Implementation of Bluetooth Secure Simple Pairing (SSP) using Elliptic Curve Cryptography (ECC)

[1,]Dr.Ahmad Hweishel A.Alfarjat, [2,]Dr.Hanumanthappa J., [3,]Dr. Hatem S. A. Hamatta
ahmed_alfarajat@bau.edu.jo hanumsbe@gmail.com Hatem@bau.edu.jo
[1]Applied Science Department, AlBalqa Applied University, Aqaba, Jordan
[2]Associate Professor, DoS in Computer Science, University Of Mysuru
[3]Applied Science Department, AlBalqa Applied University, Aqaba , Jordan

Abstract
In this paper we study the problem of implementation of security issues of blue tooth, especially secure simple pairing, with the help of an efficient four user authenticated key (4UAK) for an elliptic curve cryptography (ECC). This paper also deals with the design, implement and performance evaluation of secure simple pairing (SSP) using an elliptic curve cryptography, such as Diffie Hellman protocol when four users are involved. Here, we also compute the best, worst and average case step counts (time complexities). This work puts forth an efficient way of providing security in blue tooth. The time complexity of $O(n^4)$ is achieved using Rabin Miller Primality methodology. The method also reduces the calculation price and light communication loads.

Keywords:
Bluetooth, 4UAK, Elliptic Curve Cryptography, Diffie Hellman, NUAK (N Users Authenticated Key) Protocol.

.1. Background

Bluetooth technology finds a wide applications in local wireless communications [1,2,3]. The primary goal of blue tooth is a cable replacement protocol for wireless connectivity. Bluetooth plays a vital role as a electronic radio frequency technology. The blue tooth technology was implemented by Ericsson as a substitute for the RS-232 data cable. Bluetooth radio frequency mechanism is intended for short distance data swapping usually within a 10 meter distance but some of the kinds of blue tooth also act at a distance of 1 to 100 meters range [9]. Bluetooth operates in the range of 2.4 GHz–2.4835 GHz ISM frequency band and supports data rates up to 720 Kbps [1..3]. The blue tooth standard uses a frequency-hopping spread spectrum (FHSS) mechanism to tackle interference research challenges. The FHSS methodology utilizes 79 heterogeneous radio channels by modifying the frequency about 1600 times/sec. The blue tooth technology is used to create small scale wireless networks between a wide range of electronic devices to forward voice and data at lower cost and low power [1,2,3,9]. The blue tooth technology also creates a pico net with multiple blue tooth equipments on an ad-hoc basis [9].

1.1. Elliptic Curve Cryptography

Cryptography with private and public keys is a direct forward methodology with the help of bit generator. Cryptography is a set of mathematical ideas, related to the techniques of information security such as confidentiality, authentication, privacy, integrity and non-repudiation. The elliptic curve cryptography (ECC) is a branch of cryptography, proposed and introduced by Miller in the year 1986 and Neal Koblitz in the mid 1980's. The elliptic curve is based on the ellipse. ECC is an efficient approach for public key crypto systems. The ECC is broadly categorized into RSA systems and discrete logarithm based systems. ECC is combined with Diffie Hellman approach to provide key swapping technique for two communication parties. It is also used for generating digital signature, data encryption and decryption. The elliptic curve digital signature algorithm (ECDSA) uses ECC to create digital signature for authentication and other security purposes. ECC is a kind of public key cryptography methodology which is highly superior to the well-known RSA cryptography, which provides higher security for the same key size.

Several researchers have addressed different kinds of techniques to improve the security issues of secure simple pairing of blue tooth using elliptic curve cryptography.

Dr. Hanumanthappa J., Ahmad Hweishel Alfarjat [1,2,3,4,8,9,14] et al have presented security issues of blue tooth using digital signature based on elliptic curve cryptography. They have also proposed how to improve security issues of blue tooth using ECC. They have also computed time complexity of security issues of blue tooth based elliptic curve digital signature authentication using miller rabin primality technique is O (n^4) and the time complexity by using broker and steven hagen is O (n^3). Finally, they have concluded that encryption is a beautiful process to send any text message from one source location to another destination location using elliptic curve based digital signature. They have also proposed a mathematical

Manuscript received March 5, 2021
Manuscript revised March 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.3.9

model for security issues of wlan by investigation, design, implementation and performance analysis using Digital Signal Processing (DSP) space time processing with the help of alamouti code [1..3][8..9]. Their research also elaborates space time processing as a concept to implement the security issues of wlans by presenting alamouti technique. In their research work it is also possible to increase number of antennas at both transmitter and receiver without using interference in between antennas is also one of an important technique to improve the security issues of WLANs [1][2][3].

Dr.Hanumanthappa .J. and Ahmed Hweishel A.Alfarjat [1,2,3,4,8,9,14] have first time shown the investigations into the design, performance and security evaluation issues of blue tooth using ECC and they have composed mathematical model on the same. They have also shown that, in security issues of blue tooth based ECC, the asymmetric key cryptography is the best solution MITM. Their research manuscript also compares and contrast the differences between IPv6 issues with blue tooth issues and security issues of blue tooth vs security issues of IPv6 using IPSec etc.

Keijo Haataja and Pekka Toivanen have proposed two practical man-in-the middle attack against blue tooth secure simple pairing [18]. The first attack is proposed using out-of-band (oob) channel and the second, using secure socket enabled blue tooth headsets and hand free devices. They have also described a new MITM attack on blue tooth SSP using “no input no output” [18].

Xiaojiang Du [57] has utilized ECC in the design of an efficient key management technique for sensor nodes. The propounded key management technique utilizes the fact that a sensor only communicates with a small portion of its neighbors and greatly reduces the communication and computation overheads of key setup. He has also confirmed that routing driven ECC performance evaluation and security analysis technique can significantly decrease the communication overhead, sensor storage requirement and energy consumption while achieving better security (stronger resilience against node compromise attack) than a popular key management technique for sensor networks.

Diffie and Hellman have introduced the concept of public key cryptography. The cryptographic importance of the apparent intractability of the discrete logarithm has been determined. They have proposed a key swapping algorithm whose security is dependent on discrete logarithm problem in $*_q$ and subsequently, El Gamal formed a public key cryptosystem based on the same underlying query.

Taher El Gamal [1985] has first described how this problem may be utilized in public key encryption and digital signature schemes. The Elgamal algorithm is a type of public key cryptosystem which is considered over finite fields and its security is based on discrete logarithm problem (DLP). The DLP first employed by Diffie Hellman in their key agreement protocol, was defined explicitly as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers modulo a prime, this technique also can be extended to arbitrary groups.

Miller and Koblitz separately proposed using the group of points on an elliptic curve defined over a finite field in discrete log cryptosystems. The primary advantage that ECCs have over system based on multiplicative group of a finite field, is the absence of a sub exponential time logarithm that could determine discrete logs in these groups. While consequently we can use an elliptic curve group which is smaller in size while maintaining same level of security. Miller and Koblitz also suggested to substitute the finite field q with an elliptic curve E with the hope that the discrete logarithm problem in an elliptic curve group E (q) is very difficult to solve than the discrete logarithm problem in the multiplicative group $*_{q.}$

Debiao He, Sherali zeadally have shown a review of elliptic curve cryptography RFID authentication techniques in terms of performance and security. Jen-Ho Yang, Chin-Chen Chang [20] have proposed an efficient three party authenticated key swapping protocol using ECC. Based upon ECC, the proposed protocol has less computation costs and lower communication loads. In 1992 Bellovin and Merrit have first propounded a two party password-based authenticated key swapping (2PAKE) protocol. In their protocol, two communication parties can authenticate each other via a public network and share a session key for their subsequent communications.

Pritam Gajkumar Shah, Dr.Xu Huang et have used MITM attack in the wireless sensor networks. They have also confirmed that their research is to make WSN secure symmetric key protocols, but at the same time public key cryptography has received little attention from researchers [49].

Jakobson .M. and Wetzel .S. for the first time formulated MITM attack on blue tooth for version 1.0B. By passive eavesdropping on the initialization key establishment protocol they also developed a technique to acquire the link key using an off-line PIN crunching attack. They pointed few limitations of version 1.0B like usage of the unit key the short blue tooth PIN and the confidentiality problem caused by site tracking.

Joseph H. Silverman explains Weirstrass equations and the minimal discriminant of an elliptic curve. He has also explained the method of solving ECC problems using an arithmetic equation.

Sylvain Duquesne has improved the arithmetic of elliptic curves by using Jacobi model. He has also provided better unified addition formulae for elliptic curve having a 2-torsion point by introducing a new system of coordinates on the Jacobi quadratic model. Nigel examines the relative efficiency of four techniques for finite field specification in the context of ECC. He has also concluded that a set of optimized extension fields (OEFs) give greater performance

even when used with affine coordinates, when compared against the type of fields recommended in the emerging ECC standards. Chen.T.H., Lee.W.B., Chen.H.B. have proposed an efficient three party authenticated key exchange protocol based on Schnors digital signature scheme. Compared with other 3PAKE protocols Chen et al's., protocol use fewer communication rounds to accomplish the mutual authentication and the key exchange between any two parties in a large group.

2. Proposed Methodology

The proposed method is broadly categorized into two heterogeneous kinds such as existing system and propounded system. In this research work first we are concentrating on the existing system as follows. In the existing system, Jen Ho Yang and Chin-Chen Chang [20] have proposed an efficient three party authenticated key swapping protocol using ECC. Keijo Haataja and Pekka Toivanen [18] have proposed two practical MITM attack against blue tooth secure simple pairing [18]. Here, we are updating the research issues proposed by Keijo Haataja and Pekka Toivanen who have proposed secure simple pairing concept implementation using Diffie Hellman routing protocol (Diffie Hellman handshake, Diffie Hellman Merkle key exchange, Diffie Hellman key agreement, Diffie Hellman key negotiation and Exponential key exchange) with three-user authenticated key (3UAK) protocol. Later, we deal with the security issues of blue tooth SSP association model using NUAK (N Users Authentication Key) and 4UAK protocol along with the performance comparisons.

The fundamental Bluetooth security configuration is done by the user who decides how a blue tooth equipment will implement its connect ability and discoverability options. The blue tooth version 2.1+ EDR sums a new specification for the pairing procedure such as SSP. The main theme of secure simple pairing is to enhance the pairing security by providing protection against passive eavesdropping and also by MITM attacks. On behalf of short length pass keys as a source of entropy for creating link keys, the SSP employs elliptic curve Diffie Hellman public key cryptography. The blue tooth device uses public-private key pairs, a number of nonces and blue tooth addresses of the devices to construct a link key. The passive eavesdropping is mainly thwarted by SSP, which takes a keen interest to run an exhaustive search on a private key with approximately 95 bits of entropy, is infeasible in short time. In order to provide security against MITM attacks the SSP model uses an out-of-band channel, such as near field communication (NFC) for the user's help. This research work also brings to the notice that, out of band channel is not controlled by the MITM attack. The SSP model utilizes four heterogeneous association models such as numeric key comparison, passkey entry, just works and out of band. The SSP is broadly categorized into six different kinds of levels such as capabilities swapping, public key swapping, authentication stage 1, authentication stage 2, link key computation and LMP authentication and encryption.

2.1. Public key cryptosystem in elliptic curve cryptography

Heterogeneous blue tooth equipment's constitute keyboards, printers, mobile phones, head sets and hands free devices [53]. All these devices support SSP model. Blue tooth is a well known technology for data transfer between the devices that span short distances [17][53]. ECC supports high level security with a smaller key length, making it one of the most popular public key cryptosystems [17][53]. Public key cryptosystems rely on what are known as one-way trapdoor functions. These are very easy to calculate injective functions f:A→B, with the characteristic feature that f^{-1} is very difficult to compute in general. But it is easier to calculate if someone possesses an extra piece of information k [17][53]. The public key cryptography is too expensive for small sensor nodes, because traditional public key algorithms such as RSA requires extensive calculations and are not used for small sensors.

2.2. Four User Authenticated Key (4UAK) Swapping Protocol for Blue tooth Secure Simple Pairing using an Elliptic Curve Cryptography.

4UAK is broadly split into two levels, the initialization level and the authenticated key swapping protocol level in SSP. The various responsibilities of the protocol are user-1 AHJ, user 2 DA, user 3 HJD and user 4 RHJ. We define some of the notations that will be used further in the paper.

Table 1. The symbols used

Sl. No	Parameters	Description
1	IDA	Identity of user A
2	N and G	N and G are two large prime numbers satisfying G/N-1
3	g	Generator satisfying $g^q \equiv 1 (\text{mod } p)$ in Z_p^*
4	x,y	The private key x, and the public key y of user H satisfying $y \equiv g^x (\text{mod } p)$
5	PkAH,PkDA,PkHJ,PkRHJ	
6	SkAH, SkDA,SkHJD,SkRHJ	Secret key of user AH, Secret key of user DA,

		Secret key of user HJ, Secret key of user RHJ.
7	DHkey	Diffie Hellman key created after swapping.

In this research work we have assumed that both user A and user D wish to authenticate each other and share a session key through H on a public network. Now we introduce the protocol as follows:
The initialization level and the authentication key swapping level

1.The initialization level: In this level, users A and D must register to H to make two valid users. With respect to that the user H also shares a secret key with each user for later authentication. Here H also calculates the authentication information for A by the following steps. Before establishing a symmetric key, it is necessary for the two parties to choose two numbers N and G (G < N), which is a primitive root of N. The first number N is a large prime number with the necessary condition that (N-1)/2is also a prime number. The second number G is also a large prime number which also has restrictions. Here, we have not considered Both N and G as confidential, but they can be sent through the Internet, however they are treated as public.

Step-1: AH (User A) chooses a large random number (private key) v and computes $Z_1=G^v \bmod N$.
Step-2: AH (User A) forwards the whole public key (G, N and Z_1) to DA.
Step-3: DA (User B) picks another large random number (private key) w and computes $Q_2=G^w \bmod N$.
Step-4: DA sends the entire public key (G, N and Q_2) to AH and DA does not send only the value of w but however she only sends Q_2.
Step-5: AH computes $L= (Q_2)^v \bmod N$. AH also computes another $L= (Z_1)^w \bmod N$, where L is a symmetric key for the session.

The answer is an equality confirmed in number theory

$L= (Q_2)^v \bmod N$ i.e $(G^w \bmod N)^v = G^{wv} \bmod N$ ----(i)
$L= (Z_1)^w \bmod N$ i.e $(G^v \bmod N)^w = G^{vw} \bmod N$----(ii)

Where L is a common secret key used for secret key encryption which is highly difficult to discover for others. Hence the proof according to the number theory.

3. Implementation of Bluetooth SSP using Diffie Hellman 4UAK and ECC.

Diffie Hellman key swapping agreement is not only limited to negotiating a key shared only by two users. We have already studied in our research work that any number of users can participate in an agreement by doing iterations of the agreement protocol and swapping intermediate non secured data and information.
For example when AH, DA, HJ and RHJ participate in a diffie hellman protocol agreement as follows with all operations taken to be modulo p.

Algorithm-1: Diffie Hellman with 4 different users with an authenticated key.

Input: G and N are two large prime numbers satisfying N/G-1.
Output: Securely swapping of cryptographic symmetric keys over a communication public communication channel.

Step-1: The four users agree on the DH algorithm parameters G and N.
Step-2: The users generate their private keys such as v, w, x and y.
Step-3: AH chooses a large random number (private key) v and computes $Z_1= G^v \bmod N$.
Step-4: AH forwards the whole public key (G, N and Z_1) to DA
Step-5: DA picks another large random number (private key) w and computes $Q_2= (Z_1)^w \bmod N$ ie $G^{vw} \bmod N$.
Step-6: DA sends the entire public key (G, N and Q_2) to HJ.
Step-7: HJ selects another big private integer x and calculates $S_3=(Q_2)^x \bmod N$. i.e $(G^{vw} \bmod N)^x$ i.e $G^{vwx} \bmod N$.
Step-8: HJ gives the whole public key (G, N and S_3) to RHJ.
Step-9: RHJ picks another large random integer y and computes $P_4=(S_3)^y \bmod N$. i.e $(G^{vwx} \bmod N)^y$ i.e G^{vwxy} mod and uses P_4 as her secret key.
Step-10: DA computes $D_2= (G_1)^w \bmod N$ ie $G_1^w \bmod N$ and sends it to HJ.
Step-11: HJ calculates $F_3= (D_2)^x$ and sends $G_1^{wx} \bmod N$ it toAH.
Step-12: AH calculates $O_1= (F_3)^v$ and computes $G_1^{wxv} \bmod N$ and forwards to the RHJ.
Step-13: RHJ computes $J_4= (O_1)^y$ and calculates $G_1^{wxvy} \bmod N$ and chooses J_4 as her secret key.

In the above algorithm P_4 and J_4 are called symmetric keys.

Algorithm-2: *Secure simple pairing of blue tooth using numeric comparison association model and an elliptic curve cryptography for four users authenticated key(4UAK).*

Process-1: Public key swapping.

Public Key of AH is PK_{AH} and Public Key of DA is PK_{DA}.

Step-1: AH and DA swaps their public keys.
Step-2: Compute diffie hellman key (DHKey=P_{DHKey}= (private key of AH, public key of DA) at AH user 1 side.
Step-3: Calculate diffie hellman key (DHKey=P_{DHKey}= (private key of DA, public key of AH) at DA user 2 side.

Process-2:Authentication Stage 1

Step-4: Choose random integer of nonce AH.
Step-5: Pick random integer of nonce DA.
Step-6: Set random number of AH to 0 in the number comparison association model.
Step-7: Set random numeric of DA to 0 in the number comparison association model.
Step-8: Calculate commitment domain of DA=f1 (PK_{DA},PK_{AH},Nb,0).
Step-9: Nonce created by equipment AH.
Step-10: Rectify that C_{DA}=f1 (PK_{DA}, $PK_{AH,}N_{DA,}0$).
Step-11: Nonce created by DA (N_{DA}).
Step-12: Calculate V_{AH} =g($PK_{AH,}PK_{DA,}N_{AH,}N_{DA}$). Ask the users AH and DA to compare the numbers V_{AH} and V_{DA} shown on the displays;proceed if user confirms ok .
Step-13:Compute V_{DA}=*g(*$PK_{AH,}$ $PK_{DA,}$ N_{AH}, N_{DA}).
Step-14:E_{AH}

Process-3: Authentication Stage 2

Step-15: Rectify that E_{AH} =f_3 (DHKey,N_{AH}, $N_{DA,}$0, IO_{cap}AH, AH,DA)
Step-16: Compute E_{DA}=f_3 (DHKey, N_{DA},$N_{AH,}$0, IO_{cap}DA, DA, AH)
Step-17: Verify that E_{AH} =f_3 (DHKey, N_{AH},$N_{DA,}$0, IO_{cap}AH, AH, DA)
Step-18: E_{DA}=f_3 (DHKey,N_{DA},$N_{AH,}$0,Io_{cap}DA,DA,AH)

Process-3: Link key computation

*Step-19: All users compute link key as LK=f2 (*DHKey,N_{master},N_{slave},"btlk", BD-$ADDR_{master}$,BD-$ADDR_{slave}$*)*

Process-4: Encryption

Step-20: Create encryption keys as in legacy pairing.

Algorithm-4: Implementation of pairing details using ECC and *four users authenticated key (4UAK)*

Process-1: Public key swapping.

In this research work we have assumed that Public Key of AH (PK_{AH}*), Public Key of DA (*PK_{DA}*),* SK_{AH}, SK_{DA} where SK_{AH}, SK_{DA} are the two important secret keys for swapping of information between AH and DA.

Process-1: Assumption 1

Step-1: Both AH and DA swaps their public keys. i.e AH sends his public key PK_{AH} to DA and DA sends her public key to AH.

Process-2: Initialization

Public Key of AH is PK_{AH} and Public Key of DA is PK_{DA}.

Step-1:AH and DA swaps their public keys.
Step-2:Calculate DHKey at initiating device-A as DHKey=P312 (SK_{AH}, $P_{DA}{}^{1}$).
Step-3:Compute DHKey at user 1 as DHKey=P312 (SKmitm (witm), P_{AH}).
Step-4:Calculate DHKey at user 2 as DHKey=P312 (SKmitm (witm), P_{DA}).
Step-5:Compute DHKey at non-initiating equipment B as DHKey=P312 (SK_{DA}, $P_{AH}{}^{1}$).

Process-3: Authentication Stage 1:

Step-1: Choose random number (rnAH) and random number (rnDA)
Step-2: Set random number of rnAH to 0 in the number comparison association model.
Step-3: Set random numeric of rnDA to 0 in the number comparison association model.
Step-4: Calculate that C_{DA}= f_1 (PK_{AH},PK_{DA},N_{DA},0)
Step-5: Rectify that C_{DA}= f_1 (PK_{AH},PK_{DA},N_{DA},0)
Step-6: Calculate V_{AH} = g(PK_{AH},PK_{DA},N_{AH},N_{DA},0)
Step-7: Compute V_{DA} = g(PK_{AH1},PK_{DA},N_{AH},N_{DA})
Step-8: Proceed if user confirms ok at initiating device A.
Step-9: Proceed if user confirms ok at initiating device B.

Process-4:Authentication Stage 2:

Step-10: Compute E_{AH}=f_3 (DHKey, N_{AH}, $N_{DA,}$0, IOcapAH, AH, DA^1)
Step-11: Calculate $E_{DA}{}^{1}$=f_3 (DHKey, $N_{DA}{}^{1}$, $N_{AH,}$0, NoinputNooutput, DA^1,AH)
Step-12: Compute $E_{AH}{}^{1}$=f_3 (DHKey, N_{AH}, $N_{DA,}$0, No input No output, AH^1,DA)
Step-13: Compute E_{DA}=f_3 (DHKey, N_{DA}, $N_{AH,}$0, IOcapDA, DA, AH^1)
Step-14: E_{AH1}
Step-15: Verify that $E_{AH}{}^{1}$=f_3 (DHKey, N_{AH}, $N_{DA,}$0, No input No output, AH^1, DA)
Step-16: f_3 (DHKey, $N_{DA}{}^{1}$, $N_{AH,}$0, Noinput Nooutput, DA^1, AH)

Process-5: Link key (LK) calculation

Step-1: LK = f2 (DHKey, N_{master}, N_{slave}, "btlk", BD-$ADDR_{master}$, BD-$ADDR_{slave}$)

Process-6: Encryption

Step-1: Create encryption keys as in legacy pairing.

4. Implementation results and performance analysis of the proposed research work.

In this section we give the performance and security analysis of the proposed an efficient four users authenticated key (4UAK) for an elliptic curve cryptography. In order to measure the transmitted message size we assume that the size of q used in ECC of our newly proposed algorithm is 320 bits. The cipher text size using symmetric key encryption decryption AES is 256 bits. Therefore total size of our plain text is

2x256 + 2x320 + 2x256 = 1664 i.e more than 1Kilo bytes (1Kb).We will also prove that our proposed protocol is more efficient and effective for the security issues of blue tooth, other wireless equipments and the upcoming 5G equipments. For the simplicity of our proposed calculation we prohibit the calculation costs of symmetric key cryptography and hash function. According to the research results proved by Hankerson et al (2004) and Koblitz (1987),the calculation cost of point multiplication on ECC is much less than that of modular exponentiation in discrete logarithm problem (DLP) and both have the same security level. It is highly essential that the security of our proposed 4UAK is really dependent on elliptic curve DLP (ECDLP) and the symmetric encryption algorithm such as advanced encryption scheme (AES).

The Table 1 shows the comparison and contrast between the chen et al, Jin-Ho Yang and Chin-Chen Chang and our proposed methodology for the three messages such as X,Y and Z.

Table 2. Comparison and contrast between the chen et al, Jin-Ho Yang and Chin-Chen Chang and our proposed methodology for the three messages such as X,Y and Z.

Protocols	Message sizes	Calculation costs for message X	Calculation costs for message Y	Calculation costs for message Z
Chen at al	5824 bits	4ME+1MM+4H	4ME+1MM+4H	1ME+2MM+6H
Jin-Ho Yang and Chin-Chen Chang	832 bits	5PM+2SE	5PM+2SE	5PM+4SE
Our proposed methodology	>1 kilo bytes	2PM+1SE	1PM+1SE	2PM+1SE

Where, PM:Point Multiplication, SE:Symmetric encryption and decryption, ME:modular exponentiation, MM: Modular multiplication and H: Hash function.

5. Simulation results

In this research work paper we are simulating the security issues of blue tooth secure simple pairing (ssp) using elliptic curve cryptography (ecc).We are also planning to calculate the security performance issues of blue tooth using elliptic curve cryptography such as throughput, end–to-end delay and packet loss rate(plr). The throughput is one of the first important performance metric to compute the performance and security issues of blue tooth secure simple pairing (ssp) using elliptic curve cryptography (ecc). The throughput is directly proportional to the packet size. When the packet size is increasing rapidly the throughput also increases rapidly. The table 2 shows the different values of throughput in % when a packet is varies from 832, 1664 and 5824 bits. The throughput of a network represents the amount of network bandwidth available for a network application at any given moment, across the network links. Performance of the throughput between networks can be impacted/affected by some activities such as network LAN cards, switches, routers and the network design etc[21][30][33].

The mean throughput for a sequence of packets of specific size can be computed using the formula,

Mean Throughput (Thr) = $\sum_{i=1}^{n} Thri\ /N$ **----- (iii)**

Thr_i = (Paccept / Pcreate) x 100 ----- (iv)

Where the Thr_i=The throughput value when the packet '**i**' is accepted at the intermediate device like router or blue tooth secure simple pairing using elliptic curve cryptography gateway and '**N**' is the total number of packets received at router and Paccept is the number of received packets at router and Pcreate is the number of packets created by the source hosts,the mean throughput is the mean value for each communication. The table 2 shows an efficient throughput computed for an efficient blue tooth based SSP using ECC.

Table 3.The throughput of the corresponding blue tooth SSP using ECC with congestion.

Sl. No	Packet size (bits)	Throughput (%)
01	32	48
02	64	44
03	128	42
04	256	41
05	512	40
06	768	38
07	832	34
08	1664	28
09	5824	16

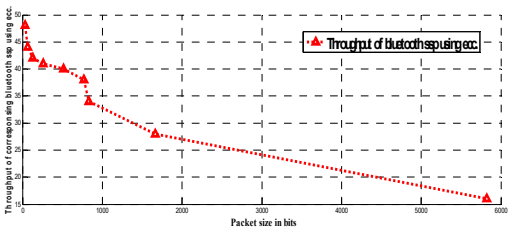

Fig 1. Throughput of blue tooth ssp using ecc when the congestion occurs.

Usually the throughput is directly proportional to the size of packets in bits or bytes. In this research paper the throughput is indirectly proportional to packet size in bits due to the traffic congestion which occurs and leads for dropping some packets in a blue tooth secure simple pairing elliptic curve cryptography.

The Throughput calculated when there is no congestion using blue tooth secured simple pairing (ssp) using elliptic curve cryptography. The table 3 shows the throughput computed for the blue tooth secured simple pairing (ssp) using elliptic curve cryptography.

Table 4. The throughput of the corresponding blue tooth secure simple pairing using elliptic curve cryptography without congestion.

Sl.No	Packet size (bits)	Throughput (%)
1	32	18.4
2	64	28.8
3	128	33.4
4	256	46.1
5	512	58.9
6	768	65.7
7	832	73.2
8	1664	82.6
9	5824	100.0

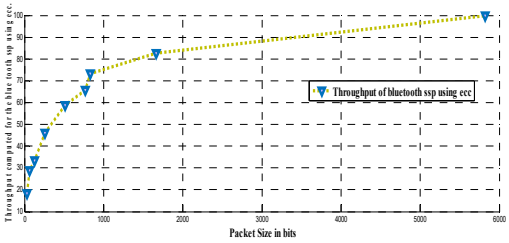

Fig 2. Throughput computed for blue tooth SSP using ECC.

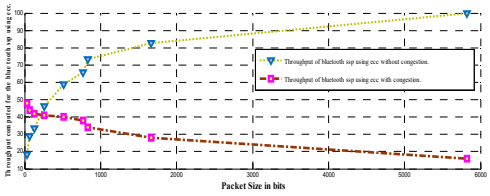

Fig 3. Throughput computed for blue tooth secured simple pairing using ecc with and without congestion.

When the n number of blue tooth devices connected to a piconet then the corresponding throughput with and without congestion is calculated as follows.

Table 5.Throughput computed for number of blue tooth devices with secured simple pairing using ecc with and without congestion.

Sl. No	Number of blue tooth devices connected to pico net.	Throughput with congestion (%)	Throughput without congestion (%)
1	06	99.6	15
2	20	84.8	26
3	50	75.6	33
4	80	64.3	45
5	120	54.7	58
6	150	45.8	65
7	180	34.9	70
8	210	23.2	80
9	240	14.1	90

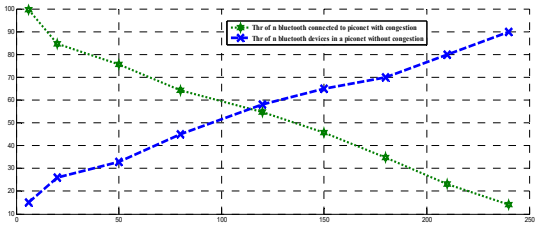

Fig 4. Throughput computed for n number of blue tooth devices connected to a pico net using secured simple pairing using ecc with and without congestion.

End–to-End Delay or RTT(Latency): It is the amount of time taken in a network communication when one packet likes to travel from one source host to another destination host and back to the originating host(source host). The RTT is one of the most important performance metric i.e. measured in research work simulation. The performance metric for RTT can be calculated in micro seconds.

The mean RTT for a specific size packet in each communication can be calculated as follows.

Mean RTT = $\sum_{i=0}^{i=n} RTTi/N$ **----- (v)**

Where **'i'**is a packet number and **'N'** is a number of packets sent. It is worth noted that the packet size is directly proportional to Round Trip Time (RTT)

$RTT_i = Tr_i - Ts_i$ ----- (vi)

Where as RTT_i is the Round trip time of packet "**i**", Tsi is the created time of a packet "**i"** at source host, Tri is the received time of a packet "**i**" at the destination host at the end of its journey. N is the number of packets received at the source node and the mean RTT is the mean RTT cost for each communication session.

The table 6 shows the end to end delay of blue tooth based secure simple pairing using elliptic curve cryptography.

Table 6. Computation of end to end delay of blue tooth based secure simple pairing using elliptic curve cryptography.

Sl.No	Packet size in Bits	End to End delay (milli seconds)
1	32	8
2	64	18
3	128	27
4	256	49
5	512	181
6	768	270
7	832	284
8	1664	512
9	5824	2080

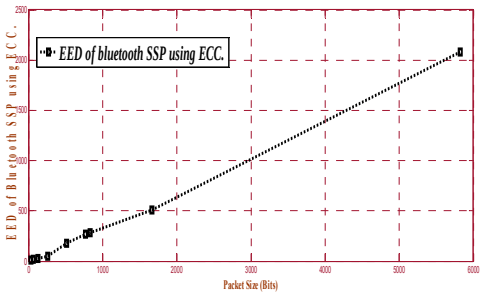

Fig 5. EED of blue tooth ssp using ecc.

Table 7: Appropriate End to End delay for n number of blue tooth devices connected in a piconet

Sl.No	Number of blue tooth devices connected to a pico net	Computed appropriate end to end delay (EED) (ms).
1	6	12
2	20	16
3	50	20
4	80	28
5	120	34
6	150	39
7	180	45
8	210	53
9	240	60

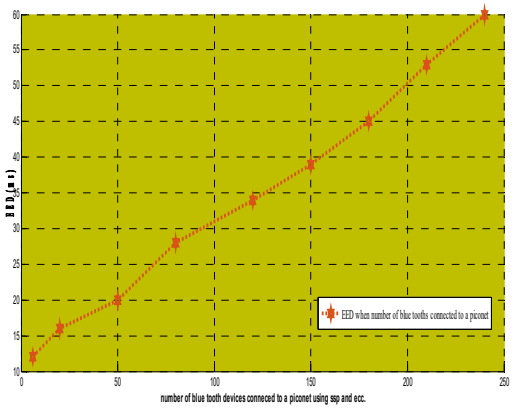

Fig 6. EED of blue tooth devices connected to a pico net with SSP using ECC.

Packet Loss Rate(PLR): Packet loss occurs during the communication between two or more hosts across the network. When two hosts exchange packets between their operating systems and some of the packets get dropped during the transmission due to overload which is called Packet Loss Rate. Most commonly, the packet gets dropped before the destination can be reached.

Packet Loss Rate/dropped rate (Pd) = Ps – Pr----------(vii).

Where Ps is the amount of packet sent at source and Pr is the amount of packet received at destination.

Jitter:Jitter is one which is defined as fluctuation of end to end delay from one packet to a next connection flow packet.

Jitter (J) = Di + 1 - Di----------(viii)

Where Di+1 is delay of i+1th packet and Di is the delay of ith communication packet. The table 4 shows the corresponding packet loss (drop) rate of blue tooth based secure simple pairing using an elliptic curve cryptography.

Table 8: Packet drop rate(Pdr) of blue tooth based secure simple pairing using an elliptic curve cryptography.

Sl.No	Packet size (bits)	Packet loss rate (%)
1	32	0.07
2	64	0.34
3	128	0.64
4	256	0.82
5	400	0.94
6	512	1.10
7	768	1.24
8	850	1.40
9	1664	2.20
10	5824	4.15

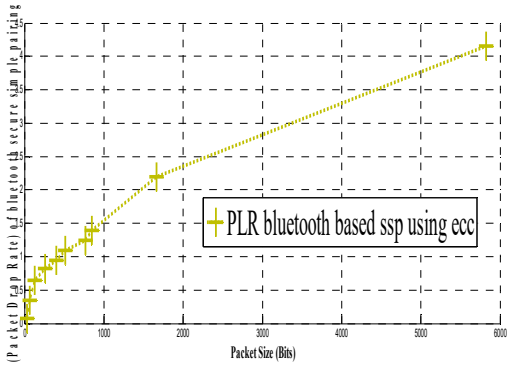

Fig 7. Corresponding packet loss rate of blue tooth secure simple pairing using ECC.

Table 9. Corresponding PDR calculated in (%) for different kinds of blue tooth devices connected in a Pico net

Sl. No	Blue tooth devices connected to a Pico net	PDR (%)
1	06	0.13
2	20	0.18
3	50	1.10
4	80	1.67
5	120	2.18
6	150	2.82
7	180	3.67
8	210	3.84
9	240	3.96

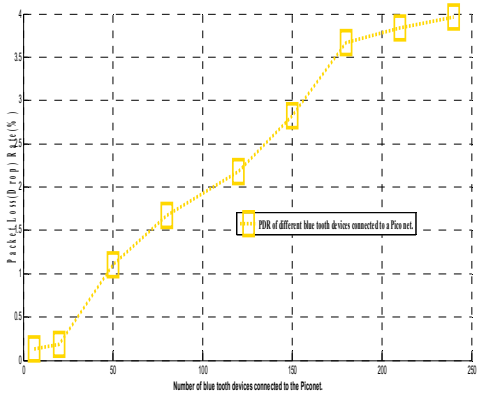

Fig 8. PDR of different blue tooth devices connected to a Pico net.

6. Concluding remarks

In this research paper we have taken an opportunity to study the problem of security issues of blue tooth i.e design, implementation and performance and security analysis of secure simple pairing (ssp) with elliptic curve cryptography using an efficient four party authenticated users (4UAK) blue tooth based secure simple pairing using an elliptic curve cryptography. In this paper we have taken an opportunity to evaluate the performance and security issues of blue tooth based secure simple pairing concept using elliptic curve cryptography with the help of various performance metrics such as throughput, end to end delay and packet drop rate. Our research results prove that Bluetooth also supports to the security issues using securing simple pairing with an elliptic curve cryptography.

Reference

[1] Mr.Ahmad Hweishel A.Alfarjat, Dr.Hanumanthappa.J., Prof.H.S.Sheshadri.,A Mathematical model to the Security issues of Bluetooth using Elliptic Curve Cryptography: International Journal of Computer Applications (IJCA),vol.46,no.5,pp.7-15,ISSN:0975-8887.

[2] Mr.Ahmad Hweishel A.Alfarjat, Dr.Hanumanthappa.J., A Survey over the Security Issues of Bluetooth Using Elliptic Curve Cryptography (ECC) International Journal of Computer Applications (IJCA),vol.150,no.8,pp.14-17,ISSN:0975-8887.

[3] Mr.Ahmad Hweishel A.Alfarjat, Dr.Hanumanthappa.J., Prof.H.S.Sheshadri 2017.,Security issues of Bluetooth based on Digital Signature using Elliptic Curve Cryptography (SBECDSA):International Journal of Current Multidisciplinary Studies (IJCMS),vol.3,Issue.01,pp.1-7,ISSN:2455-3107.

[4] Mr.Ahmad Hweishel A.Alfarjat, Prof.H.S.Sheshadri.,Study of Elliptic Curve Cryptography (ECC) for Bluetooth Security:A review,in proceeding of the two days International Conference on "Advances in Colloborative Research for Economics,Management,Humanities,Social Sciences and Computer Technology",June-2016.

[5] Jr.Burton,S.Kaliski,elliptic curves and cryptography:A Pseudorandom bit generator and other tools,Ph.D thesis,MIT,USA,1988.

[6] Andrew S.Tanenbaum,"Computer Networks",Pearson Education Inc,FourthEdition,2003.

[7] Ellis Horowitz Sartaz Sahni,Sanguthevar rajasekaran,Computer Algorithms,Galgotia publication.

[8] Dr.Hanumanthappa.J.,Ahmed Hweishel A.Alfarjat,"Security issues of Bluetooth based on Digital Signature using Elliptic Curve Cryptography (SBECDSA)",InterNational Journal of Current Multidisciplinary Studies",Vol.1.,Issue.01,July-2017,pp:1-7.

[9] Hanumanthappa.J.,IPv6 over Bluetooth:Security Aspects,Issues and its Challenges,in proceedings of NCWNT-09,Nitte-574110,Karnataka,INDA-12-17,2009.

[10] W.Stallings,1998.Cryptography and Network Security:Principles and Practice,Prentice Hall,p 399-432.

[11] B.Miller and C.Bisdikian, Bluetooth revealed:The insiders guide an open specification for global wireless'communications.Prentice Hall 2000.

[12] Bluetooth SIG,http://www.Bluetooth.com.

[13] K.Rabah,Theory and Implementation of Elliptic Curve Cryptography,Journal of applied science.,5:604-633.

[14] Hanumanthappa.J.,Ahmed Hweishel A.Alfarjat,Prof.H.S.Sheshadri,Implementation of Secure Simple Pairing using Bluetooth using elliptic curve cryptography,Dec-2017.

[15] Neal Koblitz ,elliptic curve cryptosystems,mathematics of computation,vol.48,pp.203-209,1987.

[16] N Koblitz,A Course in number theory and cryptography,2nd ed,Graduate texts in mathematics,vol.114, springer 1994.

[17] I.F.Blake,G.Seroussi,N.P.Smart,2000.Elliptic Curves in Cryptography,volume 265 of London Mathematical society lecture notes series.Cambridge University Press,Cambridge.

[18] Keijo Haataja,Pekka Toivanen,2008.Practical Man in the Middle Attacks against Bluetooth Secure Simple Pairing,in Proceedings of the IEEE international Conference,pp:1-5.

[19] Huaizhi Li,Mukesh Singhal,2005.A Key establishment Protocol for Bluetooth Scatternets,In Proceedings of the 25th IEEE international conference on Distributed Computing Systems Workshops (ICDCSW'05).

[20] Jen-Ho Yang,Chin-Chen Chang,2009.An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile commerce environments,Journal of Systems and Software,82(9), pp:1497-1502.

[21] E.Barker,D.Johnson and M.Smid,2007.Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography.Speacial Publication 800-56A.National Institute of Standards and Technology.

[22] K.Jarvinen and J.Skytta,On parallelization of high speed processors for elliptic curve cryptography, IEEE Transactions on very large scale integration(vlsi) systems,16(9) (2008) 1162-1175.

[23] T.M.apostol,Introduction to analytic number theory,Springer verlag,New York,1976,Undergraduate texts in mathematics.

[24] A.O.L Atkin and F.Morain,Elliptic curves and Primality proving,Math.Comp 61(203),29-68,1993.

[25] Darrel Hankerson,Alfred Menezes,Scott Vanstone,2003.Guide to Elliptic Curve Cryptography,Springer.

[26] Darrel Hankerson,Julio Lopez Hernandez,Alfred Menezes,2000.Software implementation of Elliptic Curve Cryptography over Binary Fields.

[27] Vincent Verneuil,2012.Elliptic Curve Cryptography and Security of embedded devices,Ph.D Thesis,pp:1-176.

[28] John Padgette,Karen Scarfone,Lily Chen,2012.Guide Bluetooth Security,National Institute of Standards and Technology,pp:1-39.

[29] Gustavo Padovan,2011.Bluetooth Security,University of Campinas-Brazil,pp:1-9.

[30] B.J.Birch,Cyclotomic fields and kummer extensions,In algebraic number theory,pp:85-93,Thomson,Washington,DC,1967.

[31] Gyozo Godor,Sandor imre,2011.Elliptic Curve Cryptography based Authentication protocol for Low-cost RFID tags,in proceedings of the IEEE international conference on RFID technologies and applications,pp:386-393.

[32] Jen-Ho Yang,Chin-Chen Chang,2009.An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile commerce environments,Journal of Systems and Software,82(9),pp:1497-1502.

[33] Juan-Carlos Cano,David Ferrandez-Bell,Pietro Manzoni,2004:Evaluating Blue tooth Performance as the support for context aware applications in proceedings of the IEEE International Conference on ICCCN,pp:345-350.

[34] Duesne.S.,Fouotsa.E.,2012.Tate pairing computation on Jacobi's elliptic curves,Pairing-Based Cryptography,Pairings,LNCS Springer verlag,vol.7708,pp:254-269.

[35] E.DeWin,S.Mister,B.Preneel,M.Weiner,1998.On the Performance of Signature Schemes Based on Elliptic Curves.In Algorithmic Number Theory:3rd International Symposium,Springer Lecture notes in computer science,pp:252-266.

[36] T.Pornin,2013.Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm,pp:1-79.

[37] D.Poulakis,2011.Some lattice attacks on DSA and ECDSA,Applicable Algebra in Engineering Communication and Computing,vol.22,pp.347-358.

[38] Prashanth Rewagad,Yogita pawar,2013.Use of Digital Signature with Diffie Hellman Key exchange and AES encryption algorithm to enhance Data Security in Cloud Computing,in proceedings of the IEEE international conference on communication systems and network technologies,pp:437-439.

[39] Diego F.Aranha,Ricardo Dahab,2010.Efficient implementation of Elliptic Curve Cryptography in WSN's,Advances in Mathematics of Communications,vol.4,no.2,pp:169-187.

[40] Hamish Silverwood,2007.A Matlab implementation of Elliptic Curve Cryptography,Summer Research Project

[41] J.H.Silverman,The neron-Tate height on elliptic curves,Ph D thesis,Hardvard University,1981.

[42] N.P.Smart.S-integral points on elliptic curves,Math proceedings.Cambridge philos.Soc.,116(3):391-399,1994.

[43] L.C.Washington,2008.Elliptic Curves,Discrete Mathematics and its applications (BocaRaton).Chapman & hall/CRC,Boca Raton,FL,Second edition,Number theory and Cryptography.

[44] E.Bekyel,2004.The density of elliptic curves having a global minimal Weirstrass equation.J number theory,109(1):41-58.

[45] F.Brezing and A.Weng,2005.Elliptic Curves Suitable for pairing based Cryptography.Des codes Cryptogr.,37(1):133-141.

[46] C.Breuil,B.conrad,F.diamond.,R.Taylor,2001.On the modularity of elliptic curves over Q:wild 3-adic exercises.J.Amer.Math.Soc.,14(4):843-939 (electronic).

[47] Pritam Gajkumar shah,Dr.Xu Huang,An enhancement of elliptical curve cryptography for the resource constrained wireless sensor networks,Ph.D thesis,University Of Canberra,2010.

[48] V.S.Miller,Use of elliptic curves in cryptography.In advances in cryptology-CRYPTO'85,vol,218 of lecture notes in comput.sci.,pages 417-426.Springer,Berlin,1986.

[49] J.S.Milne elliptic curves,Book surge publishers,Charleston,SC,2006.

[50] A.J.Menezes,P.C.van Oorschot and S.A.Vanstone,Handbook of Applied Cryptology.CRC press Series on Discrete Mathematics and its applications,FL,1997.

[51] Kenneth H.Rosen,Elliptic curves number theory and Cryptography,Second edition,Taylor and Francis group LLC,2008.

[52] Bundesamt fur Sicherheit in der informationstechnik,Technical guideline,Elliptical Curve Cryptography,version 2.0.

[53] J.H. Silverman,The arithmetic of elliptic curves,Graduate Text in Mathematics,vol 106,Springer,Berlin,1986.

[54] P.C.Kocher,Timing attacks on implementations of DH,RSA,DSS and other systems in:CRYPTO'96,in:Lecture notes in Comput.Sci.,vol.1109,Springer,Berlin,1996,pp.104-113.

[55] Xiaojiang Du,A routing driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks,IEEE Transactions on Wireless Communications,vol.8,no.3,March 2009.

[56] WhiteField Diffie,Martin.E.Hellman,New Directions in Cryptography,IEEE Transactions on Information Theory,Vol-22,NO.6,Nov,1976.
[57] R.Merkle,Secure communication over an in secure channel,Communications of the ACM.
[58] D.Knuth,The Art of Computer Programming,Vol.2.,Semi numerical algorithms,Reading,MA.:Addison Wesley,1969.
[59] W.Diffie,M.E.Hellman,Multiuser cryptographic technique,presented at National Computer Conference,New York,June 7-10,1976.
[60] A.V.Aho,J.E.Hopcroft and J.D.Ullman,The Design and Analysis of Computer Algorithms,Reading,MA.:Addison Wesley,1974.
[61] J.Hanumanthappa,"IPv6 and IPv4 Threat reviews with Automatic Tunneling and Configuration Tunneling Considerations Transitional Model:-A Case Study for University of Mysore Network",*International Journal ofComputer Science and Information Security*,vol.3.,No.1.,2009,pp 1-12.
[62] J.Hanumanthappa(2014),"DW&C:Dollops Wise Curtail IPv4/IPv6 Transition Mechanism Using NS2",International Journal Of Engineering Trends and Technology (IJETT),Vol.14,No.6.,pp 271-279.
[63] J.Hanumanthappa,2009,An Overview of Study on Smooth Porting process scenario during IPv6Transition (TIPv6),in Proceedings of IEEE IACC-09,Patiala,Punjab,INDIA-6-7,March-2009,pp 2217-2222.
[64] J.Hanumanthappa,"An Innovative Simulation,Comparison Methodology & Framework for evaluating the Performance evaluation metrics of a Novel IPv4/IPv6 Transition Mechanisms:BD-SIIT vs.DSTM,in proceedings of the IEEE First International Conference on Integrated Intelligent Computing(ICIIC-2016),SJBIT,Bengaluru,pp 258-263.
[65] J.Hanumanthappa(2011),A Simulation study on the performance of divide- and-conquer based IPv6 Address LPR in BD-SIIT IPv4/IPv6 transition using a Novel Reduced Segment Table(RST) algorithm in BD-SIIT Translator,Proceedings of International Conference on Computer's and Computing(ICCC'11),Lanzarote,Canary Islands,Spain(ISBN:978-1-61804-0008).
[66] J.Hanumanthappa,AbdulMalek Maresh Hassan Ali (2017),Quad Tree Based Static Multi Hop Leach Energy Efficient Routing Protocol:A Novel Graph Theoretic approach**,** International Journal of Computer Network and Communications(IJCNC),Vol.10.No.8,pp 1-21.
[67] J.Hanumanthappa,Ahmed Weishel A.Alfarjat,Prof.Sheshadri.H.S (2017),"Mathematical Modeling of Security Issues of WLAN's using Space Time Processing in DSP", *International Journal of Computer Science and Information Security (IJCSIS)*,Vol.15.No.8,pp 320-330.
[68] J.Hanumanthappa(2015),"Investigations Into The Design, Performance And Evaluation Of A Novel Energy Efficient Multipath Routing Algorithms in Wireless Sensor Networks", in Proceedings of *National Conference on Computer Science and its Applications (NCCSA)*,Dept of CS, Shri Shiradi Saibaba College of Engineering,Bengaluru.
[69] J.Hanumanthappa,Abdulmalek Maresh Hasan Ali(2017),"Comparison and Contrast between the performance issues of mDBR and mCoDBR novel cooperative routing protocols in under water sensor networks (UWSN's)", in *International Journal Of Research Science,Engineering Technology (IJRSET)*,pp 21-28.
[70] J.Hanumanthappa,Abdulmalek Maresh Hasan Ali(2017)," Node multi homing based policy routing using Mobile IPv6 in ns2",in proceedings of the *national conference on advanced information technology (NCAIT)*,SJBIT,Bengaluru,pp 169-175.
[71] J.Hanumanthappa(2015),"Mathematical Modeling of K-CCP Protocol of Coverage and Connectivity in wireless sensor networks",in Proceedings of the *National Conference on Computer Science and its Applications (NCCSA)*,Dept of CS,Shri Shiradi Saibaba College of Engineering,Bengaluru.
[72] J.Hanumanthappa(2015),"Performance and Evaluation of an Intra Cluster and Inter Cluster Novel Graph Theoretic Routing Algorithm (GTRA) in MANET's", in proceedings of the *UGC Sponsored State Level Conference on Next-Gen Computing (NGC):Challenges and Opportunities*,Post Graduate Department of Computer Science,SBRR Maha Jana First Grade College,pp109-115.
[73] J.Hanumanthappa(2015),"Comparison and Contrast between the Performance issues of T-SEP and E-SEP in Energy Efficient Wireless Sensor Networks (EFWSN's)", in proceedings of the *UGC Sponsored State Level Conference on Next-Gen Computing (NGC-2015):Challenges and Opportunities*,Post Graduate Department of Computer Science,SBRR Maha Jana First Grade College,pp 89-101.