2011 International Conference on Software and Computer Applications
IPCSIT vol.9 (2011) © (2011) IACSIT Press, Singapore

Analysis of Optimized Elliptic Cryptographic Protocol on Resource Poor Tiny Node

Arpit [1] and Ashwini Kumar [2]

IERT, 26 Chatham lines, Prayag Allahabad (UP) INDIA
[1]arpittabelabux@gmail.com and [2]simplyashwini@gmail.com

Abstract. Wireless communication is inherently unreliable and can cause packets to be damaged or dropped. This unreliability in communication poses additional threats to the nodes if dropped packets are taken over by adversaries. Optimized Elliptic curve cryptography (O-ECC) can assist more secure towards WSN security and better protocol design. Optimized Elliptic curve cryptography is not only emerged as an attractive public key crypto-system for mobile / wireless environments but also provides bandwidth savings. This paper presents a light security algorithm i.e. Optimized ECC which is enhancement of traditional Elliptic Curve Cryptography for wireless sensor network.

Keywords: Cryptography, ECC, Security, Wireless Sensor.

1. Introduction

Technological enhancement in the areas of micro electro-mechanical systems and miniaturization has encouraged the development of a new kind of network. This network is comprised of small-scale, relatively low in price sensors adequate to intelligent sensing. Sensor network envision a future in which thousands to millions of tiny sensor nodes will be engrafted in almost every aspect of life. The intention is to create an intelligent environment which is adequate to collecting massive amounts of relevant information, acknowledging significant events automatically, and reacting suitably. Without a doubt security schemes optimized for wireless sensor networks have not been fully developed. Current techniques face weaknesses in certain situations, as aggregation or routing aspects prevent top efficiency. The ad hoc nature of sensor networks poses unique challenges regarding their security and reliability. The limited memory, power, processing abilities, and low coverage of the sensor nodes makes them vulnerable to intrusion, interception, modification and fabrication so traditional security techniques cannot ensure confidentiality, integrity, reliability and availability. Wireless communication is inherently unreliable and can cause packets to be damaged or dropped. This unreliability in communication poses additional threats to the nodes if dropped packets are taken over by adversaries. Optimized Elliptic curve cryptography (O-ECC) can assist more secure towards WSN security and better protocol design. In following sections contain introduction to Elliptic curve cryptography and the propose method on the mechanism to Optimized it and simulate it on Tiny OS [4].

2. Elliptic curve cryptography

Elliptic curve cryptography (ECC) [1] is an approach intended to deal public-key cryptography which is founded on the mathematics of elliptic curves. It offers fast decryption and digital signature processing by using Elliptic Curve DSA (ECDSA) [2] and key establishment by using Elliptic Curve Diffie-Hellman (ECDH)[3]. The main advantage of ECC is that under certain situations it applies smaller keys than other methods such as RSA while offering a same or higher level of security. ECC employs points on an elliptic curve to derive a 160-bit public key which is same as in strength to a 1024-bit RSA key. Hence smaller numbers of key contribute to faster key operation and less memory overhead. It is said to be ideal for

resource-constrained devices because it provides more "security per bit" than other types of asymmetric cryptography in lesser cost.

2.1. Elliptic Curve: Its Derivation and Use

The ECC named because of the fact that ellipses are formed by quadratic curves. Elliptic curves are always cubic and have a relationship to elliptic integrals in mathematics [10] where the elliptic integral can be used to determine the arc length of an ellipse. An elliptic curve in its "standard form" is described by

$y^2 = x^3 + ax + b$

For the polynomial $x^3 + ax + b$, the discriminant can be given as $D = -(4a^3 + 27b^2)$

This discriminant must not become zero for an elliptic curve polynomial $x^3 + ax + b$ to possess three distinct roots. If the discriminant is zero, that would imply that two or more roots have coalesced, giving the curves in singular form. It is not safe to use singular curves for cryptography as they are easy to crack. Due to this reason we generally take non-singular curves for data encryption.

2.2. Elliptic Curve Cryptography as fine balance for sensor network

It has been claimed by some researchers that public key cryptosystems are not viable to implement in these tiny devices because they are resource constrained but this is not true. Let's see some of the features of elliptic curve cryptography (ECC) and later see the justification so as to need this in the sensor networks.

1) ECC offers considerably greater security for a given key size.

2) The smaller key size also makes possible much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software. This means less heat production and less power consumption — all of which is of particular advantage in constrained devices, but of some advantage anywhere else.

3) There are extremely efficient, compact hardware implementations available for ECC exponentiation operations, offering potential reductions in implementation footprint even beyond those due to the smaller key length alone.

In short: asymmetric cryptography is demanding but looking at the cryptosystem for more security per bit, ECC is a better choice.

2.3. Optimized-Elliptic Curve Cryptography

Traditional Elliptic Curve cryptography [5] is not optimized one for resource constraint sensor nodes because it adds extra overhead in terms of computation and memory cost. So there is need for optimization, We have considered that problem and optimized the existed elliptic curve cryptography Optimization can be achieved by simplifying the calculations such as modular multiplication, or by reducing number of steps required for point addition and point doubling. Next section elaborates optimizations which are done to reduce complexity while maintaining same security level as ECC.

2.4. Optimizations for Large Integer Operations

Barrett Reduction [6]: As we know that public-key cryptosystems Elliptic curve Cryptography is based mainly on modular operations (modular multiplication and modular exponentiation) of very large integers, ranging on the order of 38-616 decimal digits, or 128-2048 binary bits. Performing computation of numbers of this large size with multiple precisions is not easy or fast to implement. Most methods rely on modular reduction algorithm functions to reduce the size and complexity of the required arithmetic operations to carry out their public-key cryptosystem implementations more efficiently. Barrett Reduction is a nothing but method of reducing a number modulo another number. Barrett reduction, when used to reduce a single number, is slower than a normal division algorithm. However, by pre computing some values, one can easily far exceed the speed of normal modular reductions. A straightforward style to perform large integer modular reductions is to use division [6]. A nice side effect is that it reuses the code of division, thus resulting in more compact code size. So Barrett reduction converts the reduction modulo an arbitrary integer to two multiplications and a few reductions modulo integers of the form $2n$.In Optimized-Elliptic Curve Cryptography, since almost all the modular operations are modulo the same prime number *q*, Barrett reduction can potentially speed up the computation. However, this requires the implementation of a separate reduction algorithm, which implies larger code size (i.e., greater ROM requirement) on sensor nodes. In addition, Barrett reduction also increases RAM use. Assume the target microcontroller has a *w*-bit word size. Given a finite field *Fq*, where *q* is a *k* words long prime number, Barrett reduction requires the pre-computation of $\mu = \texttt{floor}(b^{2k} / q)$, where $b = 2w$ *or* where b is the "base" of the integers used (e.g., $b =$

2^8 on a 8-bit processor). This number m has to be stored and used throughout all the modular reductions. Thus, to exchange for faster computation, Barrett reduction requires more ROM and RAM than the traditional division based modular reduction. A normal division algorithm or Classical Division Algorithm is as follows:-

The classical algorithm is a formalization of the ordinary l-k (l is size of argument, k is size of m) step pencil-and-paper method, each step of which is the division of a (k+1) digit number x by the k-digit divisor m. This yields the one-digit quotient q and the k digit remainder r. Each remainder r is less than m, so that it can be combined with the next digit of the dividend into the (k+1) digit number rb + (next digit of dividend) to be used as the new x in the next step.The pseudo code of the classical algorithm given

$m_{k-1} \geq b/2$ follows:

if ($x > mb^{l-k}$) then
$x = x - mb^{l-k}$;
for ($i = l- 1$; $i > k - 1$; i--) do
{
if ($x_i = = m_{k-1}$) then
$q = b - 1$;
else
$q = (x_i b + x_{i-1})$ div m_{k-1};
while ($q\ (m_{k-1}b + m_{k-2}) > x_i b^2 + x_{i-1}b + x_{i-2}$) do
$q = q- 1$;
$x = x- q\ m\ b^{i-k}$;
if ($x < 0$) then
$x = x + m\ b^{i-k}$;
}
//Whereas for Barrett Reduction the generalized algorithm will be as follows
(for $\mu = \text{floor}\ (b^{2k} / m)$)
$q = ((x \text{ div } b^{k-1}) \times \mu \text{ div } b^{k+1}$;
$x = x \bmod b^{k+1} - (q\ m) \bmod b^{k+1}$;
if ($x < 0$) then
$x = x + b^{k+1}$;
while ($x \geq m$) do
$x = x- m$;

3. Optimizations for ECC Operations

3.1. Projective Coordinate Systems

An elliptic curve comprises of the infinity point Ô and the set of points in the affine coordinates (x, y) for x, y a finite field *Fq* that satisfies the defining equation. Alternatively, a point on an elliptic curve can be represented in a projective coordinate system in the form of (x, y, z). Point addition and point doubling are decisive operations in ECC, which are building blocks for scalar multiplications required by all ECC schemes. These operations in affine coordinate system necessitate modular inversion operations, which are much more expensive than other operations such as modular multiplications, which is not suitable for resource constrained devices. Using a projective coordinate system [7], modular inversions can be moved out with the compensation of a few modular multiplications and squares operation. Due to this, the execution times of point addition and point doubling based on projective coordinate system are faster than those based on affine coordinate system, respectively [7].Optimized-ECC uses two additional optimizations along with projective coordinate representation, which can further minimize both the execution time and the program size. The first one is a mixed point addition algorithm [7], which simply adds a point in projective coordinate and a second point in affine coordinate. This algorithm can be used in scalar multiplications to further reduce the number of modular multiplications and squaring operation, which leads to smaller and faster code. The other one is repeated Doubling [8] for scalar multiplication. If consecutive point doublings are to be performed, the repeated doubling algorithm may be applied to achieve faster performance instead of using

doubling formula rapidly. In m consecutive doublings process, this algorithm trades m−1 field additions, m−1 divisions by two, and a multiplication for two field squaring (in comparison with repeated applications of the plain point doubling algorithm) [8]. Although reducing the execution time, the projective coordinate representation needs a larger code size (for implementing more complex formula) and more RAM (for storing additional required variables) than the affine coordinate system.

3.2. Curve Specific Optimization

A number of elliptic curves specified by NIST [9] and SECG [8] employ pseudo-Mersenne primes. A pseudo-Mersenne prime is of the form $p = 2n - c$, where $c \in 2n$. Reduction modulo a pseudo-Mersenne prime can be performed by a few modular multiplications and additions without any division operation. As a result, the time for modular reduction can be reduced significantly. Thus, using elliptic curves over a pseudo-Mersenne prime can achieve additional performance gain.

4. Quantitative Overhead Analysis

4.1. Test Setup

Projects dealing with WSNs use TinyOS as their operating system. TinyOS [11] is an event-driven operating flexible, application-specific operating system for sensor networks. System projected for sensor network nodes that have very limited resources. TinyOS and programs for TinyOS are written in NesC [11]. The NesC programming language is designed specifically for TinyOS and it is based upon the concept of components that are connected or wired together to form a program. MICA2 and MICAZ and TelosB from Crossbow, platforms for performance evaluation. There are four nodes of both types available for the experiments. Because the MICA2s are easier to work with, due to their simpler connection to a PC, they are used instead of the MICA2DOTs.

The simulator that is used is TOSSIM [8], which stands for TinyOS Simulator. It is included with TinyOS together with a program called TinyViz that can be used to visualize the WSN network running in the simulator and also process debug data from some or all of the nodes. To use it, a TinyOS application needs to be compiled specifically for the simulator. The compiled executable can then be started with command line arguments telling the simulator how many nodes to simulate, what radio model and topology to use and its debugging and visualization settings. The simulations will either start running immediately or if specified, wait for TinyViz to connect to it. TinyViz can then show which node is sending messages to other nodes, who is broadcasting and which LEDs on the nodes are on and off. One drawback of the simulator is that all simulated nodes run the same application. This is a disadvantage when one of the nodes needs to act as a node that is performing an attack. To measure energy consumed by various cryptographic protocol PowerTOSSIM is used. This is extension of TOSSIM and provides an accurate per node estimate of power consumption. In PowerTOSSIM, specific hardware peripherals such as radio, EEPROM, LEDs and CPU are instrumented to obtain a trace of each peripheral's activity during the simulation run time. PowerTOSSIM energy model is based on the Mica2 sensor node platform [8].

4.2. Optimized-ECC Performance Evaluation

We have implemented optimized-ECC for TelosB and Mica2 platform, it can also be extended for other sensor platforms as well, and for evaluating required time to generate signature and for signature verification we have written a java code using jdk 1.5 and javacomm package. Firstly, I've used two TelosB motes for testing my algorithm, one mote is Alice, and another is Bob. Let us suppose Alice's (mote 1) public key is pre deployed in Bob (mote 2). Alice broadcasts packets with her signature. Bob receive packets and verifies all packets from Alice. Red LED for Alice indicates the signature generation whereas red LED for Bob means, Bob is verifying the signature. If computed signature is correct, Bob will start toggling the green LED, else Bob will turn on all three LEDs. One mote which generates the signature and one TelosB is directly connected to PC which verifies the signature; basically following simulation demonstrate the running of ECDSA.

5. Result Discussion

Using POWERTOSSIM simulator, Figure 1. Shows the execution time required ECDSA initialization, Signature generation and signature verification, ECIES initialization, Encryption, decryption ECDH initialization, key establishment and Figure 2. Shows Energy consumption (in mJ) for digital signature scheme (ECDSA- Elliptic Curve Digital Signature Algorithm), public key encryption scheme (ECIES-Elliptic Curve Integrated Encryption Scheme) and a key exchange protocol scheme (ECDH - Elliptic Curve Diffie-Hellman). The analysis shows that the TelosB performance is higher than Mica2.

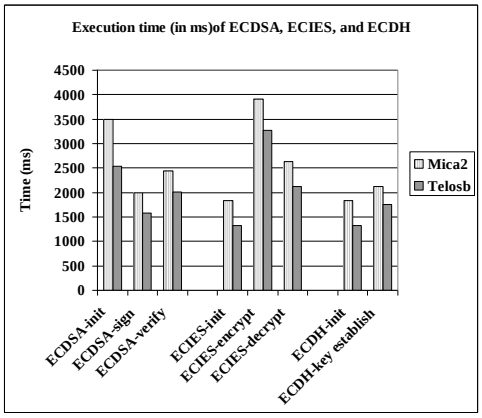

Figure 1. Eecution Time (ms) for ECDSA, ECIES and ECDH operation on Mica2 and telosB motes

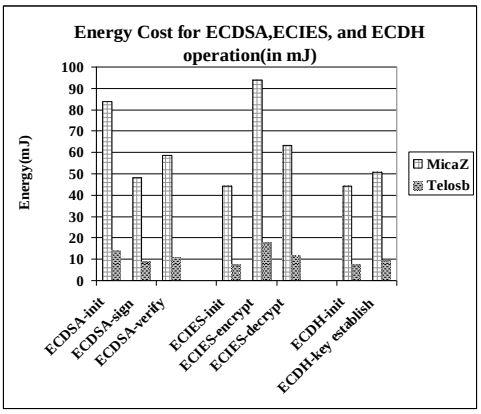

Figure 2. Energy Cost (mJ) for ECDSA, ECIES and ECDH operation on Mica2 and telosB motes

6. Conclusion and Future Scope

We work brought out a light security algorithm i.e. Optimized ECC which is enhancement of traditional Elliptic Curve Cryptography. The idea for Optimized ECC has been taken from Mathematics where the unique property of Elliptic curves have been used and optimization is provided using easy computation , mathematically it is proved that Asymmetric Cryptography can be implemented in these minuscule sensor devices. As observed it drains the battery power but there has to be a trade off between the energy utilization and security level. Paper also described and compares the energy consumption as well as running time for TinySec and Optimized ECC. Most of the modern sensors today operate on renewable energy source hence public key cryptography can be implemented in these resource constraint embedded sensor devices. There is scope of resolve DoS attack and more optimization O-ECC toward light & ad hoc network. Further work remains in minimization encryption and decryption operation implementation. Optimized-ECC performance evaluation can also be extended for other sensor platforms.

7. References

[1] Anoop MS :*Elliptic Curve Cryptography – An Implementation Tutorial*:www.tataelxsi.com/whitepapers/ECC_Tut_v1_0.pdf?pdf_id=public_-key_TEL.pdf

[2] Don B. John :*Elliptic curve DSA (ECSDA): an enhanced DSA :* 7th conference on USENIX Security Symposium - Volume 7 USENIX Association Berkeley, CA, USA ©1998

[3] S Wang :*Efficient implementation of elliptic curve Diffie-Hellman (ECDH) key*: IEEE COMMUNICATIONS LETTERS, VOL. 12, NO. 2, FEBRUARY 2008. 149

[4] An Liu; Peng Ning :*TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks* : Information Processing in Sensor Networks, 2008. IPSN '08

[5] Menezes, *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.

[6] Faster *Interleaved Modular Multiplication Based on* Barrett : www.cosic.esat.kuleuven.be/publications/article-1191.pdf

[7] Performance *analysis of Point multiplication methods for Elliptic* : www.rimtengg.com/iscet/proceedings/pdfs/misc/172.pdf

[8] Levis, N. Lee, M. Welsh and D. Culler, "*TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications*," Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 2003, pp 126-137.

[9] Certicom Research. Standards for efficient cryptography SEC 2: *Recommended elliptic curve domain parameters*.:www.secg.org/collateral/sec2_final.pdf, September 2000.

[10] A.J.Menezes, P. C. van Oorschot, and S.A.Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[11] http://www.tinyos.net/tinyos-1.x/doc/tutorial