American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-03, Issue-01, pp-50-56
www.ajer.org

Research Paper Open Access

Security in Wireless Sensor Networks using Cryptographic Techniques

Madhumita Panda
*Sambalpur University Institute of Information Technology(**SUIIT**)Burla, Sambalpur, Odisha, India.*

Abstract: **-**Wireless sensor networks consist of autonomous sensor nodes attached to one or more base stations.As Wireless sensor networks continues to grow,they become vulnerable to attacks and hence the need for effective security mechanisms.Identification of suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy,computation capability and storage resources of the sensor nodes.Symmetric based cryptographic schemes donot scale well when the number of sensor nodes increases.Hence public key based schemes are widely used.We present here two public – key based algorithms, RSA and Elliptic Curve Cryptography (ECC) and found out that ECC have a significant advantage over RSA as it reduces the computation time and also the amount of data transmitted and stored.

Keywords: *-Wireless Sensor Network,Security, Cryptography, RSA,ECC.*

I. WIRELESS SENSOR NETWORK

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed to monitor and affect the environment [1]. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security.

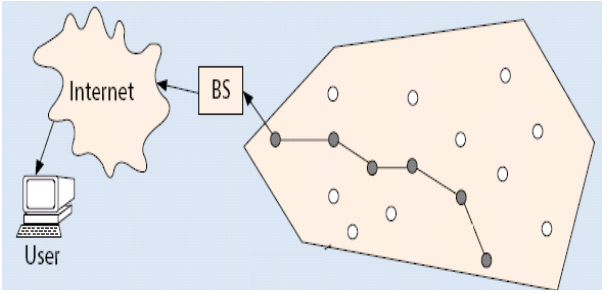

Figure 1:Wireless Sensor Network

11.SECURITY REQUIREMENTS IN WIRELESS SENSOR NETWORK

The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour. The security requirements in WSN include:

Confidentiality:

Confidentiality is hiding the information from unauthorized access. In many applications, nodes communicate highly sensitive data. A sensor network should not leak sensor reading to neighbouring networks.Simple method to keep sensitive data secret is to encrypt the data with a secret key that only the intended receivers'possess, hence achieving confidentiality.As public key cryptography is too expensive to be

used in the resource constrained sensor networks,most of the proposed protocols use symmetric key encryption methods.For symmetric key approach the key distribution mechanism should be extremely robust.

Authentication:

Authentication ensures the reliability of the message by identifying its origin.In a WSN,the issue of authentication should address the following requirements:[1] communicating node is the one that it claims to be(ii)the receiver should verify that the received packets have undeniably come from the actual sensor node**.**For Authentication to be achieved the two parties should share a secret key to compute message authentication code(MAC) of all communicated data.The receiver will verify the authentication of the received message by using the MAC key.

Integrity:

Integrityis preventing the information from unauthorized modification.Data authentication can provide data integrity also.

Availability:

Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks**.**

III.OBSTACLES OF SENSOR SECURITY

A wireless sensor network is a special network which has many constraintscompared to a traditional computer network. Due to these constraints itis difficult to directly employ the existing security approaches to the areaof wireless sensor networks. Therefore, to develop useful security mechanismswhile borrowing the ideas from the current security techniques, it isnecessary to know and understand these constraints first [2].

3.1 Very Limited Resources

All security approaches require a certain amount of resources for the implementation,including data memory, code space, and energy to power thesensor. However, currently these resources are very limited in a tiny wirelesssensor.

• Limited Memory and Storage Space:

A sensor is a tiny device withonly a small amount of memory (few KB) and storage space for the code. Inorder to build an effective security mechanism, it is necessary to limitthe code size of the security algorithm.

• Power Limitation:

A Sensor node has to economize with the shipped battery,i.e.the supplied energy must outlet the sensor's life.This is resulting from the fact that the sensor's battery can neither be replaced nor recharged,once deployed in a difficult access area or hostile environment.The energy of a sensor node is consumed by mainly three essential components:the sensor unit,the communication unit and the computation unit.Because of the limited energy reserves,energy is often one of the primary metrics in WSNs routing algorithms[3].Many Operating systems for WSNs provide certain features to preserve energy[4].

- **Transmission range:**

To minimize the energy needed for communication it is very common that sensor nodes use a rather small transmission range.This results in the necessity of using multiple-hops to transfer data from a source to a destination node through a large network.

3.2 Unreliable Communication

Certainly, unreliable communication is another threat to sensor security.The security of the network relies heavily on a defined protocol, which inturn depends on communication.

• Unreliable Transfer:

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packetsmay get damaged due to channel errors or dropped at highly congestednodes. The result is lost or missing packets. Furthermore, the unreliablewireless communication channel also results in damaged packets.Higher channel error rate also forces the software developer to devoteresources to error handling. More

importantly, if the protocol lacksthe appropriate error handling it is possible to lose critical securitypackets. This may include, for example, a cryptographic key.

• **Conflicts**:

Even if the channel is reliable, the communication may stillbe unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occurand the transfer itself will fail. In a crowded (high density) sensornetwork, this can be a major problem. More details about the effectof wireless communication can be found at [5].

• **Latency:**

The packet-based multihop routing in WSNs increases the latency due to congestion in the network and additionally require processing time. Besides, the routing process in WSNs is often causing delays:For example, if a routing algorithm uses different paths between a source and a destination to distribute energy load, not always the shortest path is used so that additional delays are predictable.

3.3 Unattended Operation

Depending on the function of the particular sensor network, the sensor nodesmay be left unattended for long periods of time. There are three maincaveats to unattended sensor nodes:

• **Exposure to Physical Attacks:**

The sensor may be deployed in anenvironment open to adversaries, bad weather, and so on. The likelihoodthat a sensor suffers a physical attack in such an environmentis therefore much higher than the typical PCs, which is located in asecure place and mainly faces attacks from a network.

• **Managed Remotely:** Remote management of a sensor network makesit virtually impossible to detect physical tampering (i.e., through tamperproofseals) and physical maintenance issues (e.g., battery replacement).

• **Lack of Central Management Point:**

A sensor network should be adistributed network without a central management point. This willincrease the vitality of the sensor network. However, if designed incorrectly,it will make the network organization difficult, inefficient, andfragile.Perhaps most importantly, the longer that a sensor is left unattended themore likely that an adversary has compromised the node.

IV.CRYPTOGRAPHY

Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. But as the sensor nodes are limited in their computational and memory capabilities,the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them.

4.1Symmetric Cryptography

Symmetric encryption(also called as secret-key cryptography) uses a single secret key for both encryption and decryption as shown in Figure 2.

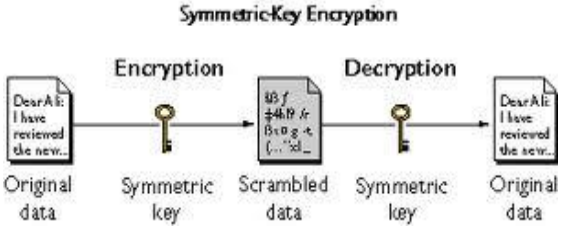

Figure 2:Symmetric -Key Cryptography

This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are usedto achieve the security requirements, several researchers have focused on evaluating crypto graphical algorithms in WSNs and proposing energy efficient ciphers. Symmetric key algorithms are much faster computationally than asymmetric algorithms as the encryption process is less complicated. Examples are AES,3DES etc.

We first focus on Symmetric Cryptography due to the assumption that symmetric cryptography has a higher effectiveness and require less energy consumption, in contrast to public key cryptography.

According to [6]public key is used in some applications for secure communications eg.SSL(Secure Socket Layer) and IPSec standards both use it for their key agreement protocols.But it consumes more energy and it is more expensive as compared to symmetric key.

[7] has given a reason that public key consumes more energy due to great deal of computation and processing involved ,which makes it more energy consumptive as compared to symmetric key technique e.g. a single public key operation can consume same amount of time and energy as encrypting tens of megabits using a secret key cipher.

According to [8],the more consumption of computational resources of public key techniques is due to the fact that it uses two keys. One of which is public and is used for encryption ,and everyone can encrypt a message with it and other is private on which only decryption takes place and both the keys has a mathematical link, the private key can be derived from a public key.In order to protect it from attacker the derivation of private key from public is made difficult as possible like taking factor of a large number which makes it impossible computationally.Hence,it shows that more computation is involved in asymmetric key techniques thus we can say that symmetric key is better to choose for WSN.

According to [9] the cost of public key is much more expensive a s compared to symmetric key for instance, a 64 bit RC5 encryption on ATmega 128 8 MHZ takes 5.6 milliseconds,and a 160 bit SHA1 function evaluation takes only 7.2 millisecond's.These symmetric key algorithms are more than 200 times faster than Public key algorithms.

Public Key cryptography is not only expensive in computation but also it is more expensive in communication as compared to symmetric key cryptography.According to [10] to send a public key from one node to another, at least 1024 bits required to be sent if the private key is 1024 bits long.

Two types of symmetric ciphers are used: block ciphers that work on blocks of a specific length and stream ciphers that work bitwise on data. A stream cipher can be seen as a block cipher with a block length of 1 bit.

Law et al. [11] investigate in their survey in the evaluation of block ciphers for WSNs, based on existingliterature and authoritative recommendations. The authors do not only consider the security properties of thealgorithms, but additionally they try to find the most storage- and energy-efficient ones. To compare the differentblock ciphers, benchmarks are conducted on the 16-bitRISC-based MSP430F149 considering different cipher parameters, such as key length, rounds and block length; anddifferent operation modes, such as cipher-block chaining(CBC), cipher feedback mode (CFB), output feedback mode(OFB) and counter (CTR). Based on a review of differentcryptographic libraries, such as OpenSSL, Crypto++,Botan and Catacomb, most of the code was adapted fromOpenSSL [12]. Ciphers without public implementationswere implemented based on the original papers. For thecompilation of the sources the IAR Systems' MSP430 CCompiler was used. The evaluation results of the conductedbenchmarks show that the most suitable block ciphers forWSNs are Skipjack, MISTY1, and Rijndael, depending onthe combination of available memory and required securitylevel. As operating mode "Output Feedback Mode (OFB)"for pair wise links, i.e. a secured link between two peers, issuggested. In contrast, "Cipher Block Chaining (CBC)" isproposed for group communications, for example, to enablepassive participation in the network.

Fournel et al. [13] investigate in their survey streamciphers for WSNs. The chosen stream cipher algorithms(DRAGON, HC-256, HC-128, LEX, Phelix, Py and Pypy,Salsa20, SOSEMANUK) are all dedicated to software usesand were originally submitted to the European ProjectEcrypt in the eStream call (Phase 2). To extend the selectionof stream ciphers, the famous RC4, SNOWv2 and AESCTRwere considered for evaluation. The performedbenchmarks on an ARM9 core based ARM922T aimedat finding the most storage-efficient and energy-efficientstream ciphers for this platform. Based on the methodologyof the eStream testing framework [14], four performancemeasures were considered: encryption rate for long streams,packet encryption rate, key and IV setup, and agility.Furthermore, the code size required for each algorithm onthe ARM9 platform was investigated. The used streamcipher algorithms, originally developed in C for thetraditional PC platform, were executed on the ARM9platform without any optimizations. The results of thebenchmarks show that the stream ciphers Py and Pypy, thetwo most efficiently running algorithms on traditional PCplatforms, do not work as fast on the ARM9 architecture. Incontrast, SNOWv2, SOSEMANUK and HC-128 performed similarly fast on both

platforms. For SOSEMANUK, thekey setup was very huge in comparison to the key setup onthe traditional PC platform.

4.2Asymmetric Cryptography

Asymmetric encryption (also called public-key cryptography) uses two related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed.

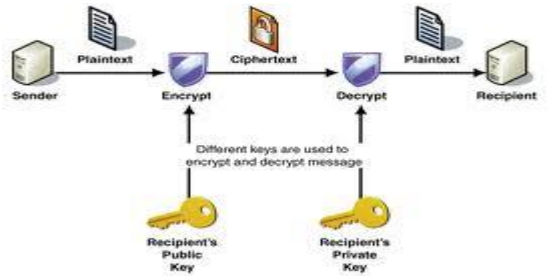

Figure 3:Asymmetric Key Cryptography.

A message that is encrypted by using the public key can only be decrypted by applying the same algorithm and using the matching private key. Likewise, a message that is encrypted by using the private key can only be decrypted by using the matching public key. Examples are RSA,ECC etc.

Public key Cryptography was omitted from the use in WSN because of its great consumption of energy and bandwidth which was very crucial in sensor network. Now a days a sensor become powerful in terms of CPU and memory power so, recently there has been a change in the research community from symmetric key cryptography to public key cryptography. Also symmetric key does not scale well as the number of nodes grows[15].

Arazi et al. [16] describe the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique forWSN which provides a good trade-off between key size and security.

Liu and Ning [17] also emphasize that ECC is oneof the most efficient types of public key cryptographyin WSNs. The steps of design, implementation andevaluation of TinyECC, a configurable and flexible libraryfor ECC operations in WSNs, are presented. The libraryprovides a number of optimization switches that can becombined according to the developer's needs for a certainapplication, resulting in different execution times andresource consumptions. The TinyECC library was alsoevaluated on several sensor platforms; including MICAz,Tmote Sky, and Imotel; to find the most computationally efficient and the most storage efficient configurations.

In Public key Cryptography mostly two algorithms RSA and ECC use. The ECC is offer equal security for a far smaller key size than any other algorithm.So that it reducing processing and communication overhead. For example, RSA with 1024 bit keys (RSA-1024) provides a currently accepted level of security for many applications and is equivalent in strength to ECC with 160 bit keys (ECC-160) .To protect data beyond theyear 2010, RSA Security recommends RSA-2048 as the new minimum key size which is equivalent to ECC with 224 bit keys (ECC-224)[18].

[19]described the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique for WSN which provides a good trade-off between key size and security. Lopez, 2006 focused on the security issues by analysing the use of symmetric cryptography in contrast with public-key cryptography. The author also discussed the important role of elliptic curve cryptography in this field.

A.RSA algorithm

A method to implement a public key cryptosystemwhose security is based on the difficulty of factoringlarge prime numbers was proposed in [20].*RSA* standsfor Ron Rivest, Adi Shamir and Leonard Adleman, whofirst publicly described the algorithm in 1977. Throughthis technique it is possible to encrypt data

and createdigital signatures.It was so successful that today *RSA*public key algorithm is themost widely used in theworld.

Key generation:
1. Choose two distinct prime numbers, p and q.
2. Compute modulus n = pq
3. Compute phi, φ= (p - 1)(q - 1) where φ is Euler's Totient Function.
4. Select public exponent *e* such that 1 < e < φ and gcd(e, φ) = 1
5. Compute private exponent d = $e^{-1} \bmod \varphi$
6. Public key is {n, e}, private key is d

Encryption: $c = m^e \pmod n$.
Decryption: $m = c^d \pmod n$.
Digital signature: $s = H(m)^d \bmod n$, Verification: $m' = s^e \bmod n$, if m' = H(m) signature is correct. H is a publicly known hash function.

***B.*ECC(Elliptic curve cryptography)**[21]

This algorithm is mainly depend on the algebraicstructure of elliptic curves.The difficulty in problemis ,the size of the elliptic curve. The primary benefitpromised by ECC is a smaller key size, reducingstorage and transmission requirements—i.e., that anelliptic curve group could provide the same level of security afforded by an RSA-based system with alarge modulus and correspondingly larger key—e.g., a 256bit ECC public key should providecomparable security to a 3072bit RSA public key(see #Key sizes).For current cryptographicpurposes, an *elliptic curve* is a plane curve whichconsists of the points satisfying the equation***:*** $y^2=x^3+ax+b$***,***

Compared to RSA,ECC has small key size,low memory usage etc.Hence it has attracted attention as a security solution for wireless networks [22].

4.3 Hybrid Cryptography

Symmetric key algorithm has a disadvantage of keydistribution[23] and asymmetric algorithm needmuch computation so the power of the sensor iswasted in it[23] and it is not feasible to use as poweris wasted then sensor will be of no useThus the algorithm which combines both thealgorithm i.e. asymmetric and symmetric so theadvantages of both the algorithm can be utilized in it.
A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to it's best advantage. One common approach is to generate a random secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient.
The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message. This is basically the approach used in PGP. Some of the hybrid algorithm like DHA+ECC[24] is described in detail.

V.CONCLUSION

The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches.We have compared two schemes in this paper ECC, and RSA and found out that ECC is more advantageous compared to RSA,due to low memory usage,low CPU consumption and shorter key size compared to RSA.ECC 160 bits is two times better than RSA 1024 bits when code size and power consumption are the factors of consideration. Tests were performed in 8051 and AVR platforms as in[25].ECC 160 bits use four times less energy than RSA 1024 bits in Mica2dot as in[26].Recently a new scheme called Multivariate Quadratic Almost Group was proposed which showed significant improvements over RSA and ECC.

REFERENCES

[1]. Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton "Resuscitation monitoring with a wireless sensor network", in Supplement to Circulation: Journal of the American Heart Association, October 2003.

[2] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs,Network Associates, Inc., Glenwood, MD, 2000.

[3]. K.Akkaya and M.Younis,*A survey on routing protocols for wireless sensor networks*,Ad Hoc Networks,3(2005),325-349.

[4]. M.Healy,T.Newe,andE.Lewis. *Power management in operating systems for wireless sensornodes*, in Proc. of the IEEE Sensor Applications Symposium(SAA'07),San Diego,CA,2007,1-6.

[5]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks.*IEEE Communications Magazine*, 40(8):102–114, August 2002.

[6]. Ning P, Wang R and Du W (2005), "An efficient scheme for authenticating public keys in sensor networks", Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL, USA, pp. 58-67.

[7]. Goodman J and Chandrakasan P (2001), "An Energy Efficient Reconfigurable Public Key Cryptography Processor ", IEEE journal of solid state circuits, pp. 1808-1820, November 2001.

[8]. RSA Security (2004), "Cryptography ", Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2152.

[9]. Ganesan P, Venugopalan R, Peddabachagari P, Dean A, Mueller F and Sichitiu M (2003), "Analyzing and modelling encryption overhead for sensor network nodes ", In Proceeding of the Ist ACM international workshop on Wireless sensor networks and application, San Diego, California, USA, September 2003.

[10]. Ling Tan, Shunyi Zhang, and Yanfeng Sun, Jing Qi "Application of Wireless Sensor Networks in Energy Automation", Sustainable Power Generation and Supply, 2009. Supergen '09.International conference.

[11]. Y.W.Law,J.Doumen,andP.Hartel,*Survey and benchmark of block ciphers for wireless sensor networks*,ACM Transactions on Sensensor Networks(TOSN),2(2006),65-93.

[12]. E.A.Young,T.J.Hudson,and R.S.Engelschall,*OpenSSL*.Availableonline:http://www.openssl.org/,2010.

[13]. N. Fournel, M. Minier, and S. Ub´eda, *Survey and benchmark of stream ciphers for wireless sensor networks*, in Information Security Theory and Practices: Smart Cards, Mobile and Ubiquitous Computing Systems, D. Sauveron, K. Markantonakis,A. Bilas, and J.-J. Quisquater, eds., vol. 4462 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2007, 202–214.

[14]. C. De Canni`ere, *eSTREAM Optimized Code HOWTO*. Available online: http://www.ecrypt.eu.org/stream/perf/, 2005.

[15]. IAN F.Akyildiz, Weilian Su, YogeshSankarasaubramaniam,ArdialCayirci,"A Survey on Sensor Networks",IEEE Communications Magazine,August 2002,pages 102-114.

[16]. B. Arazi, I. Elhanany, O. Arazi, and H. Qi, *Revisiting public-key cryptography for wireless sensor networks*, Computer, 38 (2005),103–105.

[17]. A. Liu and P. Ning, *TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks*, in Proc. of the International Conference on Information Processing in Sensor Networks (IPSN '08), St. Louis, MO, 2008, 245–256.

[18]. The Scheme of Public Key Infrastructure for improving Wireless Sensor Networks Security Zhang Yu.

[19]. Arazi,B.,Elhanany,L.,Arazi,O.,Qi,H.,2005:Revising public –key cryptography for wireless sensor networks. IEEE Computer,38(11):103-105.

[20]. R.L.Rivest,A.Shamir,and L.Adleman,"A method for obtaining digital signatures and public-key cryptosystems",Communications of the ACM,21(2):120-126,1978.

[21]. Kristin Lauter, Microsoft Corporation , ―The Advantages Of Elliptic CurveCryptography For Wireless Security IEEE Wireless Communications ,Vol 3,pp 22-25,February 2004.

[22]. Dona Maria Mani,Nishamol P H,"A Comparision Between RSA And ECC In Wireless Sensor Networks",International Journal of Engineering Research & Technology,Volume.2 Issue 3,March-2013.

[23] Yong Wang, GarhanAttebury, Byrav Ramamurthy,―A Survey of Security Issues In Wireless SensorNetworks‖ , IEEE Communications Surveys & Tutorials •,pp223-237 2nd Quarter 2006.

[24] Mohd. Rizwan beg1 and Shish Ahmad ―EnergyEfficient PKI Secure Key ManagementTechnique in Wireless Sensor NetworkusingDHA & ECC‖ International Journal of Ad hoc,Sensor& Ubiquitous Computing (IJASUC) Vol.3, No.1,pp 256- 262,February 2012.

[25]. Nils Gura, ArunPatel,ArvinderpalWander,HansEberle,andSheueling Chang Shantz,"Comparing Elliptic Curve and Cryptography and RSA on 8-bit CPUs"In Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems(CUES 2004),Boston Marriott Cambridge(Boston)August,2004.

[26]. Shish Ahmad,Mohd.Rizwanbeg,andQamarAbbas,"Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography",IJCA Special Issue of Mobile Ad-hoc Networks,pages 167-172,2012.