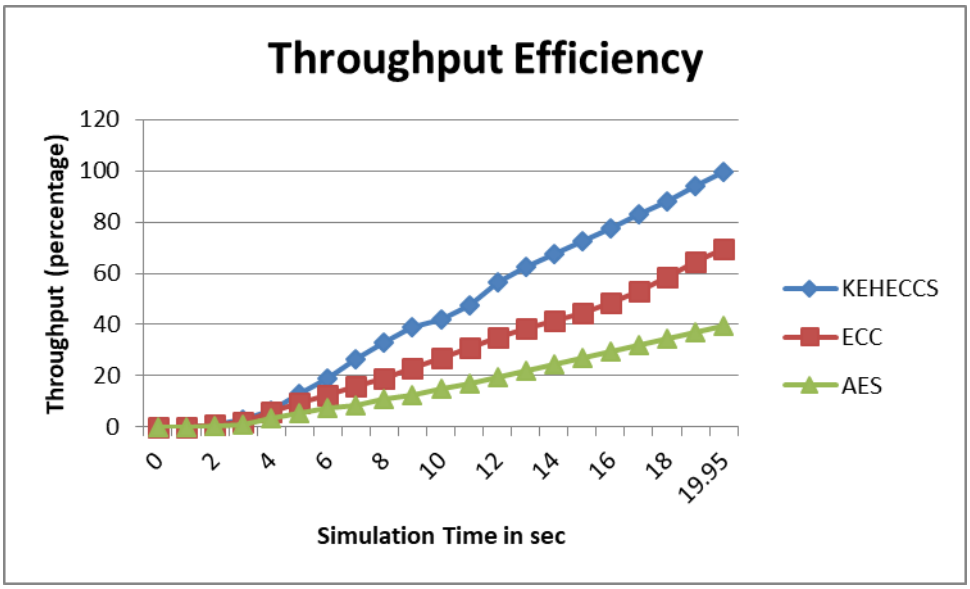

Figure 7 Throughput Efficiency

Table 4 Throughput Efficiency

Time	KEHECCS	ECC	AES
0	0	0	0
1	0	0	0
2	1.05	1.04	0.48
3	2.73	2.16	1.04
4	6.37	5.88	3.62
5	12.81	9.52	5.4
6	18.97	12.32	7.26
7	26.25	15.88	8.6
8	32.76	19.12	10.72
9	38.85	23.04	12.48
10	41.93	27.04	14.84
11	47.46	30.96	16.8
12	56.49	34.8	19.34
13	62.37	38.28	21.8
14	67.69	41.36	24.52
15	72.38	44.6	26.88
16	77.49	48.4	29.32
17	82.95	52.88	31.84
18	88.06	58.52	34.36
19	93.8	64.4	36.86
19.95	99.61	69.48	39.44

6. CONCLUSION

The secret data communication using collaborative key management scheme provides strong confrontation against key compromise attacks. The Proposed Collaborative key management scheme using Signcryption based Key Escrow and Elliptical Curve Cryptography Algorithm provides improvised performance in terms of throughput efficiency without compromising on Storage Cost and Communication Overhead. The innovative mechanism signcryption based KEHECCS provides two algorithms namely SSKG and GSKG which is used in secret key sharing and group key sharing respectively. Based on the calculated number of beacons that are received by a node and transmitted by a node, we can select the best gateway node than previously designed protocols. Also, the subgroup and group secret keys can be secret keyed whenever the membership changes (a node is joining or leaving). Our scheme provides better storage cost, less communication overhead and better throughput efficiency than other approaches like DES, AES and ECC.

REFERENCES

[1] Pang, L., Wei, M. and Li, H., 2019. Efficient and Anonymous Certificateless Multi-Message and Multi-Receiver Signcryption Scheme Based on ECC. *IEEE Access*.

[2] Nicanfar, H., Jokar, P., Beznosov, K. and Leung, V.C., 2013. Efficient authentication and key management mechanisms for smart grid communications. IEEE systems journal, 8(2), pp.629-640.

[3] Halford, T.R., Courtade, T.A., Chugg, K.M., Li, X. and Thatte, G., 2015. Energy-efficient group key agreement for wireless networks. IEEE Transactions on Wireless Communications, 14(10), pp.5552-5564.

[4] Huang, J., Zhu, L., Liang, Q., Fan, B. and Li, S., 2018. Efficient Classification of Distribution-Based Data for Internet of Things. IEEE Access, 6, pp.69279-69287.

[5] Denning, D.E. and Smid, M., 1994. Key escrowing today. IEEE Communications Magazine, 32(9), pp.58-68.

[6] Abe, M. and Kanda, M., 2002. A key escrow scheme with time-limited monitoring for one-way communication. The Computer Journal, 45(6), pp.661-671.

[7] Yanguo, P., Jiangtao, C., Changgen, P. and Zuobin, Y., 2014. Certificateless public key encryption with keyword search. China Communications, 11(11), pp.100-113.

[8] Seo, S.H., Nabeel, M., Ding, X. and Bertino, E., 2013. An efficient certificateless encryption for secure data sharing in public clouds. IEEE Transactions on Knowledge and Data Engineering, 26(9), pp.2107-2119.

[9] Lin, J., Zhu, W.T., Wang, Q., Zhang, N., Jing, J. and Gao, N., 2014. RIKE+: Using revocable identities to support key escrow in public key infrastructures with flexibility. IET Information Security, 9(2), pp.136-147.

[10] Lim, H.W. and Yang, G., 2015. Authenticated key exchange protocols for parallel network file systems. IEEE transactions on parallel and distributed systems, 27(1), pp.92-105.

[11] Xia, Z., Zhang, L. and Liu, D., 2016. Attribute-based access control scheme with efficient revocation in cloud computing. China Communications, 13(7), pp.92-99.

[12] Wang, Q., Li, X. and Yu, Y., 2017. Anonymity for Bitcoin from secure escrow address. IEEE Access, 6, pp.12336-12341.

[13] Waters, B., 2011, March. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In International Workshop on Public Key Cryptography (pp. 53-70). Springer, Berlin, Heidelberg.

[14] Lin, G., Hong, H. and Sun, Z., 2017. A collaborative key management protocol in ciphertext policy attribute-based encryption for cloud data sharing. IEEE Access, 5, pp.9464-9475.

[15] Lin, H.Y., 2018. A new certificateless strong designated verifier signature scheme: non-delegatable and SSA-KCA secure. IEEE Access, 6, pp.50765-50775.

[16] Yang, B., Hu, Z. and Xiao, Z., 2009, December. Efficient certificateless strong designated verifier signature scheme. In 2009 International Conference on Computational Intelligence and Security (Vol. 1, pp. 432-436). IEEE.

[17] Ma, L., Liu, X., Pei, Q. and Xiang, Y., 2018. Privacy-preserving reputation management for edge computing enhanced mobile crowd sensing. IEEE Transactions on Services Computing.

[18] Pang, L., Wei, M. and Li, H., 2019. Efficient and Anonymous Certificateless Multi-Message and Multi-Receiver Signcryption Scheme Based on ECC. IEEE Access.

[19] Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y. and Hu, J., 2019. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. Journal of Network and Computer Applications, 125, pp.82-92.

[20] Gao, R., Zeng, J. and Deng, L., 2018. Efficient Certificateless Anonymous Multi-Receiver Encryption Scheme without Bilinear Parings. Mathematical Problems in Engineering.

[21] Rajesh, R., Ramakrishnan, M. and Sugumar, B., 2017, December. A modest approach on MANET using certificateless cryptography. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 1197-1204). IEEE.

[22] Sugumar, B. and Ramakrishnan, M., 2018. An Exhaustive Investigation of Security Issues Tended to by Different Cryptographic Algorithms.

[23] Zhou, X. and Yang, X., 2009, December. Hyper-elliptic curves cryptosystem based blind signature. In 2009 Pacific-Asia Conference on Knowledge Engineering and Software Engineering (pp. 186-189). IEEE.

[24] Ch, S.A. and Amin, N., 2011, December. Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In 8th International Conference on High-capacity Optical Networks and Emerging Technologies (pp. 244-247). IEEE.

[25] Wanda, P. and Hantono, B.S., 2014, November. Efficient message security based Hyper Elliptic Curve Cryptosystem (HECC) for mobile instant messenger. In 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering (pp. 245-249). IEEE.

[26] Ullah, S., Li, X.Y. and Zhang, L., 2017, August. A review of signcryption schemes based on hyper elliptic curve. In 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM) (pp. 51-58). IEEE.

[27] Syeda Kausar Fatima, Dr. Syeda Gauhar Fatima, Dr. Syed Abdul Sattarand Syed Mohd Ali, A Relative Study on Cellular, WSN and Manets, *International Journal of Advanced Research in Engineering and Technology*, 10(2), 2019, pp.238-244

[28] Syeda Kausar Fatima, Dr. Syeda Gauhar Fatima, Dr. Syed Abdul Sattar and Dr. D. Srinivasa Rao, 2019, An Analysis on Cooperative Attacks in Manets, *International Journal of Advanced Research in Engineering and Technology,* 10(2), pp.245-253

[29] Pankaj Kumar Sharma and Dr. A.K. Sinha, 2018, Development of an Intelligent Manet System Model for Detection and Prevention of Annomaly Using Anfis, *International Journal of Mechanical Engineering and Technology*, 9(3), pp. 301–312

[30] Dr. Imad S. Alshawi, Dr. Kareem R. Alsaiedy, Vinita Yadav, Rashmi Ravat, 2014, Defense Framework (Stream) for Stream-Based DDOS Attacks on Manet, *International Journal of Information Technology & Management Information System*, 5(1), pp. 42–52

[31] Neha Kaushik and Ajay Dureja, 2013, A Comparative Study of Black Hole Attack in Manet, *International Journal of Electronics and Communication Engineering & Technology*, 4(2), pp. 93–102