DYNAMIC KEY DISTRIBUTION MANAGEMENT USING KEY ESCROW BASED ECC ALGORITHM IN MANETS

B. Vanathy

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

M. Ramakrishnan

School of Information Technology, Madurai Kamaraj University
Madurai, Tamilnadu, India

ABSTRACT

In the Information and Communication (ICT) Era, the data transmission through wireless communication has become most proficient and rapid tool around the world. IEEE standard 802.11 for WLAN has been meeting out the communication prospect in any organization. A Mobile Adhoc Network (MANET) is defined as the collection of independent mobile nodes that can communicate with each other via radio waves. In mobile ad hoc networks, the key distribution is the main constraint in data transmission. 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. For secure data communication, a group secret key must be shared by all group members. This group secret key should be updated when the existing group members are leaving the network or new members are entering into the existing network. In this paper, we propose an efficient group secret key agreement procedure called Key distributed management protocol which is based on Elliptic curve cryptography. 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 Elliptic Curve Cryptography management algorithm. In KEYBECC, we develop two protocols namely, Subgroup Secret Key Generation (SSKG) and Group Secret Key Generation (GSKG) based on ECDH for subgroups and outer groups respectively. These subgroup keys and group keys should be changed when there are membership changes (such as when the current member leaves or the new member joins). In the paper, we propose and implement a new methodology for dynamic key distribution. We simulate the environment for mobile networks with the proposed algorithm named Enhanced Key Escrow Based ECC (KEYBECC) with comparison of the traditional algorithms prevailing for MANETs. Compared to the existing approaches, KEYBECC demonstrates advanced key distribution features with better throughput efficiency without compromising on communication overhead and storage cost. From the

simulation analysis, the proposed dynamic group key agreement protocol performs well for the distributed key establishment problem in mobile ad hoc network in terms of throughput efficiency, communication overhead and storage cost.

Keywords: ECC, Key Distribution, Key Escrow, MANET, Security

Cite this Article: B. Vanathy and M. Ramakrishnan, Dynamic Key Distribution Management using Key Escrow based ECC Algorithm in MANETs, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 11 (1), 2020, pp 116-128.

<http://iaeme.com/Home/issue/IJARET?Volume=11&Issue=1>

1. INTRODUCTION

Internet applications are enhanced and increasing at very rapid. Due to the industrial development, secured way of data broadcast over the wireless communication path is becoming a probing task. Mobile Adhoc Networks are 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 Scenario

But in such high volume data transfer, there is a chance of malicious attacks. Intruders hack the data and use it for their favourable purpose. To overcome these unwanted acts, cryptography is used to ensure security of the covert and secure message. 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.

A 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 permuted to transform the order of its bits. Two 28-bit halves are divided by 56-bit key. Each half is than circular-shifted 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 iteration 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 dependent relative on 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 is a 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 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. 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. Sender will encrypts the data using receiver's public key and then receiver will decrypt the data using his own private key. It uses two prime numbers for generating 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 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. Any party can verify the signatures but only one party with the secret key can sign the messages

2. PROBLEM STATEMENT

The following observations have been identified during the secret key distribution in mobile adhoc networks.

- 1) Short length single key is not capable to provide secured cryptographic model and long length key can be able to provide secured cryptographic model.
- 2) Asymmetric keys are used and preferred for high level security.
- 3) There should be a proper key arrangement in order to achieve secure cryptographic model.
- 4) There is also another problem of data loss.

To overcome this data loss during transmission and to encourage faster transmission, many different compression algorithms are used to reduce the size of the data. Usually lossless compression algorithms are preferred for recovery of original and all data present without any loss before going for encryption. Selection of best encryption algorithm in terms of performance such as security and time constraints should be developed in future. The compression algorithm should be performed before encryption so the data will be in reduced form. There are some of the important points which contribute to cryptography system such as key selection for security and encryption, decryption process are relatively less investigated. Hence this survey work [1] is focused on such issues. These are all some different approaches to secure the system to achieve high level of security. Thus by selecting a suitable encryption algorithm will result in secured information system that may defeat several attacks.

Another method of policy-based encrypted cryptography was dignified in 2005 [2]. This gives an outline for operating cryptographic operations with respect to policies dignified as monotone Boolean operations written in standard normal procedures. A policy based encryption scheme permits encrypting of the message with respect to a policy in such a way that only the policy acquiescent users are able to decrypt the meaning. A policy consists of logical AND operation and logical OR operations, where each state is satisfied by a digital license representing the signature of a specific license issuer on a certain declaration. A node is thus acquiescent with a policy if and only if he has been issued a skilled set of recommendation for the policy i.e. a set of certificate fulfilling the combination of situation defined by the policy. Policy based encryption is the important filed of cryptographic schemes. Policy based cryptosystems have the ability sharing to incorporate encryption with license based access networks. This facility allows several attractive applications in different structure but not restricted to intruder access control [3], trust arbitration, and cryptographic procedure [4]. Another important area that is the focus of recent research is quantum cryptography [5]. This gives as a potential key to the secret key construction problem but the scope has elaborately signified. Most of the current study concentrates on new physics but the collision of the results could be important. Basically all recent activity in quantum cryptography is in quantum key exchange (QKE) in the network [6]. The algorithm use photons to create a shared bit string between two nodes in the network. The security of QKE relies on the physical procedure that it is impossible to produce information about the quantum state of a particle without introducing a malicious attack. Any intruder effort can be detected. The security of QKE does not rely on any assumptions in particular, shared keys established by QKE never become insecure when faster computers or new procedures are implemented. Photons can be elated either through optical fibres or in free space. Recent experiments in free space have established QKE over distances of the order of 20 km. A future work within the reach of present technology is QKE between the ground and a satellite [7]. This technology limits QKE using optical fibres to distances of less than roughly 100 km. Basic. Current challenges include the development of reliable single photon sources, higher detector efficiencies, better key generation rates, authentication, and the integration of a QKE system into a computer distributed network. Overall cryptography combines the science of electrical, mathematical and computer engineering, and a warped frame of mind that can shape out how to get around rules, break systems, and challenge the designers 'intentions.

3. PROPOSED SCHEME

The usage of internet is very complex in information and communication technologies. Radio-frequency identification (RFID) is the most important wireless communication technologies used in the Internet of Things as it can store sensitive data, used for wireless communication with other applications, and identify/track particular application automatically. Elliptic curve cryptography is the best method to provide authentication in RFID scheme. Elliptical curve cryptography (ECC) is a public key cryptosystem and it is used to create smaller, faster, and more efficient cryptographic keys in the work [8]. ECC authentication scheme is more suitable for wireless applications where the data is more confidentiality. It uses smaller key size and low computational system requirements. The low processing power associated with ECC authentication scheme is to make suitable for use with RFID tags because they have consuming limited computing power

Elliptic Curve Cryptography is an electronic technique that is used to protect sensitive data over transmission. Mainly cryptography is knowledge to provide security to information. To protect our data by using different validation scheme is the main objective of cryptography. When authentication of data is a key consideration, it should be of less cost than the value of unique information.

Elliptical curve cryptography (ECC) is a (PKC) public key encryption technique based on elliptic curve concept that can be used to evaluate faster in speed, smaller in size, and more efficient Cryptographic keys to provide certification scheme to RFID system. Previous research describes that the security level that is provided by RSA, using ECC 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. ECC algorithm can be implemented on minimum size of RFID tags. So ECC authentication scheme is well suited for wireless applications. ECC point of multiplication operation is more computationally effective than 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 case of passive attacks, the attacker can interrupt and make statistics about the communication. The detection of these attacks is difficult, so the goal is to prevent them.

An RFID authentication scheme includes three main parts:

- (1) The RFID tag
- (2) The RFID reader
- (3) The server

To implement certification between the tag and the server, some of the secret data that are transmitted are already predefined between tag and the reader when the system is firstly arranged. The interruption can be easily occurred in wireless channel during data transmission. So to prevent data proper certification scheme is needed between RFID tag reader and RFID server.

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 consume less power and less heat construction. The less significant key size makes faster cryptographic operations, running on smaller chip and on more compressed software in [9].

So for data security ECC is the great choice for following reason:

1. ECC provide better security of given key size
2. By using smaller keys it make more compressed implementation, high-speed cryptographic operations.
3. Less heat construction and less power consumption.
4. In ECC, there is efficient and compressed hardware implementation
5. It is almost impossible to find private key so it is not potential for third party to obtain the secret.

3.1. Challenges

Building Secure Algorithm in cryptography is very hard. Most cryptography algorithms on the network are insecure. Some are clearly inconsistent. Others are more delicately imperfect. Sometimes we have identified the flaws quickly, while for some others will take to identify errors in large time. Sometimes we have to use mathematics to break the system network. The errors can be in the distributed model, the algorithm design, protocols and the implementations of the source code in the network. The errors cannot be found through normal secret key algorithm. Most importantly, a single error breaks the security of the entire network [10]. If cryptography is a queue then the scheme is only as secure as its weakest line.

This means the whole thing has to be secured. It is not enough to make the encryption algorithms and communication protocols perfect but the entire framework must be perfect. A great framework with a not working algorithm is useless and a great algorithm, protocol, and implementation can be broken by a flawed random number creator [11]. Under these situations the most reasonable design decision is to use as few links as possible, and as high a percentage security of strong links as possible. It is impossible for a distributed system designer to analyze a completely new network crypt analysis system, a smart designer reuses elements that are generally believed to be secure, and only invents new enhanced cryptography where absolutely necessary in the mobile network [12]. Some data is transmitted openly in the information understanding stage, which can be analysed by the intruder as well. These can potentially cooperation with the security of the secret key succession. Privacy implication is then employed to remove the exposed information from the trusted threshold key sequence at Alice's and Bob's side [13]. This can be implemented by extractor [14], or universal hashing functions, such as leftover hash lemma [15], [16], cryptographic hash functions such as secure hash algorithm in [17], [18]. Privacy implication and information settlement always appear together, which requires a cross design between these two process. However, in practice, it is not easy to quantify the amount of the leaked information, or to identify where the leakage occurs in the data the key generation implementation is usually low cost, as it only requires non-complex operations such as sampling and storing data in the channel searching stage. All these operations can be implemented using the off-the-shelf applications, with only a change to the controller. The key generation procedures vary according to the system implementation [19]. All the key generation systems need channel sampling and quantization while information settlement and privacy implication may be not applied due to specific performance and surroundings where the systems achieve ideal agreement after quantization [20].

Our proposed elliptic curve distributed key management scheme achieves the correctness and secrecy requirements necessary to provide a distributed key generation protocol based on ECC. 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 $t+1$ nodes done the same secret key. All honest nodes have the same value of the node secret public key.
- 2) Secrecy: At least $t+1$ server 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 $t+1$ nodes 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. New ordinary node cannot receive the previous keying information before joining the network. 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 reject the backward secrecy of the existing scheme.

4. SYSTEM MODEL

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 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 pseudo code for the system model is presented in Table 1.

Table 1: Pseudo Code for Dynamic Key Distribution System Model for Manet

```
/*ReSecretkeying : Node join & leaves*/
m – new node is joining into G
1. if new node ‘m’ enters in to the subgroup G.
2. ‘m’ – generates its private key.
SKm & SUM = PKm x G.
3. GN sends the public keys of i and j, group key of [i,j]
4. ‘m’ uses the group key of [i,j] and compute SKi,j,m = PKn x SKi,j
5. ‘m’ calculates the following public keys
PUj,m = PKm* PUj and PUi,m = PKm * PUi
6. user ‘m’ broadcasts these group keys to i and j
7. j computes a new subgroup secret key SKi,j,m = PKj * PUi,m
8. i computes a new subgroup secret key SKi,j,m = PKi * PUj,m
9. check the new subgroup secret key of i,j and m is SKi,j,m
‘j’ leaves from G /* when node ‘j’ leaves from the subgroup */
1. GN, ‘i’ changes its private key PKi, then calculates new public key PUi = PKi* G
2. ‘i’ shares its public key with user ‘n’
3. m computes the subgroup key as SKm = PKm * PUi
4. i computes the subgroup key as SKi = PKi * PUm
5. check SKi = SKm
6. Then GN ‘i’ stores this key as SKi,m
/* when GN leaves from G */
1. Previous GN ‘j’ act as a new GN or a new GN is selected as per Algorithm1
2. GN ‘j’ changes its private secret key PKj, then calculates new public key PUj = PKj* G
3. ‘j’ shares its public secret key with user ‘n’
4. ‘j’ calculate new subgroup secret key SKj = PKj * Pum
5. ‘m’ calculate new subgroup key SKm = PKm * PU.
6. New GN sends message to external gateway node (OGN).
7. Current OGN selects new OGN as per the stability criteria.
/* new OGN is selected */
1. Gateway members i,j and m of different subgroups are grouped together.
2. Group Key is generated as per the subgroup secret key generation algorithm.
3. The group key is resecret keyed
```

The secret key sharing among the group nodes and between group nodes and gateway nodes using SSKG and GSKG is shown in Figure 2.

Figure 2: Secret Key Sharing in MANET

In the present work, distributed key management protocol based on key escrow and elliptic curve cryptography has been analysed. 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. NS-2 simulations show that our proposed scheme is robust in the mobility environment of Mobile networks.

5. PERFORMANCE ANALYSIS

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 KEYBECC algorithm, the mobile network environment is simulated to measure the performances based on the metrics, Storage Cost, Communication Overhead and Throughput Efficiency.

5.1. Storage Cost

Storage cost is defined as the memory required for storing the data in the secured data transmission path in 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 dynamic key distribution environment, the implementation of KEYBECC is compared with the other traditional algorithms like AES and Discrete Logarithm Problem (DLP). The simulation results prove that KEYBECC has less storage cost when compared to AES and DLP. 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 DLP 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 3 and the tabulated values are charted in Table 2.

Figure 3: Storage cost

Table 2: Storage Cost

Time	KEYBECC	DLP	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

5.2. 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 gate way 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 DLP 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 more 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 a better performance in our approach. The graphical representation of communication overhead comparison between various algorithms is presented in Figure 4 and tabulate values are shown in Table 3.

Figure 4: Communication Overhead

Table 3: Communication Overhead

Time	KEYBECC	DLP	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

5.3. Throughput Efficiency

The overall system performance is analysed 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 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 dynamic key generation scheme using KEYBECC shows better throughput efficiency when compared to the traditional algorithms like AES and DLP.

Figure 5: Throughput Efficiency**Table 4:** Throughput Efficiency

Time	KEYBECC	DLP	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

In the ever growing data communication realm, the transfer of secret information in a cost effective and efficient means is of paramount importance. The Proposed Dynamic key distribution scheme using Key Escrow and Elliptical Curve Cryptography Algorithms provides enhanced performance in terms of throughput efficiency without compromising on Storage Cost and Communication Overhead. The innovative mechanism KEYBECC 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 a best gateway node than previous designed protocols. Also the subgroup and group secret keys can be resecret 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 DLP.

REFERENCES

- [1] Jacob Sayid¹, Isaac Sayid² and Jayaprakash Kar³, "Certificateless Public Key Cryptography: A Research Survey", International Journal of Security and Its Applications Vol. 10, No. 7 (2016) pp.103-118 <http://dx.doi.org/10.14257/ijisia.2016.10.7.10>
- [2] W. Bagga and R. Molva. Policy-based cryptography and applications. In Proceedings of Financial Cryptography and Data Security (FC'05), volume 3570 of LNCS, pages 72–87. Springer Verlag, 2005
- [3] J. Holt, R. Bradshaw, K. E. Seamons, and H. Orman. Hidden credentials. In Proc. of the 2003 ACM Workshop on Privacy in the Electronic Society. ACM Press, 2003.
- [4] S.S. Al-Riyami, J. Malone-Lee, and N.P. Smart. Escrow-Free Encryption Supporting Cryptographic Workflow. Cryptology ePrint Archive, Report 2004/258, 2004. <http://eprint.iacr.org/>.
- [5] David Williams, A new information science Quantum Information Processing is Based on Quantum Mechanical Principles and Includes Quantum Computing and Cryptography. Materials Today July-August 2007 Volume 10
- [6] Fred Piper, Some Trends in Research in Cryptography and Security Mechanisms. Research in Cryptography And Security Mechanisms Elsevier Science Ltd March 2003 pp 23-26
- [7] Michael P. Howarth, Sunil Iyengar, Zhili Sun, Member, IEEE, and Haitham Cruickshank, Member, IEEE. Dynamics of Key Management in Secure Satellite Multicast, IEEE Journal On Selected Areas in Communications, Vol. 22, No. 2, February 2004 pp 308-319
- [8] M. Guru Vimal Kumar, U.S. Ragupathy, A Survey on Current Key Issues and Status in Cryptography, presented at the IEEE WiSPNET 2016 conference.
- [9] S. S. Al-Riyami and K. G. Paterson, Certificate Less Public Key Cryptography, in Advances in Cryptology - ASIACRYPT 2003, C.-S. Lai, Ed. Springer Berlin Heidelberg, (2003), pp. 452–473.
- [10] Z. Zhang, D. S. Wong, J. Xu and D. Feng, Certificateless Public-Key Signature: Security Model and Efficient Construction, in Applied Cryptography and Network Security, J. Zhou, M. Yung, and F. Bao, Eds. Springer Berlin Heidelberg, (2006), pp. 293–308
- [11] J.Kar, Non-interactive Deniable Authentication Protocol using Generalized ECDSA Signature Scheme, International Journal of Smart Home. Korea, vol. 5, no. 4, (2011) Oct., pp. 39-49.
- [12] Himja Agrawal, Prof. P.R. Badadapure "A Survey Paper on Elliptic Curve Cryptography", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395 - 0056, Volume: 03 Issue: 04, Apr-2016
- [13] Catherine Meadows, Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends. IEEE Journal on Selected Areas in Communication. VOL. 21, NO. 1, JANUARY 2003 pp 44-54
- [14] P. Caballero-Gil, C. Henández-Goya, C. Bruno-Castaneda, A Rational Approach to Cryptographic Protocols, Mathematical and Computer Modelling 46 (2007) pp 80–87
- [15] S. Muhammad, R. K. Guha and Z. Furqan "A Simplified Logic Based Framework for Formal Analysis of Cryptographic Protocols". Computer Science Technical Report CS-TR-05-10, School of Computer Science, University of Central Florida, Oct. 2005.

- [16] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks," in Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM), Shanghai, China, Apr. 2011, pp. 1422–1430
- [17] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret Key Extraction from Wireless Signal Strength in Real Environments," IEEE Trans. Mobile Comput., vol. 12, no. 5, pp. 917–930, 2013.
- [18] Y.Liu,S.C.Draper,andA.M.Sayeed,"Exploiting Channel Diversity in Secret Key Generation from Multipath Fading Randomness," IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1484–1497, 2012
- [19] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility Assisted Secret Key Generation Using Wireless Link Signatures," in Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM), San Diego, California, USA, Mar. 2010, pp. 1–5.
- [20] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving Channel Reciprocity for Effective Key Management Systems," in Int. Symp. Signals, Syst., and Electron. (ISSSE), Potsdam, Germany, Oct. 2012, pp. 1–4.
- [21] S. Radha Rammohan. Anomaly Detection in Mobile Adhoc Networks (MANET) using C4.5 Clustering Algorithm. International Journal of Information Technology & Management Information System (IJITMIS), 7(1), 2015, pp. 01-10
- [22] Nisma Mobinunnisa and V. Sessa Bhargavi, Detection of Multiple Malicious Nodes in MANETS in a Single Query. International Journal of Computer Engineering & Technology, 8(6), 2017, pp.45–53
- [23] Shah Vrutik, Dr. Nilesh Modi, Patani Ashwin, AODVGAP-AN Acknowledgment Based Approach to Mitigate Selective Forwarding Attacks in MANET, International Journal of Computer Engineering and Technology (IJCET), 3(2), 2015, pp. 458-469
- [24] S. Kanimozhi Suguna, Dr. S. Uma Maheswari, Comparative Analysis of Bee-Ant Colony Optimized Routing (BACOR) with Existing Routing Protocols for Scalable Mobile Ad HOC Networks (MANETS), International Journal of Computer Engineering and Technology (IJCET), 3(1), 2012, pp. 232-240
- [25] Dr. Imad S. Alshawi, Dr. Kareem R. Alsaiedy, Ms. Vinita Yadav, Ms. Rashmi Rava, Defense Framework (STREAM) For Stream-Based DDoS Attacks on MANET, International Journal of Information Technology & Management Information System (IJITMIS), 5(1), 2014, pp. 42-52.