Improvement of Data Security and Privacy in the Wireless Sensor Network Using Elliptical Curve Cryptography

Srinivasachary Sirisinahal

Research scholar in Computer Science, Osmania University, Hyderabad

MV Ramana Murthy

Professor & Head, Dept. of M& H, M G I T, Hyderabad

S China Ramu

Professor in Computer Science Engineering,CBIT, Hyderabad

C R K Reddy

Professor in Computer Science Engineering,CBIT, Hyderabad

Abstract - With the expanding use of wireless sensors in a number of applications, including the Internet of Things, academics have focused on the security aspects of wireless sensor networks. Designing efficient security algorithms for wireless sensor networks has always been a difficulty due to resource limits in wireless sensor networks. This paper presents an elliptic curve signcryption-based security protocol for wireless sensor networks that provides anonymity, confidentiality, mutual authentication, forward security, secure key establishment, and key privacy while also resisting replay, impersonation, insider attack, offline dictionary attack, and stolen-verifier attack.

Keywords: Elliptic curve cryptography, User Authentication, Access control, Wireless Sensor Networks

Introduction

The security of wireless sensor networks is becoming increasingly important as they grow more ubiquitous. This is especially true for products like medical sensors, where confidentiality is critical. These devices frequently communicate sensitive data, necessitating the use of a cryptographic technique that ensures data confidentiality and integrity, as well as the legitimacy of people using the sensor network's devices. All of these are provided by public-key cryptography; but, owing of computational and battery power limits, the most prevalent public-key algorithm (RSA) cannot be used because it is too computationally expensive. Because it requires substantially smaller key sizes, Elliptic Curve Cryptography (ECC) presents an option that provides comparable security strength with significantly less computation.

Data encryption, digital signatures, user authentication, and other applications have all made substantial use of public-key cryptography. In comparison to the widely used symmetric key cryptography in sensor networks, public-key cryptography offers a more flexible and straightforward interface that requires no key predistribution, pairwise key sharing, or a sophisticated one-way key chain mechanism. However, there is a widespread perception in the sensor network research community that public-key cryptography is not feasible since the required computational intensity is incompatible with sensors with limited processing power and energy budget. The preliminary investigation appears to debunk this myth.

The Wireless Sensor Network (WSN) is a self-organizing network that consists of a collection of sensor nodes that collect environmental data and communicate it to a sink or base station. The information can be gathered from the base station for further assessment. Sinks in WSNs can be either static or dynamic. For some applications, a static sink is utilised as a battlefield environment, whereas a dynamic sink is used as a disaster management system.

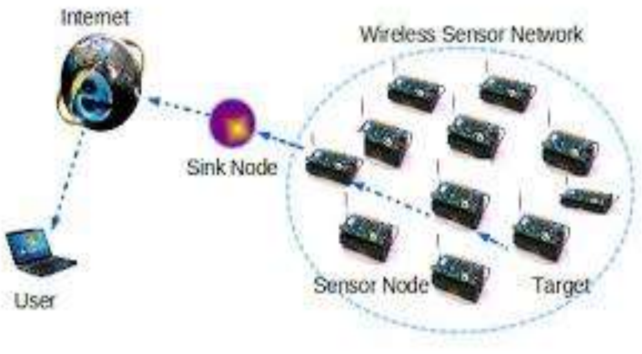

Fig. 1: WSN Architecture

Sensors are inexpensive but those have limited batterypower and limited resources. The main characteristics ofWSN are Low cost, Ease of use, Scalability, Mobility ofnodes, Ability to cope with node failures.

The data can be made secure by employing cryptographic techniques. Encryption and decryption are the two primary procedures of cryptography. Encryption is a procedure that uses cryptography to hide the original data and transfer it to secret data. Plain text refers to the original data, while cypher text refers to the secret data. The encryption text can be converted back to plain text using the Decryption method.

WSN Security Challenges

Designing efficient security protocols for WSNs have been a continuous challenge due to the following technical limitations.

- Wireless sensor nodes typically have a processing capacity of a few MIPS, RAM of a few hundred KB, and flash memory of less than one megabyte. Because wireless sensors have limited processing capabilities, devising and implementing security methods that meet all of the essential security functionality is difficult.
- Limited Power Supply – Since sensor nodes operate on limited battery power, the security mechanisms should be selected and implemented such that they avoid heavy computations.
- Unreliable Communication – The data is sent by the sensor nodes through wireless channels which are unreliable medium and are vulnerable to many threats and attacks. This requires the implementation of strong security schemes which thwart the attacks on WSN.

  These limitations enforce the two major challenges in securing WSNs – threats and the attacks on WSNs, and difficulties in implementing efficient security measures to counter these threats and attacks.

Dhakne and Chatur [1] have presented “an exhaustive survey over attacks made on WSNs and divided them into five categories attacks on authentication, attacks on privacy, attacks based on perspectives, attacks on layers, and other attacks”.

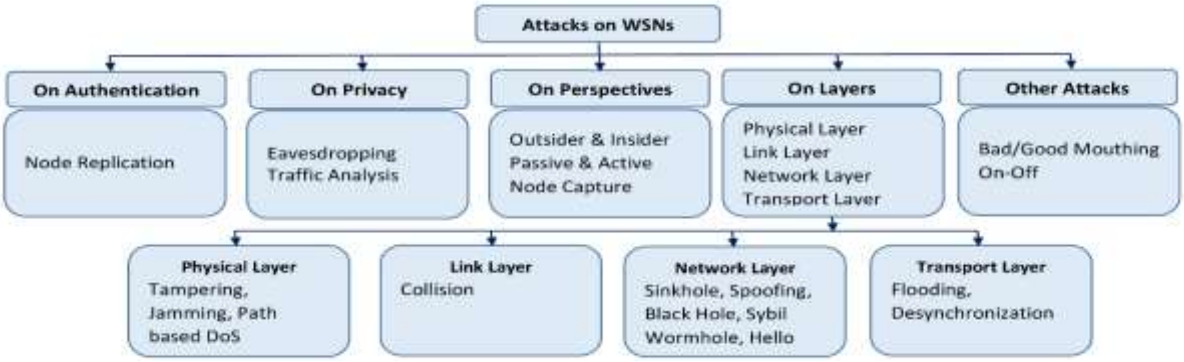

Fig. 2: Common Attacks on WSN

Related Work

"Various security protocols for WSNs based on different cryptographic systems with different level of security have been proposed by different authors. But the recent focus of the researchers has been on designing Elliptic Curve Cryptography (ECC) based security mechanisms for WSNs, since ECC based solutions are suitable for applications involving low computing power devices like wireless sensors" [2].

Choi et al. [3] presented an "ECC based authentication mechanism for WSNs which addressed the security flaws of session key attacksensor energy exhausting attack, and stolen smart card attack, in the protocol given by Shi and Gong" [4].

Wu et al. [5] "designed a mutual authentication scheme for the mobile network, which provides forward security and resistance against insider attack, de-synchronization attack, forgery attack, replay attack, and known-key attack."

Amin et al. [6] "suggested a 3-factor key agreement and authentication scheme which was an improvement over the protocol developed by Farash et al. [7]. They stated that their protocol provides additional security features of identity change and smartcard revocation phases, at the same time protecting from stolen smart-card attack, user impersonation attack, session-specific attack, and password guessing attack".

Y.H. Park and Y. Park [8] suggested "a 3-factor ECC based key-agreement and biometric authentication scheme which provides user anonymity, forward security, intractability, mutual authentication, secure password update and can resist from stolen smart card attack, user impersonation attack, replay attack, man-in-the-middle attack, and off-line password guessing attack".

Later, Jiang et al. [9] proved that scheme of Amin et al. [6] is prone to "lost smart card attack, KSSTI (known-session specific temporary information) attack, and tracking attack. They also designed a Rabin Cryptosystem based 3-factor authentication and key establishment protocol which overcome all the weaknesses of the protocol" given by Amin et al.

Jung et al. [10] exposed that "the protocol given by Chang et al. [11] cannot protect against password guessing, session key compromise, and user impersonation. Furthermore, Jung et al. pointed out that Chang's protocol puts a high computational load on the gateway. They also designed an anonymous key establishment and authentication scheme for WSNs overcoming security flaws of Chang et al. scheme while consuming less computational cost".

ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

Elliptic Curve Cryptography (ECC) was proposed in 1985 by Neal Koblitz and Victor Miller.ECC is also a public keycryptography technique and is an asymmetric cryptographymethod. In this method public key is distributed to all andprivate key is known by particular user only. Themathematical operation of ECC is defined over the ellipticcurve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$.

Each value of the 'a' and 'b' gives a different elliptic curve.The public key is a point in the curve and the private key isa random number. The public key is obtained bymultiplying the private key with the generator point G in thecurve.

The key length of ECC is 160 bits which gives the samesecurity level of 1024 bits of RSA Algorithm. Symmetrickey algorithm provides only confidentiality but theasymmetric key algorithms provide more than that ofconfidentiality. The security is based on the difficultly of a problem [12].

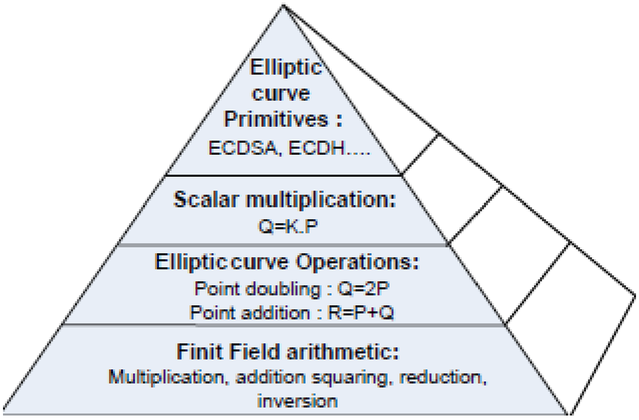
Elliptic curve Primitives :
ECDSA, ECDH....
Scalar multiplication:
Q=K.P
Elliptic curve Operations:
Point doubling : Q=2P
Point addition : R=P+Q
Finit Field arithmetic:
Multiplication, addition squaring, reduction, inversion

Fig.3: Hierarchy of ECC

Elliptic curve crypto systems have a layered hierarchy as a pyramid as shown in Fig.3. At the top layer there are elliptic curve primitives as key agreement with ECDH and digital signatures with ECDSA.

Elliptic Curve Arithmetic

An Algebraic Expression for Adding Two Points on an Elliptic Curve over Fp. Let FP, where p an odd prime number, be a prime finite field given two points used on the first point is an Q = (x1, y1) and another point is an R = (x2, y2) on an elliptic curve E (a,b), we have to compute the point Q + R.

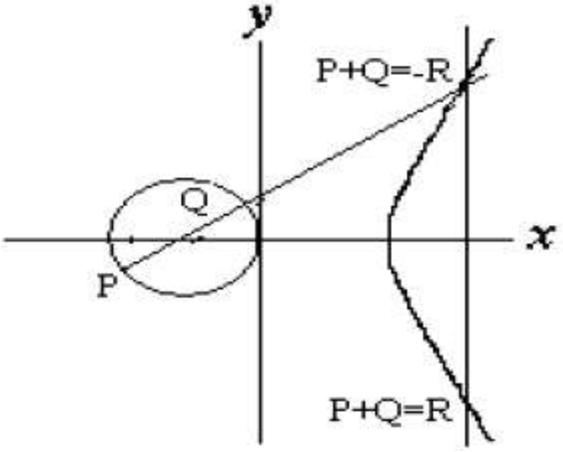

Fig.4: Elliptic Curve

We first draw a straight line processor through the two point P and Q. Next, we find the third coming together of this line with theElliptic curve denote this point of intersection by R. Then P + Q is Equal to the mirror reflection of R about the x-axis. In other words, if the points P, Q and -R are the three intersections of the straight line with the elliptic curve processor Curve, thenP + Q = - R

Encryption Algorithm

Step 1.First algorithm can be taking the message to be encrypted from the sender.

Step 2.Convert it to its 7bits binary element form using the ASCII code of the message.

Step 3.Convert the binary form of each word of the Message into an x 7 binary matrix where n is a Number of letters in each word of the message.

Step 4.To get the compressed decimal matrix of size n x 1, we will multiply the n x 7 matrix with the masked matrix process of size 7 x 1.

Step 5.We will get n values of „x‟ and to get the value of an data can Corresponding „y‟ values we will use the formula Y^2=x (i) ^3+j Where, i = 1 to n SS (and n is the no. of rows

in the resultant Matrix) j is the variable which will keep on incrementing every time we get a y for a particular x value. The initial value of j = 1.

Step 6. Using the formula we will get (x, y) points.

Decryption Algorithm

Step 1.The receiver will get the x and y values after Comparing two images and finally get the values of y with the help of the matrix containing the values of y (after decimal points).

Step 2.The required matrix will be generated using the “x” values and the prime matrix which is public.

Step 3.We will multiply the “x” values with the prime elements and will check the result of the co-efficient with the generated public equation.

Step 4. In this way the receiver will generate the required matrix which will contain the binary form of the ASCII codes of the same hash algorithm and then uses the signature verification algorithm to verify the signature. If the message is verified successfully receiver authenticates the sender. In the following, H denotes a cryptographic hash function whose outputs have bit length no more than that of n.

Strength of Elliptic Curve Cryptography

The strength of the elliptic curve-based cryptosystem is ensured by the three computationally hard problems given below. An elliptic curve (Fq) has been considered in the definition of these problems.

- Elliptic Curve Based Discrete Logarithmic Problem (ECDLP) – For known two points$Q$,R∈(Fq), it is computationally infeasible to get an integer$k$ so that$R=kQ$.
- Elliptic Curve Based Diffie-Hellman Problem (ECDHP) – Given a point$Q$∈(Fq), and consider two other points $R=aQ$ and $S=bQ$ on the same elliptic curve$E(Fq)$, wherea,b∈$Integer$. Determining a point $T=abQ$ is computationally hard.
- Elliptic Curve Based Decision Diffie-Hellman Problem (ECDDHP) - Given a point$Q$∈(Fq), and consider three other points$R=aQ$,$S=bQ$ and$T=cQ$. It is computationally infeasible to conclude that if$T=abQ$.

Conclusion

WSNs are widely utilised in a variety of vital applications, so securing them has been a top focus for the research community. An elliptic curve-based security protocol for WSNs is provided in this work, which successfully provides user anonymity, secrecy, mutual authentication, and safe key formation while consuming less computational time than existing related systems. The proposed protocol also protects against offline dictionary attacks, insider attacks, impersonation attacks, replay attacks, and stolen verifier attacks, according to the researchers. Our signcryption-based protocol uses the least computing time for the gateway in contrast to existing protocols while delivering the same or higher security level, making it appropriate for security and privacy-critical WSN applications.

References

[1]. Dhakne, and P. Chatur, "Detailed Survey on Attacks in Wireless Sensor Network," inProc. of the International Conference on Data Engineering and Communication Technology. Advances in Intelligent Systems and Computing, Singapore, 2017, pp. 319-331.

[2]. A.K. Singh, and B.D.K.Patro, "Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions," Cybernetics and Information Technologies, Vol. 19, No. 1, 2019, pp. 133-164.

[3]. Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," Sensors, Vol. 14, 2014, pp. 10081-10106.

[4]. W. Shi, and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography,"International Journal of Distributed Sensor Networks, 2013pp. 1-7. doi. 10.1155/2013/730831.

[5]. F. Wu, L. Xu, S. Kumari, X. Li, A.K. Das, M.K. Khan, M. Karuppiah, and R. Baliyan, R,"A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks,"Security and Communication Networks, Vol. 9, 2016, pp. 3527-3542.

[6]. R. Amin, S.K.H. Islam, G.P. Biswas, M.K. Khan, L. Leng, and N. Kumar, "Design of anonymity preserving three-factor authenticated key exchange protocol for wireless sensor network,"Computer Networks,Vol.2016, 2016, pp. 1-22.

[7]. M.S. Farash, M. Turkanovic´, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment,"Ad Hoc Networks, Vol. 36, 2016, pp. 152-176.

[8]. Y. Park, and Y.H. Park, "Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks," Sensors, Vol.16, No. 2123, 2016, pp. 1-17.

[9]. Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three factor authentication and key agreement protocol for internet integrated wireless sensor networks,"IEEE Access, Vol. 5, 2017,pp. 3376–3392.

[10]. J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and Security Enhanced Anonymous Authentication with Key Agreement Scheme in Wireless Sensor Networks," Sensors, Vol. 17, No. 644, 2017, pp. 1-21.

[11]. I.P. Chang, T.F. Lee, T.H. Lin, and C.M. Liu, "Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks," Sensors, Vol.15,2015, pp. 29841-29854.

[12]. Asha Rani Mishra, Mahesh Singh, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network", International Journal of Engineering Research & Technology (IJERT), Volume 01, Issue 03, May 2012.