EEoP: A Lightweight Security Scheme over PKI in D2D Cellular Networks

Yasir Javed[1,2], Adnan Shahid Khan[1], Abdul Qahar[1,3] and Johari Abdullah[1]
[1]*Network Security Research Group, Faculty of Computer Science and Information Technology,*
Universiti Malaysia, Sarawak.
[2]*RIOTU, CCIS, Prince Sultan University, Riyadh, KSA.*
[3]*The University of Punjab, Lahore, Pakistan.*
skadnan@unimas.my

***Abstract*—Device-to-Device (D2D) communication is a promising technology that facilitates the deployment of devices to provide extended coverage where devices can act as user or relays. However, introducing such technology where the user can act as semi-intelligent relays, open a wide range of security threats, specifically, in terms of confidentiality and integrity. Another key issue of these devices is the limited computational and storage capabilities. Thus, to address the above challenges, this paper proposed a computationally lightweight crypto system based on Elliptic curve and ElGamal over public-key infrastructure (EEoP). It uses ECC for creation of keys while uses ElGamal for encryption and decryption over public-key infrastructure. Mathematical analysis shows that EEoP ensures the confidentiality and integrity of the communication. Performance analysis shows that proposed scheme outperformed the baseline protocols. The proposed crypto system can be used in relay-based communication.**

***Index Terms*—Elliptic Curve Cryptography; Elgamal Cryptography; Public Key Infrastructure; Security Threats.**

I. Introduction

Due to lack of physical boundaries, all sorts of wireless communications are always prone to security threats. Recently, with the advent of long term evolutions-advanced (LTE-A) and 5th generations (5G) cellular networks, device to device (D2D) communication become very popular amongst the research based society. Unlike mobile adhoc networks, social networks, opportunistic networks etc. where involvement of base stations (BS) is extremely not required (infrastructure less networks), D2D communication do require BS. However, in multihop D2D communication, intermediate small devices have taken BS role. These small devices are mobile stations or user equipment and can act as semi-intelligent relays. These architecture is similar to current relay-based architecture, (e.g. if no relays involve IEEE 802.16e and if relays involve IEEE 802.16j) where such relays can act as transparent relays (amplify and forward) and semi-intelligent (semi-transparent) relays (decode and forward). These relays are in the shape of roadside unit in vehicular networks or deployed in buses of buildings to support small cells. Power, storage, computational capabilities and communication overhead are somehow not a critical challenge. However, in D2D communications, user equipment or mobile stations can act as semi- intelligent relay devices under the supervisions of BS, where power, storage, computational capabilities and communication overhead are one of the critical challenge. Inclusion of such semi-intelligent devices create a severe security concerns amongst the researchers of D2D communication. The current security measures of relay-based architecture is not applicable to D2D communications due to above-mentioned critical challenges. Secondly, D2D communication is prone to impersonation, where the adversary can create replay attacks, which consequently generate either denial of service attack or Man in the middle (M-I-T-M) attack. In nutshell, integrity (DOS/Replay Attack) and confidentially (M-I-T-M attack) are the main security requirements with low power, storage, computational capabilities and communication overhead as a critical challenge. Thus, a security measure is required to fulfil above mentioned security requirements and critical challenges.

This paper proposed an elgamal based elliptic curve crypto system with PKI infrastructure. Elliptic curve cryptosystem is proven to be lightweight with less power consumption is used to create the optimum keys. Elgamal is mature form of diffie-helmen(DH) to efficiently and securely share the key while PKI is used for encryption and decryption of data. There are number of security algorithms are proposed to mitigate these challenges. However, this paper does not consider those security algorithms that require bigger key size and require high computational costs. There are a number of schemes presented for security and authentication for low power devices. Like, Algebric Eraser [1] that works on designing security protocol for Near Field Communication (NFC) and Radio Frequency identification (RFID). It requires a trusted third party to set up the secret key and authenticity between communicating devices. NTRU [2] is another technique receiving much attention recently has focused on the security of small devices and have better security but require a larger key size (typically of few kilobits) and requires higher computation. Shen, W. et.al [3] presents a DH based authentication scheme, where two mobile users can setup a key through fewer numbers of steps than normal DH scheme. The proposed scheme was tested in between two smart phones and was able to do mutual authentication thus avoiding M-I-T-M attack. Reddy et.al [4] present an elliptic curve cryptography based authentication scheme where a lightweight hash function is used such as XOR and demonstrates that it can avoid DoS, M-I-T-M attack as well as impersonation attack. Reddy et.al [5] propose a scheme based on Burrows-Abadi-Needham logic to avoid M-I-T-M and replay attacks. This approach uses biometric to identify the device users and contact it with elliptic curve hash function in order to perform the authentication. The scheme shows it outperforms other schemes identified in the literature. For Confidentiality, the symmetric key can be used but sharing of keys, and their authentication poses a great challenge. For this DH and RSA was designed to solve the key sharing problem but with advancement in processing power and computational advancements, it was shown that smaller key sizes are not secure against even brute force attacks, especially with the advent of quantum computers [6]. Lauter [7] proved that elliptic curves (EC) [8] can be used with DH. EC is computationally less expensive, and their usage in DH and RSA can make the solution for Security that is vulnerable to quantum attacks. Lauter showed that a key size of 283 bits in EC is equivalent to 3072 bits in RSA or DH. Elliptic Curve Diffie-Hellman (ECDH) a standard made by NIST [9] was proved mathematically to be more secure than their predecessors were and was lightweight. Liu et.al [10] present an ECC based library for securing the IoT Devices with two different version (1) high speed (2) less memory consumption. Both techniques are proven to secure against timing attacks. Kim et.al [11] presented an asymmetric scheme for broadcasting in order to achieve low computation overhead and complexity. It used broadcast encryption scheme and forward was done in grouping for keys. It was also based on ECC. This technique proved too efficiently lighter than other key sharing schemes. Laiphrakpam and Khumanthem [12] presented the DH with ECC using a simple hash algorithm for secure transmission of images using Arnold's transform for encryption. The resultant algorithm provides confidentiality and also proved strong against Brute force attack. Sedidi and Kumar [13] did a) Diffie-Hellman key exchange algorithm using normal version, (b) using the ACK/NACK messages for delivery of packet to base station (c) Macro station sent a verification code to verify the reception of data and provide authentication. It was shown that techniques were able to mitigate M-I-T-M attack as well as the problem of key distribution. Xi et.al [14] also highlighted the issues that can occur in device-to-device communication and it emphasizes on the requirement of central control. It uses receive signal strength, channel state information to design the key, and uses an algorithm based on DH in order to do the key management and sharing. It has proven to be a good defense against M-I-T-M attack. Raju et.al [15], presented an algorithm for security of traffic routing and discuss a variation of ECC with ElGamal, ECDH and ECC with RSA. It also showed that ECC proved to be best option. Dake and Ighare [16] presented an algorithm with ECC and ElGamal and compared with ELGamal scheme to prove that usage of ECC with ElGamal is a best option. The comparison was only done in terms of space and time. Jung et.al [17] used the idea of DH and Public-key infrastructure to achieve the encryption and authentication. It also did management of keys using DH.

Semi-intelligent relays will have lower computational power compared to normal BS thus will require a scheme that is lightweight, energy-efficient and can provide security against major well-known attacks. Present security schemes are mostly based on usage of DH algorithm while EEoP is based on Elgamal that overcomes the problems faced with DH. Present security techniques only uses ECC but in some cases, focuses on combination of ECC + DH while EEoP use ECC with variable key size depending on the use case and is provably secure against quantum attacks. Present security techniques focuses on mitigating M-I-T-M attack or DoS attack but EEoP also focuses on mitigating the interleaving attack along with other attacks. Moreover, EEoP is based on PKI that current security algorithm does not consider.

Section below provides a scheme for overcoming all identified problems. Section II presents a system model while Section III present tour proposed EEoP cryptosystem. Section IV present discussion and analysis of EEoP scheme along with security verification of the system while Section V presents the conclusion.

II. System Model

Figure 1 shows the system model in which Multihop Relay Base Station (MRBS) provides communication facility to all nodes to use the network and its services. In order to communicate each node or user should authenticate with each other. This model is based on dual-authentication. Our assumption is that first all semi-intelligent relays should register with CA (Certification Authority) and obtained their public and private key pair. The relays will provide connectivity as well as authenticity to devices D to do secure communication.

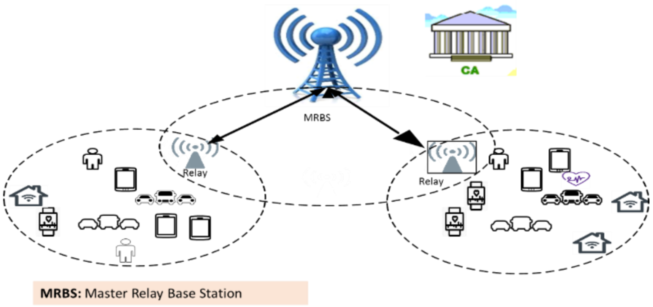

Figure 1: Showing System model diagram for proposed solution

MRBS broadcasts the Elliptic curve E and basepoint B after each interval of t seconds. E and B are only of concern for semi intelligent relays R that have capabilities of authentication and secure communication. It also distributes the load of MRBS for handling multiple devices. The question may arise about the rouge relay station. Each R should obtain a certificate from CA as well as do authentication with MRBS before getting the communication to go through. R are also allowed to select their own E and B for each communication as they are responsible for each node under their coverage area.

III. EEoP Cryptosystem

Algorithm 1 presents the proposed EEoP based signature verification scheme. EEoP is based on ECC + ElGamal and PKI. EEoP makes an assumption that (1) a handshake should have occurred between MRBS and CA to obtain its public key and private key pairs that is generated by MRBS instead of CA to avoid CA impersonation attack and reducing the load of generating keys on CA for everyone. (2) The certificate is created using ECC plus ElGamal algorithm. (3)Selection of Elliptic curve and the base point on curve is decided by CA and is updated on daily basis while the selected key size is greater than 356 bits. This research shows a communication between a MRBS and CA for authentication purpose.

Algorithm 1: EEOP Scheme for Signature Verification

```
Pre-condition: Certificate should be issued from certification authority CA
AT MRBS
    Step 1: Select secret key $K_{MRBS}$
    Step 2: Compute Public key $P_{MRBS} = (X_{MRBS}, Y_{MRBS})$
    Step 3: Compute Hash of Cipher text $H_{MRBS} = Hash(C_{MRBS})$
    Step 4: Sign the Hash $S_{MRBS} = K_{MRBS}{}^{-1} \left(H_{MRBS} + t\ * K_{MRBS}\right)$

AT $Relay\ R$
    Step 5: Compute the two Hashes
            $Hash_{Check1} = (S_{MRBS} * \text{PMRBS}) = (X_{Check1}, Y_{Check1})$
            $Hash_{Check2} = Hash(C_{MRBS})G + [X_{MRBS} \cdot P_{MRBS}]$
            $= (X_{Check\ 2}, Y_{Check2})$
    Step 6: If both hashes matches then message integrity is not compromised else compromised
```

First step is the calculation of secret key $\boldsymbol{K_{MRBS}}$ by MRBS for communication. There secret key selected must be inside the field points out of $N\ points$ where N are field points on Elliptic curve E for field $F_N\ where\ 1 < K_{SN} < N - 1$. Second step is to calculate the public key $\boldsymbol{P_{MRBS}} = (\boldsymbol{X_{MRBS}}, \boldsymbol{Y_{MRBS}})$. The public key is calculated by multiplying the secret key with based point B.

For the authentication purpose, the public and private key pair that are generated with CA are used. Initially Cipher text C_{MRBS} is calculated (explained in Algorithm 2). Once the cipher text is available then the Hash of cipher text H_{MRBS} is calculated. For hash SHA3 V3 will be used. The purpose of making sure that data integrity is not compromised. Once the Hash is calculated, the signature S_{MRBS} will be calculated that uses the private key of MRBS point multiplication with point XMRBS. The result is then point added with H_{MRBS} and taken then drawing a tangent at point X. The result is referred as H_{MRBS} as shown in Equation 1.

$$S_{MRBS} = t\ (H_{MRBS} + catl\ * K_{MRBS}\ ) \tag{1}$$

The signature S_{MRBS} along with cipher text C_{MRBS} is send to R that will then find the authenticity of message. In order to verify the integrity of Message the received data is verified by R. It uses $P_{MRBS}\ and\ S_{MRBS}$ for calculating the hash H_{check1} as shown in equation 2 and then verify the hash re-calculation H_{MRBS} using cipher text C_{MRBS}, public key P_{MRBS} and XMRBS as shown in Equation 3. All operations are performed using modulus L in order to stay in Field of Elliptic curve.

$$Hash_{Check1} = (S_{MRBS} * \text{PMRBS}) = (X_{Check1}, Y_{Check1}) \tag{2}$$

$$Hash_{Check2} = Hash(C_{MRBS})G + [X_{MRBS} \cdot P_{MRBS}] = (X_{Check\ 2}, Y_{Check2}) \tag{3}$$

If two hash $Hash_{Check1}$and $Hash_{Check1}$are equal then the data is from legitimate source else the data integrity has been compromised. Now the cipher text can be decrypted to obtain the Original message.

Algorithm 2: EEoP Scheme for Encryption

```
Pre-condition: Certificate should be issued from certification authority CA
AT $Relay\ R$
    Step 1: Select secret key $K_{SN}$
    Step 2: Compute Temporal Public key TSPR $= K_{SN} * B$

AT MRBS
    Step 3: Select secret key $K_{SM}$
    Step 4: Compute Temporal Public key TSPMRBS $= K_{SM} * B$
    Step 5: Calculate $P_{NT} = K_{SM}\ *$ TSPR $(mod\ B)$
    Step 6: Encrypt the Message $M$ to get the Cipher $C_{MRBS}$
            $C_{MRBS} = (C_{MRBS-X}, C_{RMBS-Y}\ mod\ B$
```

Algorithm 2 shows the ECC + ElGamal algorithm key sharing and process of encryption of text in a systematic process. The process is simple where initially R select a secret key K_{SN} as a random number where $1 < K_{SN} < N - 1$ as shown in Equation 4. The Elliptic curve E and base point B are already shared by MRBS in periodic broadcast to reduce huge traffic load that will be created on MRBS.

$$\text{Select a random integer } K_{SN}\ where\ 1 < K_{SN} < N - 1 \tag{4}$$

Once the private key K_{SN} is selected the next iteration is to calculate the public key we call in this algorithm as temporal public key as after each defined time the keys are updated. So, Temporal Public Key for R will be TSPR and will be calculated using Equation 5

$$TSP_R = K_{SN} * B \tag{5}$$

Now R send its public key TPSR to MRBS. MRBS then selects its private key using same rules mentioned in Equation 4. In order to calculate the public key TSPMRBS for itself the private key in point multiplied by base point B as shown in Equation 6.

$$TSP_{MRBS} = K_{SM} * B \tag{6}$$

Now that public key and private key are there, the point at which communication will occur has to be calculated. For this Elliptic curve, affine group property must be considered. That means, the public key of NTP is point multiplied with MRBS private key or public key of NTP multiplied with private key of NTP should result in same secret communication point as shown in Equation 7.

$$\begin{aligned} P_{NT} &= K_{SM} * \mathrm{TSP}_{\mathrm{R}} \left(mod\ B\right) \\ &= K_{SN} * TSP_{MRBS}\ (mod\ B) \\ &= (X_{SMN}, Y_{SMN}) \end{aligned} \tag{7}$$

Once the points are calculated now the cipher text C_{MRBS} can be calculated using the point calculation through ECC based point multiplication (repeated point doubling) as shown in Equation 8.

$$\begin{gathered} C_{MRBS} = (C_{MRBS-X}, C_{RMBS-Y}) \\ Whereas\, C_{MRBS-X} = \left(X_{SMN} * X_{original}\right) mod\ B\ \& \\ C_{MRBS-Y} = \left(Y_{SMN} * Y_{original}\right) mod\ B \end{gathered} \tag{8}$$

The cipher is calculated using the common secret key point and is shared with NRT. All the operations are kept in modulus B in order to keep the points in between field. The cipher text is used in Algorithm 1.

IV. Discussion and Analysis

Baseline authentication procedure as shown in Figure 2(a) is a minimum four-step process where authentication request and response are first two steps while in other two steps, secret key is transferred along with acknowledgment. Couple of works like Chaudhry et.al, [18] presented improved-SIP require six-step authentication scheme while Mohit, Amin & Biswas [19] presented a seven step authentication mechanism, while compared to our EEoP scheme that only require two steps.

EEoP as shown in Figure 2(b), request for communication is sent from R to MRBS and then MRBS send the response along with verified authentication. EEoP is just a two-step process compared to other scheme.

If we consider baseline communication step in authentication scheme it will need the cost for each session using Capkun equation will be session cost C_{CostT} .

$$C_{CostT} = \sum_{i=0}^{n}(AReq) + \sum_{i=0}^{n}(ARes) + \sum_{i=0}^{n}(Ak) + \sum_{i=0}^{n}(Ack) \tag{9}$$

where i is the session number and n are total session number while EEoP scheme will have cost of communication C_{CostP} as shown in Equation 10 will be only for request and response while the response includes the message , acknowledgment and freshness that were not the part of baseline scheme.

$$C_{CostP} = \sum_{i=0}^{n}(Req) + \sum_{i=0}^{n}(Res) \tag{10}$$

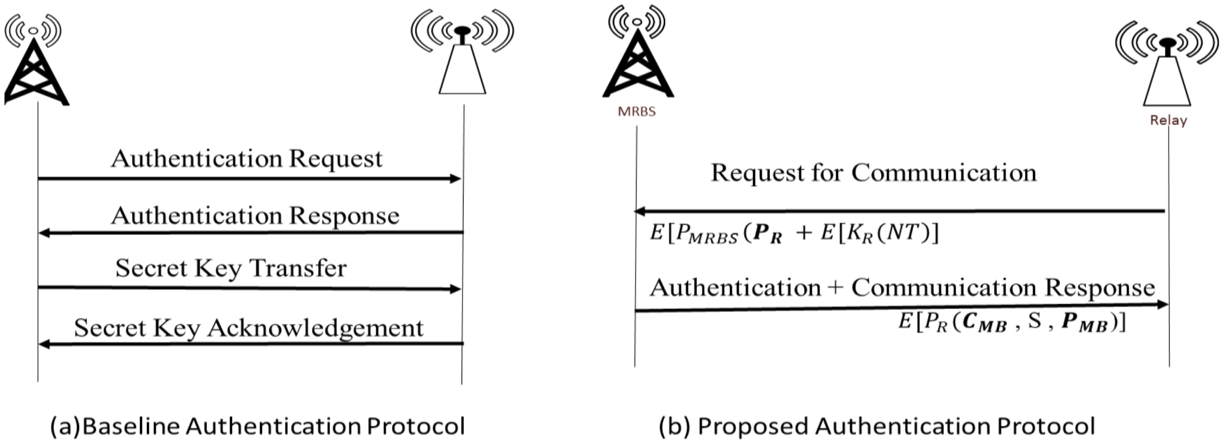
Authentication Request
Authentication Response
Secret Key Transfer
Secret Key Acknowledgement
MRBS
Relay
Request for Communication
$E[P_{MRBS}(\boldsymbol{P_R} + E[K_R(NT)]$
Authentication + Communication Response
$E[P_R(\boldsymbol{C_{MB}}, \mathrm{S}, \boldsymbol{P_{MB}})]$
(a)Baseline Authentication Protocol
(b) Proposed Authentication Protocol

Figure 2: (a) Baseline authentication protocol & (b) EEoP method of authentication with secure communication

The result shows that EEoP reduces the computational cost and provide better security and authentication. It also shows the viability of solution for limited power and computational devices. The technique can be used in current cellular network to support secure D2D communication.

From the first baseline protocol ULMAP [20] which is only based on NFC and RFID tag authentication for small number of devices, the second base line scheme Improved SIP [18] is only based on ECC and rely of number of messages transferred between them.

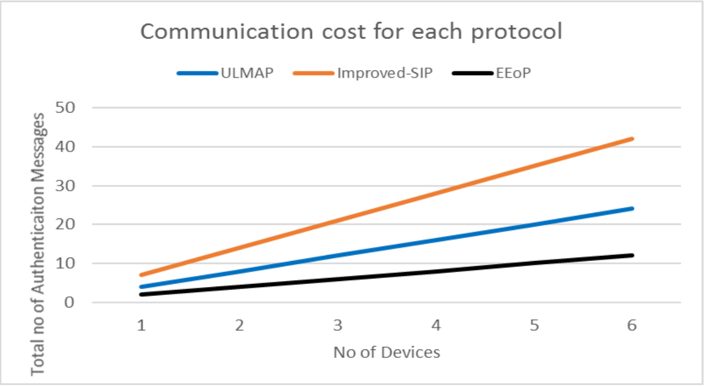

Figure 3: Showing communication cost comparison of EEoP with baseline protocols

Table 1
Security comparison for EEoP, ULMAP and Improved SIP protocol

	ULMAP	EEoP	Improved SIP
Number of Authentication messages	4	2	6
Database size	Small and should be preconfigured	Independent for any device joining	Independent for any device joining
Quantum Attacks	Yes	No	Yes
Key size	Doesn't focus	Smaller in size but have higher effect, secondly it is variable depending on the scenario	Smaller in size but have higher effect. Fixed size key
Hashing Algorithm	XOR	SHA V3	XOR
Can be used by IoT Devices?	Yes (but only in predefined conditions)	Yes	Yes (but it is heavier to work with

Figure 3 shows that when no of devices increases the communication cost will increase but EEoP outperforms in terms of cost compared to baseline protocols.

The proposed algorithm also uses a better and secure hashing algorithm SHA V3 provably quantum secure. Moreover, our proposed algorithm is used hybrid scheme to overcome the problems of each scheme that are subject to attacks. Table 1 shows that EEoP outperforms in term of security and mitigation against attack compared to baseline protocols.

EEoP scheme allows the usage of lightweight algorithm to secure the communication and solve the problem of authentication as well as rouge relay. ECC is provably lightweight then other schemes as shown in Table 2 based on results obtained in [21-23]. It shows the number of bit required as key to be used for encryption or authentication.

Table 2
Key size comparison

ECC	RSA/DH/DSA
112	512
163	1024
224	2048
283	3072
409	7680
571	15360

ECC is based on the Elliptic curve over the finite field and requires arithmetic operation over these fields [24]. Elliptic curve is based on Abelian group [24] and uses a special form of addition and multiplication where addition is point addition and multiple is called as point doubling. The complexity involved in decryption if the key is not known is referred as discrete logarithm problem (DLP). DLP is based on principle, that in a known multiplicative group, it is very difficult to calculate the exponent. DLP equations are of the following type,

$$p^x = G \tag{11}$$

where $G$is a known Multiplicative Group; p is a generator term from G; x is an element such that $x \ \in G$.

DLP says how to x in Equation 11 when p and G are known. It requires calculation of logarithm i.e. $\log_G p$ for finding x referring this as DLP [25]. There are two categories of adversaries, which can attack on proposed EEoP cryptosystems. That would use the public key generation algorithm defined in equation 5. It have already the public key and extract private key from it. Adversary pretends to be a legitimate device to achieve M-I-T-M attack.

A. Security Analysis

There are number of attacks on EEoP that can be made. Most common attack is brute force attack that can be done by adversary 'a', as stated by algorithm 2 that public key P, elliptic curve E and base point B can be known to rouge relay R.

B. Brute force / Linear search attack

The adversary know the calculation of public key using the equation P $= k * B$, Here P and B are known to adversary R that will use the different values of k to find P. As known that elliptic curve uses point addition and point multiplication.

Thus different values of k can be inserted to find P where k has to be repeatedly point multiplied in Elliptic curve E. Requiring linear steps to find will be $O(n)$ that seems to be computationally impossible. Our assumption of algorithm is based on key size of 571bits for certification purpose that is equal to 15360bits in binary scheme. Thus, requiring 2^{15360} maximum number of times to be conducted to find secret key that seems virtually impossible. EEoP algorithm share different keys for sending message that is referred as temporal key that will be on size 256 that is equivalent to 3072bits in binary system so total number of steps to crack a message will require

$$T_C = t_{keyCA}\,[t_{tempKEY}]$$

where $t_{tempKEY}$ is changed after each communication session s. Thus $if\ s\ > t_C$ then a key can be found but this means in our case session will be more than $X\ where\ X\ is\ very\ large$ years that is nearly impossible. For baseline protocol ULMAP the linear search attack can be done while for improved-SIP is also based on ECC but is based on fixed 512 bits key size that will be make computational overhead but EEoP outperforms this as it uses varaibale key size for sessions.

C. M-I-T-M Attack

Let's consider Needam-schroder protocol [26] for M-I-T-M attack in our MRBS and R case.

$$\mathbf{R1 \rightarrow R2}$$
$$\mathbf{R1 \rightarrow R2} \quad \boldsymbol{K_{R1}(P_{MRBS}, MRBS)}$$

Here instead of $R2$ some rouge relay can use its private key and send the public key of some other device for communication. As public key of $R2$ will be obtained through CA using the following method thus a chance of rouge-relay in between is failed.

$$R2 \rightarrow CA$$
$$CA \rightarrow R2 \qquad K_{CA}(P_{R1}, R1)$$

$$R2 \quad D_{P_{R1}}(K_{R1}(P_{MRBS}, MRBS)$$

It is seen in above equations that M-I-T-M will fail as the key is directly obtained from the CA with an assumption that CA is not rouge. In future, this algorithm will be extended to certificate-less authentication reducing the overhead cost posed by EEoP.

D. Baby Step, Giant Step (BSGS) Method

BSGS [27] method is one of fastest methods where it is used to solve DLP problem that is considered to strength of EEoP. BSGS makes an assumption that it can be applied to any group. Thus, algorithm will need F_N field points [28] to be calculated and store. It requires at least $\sqrt{N}$ time of space and $\sqrt{N}$ space where N is very large so $\sqrt{2}^{bits}$ wherein our case bits are 15360 then 3072 are very large so thus machining it computationally infeasible to calculate the secret key.

EEoP proves to be a secure protocol that can handle M-I-T-M attack. Its security it higher than ECC or DH or ElGamal algorithm due to introduction of session keys during the communication that will be updated at each session while update with CA is done periodically in time t where t is < 40 hours , thus making extremely complex for attacker to do the guess attack even if quantum computers are uses. Moreover, if the M-I-T-M can be avoided then Interleaving attack will also be avoided. Rouge relays cannot act in our proposed model due to verification of CA for each device.

V. Conclusion

Device-to-Device communication is filling a gap of connectivity and bandwidth where small devices having low computational capabilities like the mobile phone can provide connectivity to nearby devices in the area just acting like a small base station of a cellular network. These small semi-intelligent devices are also called as semi-intelligent relays. If these small devices can be allowed to become a semi-intelligent relay, integrity and confidentiality are a major concern that has raised. In order to address these two challenges, EEoP scheme is proposed that used Elliptic curve cryptography with ElGamal over PKI. It will solve two issues (1) it is a lightweight security algorithm that allows secure transmission of data with authentication over the cellular network (2) Rouge Relay problem cannot exit. ECC is a lightweight mechanism compared to their predecessor RSA and Diffie Hellman, Also ElGamal addresses the shortcomings of Diffie Hellman. It also uses X.509 certificates before initial communication in cellular network making sure that authenticity is always ensured. The proposed solution solves the problem of authentication and confidentiality with limited computational resources. In future, the proposed scheme will be compared with known schemes employed in other areas. In addition, this research intends to use certificate less key sharing authentication scheme in the future.

Acknowledgement

The work is fully funded by Research and Innovation Management Center (RIMC) under the grant number F08/SpSG/1403/16/4.

References

[1] A. Kalka, M. Teicher, and B. Tsaban, “Short expressions of permutations as products and cryptanalysis of the Algebraic Eraser,” *Advances in Applied Mathematics*, vol. 49, no. 1, pp. 57-76, 2012.

[2] J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A ring-based public key cryptosystem,” In *International Algorithmic Number Theory Symposium*, Springer, Berlin, Heidelberg, pp. 267-288, Jun. 1998.

[3] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, “Secure key establishment for device-to-device communications,” In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pp. 336-340, Dec. 2014. IEEE.

[4] A. G. Reddy, E. J. Yoon, A. K. Das, and K. Y. Yoo, ”Lightweight authentication with key-agreement protocol for mobile network environment using smart cards,” *IET Information Security*, vol. 10, no. 5, pp. 272-282, 2016.

[5] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo, “Design of Mutually Authenticated Key Agreement Protocol Resistant to Impersonation Attacks for Multi-Server Environment,” *IEEE Access*, vol. 5, pp. 3622-3639, 2017.

[6] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, “Securing the Internet of Things in a Quantum World,” *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116-120, 2017.

[7] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” *IEEE Wireless communications*, vol. 11, no. 1, pp. 62-67, 2004.

[8] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of computation*, vol. 48, no. 177, pp. 203-209, 1987.

[9] U.S. Department of Commerce/National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS-186-4, 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[10] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, “On emerging family of elliptic curves to secure internet of things: Ecc comes of age,” *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 237-248, 2017.

[11] J. Y. Kim, W. Hu, H. Shafagh, and S. Jha, “SEDA: Secure Over-The-Air Code Dissemination Protocol for the Internet of Things,” *IEEE Transactions on Dependable and Secure Computing*, 2016.

[12] D. S. Laiphrakpam and M. S. Khumanthem, “A robust image encryption scheme based on chaotic system and elliptic curve over finite field,” *Multimedia Tools and Applications*, pp. 1-24, 2017.

[13] R. Sedidi and A. Kumar, “Key exchange protocols for secure Device-to-Device (D2D) communication in 5G,” In *2016 Wireless Days (WD)*, pp. 1-6, Mar. 2016. IEEE.

[14] W. Xi, X. Y. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, “Keep: Fast secret key extraction protocol for d2d communication,” In *Quality of Service (IWQoS), 2014 IEEE 22nd International Symposium of*, pp. 350-359, May 2014. IEEE.

[15] M. J. Raju, P. Subbaiah, and V Ramesh, “A novel elliptic curve cryptography based aodv for mobile ad-hoc networks for enhanced security,” *Journal of theoretical & applied information technology*, vol. 58, no. 3, 2013.

[16] S. S. Dake and R. U. Ighare, “A proposed ECC algorithm for smart cards cell phones and wireless networks,” In *Nascent Technologies in Engineering (ICNTE), 2017 International Conference on*, pp. 1-4, Jan. 2017. IEEE.

[17] Y. Jung, E. Festijo, and M. Peradilla, “Joint operation of routing control and group key management for 5G ad hoc D2D networks,” In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, pp. 1-8, May 2014. IEEE.

[18] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, and M. U. Hassan, “An improved and provably secure privacy preserving authentication protocol for SIP,” *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 1-15, 2017.

[19] P. Mohit, R. Amin, and G. P. Biswas, “Design of authentication protocol for wireless sensor network-based smart vehicular system,” *Vehicular Communications*, vol. 9, pp. 64-71, 2017.

[20] K. Fan, P. Song, and Y. Yang, “ULMAP: Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G,” *Mobile Information Systems*, 2017.

[21] Y. Wang, B. Ramamurthy, and X. Zou, “The performance of elliptic curve based group diffie-hellman protocols for secure group communication over ad hoc networks,” In *Communications, 2006. ICC'06. IEEE International Conference on*, vol. 5, pp. 2243-2248, Jun 2006. IEEE.

[22] V. Gupta, S. Gupta, S. Chang, and D. Stebila, “Performance analysis of elliptic curve cryptography for SSL,” In *Proceedings of the 1st ACM workshop on Wireless security*, pp. 87-94, Sep. 2002. ACM.

[23] S. A. Vanstone, "Next generation security for wireless: elliptic curve cryptography," *Computers & Security*, vol. 22, no. 5, pp. 412-415, 2003.

[24] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, Springer Science & Business Media, 2006.

[25] N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," *Journal of cryptology*, vol. 12, no. 3, pp. 193-196, 1999.

[26] C. A. Meadows, "Analyzing the Needham-Schroeder public key protocol: A comparison of two approaches," In *European Symposium on Research in Computer Security*, pp. 351-364. Springer, Berlin, Heidelberg, Sep. 1996.

[27] K. Matsuo, J. Chao, and S. Tsujii, "An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields," In *ANTS*, pp. 461-474, Jul. 2002.

[28] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *iEEE Transactions on information Theory*, vol. 39, no. 5, pp. 1639-1646, 1993.

[29] M. Wang and Z. Yan, "A Survey on Security in D2D Communications," *Mobile Networks and Applications*, pp. 1-14, 2016.

[30] A. S. Khan, Y. Javed, J. Abdullah, J. M. Nazim, and N. Khan, "Security issues in 5G device to device communication," *IJCSNS*, vol. 17, no. 5, p. 366, 2017.

[31] M. Wang and Z. Yan, (2017) "A survey on security in D2D communications," *Mobile Networks and Applications*, vol. 22, no. 2, pp. 195-208, 2017.

[32] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86-92, 2014.

[33] M. Wang and Z. Yan, "Security in D2D communications: a review," In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1, pp. 1199-1204, Aug. 2015. IEEE.

[34] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, and H. Tullberg, "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communication Magazine*, vol. 52, no. 5, pp. 26-35, 2014.

[35] A. S. Khan, H. Lenando, J. Abdullah, and M. N. B. Jambli,, "Lightweight message authentication protocol for mobile multihop relay networks," *International Review on Computers and Software (IRECOS)*, vol. 9, no. 10, pp. 1720-1730, 2014.

[36] A. S. Khan, "Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network," *International Journal of Communication Networks and Information Security*, vol. 6, no. 3, p. 189, 2014.