Survey on Survey on Computational Effort of Public Key Cryptography for WSNs

Trupti P. Pawale, Manjunatha

Abstract---In this paper we have worked over the security issues for public key cryptanalysis for wireless network security .We have made an attempt to compare ECC and RSA for WIRELESS SENSOR NETWORKS. We found ECC to have a significant advantage over RSA as it reduces computation time and also the amount of data transmitted and stored. RSA key generation is much more time consuming as it requires the generation of large prime numbers. We also have made an effort to study the behavior of WSNs nodes.

Keywords- Wireless sensor networks, security, Public Key cryptography, energy analysis

I. INTRODUCTION

The development of public key cryptography is the greatest evolution of 1960’s ,as it has overcome the ancient substitution and permutation concept to mathematical functions of public key algorithms.

More important is that public key cryptography is asymmetric, involving the use of 2 separate keys, in contrast to symmetric encryption, which uses only one key. The use of 2 keys has profound consequences in the areas of confidentiality, key distribution and authentication.

Cryptography is used for both wired as well as wireless sensor networks. In wired data networks, nodes rely on pre-deployed trusted server to help establish trust relationships but in WSN, these trusted authorities do not exist because sensor nodes have limited memory ,CPU power & energy, hence cryptographic algorithms must be selected carefully survey of security. So this condition is almost similar to that of maximum security, limited memory space & minimum energy consumption. Security Issues in WSN are related to the sensors, which are on operations and control domain.

In section II we survey frameworks, processes and concept related to the current issues in security. Section III and IV deals with the requirements of security in WSNs and the energy analysis of RSA and ECC public key cryptanalysis. Section V deals with Time complexity of the cryptanalysis for WSNs .Section VI concludes the paper and proposes some future work.

II. CURRENT SECURITY ISSUES.

Wireless sensor networks (WSN) consist of a large number of small sensor nodes, usually spread out in hard accessible areas and communicating wirelessly. A sensor node combines the abilities to sense, compute, and communicate to other nodes. The large number of nodes with minimum capacity devices operating in constraining and demanding real-world environments impede communication within and outside the network, making the process of implementing security in wireless networks exceptionally difficult and expensive. We discuss these difficulties and what is being done to overcome them in order to meet the ever-growing and popular wireless sensor networks. Modern wireless sensor networks many times consist of hundreds to thousands of inexpensive wireless nodes, each with some computational power and sensing capability and usually operating in random unsupervised environments. The sensors in the network act as “sources” as it detects environmental events either continuous or intermittently whenever the occurrence of the event triggers the signal detection process. The data picketed up is either lightly processed locally by the node and then sent off or just sent off to the “sink” node or a base station. This kind of environment presents several security challenges/ Issues.

Security Challenges/Issues

- Aggregation
- Node Capture /Node deployment
- Energy Consumption
- Large Numbers of nodes/Communication challenges
- Mobile security at data layer
- Malware/spyware
- Compliance auditing
- Identity management
- Patch/update management
- Application defence
- Intrusion detection

One of the first tasks in setting up a sensor network is to establish cryptographic system with secure keys for secure communication. It is important to be able to encrypt and authenticate messages sent between sensor nodes. However, doing this requires prior agreement between the communicating nodes on keys for performing encryption and authentication. Due to resource constraints in sensor nodes including limited computational power, many key agreement schemes like trusted-server, public-key, and key pre-distribution used in traditional networks are just not applicable in sensor networks. Also predistribution of secret keys for all pairs of nodesis not viable due to the large amount of memory this requires when the network size is large. Although over the years, efforts have been made to propose several approaches to do this, the inherent limited computational power of sensor nodes and the huge numbers of network nodes are making public-key cryptographic primitives too expensive in terms of system overhead in key-establishment [1]. 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 [1]. Another approach to establish keys that seem more

Manuscript received February 15, 2014.

Prof. Trupti P. Pawale,E & E Dept., VTU, Begaum, KLS,s ,VDRIT, Haliyal, India.

Prof. Manjunatha.D. E & E Dept., VTU, Begaum, KLS,s ,VDRIT, Haliyal, India.

appropriate for sensor networks is via pre-distribution, where (secret) key information is distributed to all sensor nodes prior to deployment [2].

III. REQUIREMENTS OF SECURITY

The security of WSNs can be classified into two broad categories: operational security and information security. The operation-related security objective is that a network, as a whole, should continue to function even when some of its components are attacked (the *service availability* requirement). The information-related security objectives are that *confidential* information should never be disclosed, and the *integrity* and *authenticity* of information should always be assured. While it may seem that information security can readily be achieved with cryptography, there are two facts that make achieving the above objectives non-trivial in WSNs:

- As sensor nodes operate unattended they are potentially accessible, both geographically and physically, to any malicious party imaginable;
- Sensor nodes communicate through an open medium.

A. Confidentiality

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. The confidentiality objective is required in sensors' environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could over hear critical information such as sensing data and routing information.

B. Authentication

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source

As in conventional systems, authentication techniques verify the identity of the participants in a communication, distinguishing in these way legitimate users from intruders. In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then its behavior could not be predicted, and most of times the mission of WSN will not be accomplished as expected. However, authentication for broadcast messages requires stronger trust assumptions on the network nodes. The creators of SPINS [3] contend that if one sender wants to send authentic data to mutually untrusted receivers, using asymmetric MAC is insecure since any one of the receivers know the MAC key, and hence could impersonate the sender and forge messages to other receivers. LEAP [4] uses a globally shared symmetric key for broadcast messages to the whole group.

C. Integrity

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example, for the healthcare sector where lives are endangered. Integrity controls must be implemented to ensure that information is not altered in any unexpected way.

D. Freshness

One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up.

E. 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. The availability of a sensor and sensor network may decrease for the following reasons [5]:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. Besides, as communication power increases so does the chance of a communication conflict or interference.
- A single point failure exists if we use the central point scheme such as a single sink or gateway. This greatly threatens the availability of the network.

F. Secure Management

Management is required in every system that is constituted of multi components, and handles sensitive information. In the case of sensor networks, we need secure management on base station level; since sensor nodes communication ends up at the base station, issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management.

G. Quality of Service

Assuring the quality of Service objective is a big challenge to security designers. As sensor networks have several limitations (e.g. energy, processing and memory capacities etc.), the achievement of quality of service becomes even more constrained. Security mechanisms must be lightweight so that the overhead caused, for example, by encryption be minimized and do not affect the performance of the network. Performance and quality in sensor networks involve the timely delivery of data to prevent the loss of critical data or events, and the accuracy with which the data are reported compared to what is actually occurring in their environment [6].

IV. ENERGY ANALYSIS OF RSA AND ECC

Today, three types of systems, classified according to the mathematical problem on which they are based, are generally considered both secure and efficient. They are classified as follows:

- The *integer factorization* systems.
- The *discrete logarithm* systems.
- The *elliptic curve discrete logarithm* systems

A. RSA Cryptosystem

The RSA-system is based on the difficulty of factoring, P = *C* = *Z/nZ* for an integer *n* = *p.q*, where *n* (the modulus) is known to everybody, but the prime factors *p*, *q* are known only to receiver. We need in practice *p* and *q* to be very large. We take *K* to be the set of positive integers relatively prime to *lcm (p-1,q-1)*. The encryption key *e €K* is known €to everyone, but the decryption key *d €K* is known only to receiver. Then sender encrypts:

$E : P\times K \rightarrow C, \qquad E(a,e) = a^{e} \bmod n$

To decrypt the cipher text, receiver:

$D : C \times K \rightarrow P, \qquad D(b,e) = b^{d} \bmod n$

Where ed Ξ *1(mod lcm (p - 1, q - 1))* .

B. Elliptic Curve Cryptosystem (ECC)

Elliptic curves are an algebraic structure, and their use forcryptography was first mentioned in [7] and [8]. Theyfeature properties which allow the setup of a problemsimilar to the well known discrete logarithm problem offinite fields – also known as Galois fields (GF).The subsequent section gives a brief and roughmathematical background to understand our implementation.In recent years, ECC has attracted much attention as thesecurity solutions for wireless networks due to the small keysize and low computational overhead.

Arvinderpal S. [9] provides detailed measurements for the MICA2DOT. They have measured power consumption for the MICA2DOT for the following cryptographic operations:

- Signature generation/verification and client/server key exchange operations (see Table III),
- Calculation of SHA-1 hash value (5.9 μWs),

TABLE III

ENERGY COST OF RSA AND ECC (MW) [11]

Algorithm	Key	Key Exchange		Signature	
	Size	Client	Server	Sign	Verify
RSA	1024	15.4	304	304	11.9
	2048	57.2	2302.7	2302.7	53.7
ECC	160	22.3	22.3	22.82	45.09
	224	60.4	60.4	61.54	121.98

V. TIME COMPLEXITY OF THE CRYPTANALYSIS FOR WSNS

According to the details as in [10] the times elapsed for signature generation, verification and key exchange for the client and server side, when the active power consumption is equal to 13.8 mJ, are given in Table IV.

TABLE V. ESTIMATED POWER CONSUMPTION (MWs)

Algorithm	Key	Key Exchange		Signature	
	Size	Client	Server	Sign	Verify
RSA	1024	36.96	726.99	726.99	28.38
	2048	136.62	5506.38	5506.38	128.37
ECC	160	53.46	53.46	54.45	107.91
	224	144.54	144.54	147.18	291.72

VI. CONCLUSION

TABLE VI
COMPUTATIONAL EFFORT FOR CRYPTANALYSIS OF ECC COMPARED TO RSA

Key size	MIPS-years	Key size	MIPS-years
150	3.8 ×10^{10}	512	3×10^{4}
205	7.1 ×10^{18}	768	2 ×10^{8}
234	1.6 ×10^{28}	1024	3 ×10^{11}
a. Elliptic curve logarithm using the Pollard rho method		1280	1 ×10^{14}
		1536	3 ×10^{16}
		2048	3×10^{20}
		b. Integer factorization using the General number field sieve	

The security of ECC depends on how difficult it is to determine k given kP and P .This referred to as the elliptic curve logarithm problem. The fastest known technology for taking the elliptic curve logarithm is known as the Pollard rho method .Table VI compares the efficiency of this method with factoring a number into two primes using the general number field sieve, as can be seen, a considerably smaller key size can be used for ECC compared to RSA.

REFERENCES

1. Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, ArdalCayirci. " A Survey on Sensor Networks", IEEE Communications Magazine, August2002, pp 102 – 114.
2. Jay Warior. "Smart Sensor Networks of the Future". DA Systems. http://archives.sensorsmag.com/articles/0397/net_mar/main.s html
3. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D..Tygar. "SPINS: Security Protocols for Sensor Networks," in Proceedings of the 7thAnnual ACM/IEEE International Conference on Mobile Computingand Networking (MobiCom), Rome, Italy, pp. 189–199, July 2001..
4. S. Zhu, S. Setia, S. Jajodia. "LEAP: Efficient Security Mechanismsfor Large-Scale Distributed Sensor Networks", In the Proceedings ofthe 10th ACM conference on Computer and communications security,2003.
5. J. P. Walters, Zh. Liang, W. Shi, V. Chaudhary, "Security inDistributed, Grid, and Pervasive Computing", Chapter 17, CRC Press,2006.
6. R. B. Ghazali, "Security in WSN in Enhance AODV Routing",Masters thesis, Faculty of Electrical Engineering, UniversityTechnology Malaysia, 2006.
7. N. Koblitz, "Elliptic curve cryptosystems", Mathematics ofComputation, Vol. 48, 1987.
8. V.S. Miller, "Use of Elliptic Curves in Cryptography", Advances inCryptology CRYPTO 85, 1986.
9. S. Wander, N. Gura, H. Eberle, V. Gupta, Sh. Ch. Shantz,"Energy analysis of public-key cryptography for wireless sensornetworks", In PERCOM '05: Proceedings of the Third IEEEInternational Conference on Pervasive Computing andCommunications, pp. 324–328, Washington, DC, USA, 2005. IEEEComputer Society.
10. Wireless Sensor Networks Security F. Amin, A. H. Jahangir, and H. Rasifard
11. A.S.Wander,N.Gura,h.Eberle,V.Gupta,Sh.Ch. Shantz,"Energy analysis of public-key cryptography for wireless sensor networks",In PERCOM '05:Proceedings of the Third IEEE International Conference on Pervasive Computing and communications,pp.324-328,Washington,DC,USA,2005.IEEE Computer Society.
12. K.Piotrowski, P . Langendoerfer, S.Peter,"How Public Key Cryptography Influences Wireless Sensor Node Lifetime",Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks,USA,pp.169-176,2006