A Mathematical Model to the Security Issues of Bluetooth using Elliptic Curve Cryptography

Ahmad Hweishel A. Alfarjat
Dept of E&C Engineering
PES College of Engg.
Mandya, University of Mysore.

H. S. Sheshadri
Dept of E&C Engineering
PES College of Engg
Mandya-571401.

Hanumanthappa J., PhD
Dept of Studies in Computer Science
University of Mysore.

ABSTRACT
In this research paper,we are addressing the problem of aalgorithms for Wireless LAN for Secured Transmission. Our research work also proposes an overview of some of the major attacks that Bluetooth has faced over the years along with some possible solutions. The main aim of our research work also investigates security features of Bluetooth using Elliptic Curve Cryptography(ECC). The ECC is the latest and fastest encryption method which offers stronger security. As we know that although a vast majority of devices already currently now communicates using Bluetooth methodology. The Bluetooth security expert provides automatic updates to its security protocol and user privacy protection technique for every security breach so that protection of the device user's personal information becomes the primary aim. The research work also explores the Bucket Brigade Attack on Bluetooth security using Elliptic Curve Cryptography(ECC). As we know that Bucket Brigade Attack(BBA)(MITM)(WITM) is one of the amazing solution to the problem of key agreement or key swapping. The beauty of this scheme is when two parties who likes to communicate using symmetric key and an Elliptic Curve Cryptography(ECC) an Intruder(Hacker) enters in between a sender and a receiver.

Keywords
Cryptography, Bucket Brigade Attack(BBA),Elliptic Curve Cryptography(ECC),Man-in-the-Middle Attack(MITM).

1. INTRODUCTION
Bluetooth is a methodology for short range Wireless data and real time two way voice transfer cooperating data rates up to 3 Mb/s. It is also used to connect almost any instrument to any other device. In now a day's Bluetooth enabled equipments such as Mobile phone's,Head sets,PC's, Laptops and printer's,Mice and Keyboards are mainly used all over the world. In the year 2006 one billion Bluetooth equipments are shipped and this number rapidly increases in the near future. The target volume for 2016 is as high as 3 billion Bluetooth devices. Therefore it is highly essential to show keen interest on Bluetooth security issues. Bluetooth is a technology defined by Bluetooth Special Interest Group(BSIG). Initially Bluetooth was considered as a simple serial cable replacement for electronic devices. Currently as we know that Bluetooth technology supports more advanced functionalities like Ad hoc networking and AP operation for Internet connections. The ongoing developments in Bluetooth technology extends new features such as support for QoS,higher data rates,multicasting and low power consumption.When the application area trying to expand as new products with Bluetooth capability are constantly introduced. With respect to the best our knowledge the Bluetooth technology is made up of different protocol layers ranges from physical radio and baseband to object exchange and service discovery. In addition the BSIG also specifies number of profiles which specify the criteria of messages, procedures and protocols required for supporting a specific service. It is already clear that the Bluetooth instrument is one which supports for either Point-to-Point Communication or Point to Multipoint Communication. Piconet is a network which consists of Bluetooth devices.

1.1.Bluetooth Security Architecture
Security in Bluetooth can be considered as a mechanism of defense against willful acts of smart adversaries people. The word security either implicitly or explicitly protection to some extent. The word protection is defined as the defense against random events such as accidents and failures. We also took an opportunity to swap safety and protection in our research and thesis work. The security design mainly involves defining a sequence of procedures for the cooperation of algorithms, protocols and their usage. As discussed above one more important aspect of security development specifically in Bluetooth is to design an efficient implementation of opted procedures consisting of their basic elements and interaction. There are so many similarities between WLAN and WPAN therefore they can merge into an individual technology known as WLANs.

This section clearly explores how security issues have been considered in present public Bluetooth specifications such as blu01,blu03,blu04a,blu07a,1blu99a,blu99b etc. The fundamental Bluetooth specifications are genuinely implemented by the user who resolves how a Bluetooth instrument it's connect ability and discoverability preferences. The various categories of connect ability and discoverability strengths can be chunked into three different parts such as

1. *Silent Preference:In*

Silent preference the instrument will never accepts any connections. The Bluetooth simply oversees the traffic.

2. *Private Preference:*

In this phase the instrument cannot determines non-determinable instrument Connections are only accepted when the Bluetooth Instrument Address(BI_ADDR) of the device is known to the perspective Master. To the best of our knowledge BI_ADDR is a 48 bit address which globally and uniquely specifies a Bluetooth instrument.

3. *Public Preference:*

In a Public preference the instruments can be ascertained and connected to therefore it also called an ascertained apparatus.

The Bluetooth equipment at a time broadly implements the following four different categories of security preferences such as Non-Secure,Service-level enforced security

preference,Link level enforced security preference,service level enforced security preference. We have also taken an opportunity to explore all the four different preferences as follows.

1. *Non-Secure*

Phase:As we Know in this type of phase Bluetooth does not initiate any security measures.

2. *Service level enforced security Phase:*

In this phase two different instruments can authenticate a non secure ACL(Asynchronous Connection less) link.The various security principles such as Integrity,Non repudiation,Authentication,Authorization,Encryption and Decryption are initiated when a L2CAP CO(Logical Link Control and Adaptation Protocol Connected Oriented) or an L2CAP CL channel request is made.

3. *Link level enforced security mode:Security*

Procedures are really initiated when an ACL link was constructed.

4. *Service level enforced security Phase:*

This phase is exactly similar to Phase-2 except that only Bluetooth devices utilizing SSP can use it.i.e only Bluetooth 2.1+EDR instruments can use this security phase.

2. LITERATURE SURVEY

The review of literature pertaining to the subject is undertaken to understand the better prevailing aspects in the field of Security issues of Bluetooth using Elliptic Curve Cryptography. This effort has been made to search available literature from text books,refereed international journals,reputed international/national conference papers,symposium papers,book chapters,internet data etc relevant to the study. The details of some of the reviews that have been made for the research work are summarized below.

For the last twenty five years,many researcher's,scientists have been actively engaged in proposing and developing a new flexible security issues of Bluetooth using Elliptic Curve Cryptography. It has made a notable contribution to the research group to do further research on the security issues of Bluetooth algorithms using Elliptic Curve Cryptography(ECC).

Rivest R.Shamir.A. and Adleman.L[7].have discovered the principles of RSA algorithm and also they have developed a method for obtaining Digital Signatures and Public Key Cryptosystems. Already in antiquity encryption was used in warfare and diplomacy. The ancient encryption techniques are insufficient in now a days but some of their ideas are utilized in the new encryption methodology. Public Key encryption techniques use a Public key for encryption and a private key for decryption. Typically Public Key Cryptography is used.

Diffie and Hellman in the year 1976 when introduced the concept of Public Key Cryptography the cryptographic importance of the apparent intractability of the discrete logarithm has been determined.

El Gamal first described how this problem may be utilized in Public Key Encryption and digital signature schemes. ELGamal techniques have been refined and incorporated into various protocols to meet a variety of applications and one of its extension create the basis for the U.S government Digital Signature Algorithm(DSA). The Discrete logarithm problem 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. The group of points on an elliptic curve specified over a finite field the jacobian of an elliptic curve defined over a finite field and the class group of an imaginary quadratic number field. Elliptic curves have been extensively studied for over a hundred years and there is a vast literature on the topic.

In the Year 1995 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 elliptic curve cryptosystems 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.

Koyama et all have proposed elliptic curve analogues of the RSA cryptosystem. In these systems works in an elliptic curve defined over the ring Zn where n is a composite integer and the order of the elliptic curve group serves as the trapdoor. The security of these methods is based on the difficulty of factoring n.

Kurosawa,Okada et all subsequently showed that these elliptic curve analogues do not have any significant advantages over their RSA counterparts. Charlap and Robbins showed elementary self-contained proof's for some of the basic theory.

Hermelin.M.,Nyberg.K.(1999) theoretically proved that Bluetooth stream cipher with 128 bit key can be wrecked in O(264) steps.

Canniere et al(2001) had proved that E0 stream cipher of Bluetooth has some security imperfections.

Jakobsson.M. and Wetzel.S.(2001) for the first time formulated MITM attack on Bluetooth 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 Bluetooth PIN and the confidentiality problem caused by site tracking

3. PROPOSED METHODOLOGY

3.1.A Mathematical modeling to Security issues of Bluetooth using ECC.

In this research work we are Implementing the issues of Bucket Brigade Attack(BBA) using Elliptic Curve Cryptography. As we know that Bucket Brigade Attack(BBA) is one of the amazing solution to the problem of key agreement or key swapping. The beauty of this scheme is when two parties who likes to communicate using symmetric key and an elliptic curve cryptography an Intruder(Hacker) enters in between a sender and receiver. Bucket Brigade Attack is based on Public Key Cryptography. The Public Key Cryptography has devised by Diffie and Hellman in the year 1976 and created a great milestone in the history of Public Key Cryptography. RSA was developed by Rivest,Shamir and Adleman in the year 1977 and was published in 1978. The Diffie Hellman Key was based on the use of Discrete logarithm. Elliptic Curve Cryptography(ECC) is based on Mathematical Properties of elliptic curves and it shows to offer equal security to RSA for a much smaller key size. The Bluetooth version 2.1+EDR improves the security of pairing by using Elliptic Curve Diffie Hellman(ECDH) Public Key

Cryptography. ECDH is a key agreement protocol for allowing two communicating parties to establish a common secret key over an unsecured path. It becomes a variant of Diffie Hellman Key quid pro quo protocol using ECC. An elliptic curve over real numbers R is a set of points(x,y) which satisfies an equation y2=x3+ax+b in which (x,y,a,b) ε R. The elliptic curve is one which maintains an element O,which is called the point at infinity. The various computations over real number are slow and an inaccurate because due to the presence of round error. Therefore elliptic curves with x,y,a,b ε R are not usable in practical. Instead of elliptic groups modulo p(where p is a prime) are defined in the following way. Two non negative integers a,b<p which satisfies 4a3+27b2 ≠0 mod p are chosen. Ep(a,b) specifies the elliptic group modulo p where elements(x,y) are pairs of non negative integers less than p satisfying both y2 ≡x3+ax+b mod p and the point at infinity O. It is worth noting that the number of points on the elliptic curve is not infinite. Even it is not clear how to connect these discrete points on the elliptic curve is not infinite. Moreover it is clear even how to connect these discrete points to make their graph look like a curve. The geometrical definition of operations on these points cannot be used. The algebraic integrity constraints are mainly used to make calculate precisely elliptic curve groups modulo p.

The Elliptic Cryptosystem can be defined in the following ways. The domain values are as follows:

A Prime number p and parameters a and b specifying an elliptic group of points $E_p(a,b)$.

A generator point G on $E_P(a,b)$:One of an important criterion for choosing G is that the smallest value of n(n is said to be the order of point G) for which nG=0 be a large number.

The private key is an integer k,where 2<=k<=n-2.The public key is the point Q=Kg. A key swapping between obama and hanums can be performed easily with ECC as an analogue to the Diffie Hellman Key swapping. The Diffie Hellman works similar to the following way as follows.

Obama keys are (K_A,Q_A) and Hanums.J. Key are (K_B,Q_B). Obama computes the secret key $K=K_AQ_A$ and hanums computes the secret key $K=K_BQ_A$. Both computations to create the same result because $K=K_AQ_B$ $=K_Ax(K_BG)=K_BXK_AG=K_BQ_A=K$. Therefore Obama and hanums can use the symmetric key encryption of messages with 3DES, Blowfish or AES.

The encryption and Decryption procedure are as follows. The Plain text message m is specified as a point P_m on $E_P(a,b)$.The various straight forward methods of transforming the message m into coordinates on the elliptic curves exist. When Obama likes to encrypt and send P_m to hanums he picks a positive an integer k and creates the cipher text $C_m=\{kG,P_m+kK_B\}$. Hanums can try to calculate and decrypt the cipher text by computing $P_m+kQ_B-k_BX(kG)=p_m+kx(k_BG)-k_G=P_m$. Finally the hanums decodes the plain text message m from the point P_m.

3.2.Bucket Brigade Attack(Man-in-the Middle)(MITM)attack(Woman-in-the Middle)(WITM) attack using Elliptic Curve Cryptography.

Bucket Brigade Attack is one of the beautiful concept introduced in Cryptography and Network Security. *Bucket Brigade Attack(BBA) is called MITM attack.* Let us assume that Barack Obama(Obama) and Hanums.J.(Dr.Hanumanthappa.J.) are trying to communicate with each other and they wish to protect their communication by utilizing Public Key Encryption technique. In a BBA(MITM) attack Adarsha.H.(An Intruder(Hacker) intrudes between obama and Hanums.J. Adarsha.H. can easily drops eavesdrop/modify/delete/generate messages between obama and hanums.J. in such a way that his presence is unrevealed. Obama and hanums do not know that the link between them is compromised by Adarsha.H. Adarsha.H. is also able to imitate Hanums.J. when talking to obama and vice versa. The Diffie Hellman key swapping algorithm does not solve all our problems associated with the Key swapping. Diffie Hellman key swapping algorithm can fall pray to the man-in-the-middle attack(Woman-in-the Middle Attack) also called as Bucket Brigade Attack (BBA)(MITM).

The simple procedure of MITM(BBA) is as follows.

1.Obama wants to communicate with Hanums.J. securely and therefore he wants to do a Diffie –Hellman key exchange with him. For this purpose he sends the values of n and g to Hanums.J. as usual. Let n=17 and g=7.(As usual these values will form the basis of obamas A and Hanums.J. B which will be used to compute the symmetric key K1=K2=K).

Obama does not realize that the attacker Adarsha.H. is listening quietly to the conversation between his and Hanums.J. Adarsha.H. simply picks up the value of n and g and also forwards them to Hanums.J. as they originally were.

Obama	Adarsha.H.	Hanums.J.
n=11,g=7	n=11,g=7	n=11,g=7

Fig.1.Man-in-the Middle(MITM)(BBA)(WITM) Attack Part-I.

Now let us assume that Obama,Adarsha.H and Hanums.J. choose a random number x and y as shown in Fig.2.

Obama	Adarsha.H.	Hanums.J.
x=3	x=8,y=6	y=9

Fig.2.Man-in-the Middle(MITM)(BBA)(WITM) Attack Part-II.

The question usually arises why Adarsha.H. chosen two values such as x and y? Based on these values all the three persons compute the values of A and B as shown in Fig.3.

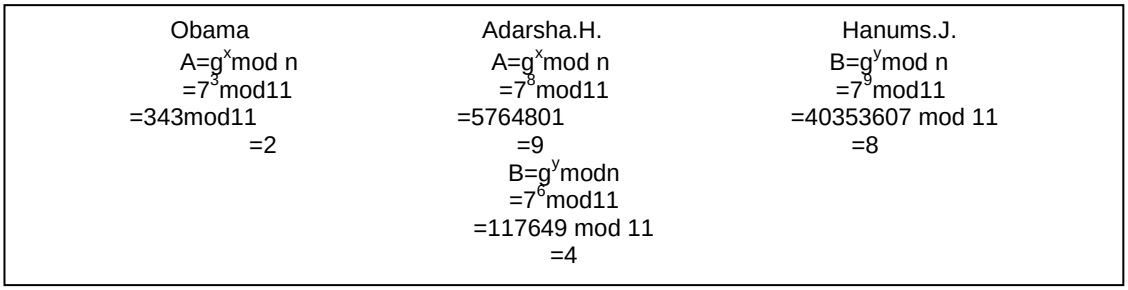

Fig.3.Man-in-the Middle(MITM)(BBA)(WITM) Attack Part-III.

Now the real drama commences here as shown in Fig.4.As shown in Fig.4. The following things happen as follows.

1.Obama sends his A(i.e 2) to hanums .J. Adarsha .H. intercepts it. and instead sends his A(i.e 9) to Hanums .J. .Hanums .J. has no idea that Adarsha .H. had hijacked Obama's A and has instead given his A to Hanums .J. In return Hanums .J. his B(i.e 8) to Obama. As before Adarsha .H. intercepts it,and instead sends his B(i.e 4) to Obama. Obama thinks that this B came from Hanums .J. He has no idea that Adarsha .H. intercepted the transmission Hanums .J. and modified B. Therefore at this juncture Obama,Adarsha.H.,Hanums .J. have the values of A and B as shown in Fig.5.

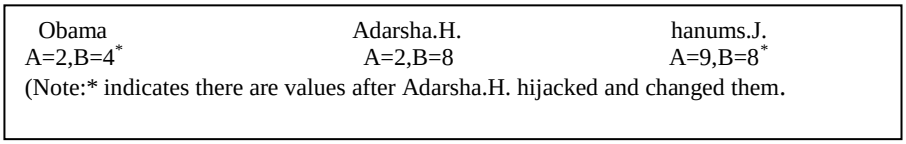

Fig.5.Man-in-the Middle(MITM)(BBA)(WITM) Attack Part-5.

4. PERFORMANCE EVALUATION OF BLUETOOTH SECURITY ISSUES USING ELLIPTIC CURVE CRYPTOGRAPHY.

4.1.Introduction to Performance security issues of Bluetooth.

The first BBA attack on Bluetooth was devised by Jakobsson and Wetzel for version 1.0B of the standard. However it works with all Bluetooth versions up to 2.0+EDR with no major security improvements were implemented in those Bluetooth specifications. The attack already assumes that link key used by two victims by equipments is known to the attacker. The authors are also shown how to obtain the link key by utilizing off-line PIN crunching attack by passing eavesdropping on the initialization key establishment protocol. The BBA(MITM)(WITM) attack requires that both devices are using public or private security phase i.e both devices suffering from victim are connectable. To prevent the jamming of communication media the victim devices such as Master and Slave operates by using two different Piconets.

Kugler further improves the attack of Jakobsson and Wetzel. Kugler also proved how a MITM attack can be performed during the paging procedure. The Master and Slave use the same channel hoping sequence but a different offset in this sequence. The attack also works in the case where both victim devices send and receive same data packets over an encrypted channel. Bluetooth 2.1+EDR supports the protection against the MITM attacks explored by means of SSP. However we have proved that MITM attacks against Bluetooth 2.1+EDR are also possible because SSP supports various association models,the selection of which depends on the capabilities of the target equipments,the attacker can force the devices to use a less secure mode by modifying the capabilities information.

4.2.Performance Analysis and Metrics.

Performance analysis is an important reference for designing a good network.The metrics which the research work used here are Latency,Throughput and Packet Loss rate.Discrete event simulator NS2 particularly popular in the wired networking community has been chosen as the common framework to simulate the various existing and the proposed IPv4/IPv6 transition scenarios in the research work. NS2 simulates the IPv4/IPv6 transition performance problems by using the various performance metrics such as Throughput,End-to-End Delay (RTT)(Latency) Packet Loss and it presents one of the best case scenarios for the typical use of IPv4/IPv6 transition. Implementation of IPv4/IPv6 BD-SIIT translators is simulated by using NS2 Simulator.

5. SIMULATION RESULTS

The various results of an Interception of Packets attack when an Encryption technique is not allowed in Security issues of Bluetooth using ECC is shown in the following Table-1.

Table-1.Interception of a Packet attack in an Encryption Mechanism is not allowed.

Packet. No	Freq	BT Clock	Data in Bytes	Acknowledgement Received.	Idle Time	Time Stamp
767890	2479	139717868	0,32,64.	Yes	358.600 Micro Sec	00811.712
767891	2408	139717869	0,32,64.	Yes	359.689 Micro Sec	00812.657
767892	2409	139717870	0,32,64	No	340.768 Micro Sec	00813.459

When an Intruder Adarsha.H. tries to hack a packet of TCP,UDP or FTP while transmitting from source to destination the intruder cannot understand the contents of the intercepted data packet. Whatever 16 bit CRC field calculated from baseband packet payload does not match the received CRC field. So our Bluetooth protocol analyzer shows the CRC field in a red to represent the mismatch between CRC checksum and the eavesdropper Adarsha.H. easily identifies the messages are easily encrypted. We are calculating Throughput,End-to-End Delay and Packet Loss Rate(PLR) of Security issues of Bluetooth with Man-in-Middle Attack(MITM)(BBA)(WITM) using Elliptic Curve Cryptography.

Table-2.Corresponding Throughput computed for Security issues of Bluetooth using ECC When the Packet Size varies from 32 Bytes to 1024 bytes

Sl.No	Packet size in Bytes	Throughput Of MITM for Security issues of Bluetooth using ECC.
01	32	97.0
02	64	95.6
03	128	93.0
04	256	84.7
05	512	82.3
06	768	77.8
07	1024	74.2

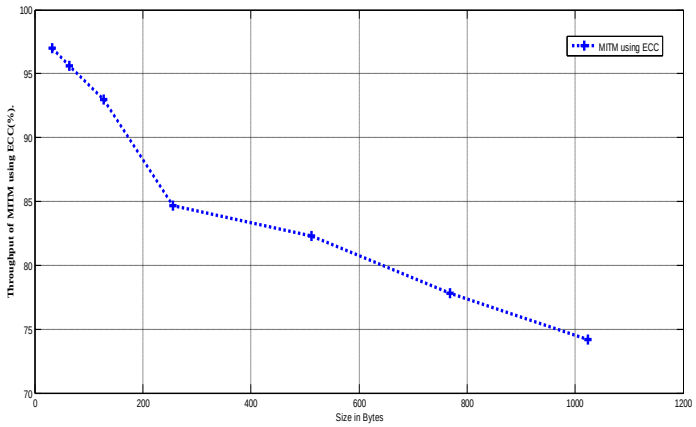

Fig.6.Throughput Computation of MITM using ECC

Table 3.End to End Delay of Man-in-The-Middle Attack(MITM) for Security issues of Bluetooth using ECC

.Sl.No	Packet size(Bytes)	EED(ms) of BD-SIIT by of HJ
01	32	15.00
02	64	35.00
03	128	55.00
04	256	98.00
05	400	248.00
06	512	353.00
07	768	540.00
08	850	620.00

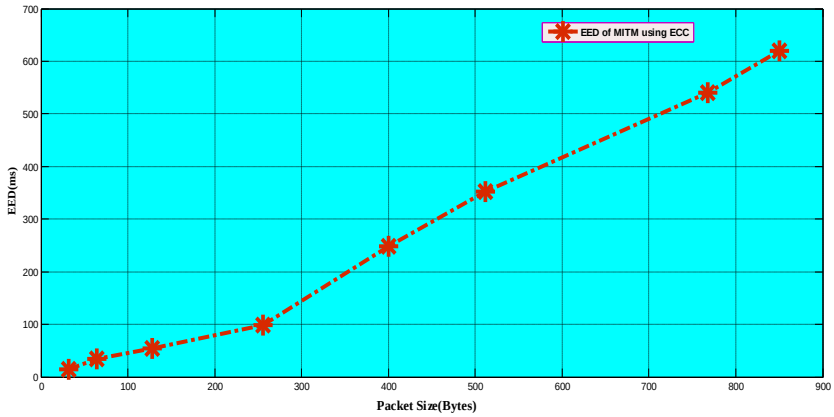

Fig.7.End-to-End Delay(EED) Calculation of MITM using ECC when a Packet Size varies from 32 to 850 Bytes.

Table 4.Calculation of Packet Loss Rate(PLR) of MITM using ECC when packet size varies from 32 bytes to 850 bytes.

Sl.No	Packet size (Bytes)	Corresponding Packet Loss Rate(%) of MITM using ECC.
01	32	0.15
02	64	0.68
03	128	1.26
04	256	1.65
05	400	1.94
06	512	2.20
07	768	2.45
08	850	2.80

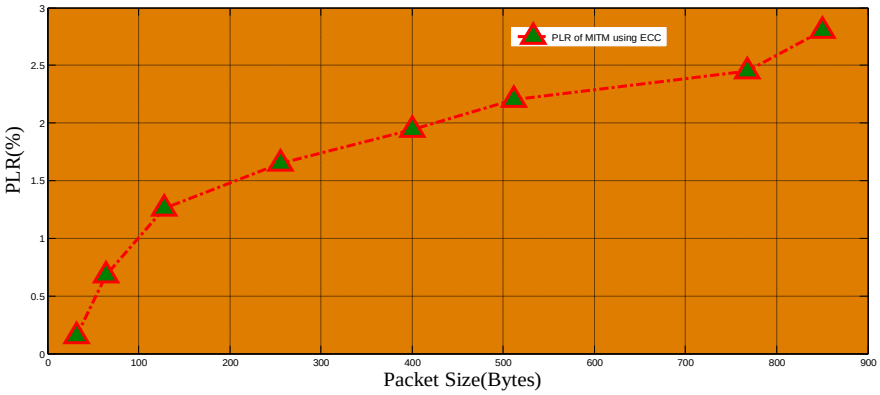

Fig.8.Packet Loss Rate(PLR) Calculation of MITM using ECC when a Packet Size varies from 32 to 850 Bytes.

6. CONCLUSION

In this research paper we have proposed and security issues of Bluetooth using Elliptic Curve Cryptography. We are practically implemented this work by using the network simulators such as NS2. We have computed the various Performance metrics such as Throughput,End-to-End Delay(EED) and Packet Loss Rate(PLR) using ECC.The Throughput is indirectly proportional to the Packet Size where as EED and PLR are directly proportional to the Packet Size.

7. REFERENCES

[1]W.Diffie and M.Hellman,New directions inCryptography,IEEE Transactions on Information Theory,Vol.22(1976),pp.644-654.

[2] Bluetooth SIG:Bluetooth Wireless Technology Surpasses One billion devices.

[3] Tan A:Bluetooth gets high speed boost.CNET Networks,ZDNet Asia,newscopy march 9,2006.

[4] Suomalainen.J.,Valkonen.J.et all:Security Associations in Personal Networks–A Comparative Analysis .Proceedings of the fourth European workshop on Security and Privacy in Ad-hoc and Sensor Networks(ESAS-2007),LNCS,Vol.4572,springer-verlog,pp.43-57.

[5] William Stallings:Cryptography and Network Security Principles and Practice.3rd Edition,Upper saddle river,New jersey,PH,2003.

[6] Spill .D. and Bittau.A.:Bluetooth –Eve meets Alice and Bluetooth,Proceedings of the first Usenix workshop on offensive technologies(WOOT-2007),Boston,MA,2007.

[7] Rivest .R.,Shamir.A. and Adleman.L.:A Method for obtaining Digital Signatures and Public Key Cryprosystems,Communications of the ACM,Vol.21,No.2,Feb,1978,pp-120-126.

[8] Borisov.N.,Goldberg.I.,and Wagner.D.,Intercepting mobile communications the insecurity on 802.11 Proceedings of the 7th Annual International Conference on mobile computing and Networking,ACM Press,2001.

[9] Bluetooth SIG:Bluetooth Wireless Technology Surpasses one Billion Devices,Bluetooth SIG,press release,Nov.13,2006.

[10] D.Kugler,Man in the Middle attacks on Bluetooth,in Proc 7th Int Conf Financial Cryptography(FC'03),Gosier,Goudeloupe,French West Indies,Jan.27-30,2003,pp.149-161.

[11] M.S.Hwang,C.C.Lee,J.Z.Lee et al,A Secure Protocol for Bluetooth piconet's using Elliptic Curve Cryptography,Telecommunication systems,vol.29,no.3,pp-165-180,2005.

[12] C.T.Hager and S.F.Midkiff,An Analysis of Bluetooth Security vulnerabilities in Proc Wireless IEEE Communication and Networking Conference(WCNC-2003),New Orleans,LA,USA,Mar-16-20,pp-1825-1831.

[13]D.Bae,J.Kim,S.Park and O.Song,Design and Implementation of IEEE 802.11i architecture for next generation WLAN in Proc 1st SKLOIS Conf Information Security and Cryptology(CISC-2005),Beijing China,Dec 15-17,Springer verlog,pp.346-357.

[14] W.C.Barker,Recommendation for the triple data encryption algorithm block cipher,National Institute of standards and Technology(NIST),Gaithersburg,MD,USA.

[15] S.Das,F.Anjum,Y.ohba et al,Security issues in Wireless IP networks in Mobile internet:Enabling Technologies and Services.

[16] E.B.Fernandez,S.Rajput,M.Vanhilst,Some Security issues of Wireless systems,Jan 24-28,2005.

[17] N.Koblitz,Elliptic curve cryptosystems,Mathematics of computation 48(1987) 203-209