International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 3, March - 2013

A Comparison Between RSA And ECC In Wireless Sensor Networks

Dona Maria Mani,
M.Tech Student(CSE),
Viswajyothi College of Engineering and Technology,
Muvattupuzha, Kerala, India.

Nishamol P H,
Assistant Professor(CSE),
ViswajyothiCollege of Engineering and Technology,
Muvattupuzha, Kerala, India.

***Abstract*– Wireless sensor networks consists of autonomous sensor nodes attached to one or more base stations. As wireless sensor networks continue 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 limitations of energy, computation capability and storage resources of the sensor nodes. Symmetric based cryptographic schemes do not scale well when the number of sensor nodes increases. Hence public key based schemes are widely used.Here we present a brief overview of some attacks and countermeasures and also discuss two efficient public-key based algorithms, RSA and Elliptic Curve Cryptography (ECC) that are widely deployed in Wireless Sensor Networks. We found ECC to have significant advantage over RSA as it reduces computation time and also the amount of data transmitted and stored.**

***Key Terms*- confidentiality, integrity, authentication, data freshness, RSA, ECC.**

I. INTRODUCTION

Wireless sensor networks(WSN)consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. These sensor nodes generally have low computational power, limited data transmission and power constraints. WSNs are increasingly present in our days and can be found in environmental area (climatic measurements, presence of smoke), health area (measurement of vital signs, temperature), home automation (motion sensor and image sensor) and other areas. They have no fixed structure, and in many cases there is no monitoring station of sensor nodes during the operational life of the network. So WSNs must have mechanisms for self-configuration and adaptation in case of failure, inclusion or exclusion of a sensor node. Fig.1. illustrates a wireless sensor network with many sensor nodes and a single base station.

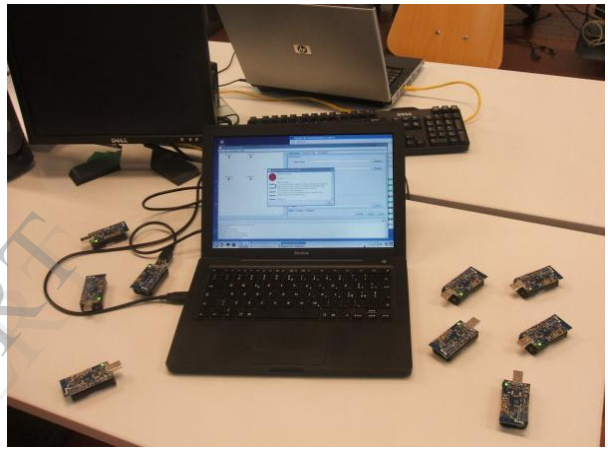

Fig.1. Wireless Sensor Network

Security requirements of WSNs are similar to conventional computer networks.Any security solution to sensor networks must preserve *confidentiality*, *integrity*, *authentication*, and *freshness*of data within the network.

Data Confidentiality ensures that the sensor readings remain secure and never leak outside the network under no circumstances.The standard approach for preventing this from happening is to use encryption, using a secret key that is known only to the intended receivers. It ensures that the data is protected from unauthorized persons.

Integrity of data in any network ensuresthe accuracy of data in thatnetwork. This implies that data between thesender and the receiver is not altered in transit by an adversary.

*Authentication*prevents unauthorized access to the network. Without authentication mechanisms in place, an attacker can easily access the network and inject malicious messages into the network without the knowledge of the receiver.

*Data Freshness*ensures that no adversary replays old messages. There are two types of freshness: weak freshness,which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delayestimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.

Not all security solutions designed for conventional computer networks can be implemented directly in WSNs due to the limitations in WSNs. For a long time, it was believed that the public key cryptography was not suitable for WSNs since it require high processing power, but later studies of encryption algorithms based on curves verified the feasibility of these techniques in WSNs.

The cryptographic algorithm *RSA* is currently the most used among the asymmetric algorithms that takes advantage of the difficulty in factoring large prime numbers. Standardized by NIST, this algorithm is widely used in transactions on the Internet. The *Elliptic Curve Cryptography (ECC)* based algorithm was created in 80s, and is based on the difficulty of solving the discrete logarithm problem on elliptic curves. Despite its complexity, the algorithm based on elliptic curve proves to be efficient. This paper describes some important attacks and countermeasures in sensor networks and also two main public key based cryptographic techniques, *RSA* and *ECC*,used in sensor networks.

II.ATTACKS AND COUNTERMEASURES

Routing protocols currently used in sensor networks do not consider security, and utilize the limited processing capabilities of sensor nodes. In conventional networks, message availability is guaranteed with the help of secure routing protocolswhereasintegrity,authenticity, andconfidentiality of messages are managed by end-to-end security mechanisms such as SSH or SSL. End-to-end security mechanisms can be adopted in conventional networks since intermediate routers do not have access to the content of messages. However, in sensor networks, these are difficult to deploysince intermediate nodes need direct access to the content of the messages.

A. Attacks

Sensor nodes are vulnerable to the following attacks:

- *Spoofing, altering, or replaying of routing information*–In this attack the routing information that is exchanged between nodes is the major target. This may result in creation of routing loops, attraction or repulsion of network traffic, extension or shortening of routes, generation of wrong error messages, partition of network, increase inend-to-endlatency,etc.

- *Selective forwarding*-In a selective forwarding attack, compromised nodes may refuse to forward certain messages.Instead the messagesare simply dropped, so that they are not propagated any further.

- *Sinkhole attack* - In a sinkhole attack, the goal of the attacker is to attract nearly all the traffic from a particular area through anattacked node, creating a sinkhole with the attacker at the center.

- *Wormholes*-In this attack [1] an intrudergathers messages received in one part of network and replays to a different part of the network. An example of this attack is a single node that exists between two other nodesforwarding messages between two of them.

- *Sybil attack*- These attacks are a great threat to the geographic routing protocols.In a Sybil attack [2], a single node presents multiple identities to other nodes in the network.The effectiveness of fault-tolerant schemes such as distributed storage, dispersity [3],multipath routing [4], and topology maintenance [5,6] are significantly reduced due to this attack. The adversary can be in more than one place at once.

- *HELLO flood attack*- In manyconventional routing protocols, nodes reveal their identity to their neighbors, by broadcasting HELLO

packets. A node receiving such a packet is under the assumption that it is in the normal range of the sender. It is possible for anattackerbroadcasting useful information and having large transmission power to convince every node in the network that the adversary is its neighbor.

B.Countermeasures

Link layer security mechanisms can help eradicate some of the vulnerabilities in sensor networks.Link layer encryption and authentication, identity verification, bidirectional link verification, multipath routing, and authenticated broadcast can protect sensor network routing protocols against outsiders, bogus routing information, sybil attacks, HELLO floods, and acknowledgement spoofing. It is feasible to use existing protocols with these mechanisms. Sinkhole attacks and wormholes pose significant challenges to secure routing protocol design and it is unlikely that there exist effective countermeasures against these attacks. It is crucial to design routing protocols in which these attacks are meaningless. Geographic routing protocols are one class of protocols that makes these attacks ineffective.

III.IMPLEMENTING SECURITY IN WSNs BY APPLYING CRYPTOGRAPHY

There are several cryptographic techniques that are used to secure sensor networks. The first step is to establish cryptographic system with secure keys for secure communication. Messages exchanged between sensor nodes must be properly encryptedand authenticated. This requires agreement between the communicating nodes on keys for performing encryption and authentication. Resource constraints in sensor nodes like limited computational power has made many key agreement schemes, like public-key and key pre-distribution,that were used in traditional networks unsuitable for sensor networks. Also pre-distribution of secret keys for all pairs of nodes is not economically affordable due to the large memory requirements.

Modern research has tried to handle the key establishment and management problem network-wide by use of a shared unique symmetric key between pairs of nodes. However, this also does not scale well as the number of nodes grows [7]. Hence public key based cryptographic techniques were used.

A.RSA algorithm

A method to implement a public key cryptosystem whose security is based on the difficulty of factoring large prime numbers was proposed in [8].*RSA* stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Through this technique it is possible to encrypt data and create digital signatures.It was so successful that today *RSA* public key algorithm is themost widely used in the world. The encryption scheme is as follows:

$$m^{ed} = m(modn) \quad (1)$$

foran integer m. The encryption and decryption schemes are presented in Algorithms 1 and 2.

The decryption works as follows:

$$c^d = (m^e)^d = m(modn) \quad (2)$$

The safety lies in the difficulty ofcomputing clear text a m from a ciphertext $cm^e \ mod \ n$ and public parameters *n(e).*

Algorithm 1: RSA Encryption

Input: RSA public key *(n, e)*

Plain text $m \in [0, n-1]$

Output: Cipher text *c*

begin

1. Compute $c = m^e \ mod \ n$
2. Return *c*.

end

Algorithm 2: Decryption RSA

Input: Public key *(n,e)*,Private key *d*,

Cipher text *c*

Output: Plain text *m*

begin

1. Compute $m = c^d mod \ n$
2. Return *m*.

end

B.Algorithm based on curves

The main idea of the algorithms based on curves is to identify a set of points of an elliptic curvefor which the discrete logarithm problem is difficult to manipulate.*Elliptic curve cryptography* (*ECC*) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curve is a plane defined by the following equation

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

The use of elliptic curves in cryptography was suggested independently byNealKoblitz and Victor S. Miller in 1985.Cryptosystemsbased on elliptic curvesachieve the same level ofsecurity such as *RSA* [9], using minor keys, and thus consuming less memory andprocessor resources. This makes them ideal for use in smart cards and otherenvironments where storage, time and energy are limited.

The number of applications that are using elliptic curve algorithmsis increasing considerablyrecentlydue to the standardization performed by NIST. The algorithmsbased on curves are standardized according to the ANSI X9.62, FIPS 186-2, IEEE 1363-2000and ISO / IEC 15946-2.

According to Amin [11] public key encryption includes algorithms for encryption, digital signatures and key agreement.Key management algorithms are used to share secret keys, encryption algorithms enable a confidential communication and digital signature algorithms authenticate a participant communication as well as validate the integrity of the message.The efficiency of this algorithm is based on finding a discrete logarithm of a random elementthat is part of an elliptic curve. The efficiency of *ECC*cryptographic algorithm with key sizes of approximately 160 bits is the same as thatobtained usingthe *RSA* algorithm with 1024 bit key.

The procedure of decryption and encryption through elliptic curve isanalogous to ElGamalencryption scheme described in algorithms 3 and 4. The pure text m is first represented as a point *M*, and then encrypted by the addition to *kQ*, where *k* is an integer chosen randomly, and *Q* is the public key.

Algorithm 3:*ElGamal elliptic curve encryption*

Input*:* Parameters field of elliptic curve

(p, E, P, n), Public key *Q*, Plain text *m*

Output*:* Cipher text*(C1, C2)*

begin

1. Represent the message m as a point *M* in $E(F_p)$
2. Select $k \in R^{[1,n-1]}$
3. Compute *C1= kP*
4. Compute *C2= M+ kQ*.
5. Return*(C1, C2)*

end

Algorithm 4:*ElGamal elliptic curvedecryption*

Input*:* Parameters field of elliptic curve

(p, E, P, n), Private key *d*,

Cipher text *(C1, C2)*

Output: Plain text *m*

begin

1. Compute *M = C2- dC1*and *m* from *M*.
2. Return *m*.

end

The transmitter transmits the points

C1=kP andC2=M + kQ to receiver who use his privatekey d to compute:

$$dC1= d(kP)=k(dP)=kQ, \qquad (4)$$

and then calculating *M= C2- kQ*. An attacker who wants to read of *M* need to calculate *kQ*.Compared to *RSA*, *ECC*has small key size, low memory usage etc. Hence it has attracted attention as a security solution for wireless networks.

IV .CONCLUSION AND FUTURE WORK

Wireless sensor networks are increasingly prone to vulnerabilities when the network grows in size. Public

key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches. We compared two schemes *ECC* and *RSA*and found 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 sizeand power consumption are the factors of consideration. Tests were performed in 8051 and AVR platforms as in [12]. *ECC* 160 bits uses four times less energy than *RSA* 1024 bits in Mica2dot as in [13].Recently a new scheme called Multivariate Quadratic Almost Group was proposed which showed significant improvements over *RSA* and *ECC*.

V. REFERENCES

[1] Y.C. Hu, A. Perrig, D.B. Johnson,"Packet leashes: a defense against wormhole attacks in wireless networks", in *IEEE Infocom, 2003*.

[2] J.R. Douceur, "The Sybil attack", in: *1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*, 2002.

[3] A. Banerjea, "A taxonomy of dispersity routing schemes forfault tolerant real-time channels", in: *Proceedings of ECMAST*,vol. 26, 1996, pp. 129–148.

[4] K. Ishida, Y. Kakuda, T.Kikuno, "A routing protocol for finding two node-disjoint paths in computer networks", in:*International Conference on Network Protocols*, 1992, pp.340–347.

[5] Y. Xu, J. Heidemann, D. Estrin, "Geography-informed energy conservation for ad hoc routing", in: *Proceedings of theSeventh Annual ACM/IEEE International Conferenceon Mobile Computing and Networking*, 2001.

[6] B. Chen, K. Jamieson, H. Balakrishnan, R. Morris,"Span:an energy-efficient coordination algorithm for topologymaintenance in ad hoc wireless networks", *ACM WirelessNetworks Journal 8 (5)* (2002) 481–494.

[7] IAN F. Akyildiz, Weilian Su, YogeshSankarasaubramaniam, ArdalCayirci,"A Survey on Sensor Networks", *IEEE Communications Magazine,* August2002, pages 102 – 114.

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

[9] I. Blake, G. Seroussi, and N, "Smart Elliptic Curves in Cryptography",Cambridge, 1999.

[10] K. Koc, Nigel Boston, and Matthew Darnall. "About Cryptographic Engineering – Ellipticand Hyperelliptic Curve Cryptography",*Springer*, 2009.

[11] F Amin, A H Jahangir, and H Rasifard,"Analysis of Public-Key Cryptography for Wireless Sensor Networks Security",*WorldAcademy of Science, Engineering and Technology*,31(July):530–535, 2008.

[12] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs"In *Proceedings of the 2004 Workshop on Cryptographic Hardware and Embedded Systems (CUES 2004)*, Boston Marriott Cambridge Cambridge (Boston)August, 2004.

[13] Shish Ahmad, Mohd. Rizwan beg, and Qamar Abbas, "Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography",*IJCA Special Issue of Mobile Ad-hoc Networks*, pages 167–172, 2012.