ISSN: 2321-7782 (Online)
Volume 3, Issue 8, August 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Security in Wireless Sensor Network Using Various Techniques: A Survey

R. Priya[1]
Head & Assistant Professor,
Department Of Computer Science,
Sreenarayana Guru College, Coimbatore, India

S. Sundaramoorthi[2]
Research Scholar,
Sreenarayana Guru College,
Coimbatore, India

Abstract: ***A remote sensor system is a system which has sensor hubs that get the data from nature and procedure the gathered data. After the procedure result is transmitted through the radio waves to the inside. Presently days wsn utilized as a part of numerous applications, for example, observing, controlling environment and following. Amid the transmission security is fundamental issue in remote sensor systems. Such a large number of security systems are utilized to ensure the information in wsn. In this paper we talk about a percentage of general society key based calculations utilized as a part of remote sensor system security for secure transmission.***

Key words: Wireless sensor system, Sensor hubs, radio waves, Applications, Security, Public key calculations.

I. INTRODUCTION

Remote sensor system comprises of gathering of hubs and every hub contain sensor, Processor, transmitter and beneficiary. By and large sensor is a minimal effort gadget that performs detecting of specific undertaking. The structural engineering of sensor hub is as per the following.

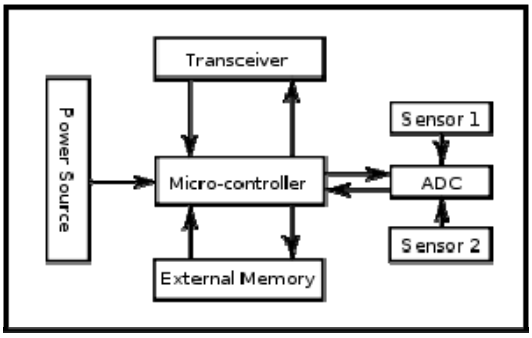

Figure 1: Sensor network components

WSN is worked out in the open uncontrolled region. In wsn information are go through different switches utilizing steering conventions. In wsn we must look after certainty, trustworthiness, accessibility and verification amid the transmission .There are two conceivable assaults in wsn against secure transmission.

1. Passive assaults
2. Active assaults

1. **Passive Attacks:** An assault that is influencing the protection of correspondence channel is called uninvolved assaults.
2. **Active Attacks:** Change the information in the correspondence channel is known as the dynamic assault.

We keep from these assaults utilizing open key cryptographic calculations. Such a large number of calculations are accessible we talk about a percentage of the calculations.

Algorithms Used In Wireless Sensor Network Security

Various types of cryptographic calculations are utilized as a part of remote sensor system. It can be ordered into taking after sorts.

a) Symmetric Encryption

b) Asymmetric Encryption

a) **Symmetric Encryption:** Symmetric key encryption is the mystery key encryption strategy .In this one and only key is utilized for both encryption and decoding.

b) **Asymmetric Encryption:** In Asymmetric encryption use open and private keys for encryption and decoding.

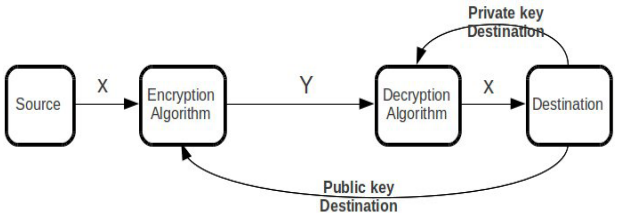

Figure 2: Asymmetric Encryption Method

Here we talk about some most ordinarily utilized uneven encryption calculations and its correlation of different creators.

RSA algorithm

Rivest-Shamir-algorithm(RSA) is one of the general population key cryptographic calculations. In this calculation security is in view of the factorizing the prime numbers. In this open and private key qualities are ascertained utilizing after steps

1. Select two arbitrary prime numbers p and q and check p! =q.
2. Compute the modulus esteem n=pq.
3. Compute phi(φ)=(p-1)(q-1)
4. Choose open type e, 1<e< Φ it fulfill gcd(e, Φ)=1.
5. Compute private type d=e-1 mod Φ.
6. (n,e) is utilized as open key and d is utilized as private key.

Encryption is performed utilizing the accompanying recipe

C=memod n

Here C is the figure content and m is the plain content. (e,n) are open keys.

In RSA decoding is performed utilizing after recipe

M=cd mod n

M-Plain content c-Cipher content d-private key n-open

Algorithm based on Curves

These sorts of calculations are taking into account the certain focuses on an elliptic bend for which discrete logarithm issue is immovable. There are two calculations in light of the bends.

a) ECC calculation

b) HECC calculation

ECC calculation

Elliptic bend cryptography(ECC) was presented in 1985 by the creators Neal kobiltz and Victor mill operator. The elliptic bend is a plane bend which comprises of focuses. The focuses must fulfill the mathematical statement y2=x2+ax+b.Elliptic bend framework accomplish the same security level of RSA with utilization of minor keys, less memory and processor assets.

Encryption in ECC

Encryption is performed in ECC utilizing after steps

Data :1) p,E,P,n (Points in Elliptic bend)

2) Public Key Q

3) Plain content M

Procedure Steps

Step 1: Represent unique Text m into bend point M

Step 2: Select K

Step 3:Compute c1=KP

Step 4: Compute c2=M+KQ

Yield: Cipher Text c1,c2

Decryption performed in ECC in following way

Information:

1) p,E,P,n (Points in Elliptic bend)

2) Private Key d

3) Cipher Text c1,c2

Procedure steps

Step 1: Compute M=c2-dc1

Step 2: Derive m from M

Yield: Plain Text m

Hyper Elliptic Curve Cryptography (HECC) algorithm

HECC and ECC algorithms are using same principle but they are differing in sequence of operations. HECC use more complex operations with small operands. HECC is more complex than the ECC but use small numbers.

Multivariate Quadratic Quasigroup algorithm (MQQ)

MQQ algorithm is based on the concept of multivariate polynomial transformations of nearly quadratic and groups. In this linear Boolean functions x=(f1...fn) is taken as input and calculate the multivariate quadratic polynomial Y. Based on that value encryption is performed. The decryption is performed based on the private keys T and S. Using that private key values and Y value again X value is calculated. Those keys are used for decryption.

Features

» This algorithm is highly parallelized but other algorithms are serialized.

» Speed of algorithm is increased.

» It is a post quantum algorithm.

Performance Evaluation

Performance of the RSA, ECC and MQQ algorithms are compared based on the Processing time, Processor usage and memory consumption.

Processing Time

It is proved that RSA algorithm is slower than the other algorithms ECC and MQQ.MQQ is 16 times better than the ECC and 230 times faster than the RSA.

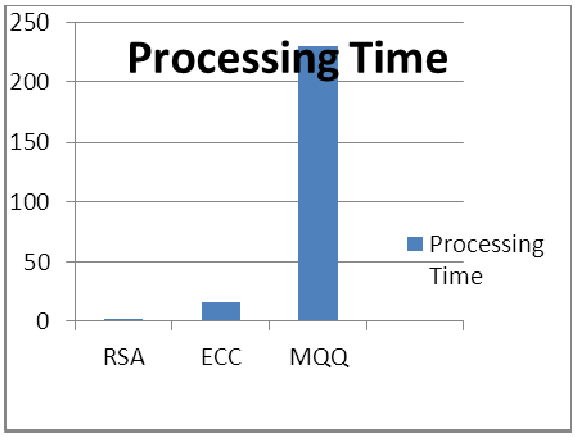

Figure 3: Comparison based on processing time

Evaluation of Processor

Evaluation of processor is based on the number of instructions, number of reads, number of writes and number of branches. If number of branches increases that decrease the performance of the processor. When compare to 3 algorithms number of branches in MQQ is 21 times less than the number of branches in ECC and 150 times lower than the RSA.The figure shows the comparison of branches in various algorithms

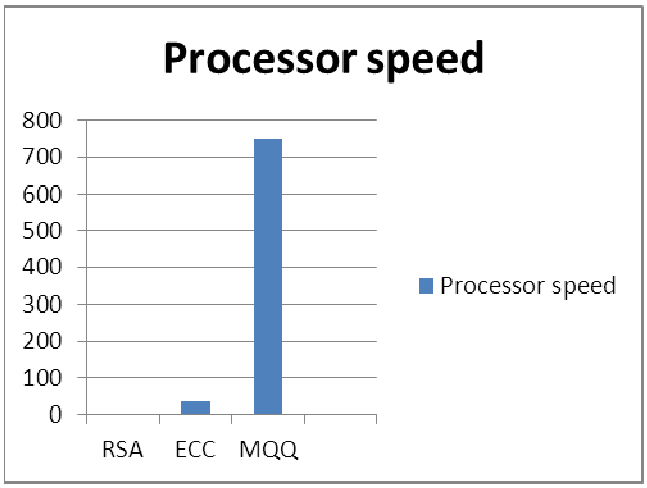

Figure 4: Comparison based on Processing Speed

Evaluation based on Memory

It is proved that Memory consumption in MQQ-160 is 61% better than the RSA-1024 and 23% better than the ECC. The given below diagram shows the memory efficiency of three algorithms.

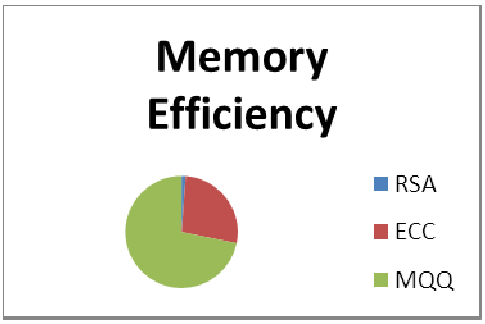

Figure 5: Comparison based on Memory

II. CONCLUSION

This paper gives the overview of wireless sensor network, Working principle and attacks in wireless sensor network. It also describes RSA, ECC, and MQQ algorithms used in wireless sensor network security. In this paper give the comparison of the performance of algorithm based on various parameters. Based on the various evaluation parameters MQQ is give better result in wireless sensor network security.

References

1. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf.Manage. Data, 2004
2. A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preserving symmetric encryption," in Proc. 31st Annu. Int. Conf. dv.Cryptology, 2009
3. A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. 31st Annu. Conf. Adv. Cryptology, 2011.
4. B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index for range queries," in Proc. 30th Int. Conf. Very Large Data Bases,2004
5. L. Xiao and I. Yen, "A note for the ideal order-preserving encryption object and generalized order-preserving encryption," IACR ePrint Archive, pp. 535–552, 2012.
6. Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno Universidade Federal de Sergipe, Brasil
7. Thomas Wollinger, Jan Pelzl, Volker Wittelsberger, ChristofPaar, GokaySaldamli, and Cetin K. Koc. Elliptic and hyperelliptic curves on embedded µP.ACM Transactions onEmbedded Computing Systems, 3(3):509–533, August 2004.
8. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz.Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. In In Proceedings ofthe 2004 Workshop on Cryptographic Hardware and Embedded Systems (CUES 2004), BostonMarriott Cambridge Cambridge (Boston)August, 2004.
9. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz.Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. In In Proceedings ofthe 2004 Workshop on Cryptographic Hardware and Embedded Systems (CUES 2004), Boston Marriott Cambridge Cambridge (Boston)August, 2004.
10. Thomas Wollinger, Jan Pelzl, Volker Wittelsberger, ChristofPaar, GokaySaldamli, and Cetin K. Koc. Elliptic and hyperelliptic curves on embedded µP.ACM Transactions onEmbedded Computing Systems, 3(3):509–533, August 2004.
11. M. El-Hadedy, D. Gligoroski, and S.J. Knapskog. High performance implementation of a public key block cipher-mqq, for fpga platforms. In Reconfigurable Computing and FPGAs, 2008. ReConFig'08. International Conference on, pages 427–432. IEEE, 2008.
12. Kristin Lauter, Microsoft Corporation , ―The Advantages Of Elliptic CurveCryptography For Wireless Security IEEE Wireless Communications ,Vol 3,pp 22-25,February 2004.
13. Madhumita Panda Sambalpur University Institute of Information Technology(SUIIT)Burla, Sambalpur, Odisha, India "Security in Wireless Sensor Networks using Cryptographic Techniques"
14. Amanjotkaur "Energy analysis of Wireless sensor networks using RSA and ECC encryption ".

