Analysis of Lightweight Security Protocol for Bluetooth Communication with ECC Approach

SAIYED FAIAYAZ WARIS
Department of Computer,Mizan Tepi University, Ethiopia

Abstract
Algorithm is proposed to transfer data more securely along Bluetooth channel. To transfer data confidentially between paired devices a 128-bit stream cipher algorithm E0 is used in Bluetooth communication .E0 is vulnerable to certain types of security attacks. Vulnerabilities present in E0 and conditions are discussed. Proposed algorithm use AES for data encryption, which can be used as block cipher [E0 works in stream ciphering mode].The keys used in AES is encrypted using elliptic curve cryptography [ECC], most secure and fast algorithm use small size keys. It is almost unfeasible to attempt a brute force attack to break the cryptosystem using ECC.

Keywords -AES; EC, Bluetooth, E0;

I. INTRODUCTION

Bluetooth technology is short range, low power wireless communication technology. Bluetooth is designed to replace cables via wireless communication. Bluetooth is able to communicate in short range of 30m and with a decent data rate of about 1mbps. Bluetooth is mainly used for communication between mobile devices and also in application we need small data rate and consume low power, Now a days Bluetooth is also used in wireless sensor networks due to its low power consumption property. Bluetooth is an open system so it can have some security risks. Nowadays a lot of mobile phones and other different devices include Bluetooth and in some cases the people who buy those devices don´t now even that the Bluetooth system is operating.

One of the biggest attractions of the implementation of this technology is the creation of networks with the Bluetooth technology is possible to form different networks in the same geographical point, with relatively high speed of transmission.

In section II is about Bluetooth technology pairing and encryption algorithms. Section III we discussed about vulnerabilities in present algorithm and section. IV discussed proposed algorithm and comparative study. Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is generally used to transfer data, establish connection in peer to peer [p2p] networks.

Bluetooth technology has been integrated to many devices but mainly in mobile terminals like laptops, palmtops and mobile phones [2].

This allows users to form ad hoc networks, Piconets between a wide variety of devices to transfer voice and data. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-Middle attacks, message modification, and resource misappropriation [1].

Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized usage of Bluetooth devices and other systems or networks to which the devices are connected.

The Bluetooth technology use a stream cipher E0, E0 is vulnerable to certain types of attacks and some cases cracked by $0(2^{64})$.In those application where data confidentiality is most important E0 is not a good option. In E0 a key stream output is exclusively or-ed with payload bits and sent to the receiving device [4]. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSR). The encryption function takes the following as inputs: the master identity (device address), the 128-bit random number, a slot number, and an encryption key, which combined initialize the LFSRs before the transmission of each packet, if encryption is enabled [3].

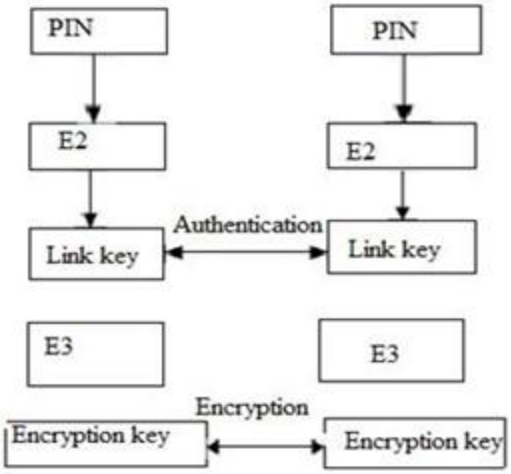

Fig1: Key generation, Authentication, Encryption[1].

II. SECUIRTY PROTOCOLS OF BLUETOOTH

A. Bluetooth security mechanism

Following are three security modes specified in Bluetooth specification

- Basic Mode 1: It is the lowest security mode, no security is provides in this mode
- Medium security mode: this is service-oriented security model. it starts after the establishment of the channel;
- Highest security mode: link-oriented security model, which install and initial before communication link is established.

Bluetooth Technology standard provides safety precautions in the application layer and link layer, communication sides, sender and receiver achieve Authentication and encryption in the same way. Link layer uses following four entities to ensure the safety: authentication keys. The secret key is changed every time you activate encryption and calculated from same authentication key. The random number can be generated by Messene twister because of its property of non-repeatability and random generation [7].

B. Process of encryption and authentication of Bluetooth. Bluetooth security mechanism has three modules, first is key generation, second authentication and third is encryption. It uses four different algorithms E0, E1, E2, E3.E2 algorithms is used to get PIN code which is entered by user. Link keys are generated by E3 algorithms by using PIN code. E0 algorithm is used to encrypt the data. Following figure is the process of Bluetooth encryption.

- The Bluetooth device addresses which is of 48 bits decided by the IEEE.
- 128 bit authentication key for authenticating entities
- 8 to 128 bit secret key for data encryption;
- 128-bit random number.

In the initialization process two keys are generated and they do not opened, encryption key is generated later in certification process from the two previously generated. The modules key generation, authentication and encryption in Fig 1 are as following:

- Key generation: user enter a 4 digit code which is used as input for E2 algorithm to generate link keys, then by using E3 algorithm encryption key is calculated by using link keys generated by E2 algorithm.
- Encryption: data is encrypted by E0 algorithm.
- Authentication: authentication process is carried out by using algorithm E1.

C. E0 algorithm

E0 algorithm is used in Bluetooth link layer to encrypt data. E0 is a stream cipher .E0 algorithm takes the data stream and XOR with pseudorandom numbers. Encryption of each packet is done separately. The linear feedback shift registers are used to generate pseudorandom numbers. During decryption exclusive-or operation is conducted one more time to get the plain text.

III. WEAKNESES OF BLUETOOTH SECURITY MECHANISM

The main weakness is with pseudo-random numbers, if pseudorandom number sequence makes a mistake, in this situation we will not get plain text in the process of decryption from the cipher text.

The security of E0 algorithm is based on internal mechanism of the secret key stream generator. If the input to E0 algorithm is sequence of 0's then the cipher text we get is the plain text. If the input is 16 bit mode, then E0 algorithm is only an XOR, which is ignoring security. At last we can say that the security of E0 depends on the XOR operation and one time pad [5].

B. Confined resources capability of LFSR

Bluetooth technology standard defines E0 algorithm for Encryption which is somewhat fragile, and it uses 128-bit key, in some cases, the complexity of their decoding is only 0.In E0 stream cipher uses 4 LFSR key stream generator. If any LFSR out of 4 LFSR key stream generators create a sequence of cycle is shorter than the key, then there is threat of divide and conquer technique used by the attacker to find keys. And software implementation of LFSR is not efficient. At the at the implementation time, it is required to refrain from the sparse feedback polynomials, because they are vulnerable to correlative attack, it is inefficient and ineffective to thickset feedback polynomial. In fact, the software implementation of LFSR algorithm is slower than the proposed algorithm based on AES and ECC [4].

C. Low Reliability of PIN

A PIN code of 4-digit and a variable is used in Bluetooth technology to generate link key and the key for encryption. A randomly chosen 4-digit code by user is only the real key transported in air. In the process of establishment of a link key, attacker can capture the communication data packet in the initial communication process. Attacker tries brute force attack on PIN to generate different types of related parameters, including the link key. If the PIN code is L bits, then in case of cipher text attack, an attacker can search the value of the PIN code through 2L times. Therefore, the reliability of the PIN code is very less; there are only 10,000 possibilities for 4 bits PIN code. We can use 16-byte PIN code in place of 4-bit PIN code, it make difficult for attacker to find the encryption key, but in each secure connection establishment we have to enter a PIN code. So using longer PIN code is very inconvenient [6].

D. Address Spoofing

Bluetooth technology standard recommends a unique address to every Bluetooth device. Its uniqueness gives rise to new problems. As the ID links to a particular fixed person, the activities performed by the person can be recorded and that person can be easily tracked. This violates the individual privacy.

All problems stated above shows that Bluetooth security systems are highly unsecure, but we generally use Bluetooth to transfer data that is not much sophisticated. Bluetooth standard are generally used in small networks as piconet where only 9 devices can be connected at same time, and securities technologies. As now a day's Bluetooth technology is also used in sensor networks due to its low power consumption and adequate data rate property. Now Bluetooth nodes are more complex and multiple, the existing algorithms for key distribution and authentication cannot meet the demands. Bluetooth technology only provides security to small networks and small scale applications, it appears to be enough for these applications, but to use Bluetooth technology more widely, we have to use more complex and powerful algorithms like AES and ECC.

IV. THE IDEA AND PROCESS OF PROPOSED ALGORITHM

Advance Encryption Standard (AES) is a symmetric key encryption algorithm, it is a block cipher and available in 128,192,256 bits key size and block size of 128 bits. Advanced Encryption Standard (AES) symmetric encryption algorithm for high throughput application (audio or video).AES is computationally faster than ECC. So for data encryption we have used AES and Elliptic Curve Cryptography (ECC) which is used as a public key mechanism. AES is based on substitution permutation. It is not a fiestel cipher like DES. AES algorithm operations are conducted on a 4×4 matrix of bytes, termed the state .State is a version of Rijndael algorithm with a larger block size and have additional columns in the state). Most calculations of AES are done in a special finite field.

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reveres rounds are applied to transform cipher text back into the original plaintext using the same encryption key .ECC is well suited for application in mobile communication. The ECC algorithm provides the same level of security as RSA but with a significantly shorter key length. Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Elliptic curves are not ellipses.

In ECC start with an affine point called Am(x, y). These points may be the Base point (G) itself or some other point closer to the Base point. Base point of elliptic curve implies that it has the smallest (x, y) coordinates, which satisfy the elliptic curve. Based on comparison of AES and ECC and using advantages of both of algorithms and avoiding their shortcomings in new algorithm. As to secure transfer of keys in key linking phase of ssp [secure simple pairing] we are using ECCDH. The key shared in that process using ECCDH are used in encryption,. Let the sender is Ua, the receiver is Ub. Ub's public key is Pb, Ub's private key is Db, K is AES encryption session key.

A. Encryption:

Data encryption is done using AES-128,A session key is generated by pseudo random number generator to generate a 128 bit session key and one session key is use only once to provide more security. Data to be sent is organized in 4×4 blocks and encrypted by AES. Then session key is encrypted using ECC, both encrypted key using ECC and encrypted data is sent to receiver. As the bits is encrypted in blocks and a session key in generation for every block, if error Accor it only affect a block not whole the message. And that block may be retransmitted Algorithm

At sender side

Step 1. Sender calculate two a random number R1 and R_2 using a random number generator, we have choose merssene twister to calculate random number because of its large period $2^{19937} - 1$.

Step 2. Calculate session key Ks as

Ks = h (R_1) h(R_2)

We are using 128 bit MD5 algorithm, 128 bit MD5 have two advantage first it converts the R to 128 bit code that can be easily used as 128 bit session key, second 128 bit hash make more difficult for attacker to guess the session key and we are calculating and the XOR of hashed R_1 and R_2 to make prediction more difficult.

Step 3.Sender encrypt the data D using the 128 bit as Encrypted data

De = E(Ks ,D)

Step 4. Calculate public key K_p using the ECDH

Step 5. Encrypt Ks using ECC encryption

$K_a = E(K_p .Ks)$

Step 6. Sender calculate hash of

(j , t_j , De ,Ka)

j is the sequence, t_j is the clock

Step 7.Sender calculate

[h(j , tj , De ,Ka), (j , tj , De ,Ka)]

Send to the receiver end.

B. Decryption At receiver side

Step 1. Receiver U_b calculate the hash of

(j , t_j , De ,Ka) And compare with the stored hash in the message; if the hash matches accept the message otherwise discard.

Step 2. Validate tj with the local current time Clock.

If the in equations

$$| Clock - tj | < \Delta t$$

Holds, then proceed to next step, else reject the message. Here Δt denotes the time of the expected network delay which can be estimated according to different applications.

Step 3. Receiver decrypts key

K_a to get Ks as $Ks = D(K_p ,Ka)$

Step 4. Using the key Ks receiver decrypt the De to get data as

Data=D(Ks, De)

C. Advantages of proposed algorithm

Proposed algorithm removes the vulnerabilities present in Bluetooth security mechanism and with little overhead; it is more useful in applications where confidentiality is bigger issue

- As the proposed algorithm used ECDH to create public keys there is no need to send AES keys before starting communication.
- We only need to create public keys once by ECDH and we only have to maintain one key secrete.
- We can also use ECDH as digital signature.
- AES is much faster and secure then E0 also AES use small size key and provide better security then other existing algorithm.

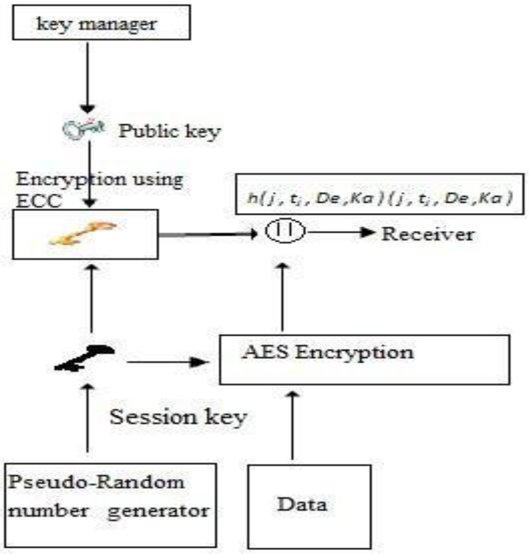

Fig 2. Encryption Process [4]

D. Safety analysis

Safety of proposed algorithm is based on the safety of ECDH and AES algorithms, operating efficiency of proposed algorithm depends upon the encryption and decryption by AES algorithm and hash function.

AES algorithm is available with key size 128, 192, 256.The strength of all key size algorithms is sufficient to protect our information up to secret level. Know attacks against AES are side –channel attacks, which works on some specific applications. AES algorithms is has the NIST/CSEC validation.

ECC is now a days a most promising for encryption, ECDH provide much higher level of security with same key size as RSA. ECDH is certified by NSA.

E. Performance Analysis

Efficiency of proposed algorithm is less than the Bluetooth standard, as we are using AES in place of E0 algorithm. The proposed algorithm is more efficient than previously algorithms for Bluetooth security which use RSA or DES.AES can be efficiently implemented on both hardware and software, as in our algorithm we require software implementation .Most of Bluetooth device have low ram and low speed processor, our algorithm work well with low ram and provide fast speed.

V. CONCLUSION

Bluetooth technology is new and has various applications. Bluetooth is a standard used in links of radio of short scope, destined to replace wired connections between electronic devices like cellular telephones, PDA, computers, and many other devices However, Security is not much emphasized in Bluetooth technology standard. As Bluetooth technology uses wireless networks and is vulnerable to more security attacks the fixed wired network, the security to data transfer is much more essential. Currently used security algorithms have much vulnerability, as discussed in our paper, while our proposed algorithm with AES and ECC provide much higher level of security to Bluetooth data transfer between devices in real time.

REFERENCES.

1. Jens Eliasson and Zheng Hu,"Network and information security", *Peking: TsinghuaUniversity Pres, 2006.*
2. Suri, P. R, Rani, S., "Bluetooth security Need to increase the efficiency in pairing", *IEEE/ Southeastcon, 2008.*
3. Falk A. The IETF, the IRTF and the networking research community[C] *,Computer Communication Review, v35, n5, Oct 2005:6970.*
4. Vanstone, S.A. and Zuccherato, R.J, "Elliptic Curve cryptosystems using curves of smooth order Over the ring Zn, Information Theory", *IEEE Transactions on, vol.43,no.4, pp.1231-1237, 1997.* Tian, X. and Benkrid, K., Merssene twister random number generation on FPGA, CPU and GPU, Adaptive Hardware and Systems, 2009. *AHS 2009. NASA/ESA Conference, pp.460-464, 2009.*
5. Jens Eliasson and Jan van Deventer and Mathias johanson,"An ad-hoc Bluetooth Sensor Network for Automotive Testing,", *IEEE Consumer Communications and Networking Conference2008,January PP-179-180.*
6. Zhihua Hu, "Progress in the Advanced Encryption Standard ,"Intelligence Science and Information Engineering (ISIE), 2011 *International Conference on,Aug 2011,pp 345-348.*
7. Sanchez-Avila, C.,"The Rijndael block cipher (AES proposal): a comparison with DES", security Technology, *2001 IEEE 35th International Carnahan Conference, Oct 2001,pp229-234,* IET Computing & Control Engineering *December/January2006/07*