American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-7, Issue-1, pp-160-169
www.ajer.org
Research Paper Open Access

Secure and Efficient Data Sharing Scheme for D2D Communication in LTE Advanced Network

Alassane Coulibaly
School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China;
Corresponding Author: Alassane Coulibaly

***ABSTRACT**: Device to Device communication (D2D) that refers to direct communication between users without passing through a base station (BS) application of LTE Advanced provides many advantages such as throughput higher spectral efficiency, reduces latency. Despite these obvious advantages the technology is still facing many security issues. In this paper we propose a secure data sharing protocol in D2D communications between users equipment's of LTE-Advanced. The proposed protocol is based certificateless digital signature and signcryption scheme working on elliptic curve group. The idea is that a user who intends access the data through D2D services sends a request to the base station (eNB) of the conventional cellular network.. eNB authenticate user and forward the message to the gateway which detects the user able to share the data. Then the trust authority (here eNB) send a notification message to both users to start the data transmission process. The users' authentication and registration phase based on certificateless digital signature scheme ensure to users privacy preservation and non-repudiation. The Data transmission based signcryption guarantee to the data confidentiality, integrity and makes transmission less complex. The advantage of the proposed protocol is dual security, the analyses of the protocol demonstrate the resistance against malicious attack and simulations, the efficiency in terms of computation cost.*

***Index Terms**: Security-Data sharing-D2D-LTE-Advanced.*

Date of Submission: 02-01-2018 Date of acceptance: 22-01-2018

I. INTRODUCTION

In recent years, with the exponential growth of wireless communication and data traffic, subscribers require improved data rates, with reduced latency and increased capacity of the system. To support increasing demands, cellular networks must undergo appropriate changes for satisfying the growing needs of users and the efficient use of scarce resources available. Device to device (D2D) communication was proposed in cellular networks as a new paradigm to improve these performances. Initial studies have shown that D2D communications have advantages such as increased spectral efficiency; reduce communication delay system and reduces latency. The short distance between D2D transmitter and receiver provides better link, efficient connection with lower energy consumption. The innovative architecture of D2D underlying LTE networks is enable efficient discovery and communication between proximate users over the D2D links. In this case, better security is expected before allowing users to use this communication model. The system must be able to verify the eligibility of user to use D2D networking and related services and a data transfer session must encompass the required security measures of D2D services. Many research conducted on D2D communication under cellular networks concerned with mode selection [1] resource allocation [2]-[4] or interference control [5], the fact remains that some have also dealt with security aspects. In authentication and session key establishment cases especially Shen et al. [6] proposed Diffie-Hellman key agreement (DHKE) for the communication between two end users of a D2D link. They take advantage of commitment scheme to realize the mutual authentication。This provides users a secure setup secret key with a small computation cost and low mutual authentication overhead. However their scheme only treats security issues of confidentiality, integrity and session key establishment. Kwon et al. [7] worked in the authentication concept based Ciphertext-policy attribute-based encryption (CP-ABE) in a mobile multi-hop network environment. The authors adopted message integrity code (MIC) to enhance integrity and confidentiality of authentication messages .Their schemes designed on the basis of Bluetooth protocol achieve fine-grained user access control and also

resist MITMA and replay attacks. However CP-ABE introduction increase the computation cost and key management overhead. Moreover [8] protocols contain an authentication and key management solutions for the three type's scenarios of (D2D): network-covered D2D without user applications, network-covered D2D with user applications and the network-absent D2D for public safety. In all three scenarios, the system resists to some conventional attacks such as eavesdropping, impersonation attack, but entity authentication and System Availability were no discussed. In[9] Zhang et al. proposed a secure D2D data sharing strategy scheme based DHKE.The devices key generation is under the control of the trust authority .They protocol shared data is protected by a symmetric cryptography and users authentication is performed with a keyed-hash message authentication code (HMAC)which provides entity authentication, data authority, integrity and nonrepudiation. The disadvantage of their protocol is user's private key generation by the base station which in practical application environment may be attacked and captured by a malicious adversary. We also note *eNB* exposition to stolen verifier table attack because of record table involvement in the system for user's real identity verification and data shared records. On other security aspects Alam et al. [10] designed a Group Anonymous D2D Communication with End-to-End Security. Their made first a scheme with network assistance and in second case with network-absent. The analysis proves they protocol supports the security features of end-to-end in LTE-Advanced. But their work doesn't take in considerations D2D discovery process. Or even Emad et al. [11] Group Key Management (GKM) mechanism to secure the exchanged D2D messages during the discovery and communication process. They employs an ID-based cryptography (IBE) scheme based on Elliptic Curve Cryptography (ECC) for securing multicast group communication .The main objective of their scheme is to secure the restricted D2D discovery and communication for any ProSe applications. Although the analysis of the protocol proves it resistance against malicious attack. but this scheme application is not suitable for a scheme including user's authentication and data transmission process Furthermore the authentication and key management for D2D communications have been already studied in other wireless and mobile technologies such as Vehicular Ad hoc Network (VANET) [12], Wireless Sensor Networks (WSN) [13], Mobile Ad hoc Networks (MANET) [14].Nevertheless, the employed models and methodologies are not well suitable for D2D in LTE-Advanced because of the computation and communication overheads followed by deploying such methods.
However, faces important challenges of security and privacy problems
In this paper, we develop a new D2D data sharing security system.

The protocol is described as follows:

1. First we propose a lightweight secure D2D data transfer framework in LTE-Advanced network. The proposed scheme employs certificateless digital signature for user authentication and communication which solve key escrow problem. And we use the signcryption a cryptographic primitive that fulfills the functions of digital signature and encryption to guarantee confidentiality, integrity and non-repudiation in a more efficient way.
2. Then the analysis of the protocol proves the security robustness and comparisons with others protocol the efficiency in terms of computational cost.

The organization of the paper is as follows.

In Section II, we introduce preliminaries and system model of the protocol and then we explain the secure data transmission scheme in Section III. Section IV analyzes the security of data sharing process and Section V evaluates the performance. Finally, we conclude our paper in Section VI

II. PRELIMINARIES AND SYSTEM MODEL

A. Preliminaries

The ECC was proposed by Koblitz (1987) in [15] and Miller [16] and its security were based on the elliptic curve discrete logarithm problem (ECDLP). One of the advantages of ECC over other systems is high security with small key size.

Let E/F_q be a set of elliptic curve points over a prime field F_q, defined by the following non-singular elliptic curve equation:

$$y^2 = \bmod q = (x^3 + ax + b) \bmod q \qquad (1)$$

where $a,b,x,y \in F_q$ and $\triangle = (4a^3 + 27b^2) \bmod q \neq 0$ .A point $P(x,y)$ is consider as elliptic point if it satisfies the equation above and the point $Q(x,-y)$ is called a negative of P ,i.e. $Q = -P$ .Let $P(x_1,y_1)$ and $Q(x_2,y_2)(P \neq Q)$ be two points in equation (1).The line l (tangent line to Equation (1) if $P = Q$) joining the points P and Q intersects the curve (1) at $-R(x_3,y_3)$ and the reflection of $-R$ with respect to x-axis is the point $R(x_3,y_3)$, i.e. $P+Q=R$ .The points $E_q(a,b)$ together with a point O form on additive cyclic group G_q , that is, $G_q = \{(x,y): a,b,x,y \in F_q$ and $(x,y) \in E_q(a,b) \cup \{O\}$ of prime order q .The scalar point multiplication on the group G_q can be computed as follows: $kP = P + P + + \cdots\cdots + P$ (k times).A point P has order n if n is the smallest positive integer such that $nP = 0$

B. System model:

The figure 1 illustrates our system model. The system model is based on D2Ddata transmission in LTE-Advanced architecture of [9] and [17]

In our scheme architecture a Device to Device communication system involves: Gateway (GW), *eNB* cellular network, the UEs of cellular users, and server provider of an SP.

We describe them as follows:

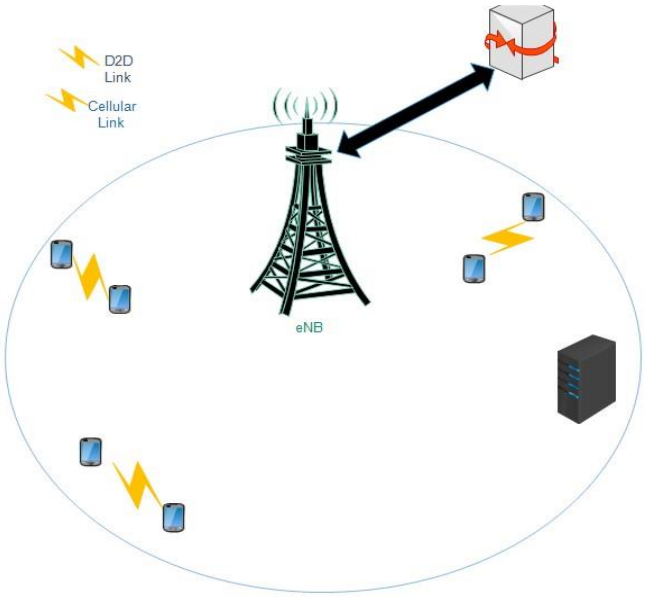

Figure 1. The system model

- **eNB:**

eNB is a base station or trust authority that is connected to the mobile phone network and Gateway, allocates resources to valid Device to Device pairs and informs both D2Dusers.

- **Gateway (GW)**

An entity in the cellular network that detects that if may be better for two communicating UEs to set up a D2D connection. It then informs the eNodeB to request measurements from the UE to check if the D2D communications offers higher throughput.

- **Users (UEs)**

UEs are the D2D communication terminals, shared available information on the device among D2D communications without increasing the additional traffic load on the cellular network.

- **Server (SP)**

It is the original data provider. SP provides authentic content when the system is established. The content is first sent to the partial EU so that they can then share the material with other devices through D2D communications. The SP can leave the system when most of the EU gets the content.

The detail of the proposed is scheme is described as follows:

III. Proposed Protocol

In this section the data sharing scheme between users is presented.

The proposed scheme is divided in three phases: system setup, users' registrations and the data transmission process. In the setup phase eNB generates the system parameters and publishes them to users. The registration includes user pseudonym attribution and the pair public/ private key obtaining from eNB. The last phase is the data transmission process between the two users.

A. System parameter generation

Given the security parameter k, eNB chooses a $k-bit$ prime and determine the tuple $\{F_q, E, F_q, G_q, P\}$, where P is the generator of G_q, chooses $r \in Z_q^*$ as master key and computes the system public key $P_{pub} = rP$. eNB chooses four cryptographic secure hash functions $H_1 : \{0,1\}^* \times G_q^2 \to Z_q^*$, $H_2 : \{0,1\}^* \times G_q^2 \to Z_q^*$ $H_3 : \{0,1\}^* \times G_q^2 \to Z_q^*$ eNB publish the system parameters $param = \{F_q, E, F_q, G_q, P, H_1, H_2, H_3,\}$ and keeps the master key s secret

Table Different 1: Notations used in this paper

Notations	Meaning
$E_q(a,b)$	A set of elliptic curve points of order n , where $a,b \in F_q$
q	A large prime number of $k-bit$
k	The security parameter
$E_q(a,b)$	The elliptic curve over F_q
s, P_{pub}	eNB private/public key
pk_a, sk_b	User public/ private
RID_{UE}, ID_{UE}	User pseudo identity /User real identity
H_1, H_2, H_3, H_3	secure hash function
$\|\|$	The Message concatenation operator
E_k / $D_k(.)$	The Symmetric/ Encryption Decryption

B. Registration Phase

The user and server connection to the system are similar, we will only present the case of user in this paper.

The user connects to the system as follows:

A user UE_a chooses x_a as secret value, computes the public value $X_a = x_a P$ and submits its real identity RID_a and the public value to eNB. eNB set first $ID_a = H_1(RID_a)$ as pseudo identity for UE_a; choose a random integer $r \in Z_q^*$,sets an expiration date (ED) and runs the partial private key by computing $R_a = r_a P$ and $d_a = r_a + xH_1(ID_a(ED), R_a, X_a) \bmod q$. eNB send $D_a = (d_a, R_a)$ and ID_{UE_a} to the user through a secure channel. The user UE_a take the pair key $sk_a = (D_a, x_a)$ as private key, then carries out $pk_a = (P_a, R_a)$ as its public key. eNB store X_a as user public key. The expiration date represents user access to D2D services.

NB: the user can verify the correctness of partial private key by checking whether the equation $d_a = R_a + H_0(ID_a, R_a, P_a)P_{pub}$ holds

— Secret Account

To complete this phase eNB creates a secret account $Ak_{UE_a} : < Ind_{UE_1}, PK_{UE_1}, VerVal_{UE_1}, Inf_{UE_1} > .Ind_{UE_1}$ which contains the user different information's (user real identity, partial private key, and records of the related information of user signature and data transfer…).

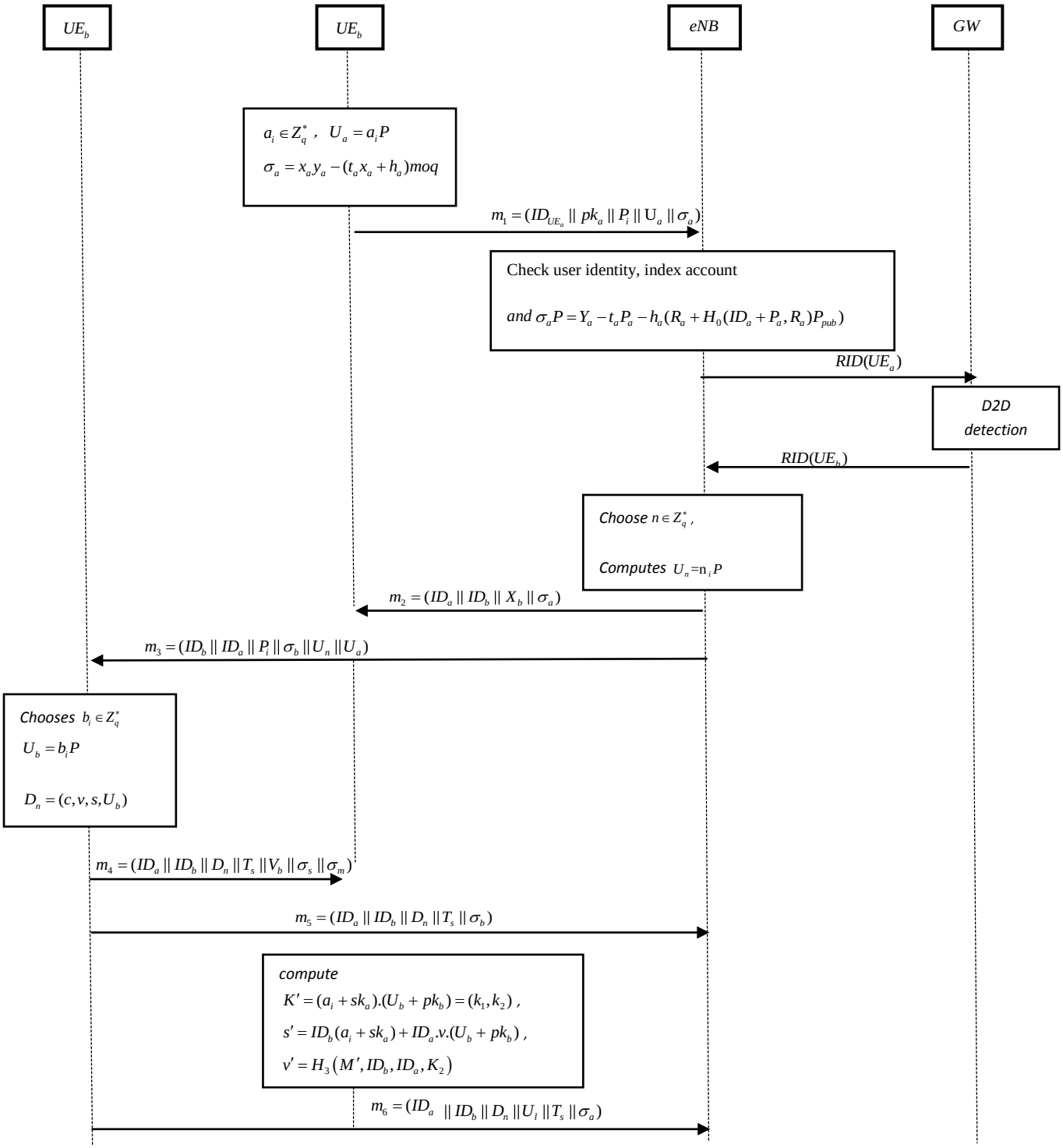

Figure 2. Data transmission process

C. Data transmission process

Step1:

In this phase, a user UE_a who intends to access D2D service sends first a request to the eNB . UE_a generates a random integer $a_i \in Z_q^*$ and computes $U_a = a_i P$ for signcryption generation.

UE_a for the message integrity and authentication generates a signature using his private key $sk_a = (D_a, x_a)$ as follows:

UE_a randomly chooses $y_a \in Z_q^*$;

Computes $Y_a = y_a P$, $h_a = H_2 = (m, ID_a, R, Y_a)$ and $t_a = H_2(m, ID_{UE_a}, P, Y_a)$.

UE_a finally output the signature $\sigma_a = x_a y_a - (t_a x_a + h_a) moq$.

UE_a sends the service request message $m_1 = (ID_{UE_a} \| pk_a \| P_i \| \mathrm{U}_a \| \sigma_a)$ to eNB .

NB: P_i is expected portion index designating the data for computation reduction. In our scheme we will not discuss about data design.

Step 2: Upon receiving the request message from the user, eNB check first the validity of the UE_a , the public key (P_a, R_a) and user identity according to its index account .If all are corrects, eNB continues verifying the message signature as follows:

eNB computes $h_a = H_1(m, ID_a, R_a, Y_a)$, $t_a = H_2(m, ID_a, P_a, Y_a)$ and check whether $\sigma_a P = Y_a - t_a P_a - h_a(R_a + H_0(ID_a + P_a, R_a) P_{pub})$ holds. If not, eNB rejects the request otherwise forward the message to gateway for peer discovery.

GW detects and replies eNB request with the real identity of user able to communicate with the user asker.

eNB to reply user request randomly generates $n \in Z_q^*$ computes $U_n = \mathrm{n}_i P$.

eNB sends the message $m_2 = (ID_a \| ID_b \| X_b \| P_i \| \sigma_a)$ to UE_a as response and simultaneously send a communication request to the selected entity $m_3 = (ID_b \| ID_a \| pk_a \| P_i \| \sigma_s \| U_n \| U_a)$.

NB: X_b is the public key acknowledged by eNB to the selected user.

Step 3: When receiving the communication request message, the selected user processes to the signcrypt of the material M with the shared key U_a of user UE_a and his owns public /private key pk_b / sk_b ,then signs the message before replying the request. He signcrypt and message signature are describe as follows:

Signcrypt/Encrypt: The user generates a random integer $b_i \in Z_q^*$ and computes:

$U_b = b_i P$.

$K = (b_i + sk_b).(U_a + pk_a) = (k_1, k_2)$, $c = E_{K_1}(M)$,

$v = H_3(M, ID_b, ID_a, k_2)$, $s = ID_a(b_i + sk_b) - ID_b.v.(U_a + pk_a)$

And output $D_n = (c, v, s, U_b)$ as cyphertext

The user signs the material M using its private key $pk_b = (D_b, x_b)$ as $\sigma_b = x_b y_b - (t_b x_b + h_b) moq$ and finally send $m_4 = (ID_a \| ID_b \| D_n \| T_a \| V_b \| \sigma_b \| \sigma_m)$ as response on request.

To complete the transmission UE_b also sends a notification message to eNB

$m_5 = (ID_a \| ID_b \| D_n \| T_s \| \sigma_b)$

NB: the second signature is server signature.

Step 4: When receiving the message, the user receiver verifies first whether time stamp T_a is fresh or not. If T_a is not fresh the user aborts the process .Otherwise UE_a compare the pseudo identity with that received from eNB and conducts the message signature verification. If all are correct the message has been send by the selected entity.

To decrypt the cyphertext, UE_a performs the following:

Decrypt/Verify:

$K' = (a_i + sk_a).(U_b + pk_b) = (k_1, k_2)$

$s' = ID_b(a_i + sk_a) + ID_a.v.(U_b + pk_b)$

$v' = H_3(M', ID_b, ID_a, K_2)$

$M' = D_{K_1}(c)$

Verify if $v = v'$ then receiver accepts the received data

The two users have then process to a data transmission.

To complete the process UE_a send a report message to eNB about the transmission process.

$m_6 = (ID_a \| ID_b \| D_n \| U_l \| T_s \| \sigma_a)$

NB: if eNB don't receive a feedback message from the user requester it will automatically remove his access to the D2D service because of expiration date setting.

Correctness

The signcrypt text (c, v, s, U_b) is a valid one; its correctness is given below.

$$K' = (a_i + sk_a).(U_b + pk_b)$$
$$= (a_i.U_b + a_i pk_b + sk_a.U_b + sk_a.pk_b)$$
$$= a_i b_i.P + a_i.pk_b + b_i.pk_a + sk_a.sk_b.P$$
$$K = (b_i + sk_b).(U_a + pk_a)$$
$$= (b_i.U_a + b_i pk_a + sk_b.U_a + sk_b.pk_a)$$
$$= b_i a_i.P + b_i.pk_a + a_i.pk_b + sk_b.sk_a.P$$

IV. SECURITY ANALYSIS

In this section we analyze the proposed scheme to prove that it satisfies the properties of D2D security.

1) **Data Confidentiality and Integrity**: The proposed protocol provides data confidentiality. The user sender in signcrypt process encrypts the data with a symmetric key which can only be decrypt by the user requester. The material M encryption is according to the figure out cyphertext $D_n = (c, v, s, U_b)$ and the user UE_a can only compute $K' = (a_i + sk_a).(U_b + pk_b) = (k_1, k_2)$ with its private key.

The data integrity is guaranteed by the message signature.

In this step we note that confidentiality, integrity and authentication are simultaneously achieved.

Proof

If a malicious adversary tries to get the original message from the encrypted text, he must know the secret K parameter. Suppose the attacker attempts to derive the secret key K , he must find out the secret parameter of the equation $U_b = b_i P$ But the Equation $U_b = b_i P$ has ECDLP properties. So it is impossible to derive K from the equation. $U_b = b_i P$ and $K = (b_i + sk_b).(U_a + pk_a)$.

UE_b generates the cyphertext D_n and signature σ_b using private key sk_b .

The protocol is also secure against Man-in-the-middle attack. Man-in-the-middle attack is only possible if an adversary can forge signature and cyphertext. It is not possible because solving the ECDLP is computationally infeasible. Therefore, the proposed scheme can resist man-in-the-middle attack.

2) **Mutual Authentication**: As an essential and important requirement, the proposed protocol ensures authentication between users and eNB . eNB authenticates user according to user secret account which contain user information's. Furthermore the user before send a request signs the message with its private key, thus the receiver can verify the correctness of signature to authenticate user. In the signcryption scheme, the user receiver can verify that whether the ciphertext is tampered or not at the time of transmission. UE_a checks the sender entity by verification of signature σ_b If the attacker modifies the cipher text c to c' . Then the original message $H_3(M, ID_b.ID_a, K_2)$ also change from M to M' .At the time of verification it is infeasible in one way hash function that $v = v$ .Therefore, our scheme provides integrity.

3) **Availability:** Users are authenticated locally by the base station. Mean the authentication procedure does not take more time and the users do not need to wait longer to start data transmission. In this proposed scheme the system initialization phase and authentication are performed by the base station. So the denial of service (DoS) attack which is mainly effects the base station will not affect the data transmission process.
4) **Inforgeability:** Inforgeability guarantees that the attacker cannot create valid encrypted text. In the proposed scheme, the attacker cannot create a valid (c, v, s, U_b) without the sender's private key. If an attacker falsifies a valid (c, v, s, U_b) of the previous (c, v, s, U_b) then (c, v, s, U_b) must satisfy $K' = (a_i + sk_a).(U_b + pk_b)$. To generate a correct v and s, the attacker must obtain a random secret. But the attacker cannot get the correct random secret b_i and s. To get b_i from $U_b = b_i P$, then the attacker should first resolve the ECDLP but it is unfeasible from a computational complexity. An attacker to generate a correct value of v and s must get a random b_i secret. But it cannot get the correct random secret b_i and s because to get b_i from $U_b = b_i P$, then the attacker should first solve ECDLP but it is unfeasible.
5) **Non-Repudiation**: The proposed scheme provides non-repudiation. The data sender entity with its private key signs the message so the user receptor can verify whether the original message is sent by sender or not. The signature of user is an evidence of non-repudiation.
6) **Conditional Privacy Preservation**: In the proposed protocol, a user real identity is hidden in a pseudonym ID generated by the trust authority. The different communication of users is accomplished with their pseudo

identity, which is the secure one-way hash value of the RID. The privacy preservation property is therefore conditional.

7) **Forward Secrecy**: The proposed scheme provides forward secrecy. If the sender's private key is lighted, but the attacker cannot retrieve the original material M from the encrypted text (c, v, s, U_b) .In our scheme the attacker cannot derive the plain text without decrypt its cyphertext by the secret key. It's obvious that Perfect forward secrecy is an important security requirement for the protocol. Due to the fact even the communication units are compromised, the adversary still cannot learn their former communication.
8) **Revocability:** The registration is automatically revoked with the expiration date ED.When receiving the data if the user doesn't give a feedback message to eNB , his access to D2D service is revoked.

V. Performance Evaluation:

A. Communication overhead:

Communication overhead of the proposed protocol includes the energy consumption broadcast from user message request to last notification message sent to eNB .In an ECC-based group G, the elliptic curve $E/F_q : y^2 = \mathrm{mod}\, q = (x^3 + ax + b) \bmod q$ is a160-bit prime number and the size of each element in G is 40 bites. Time stamp and portion index values are respectively4and 2Bytes.In our case, utilization of user pseudo identity reduces the value of user identity to 20BytesThe communication overhead in each phase of our scheme is listed in Table 2.

Table2: Communication Overhead Of the Proposed Protocol

Scheme communication overhead (bits)	
Phase 1	162
Phase 2	304
Phase 3	328
Phase 4	202
Total	994

As listed in table 2 the communication in phase 1 include the pseudo identity ID_{UE_a} the message signature $\sigma_a \in G_q$, user public key $pk_a \in G_q$,the portion index of data P_i and the key $U_a \in G_q$ .Therefore, the length total cost is the addition of different elements in the message m_1 .

B. Computational Overhead:

The proposed protocol computational overhead will concern the phase of signcryption, signature and decryption and verification of the Data transmission process. Unlike others model where the signcryption and Encryption are separated, here we associate the two steps for computational cost reduction. We will compare our proposed scheme with some others protocols signcryption signature process and also decryption verification. As the operations on pairing, exponentiation and multiplication dominate the computational overhead in these schemes, we only consider the three operations in the comparison process. To evaluate the computation efficiency of different schemes, we use the simple method from [18]. Compared with [19, 20, and 21] our protocol has more advantage due to the fact that the others protocols are using pairing and exponentiation operations that take much longer time than the multiplication operation used in our scheme. In term of computational efficiency comparison, we obtain the running time for cryptographic operations using MIRACAL [22], a standard cryptographic library. For the pairing-based scheme, to offer the same security level to 1024-bits RSA, a super singular elliptic curve $E/F_q : y^2 = x^3 + x$ x along with the Tate pairing $\hat{e}: G \times G \to G_T$ defined over this curve employed, the embedding degree of the curve E/F_q is 2, $q = 2^{159} + 2^{17} + 1$ is a 160-bit Solinas prime, and $p = 12qr - 1$ is a 512-bit prime. While For the ECC-based authentication protocol [22], the Koblitz elliptic curve $y^2 = x^3 + ax + b$ defined on $F_{2^{163}}$ has been used to achieve the same security level, where $a = 1$ and b is a random 163-bitprimenumber. The experiment run platform is PIV 2.67-GHz processor featured with Windows 7 OS and 6.00GB.The execution times of each operation are similar to scheme [20].

Table 3: Performance Comparison of the Computational Overhead among relevant schemes

Scheme	**Signcryption**	**Signature**	**Decryption**	**Verification**
Proposed scheme	$3T_M$	T_M	$2T_M$	$3T_M$
[19]	$2T_E + 3T_M$	$T_E + 2T_M$	$T_E + 3T_M + 2T_P$	$2T_M + T_P$
[20]	$4T_M$	T_M	$3T_M$	T_M

[21]	$T_E + 4T_M + T_P$	$4T_M$	$T_M + 5T_P$	$4T_P$

T_M is the time consumed for one scalar multiplication; T_E is the time consumed for one exponentiation operation; T_P is the time for one pairing operation

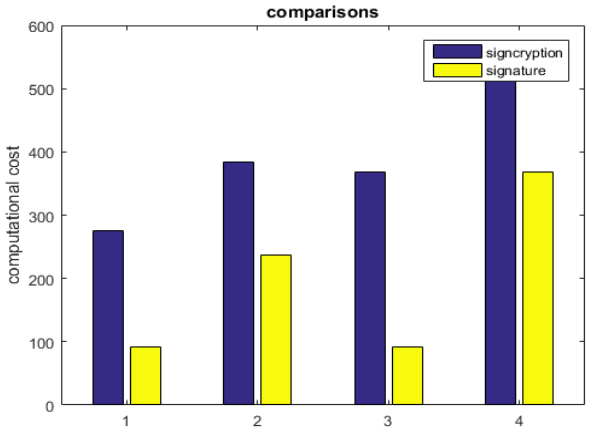

Figure 3. signcryption and signature

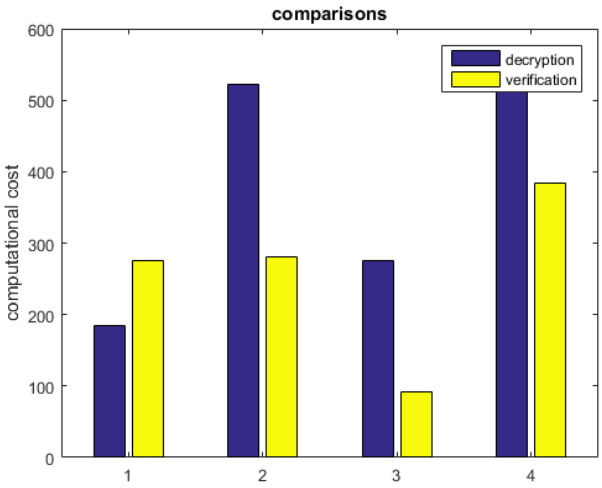

Figure 4. decryption and verification

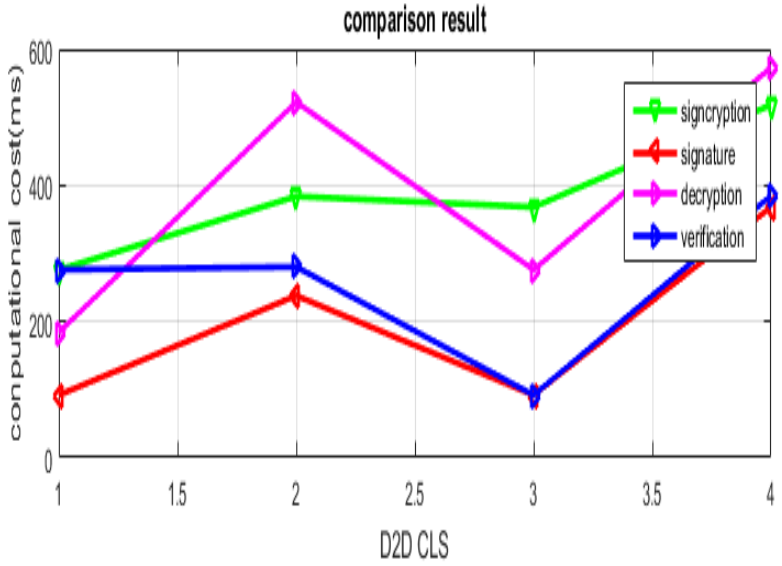

Figure 5: view of the protocol

The results showed in Table 3and the analysis of data in Fig. 3, 4and 5indicate that our scheme has lower computational cost than other relevant schemes expect for signature verification where [20] has lower computational cost than our scheme.

VI. CONCLUSIONS

In this paper, we proposed a novel D2D data sharing process scheme based certificateless signcryption in LTE-Advanced Network. The proposed protocol satisfies security goals in terms of data confidentiality and integrity.Furthemore the application of certificateless reduces users' private key expositions to malicious attacks .The system application in ECC reduces the computational cost and the analysis demonstrates our scheme efficiency. In the future we will intend to establish a protocol for the 4cases of D2D.

REFERENCES

[1]. Doppler, Klaus, et al. "Mode selection for device-to-device communication underlaying an LTE-Advanced network." Wireless Communications and Networking Conference (WCNC),2010 IEEE. IEEE, 2010.

[2]. Duong, Quang, Yoan Shin, and Oh-Soon Shin. "Distance-based resource allocation scheme for device-to-device communications underlaying cellular networks." AEU-International Journal of Electronics and Communications69.10 (2015): 1437-1444.

[3]. Kim, Tae-Sub, et al. "Proximity user detection based resource allocation scheme for device-to-device communication." IETE Journal of Research 59.4 (2013): 356-363.

[4]. Duong, Quang, Yoan Shin, and Oh-Soon Shin. "Resource allocation scheme for device-to-device communications underlaying cellular networks." Computing, Management and Telecommunications (ComManTel), 2013 International Conference on. IEEE, 2013.

[5]. Janis, Pekka, et al. "Device-to-device communication underlaying cellular communications systems." International Journal of Communications, Network and System Sciences2.03 (2009): 169.

[6]. . Shen, Wenlong, et al. "Secure key establishment for device-to-device communications." Global Communications Conference (GLOBECOM), 2014 IEEE. IEEE, 2014.

[7]. Kwon, Hyunsoo, et al. "Secure device-to-device authentication in mobile multi-hop networks." International Conference on Wireless Algorithms, Systems, and Applications. Springer, Cham, 2014.

[8]. Alam, Muhammad, et al. "Secure device-to-device communication in LTE-A." IEEE Communications Magazine52.4 (2014): 66-73.

[9]. Zhang, Aiqing, et al. "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks." IEEE Transactions on Vehicular Technology 65.4 (2016): 2659-2672.

[10]. Abd-Elrahman, Emad, Hatem Ibn-Khedher, and Hossam Afifi. "D2D group communications security." Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on. IEEE, 2015.

[11]. Hsu, R. H., & Lee, J. (2015, September). Group anonymous D2D communication with end-to-end security in LTE-A. In Communications and Network Security (CNS), 2015 IEEE Conference on (pp. 451-459). IEEE.

[12]. Busanelli, Stefano, Gianluigi Ferrari, and Luca Veltri. "Short-lived key management for secure communications in VANETs." ITS Telecommunications (ITST), 2011 11th International Conference on. IEEE, 2011.

[13]. Fu, Yingfang, et al. "Mutual authentication in wireless mesh networks." Communications, 2008. ICC'08. IEEE International Conference on. IEEE, 2008.

[14]. Merwe, J. V. D., Dawoud, D., & McDonald, S. (2007). A survey on peer-to-peer key management for mobile ad hoc networks. ACM computing surveys (CSUR), 39(1), 1.

[15]. Koblitz, Neal. "Elliptic curve cryptosystems." Mathematics of computation 48.177 (1987): 203-209.

[16]. Miller, Victor S. "Use of elliptic curves in cryptography." Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1985.

[17]. Yang, Mi Jeong, et al. "Solving the data overload: Device-to-device bearer control architecture for cellular data offloading." IEEE Vehicular Technology Magazine 8.1 (2013): 31-39.

[18]. Xiong, H., & Qin, Z. (2015). Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. IEEE transactions on information forensics and security, 10(7), 1442-1455.

[19]. Kushwah, P., & Lal, S. (2011). An efficient identity based generalized signcryption scheme. THEORETICAL COMPUTER SCIENCE, 412(45), 6382-6389.

[20]. Zhang, Aiqing, et al. "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems." IEEE Transactions on Information Forensics and Security 12.3 (2017): 662-675.

[21]. Zhou, C., Zhou, W., & Dong, X. (2014). Provable certificateless generalized signcryption scheme. Designs, codes and cryptography, 71(2), 331-3

[22]. Scott, M. (2003). Multiprecision integer and rational arithmetic cryptographic library.