Combinatorial Asymmetric Key Cryptosystem and Hash Based Multifactor Authentication Techniques for Secured Data Communication in WSN

C.VENKATACHALAM[1], DR. A. SURESH[2]

[1] *Ph.D Research Scholar (PT), Periyar University, Salem*

[2] *Head, Dept. of Computer Science, Sona College of Arts and Science, Salem*

Abstract- Wireless sensor network security pulls in considerations of numerous specialists around the globe. Security is utilized with attributes of authentication, uprightness, protection, nonrepudiation and privacy. The security benefits in WSN need to ensure the data imparted over network and assets from the assaults. Security and authentication during information communication are testing one in WSN. For secure communication in WSN, cryptographic and steganographic techniques are utilized. The information are sent or gotten to by any hub in network after authentication measure to keep from unapproved clients to get to the data. Our exploration clarifies Investigation on Combinatorial Asymmetric Key Cryptosystem and Hash Based Multifactor Authentication Techniques.

Indexed Terms- Wireless sensor network, Asymmetric Key Cryptosystem, Data Communication, Blum-Goldwasser encryption algorithm.

I. INTRODUCTION

Wireless sensor networks (WSNs) are a grounded unavoidable innovation that speaks to an ideal detecting segment in the Internet of things (IoT). They are made out of minimal effort and low force gadgets, called sensor hubs, which sense the climate, measure the gathered data and trade data through a wireless association and air quality observing. A wireless sensor network is an organization to screen physical or natural conditions, for example, temperature, sound, pressure, and so on the improvement of wireless sensor networks was inspired via air contamination observing, water quality checking, land side recognition, woods fire location, territory observing, etc. In spite of the fact that there are numerous applications in wireless sensor network space, human medical services applications play the significant job. In human medical care, sensors are utilized to screen the patient's wellbeing status, for example, temperature level, sugar level, heart beat rate, circulatory strain.

Wireless Sensor Network comprises of spatially appropriated independent sensors to screen ecological states of the earth. The advancement of wireless sensor networks was persuaded by military applications, for example, war zone reconnaissance. Wireless Sensor Networks (WSN) are conveyed at basic spots like reconnaissance, checking, air terminals, combat zone applications consequently making sure about wireless sensor networks is a difficult assignment.

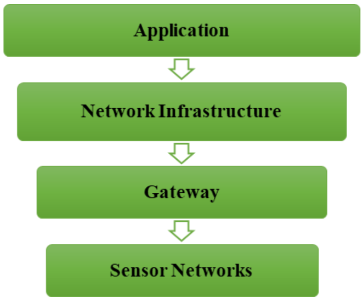


Figure 1: Secured Wireless Sensor Network

Following are the Security Requirements in Wireless Sensor Networks.

a. Confidentiality

Confidentiality prerequisite is needed to guarantee that delicate data is very much secured and not uncovered to unapproved outsiders. The confidentiality target assists with securing data going between the sensor hubs of the network or between the sensors and the base station from divulgence, since a foe having the fitting gear may snoop on the correspondence. By snooping, the enemy could catch basic data, for example, detecting information and steering data. Besides, by taking steering data the foe could bring his own pernicious hubs into the network trying to catch the whole correspondence.

b. Authentication

As in conventional frameworks, authentication techniques confirm the personality of the members in a communication, recognizing in this way genuine clients from gate crashers. On account of sensor networks, it is fundamental for every sensor hub and base station to be able to confirm that the information got was truly send by a confided in sender and not by an enemy that fooled authentic hubs into tolerating bogus information. g information and so on and that each group generally has a group head that is the hub that gets its group together with the remainder of the sensor network (implying that the communication among various groups is performed through the group heads).

c. Integrity

Integrity controls should be executed to guarantee that data won't be changed in any startling manner. Numerous sensor applications, for example, contamination and medical services observing depend on the integrity of the data to work with exact results; it is unsuitable to gauge the extent of the contamination brought about by synthetic compounds waste and discover later on that the data gave was inappropriately adjusted by the industrial facility that was found close by the checked lake. Subsequently, there is dire need to ensure that data is heading out from one finish to the next without being blocked and altered all the while.

d. Freshness

One of the numerous assaults dispatched against sensor networks is the message replay assault where a foe may catch messages traded among hubs and replay them later to create turmoil to the network. Information freshness objective guarantees that messages are crisp, implying that they comply with in a message requesting and have not been reused. To accomplish freshness, network conventions should be planned in an approach to distinguish copy parcels and dispose of them forestalling likely mistake.

e. Secure Management

Management is needed in each framework that is comprised from multi-segments and handles delicate data. On account of sensor networks, we need secure management on base station level; since sensor hubs correspondence winds up at the base station, issues like key conveyance to sensor hubs to build up encryption and directing data need secure management. Besides, bunching requires secure management also, since each gathering of hubs may incorporate an enormous number of hubs that should be confirmed with one another and trade information in a secure way.

1.1 Applications of Wireless Sensor Networks

1. Fire detection
2. Water quality monitoring
3. landslide detection
4. Air pollution monitoring
5. Data centre monitoring

1.2 Investigation on Combinatorial Asymmetric Key Cryptosystem

The asymmetric key cryptography is known as open key cryptography. In this method, the sender utilizes a public key of the collector for encryption and the beneficiary uses his private key to unscramble the message. The idea of self-accreditation is missing here rather advanced marks are utilized to affirm the keys. Asymmetric cryptography, is a cryptographic framework that utilizations sets of keys: public keys, which might be spread generally, and private keys, which are known distinctly to the proprietor. The age of such keys relies upon cryptographic algorithms dependent on numerical issues to deliver single direction capacities. Viable security just requires keeping the hidden key private; the public key can be transparently appropriated without trading off security.

This technique is more helpful and gives better validation as the security stays unblemished. There are different algorithms to execute this encryption instrument. The RSA algorithm the most broadly utilized asymmetric algorithm is installed in the SSL/TSL conventions, which are utilized to give communications security over a PC network. These are RSA, Diffie-Hellman, ECC and Digital Signature Algorithm.

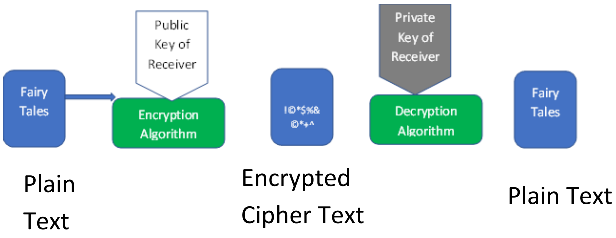


Figure 2: Combinatorial Asymmetric Key Cryptography

1.3 Multifactor Authentication Techniques

Multifactor Authentication Techniques is the client ID and secret phrase authentication system are the most old-style strategy among authentication techniques on the web; notwithstanding, it is a weak technique against snooping or replay assaults. The multifactor authentication calculation makes a one-of-a-kind single direction computerized unique mark that speaks to the substance of IoT bundles. To adapt to the three previously mentioned situations, Sensors 2019, 19, 3663 5 of 22 this paper proposed three authentication calculations, which are miniature IoT worldview authentication, full scale IoT worldview authentication, and miniature large scale worldview authentication.

These are planned dependent on the accompanying suspicions:

1. Each sensor gadget has three secure keys — two privates (K1 and K2) and one public (K_DSA: key for direct access control) — which are put away during gadget programming.
2. Each sensor gadget static or portable knows about its area.
3. Sink is a confided in base station.
4. A sensor gadget can't utilize TOTP on the grounds that it has restricted assets which influence the accuracy figuring of the supreme time that is needed in a coordinated TOTP.
5. Each IoT gadget has two secure keys—one private (KI, ID) and one public K_DSA.
6. An IoT gadget and the sink have a capacity to actualize TOTP and the TEOTP.
7. A sink or a base station has an information base that stores the total subtleties, everything being equal, and IoT gadgets.

1.4 Data Communication in Wireless Sensor Network

As wireless sensor networks have requirements as far as data transfer capacity and energy, lessening the correspondence between base station and sensors assumes fundamental job on force utilization and use of data transfer capacity. Collected wireless sensor network fill this need. The way toward gathering, handling and sending the aftereffect of the crude detected information from sensor hubs by middle person hubs called 'aggregators' is called Data Aggregation. This idea decreases the information communicated in the organization and therefore prompts delayed life season of organization. Without appropriate security component, it is absurd to expect to play out this activity. Because of the sending climate of WSNs, the actual trade off of sensor hubs and aggregators is conceivable. It might likewise prompt bogus conglomeration results. To address these issues, the primary alternative is cryptographic components utilizing which secrecy and honesty instruments can be accomplished. In view of high sending cost and correspondence cost, the sensor hubs can't for all intents and purposes utilize outsider confided in workers.

The public key conventions include significant expense for calculation. Thus, in WSNs, the better strategy for cryptography is the one which includes symmetric key cryptography. There exist part of trouble in key administration in WSNs as a result of their dynamic structure, self-association property and simple hub bargain. There are enormous number of approaches which are centered around this territory of key administration due to its trouble and significance. In view of the current techniques, the current methodologies can be named one way hash plans, half and half cryptography plans and key pre-conveyance plans, key disease plans and so on A portion of the techniques are mix of more than one of these methodologies. Figure 4 shows the methodologies of key administration in WSNs. These security challenges in WSN open up a wide examination issues around there. In this work, an endeavor has been made for plan and advancement of new key administration system among WSN segments.

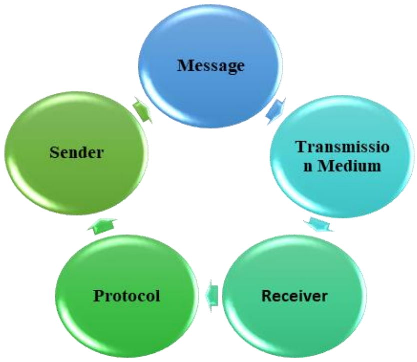


Figure 3: Data Communication

II. EXISTING SYSTEM

1. Secure Multi-Bit Encryption

Secure Multi-Bit Encryption Of course, we often want to send more than one bit. We need to define what we mean by security in that case, and construct an encryption scheme. To define security for a multi-bit case, note, first of all, that as messages get longer, cipher texts must necessarily get longer. Hence, encryption cannot hide message length. We will require it to hide everything else, though. Namely, we will allow the adversary (distinguisher) to choose any two messages, m0 and m1 after seeing the public key, then encrypt either one of them, and let the distinguisher guess which one. More precisely, D now runs in two stages. In the first stage, on input PK, D outputs (m0, m1). In the second stage, on input c, which is an encryption of either m0 or m1, D tries to guess which one it is by outputting either 0 or 1. D is allowed to keep state between stages (so you need not give it PK the second time, or give it back m0 and m1).

2. RSA Assumption

RSA Assumption, We haven't addressed the problem of generating RSA keys. That depends on whether you want a fixed e or a random e. People often use fixed small e (such as 3, 17, or 216 + 1 = 65537), because exponentiation is particularly fast. (There have been some questions raised, however, about the security of this approach—it may be possible that roots of small degree are easier to take than roots of a random degree. No one knows.)

Assumption 1: (Fixed-Exponent RSA for exponent e.) For any poly-time algorithm F, there exists a negligible function η such that, if you generate RSA public key (n, e) according to the procedure Generate Fixed-Exponent-RSA, then pick a random m ∈ Z ∗ n , Pr[F(n, e, me mod n) = m] ≤ η(k).

Assumption 2: (Random-Exponent RSA.) For any poly-time algorithm F, there exists a negligible function η such that, if you generate RSA public key (n, e) according to the procedure Generate-Random Exponent-RSA, then pick a random m ∈ Z ∗ n , Pr [F(n, e, me mod n) = m] ≤ η(k).

III. PROPOSED FRAMEWORK

In the accompanying, we clarify Investigation on Combinatorial Asymmetric Key Cryptosystem and Hash Based Multifactor Authentication Techniques for Secured Data Communication in Wireless Sensor Network how to convey the necessary keys and key chains on sensor hubs earlier organization. This cycle is refined in key arrangement stage; at that point in shared key revelation stage, we express how two sensor hubs can find a typical key for their safe communications for Wireless Sensor Networks.

- Blum–Goldwasser cryptosystem

To build up a Blum Goldwasser Cryptosystem based Asymmetric Key Encryption Technique for made sure about information communication in wireless sensor network with higher information classification rate. In BGC-AKE technique, Asymmetric Key Encryption Algorithm is utilized for made sure about information communication in WSN. Asymmetric Key Encryption Algorithm involves two cycles, specifically Public key encryption and Digital mark. In Public key encryption, information is encoded with base station public key. The encoded information isn't decoded by any individual who doesn't have coordinating private key. Public key encryption assists with expanding the information privacy rate. In Digital Signature measure, information is endorsed with sender hub's private key and checked by any individual who admittance to the sender hub's public key. This Asymmetric Key Encryption Algorithm diminishes the computational unpredictability and builds the information secrecy rate between sender hub and base station during communication in WSN. Exploratory assessment is done on variables, for example, information privacy rate, encryption time and security level during information communication as for information size.

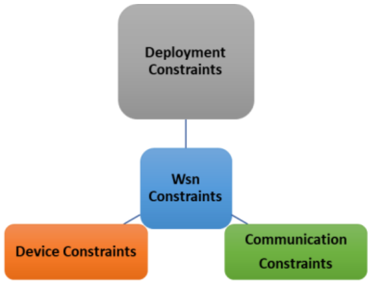


Figure 4: Communication Security

The Blum–Goldwasser cryptosystem consists of three algorithms: a probabilistic key generation algorithm which produces a public and a private key, a probabilistic encryption algorithm, and a deterministic decryption algorithm.

1. The Blum-Goldwasser encryption algorithm is described.

INPUT:

- P – a non-empty string of plaintext. The string "" is an empty string, whereas " " is a string consisting of one white space character. The plaintext can be a binary string or a string of ASCII characters. Where P is an ASCII string, then P is first encoded as a binary string prior to encryption.
- K – a public key, which is the product of two Blum primes.
- Seed – (default: None) if pp and qq are Blum primes and n=pqn=pq is a public key, then seed is a quadratic residue in the multiplicative group (Z/nZ)∗(Z/nZ)∗. If seed=None, then the function would generate its own random quadratic residue in (Z/nZ)∗(Z/nZ)∗. Where a value for seed is provided, it is your responsibility to ensure that the seed is a quadratic residue in the multiplicative group (Z/nZ)∗(Z/nZ)∗.

OUTPUT:

- The ciphertext resulting from encrypting P using the public key K. The ciphertext CC is of the form C=(c1,c2,…,ct,xt+1)C=(c1,c2,…,ct,xt+1). Each cici is a sub-block of binary string and xt+1xt+1 is the result of the t+1t+1-th iteration of the Blum-Blum-Shub algorithm.

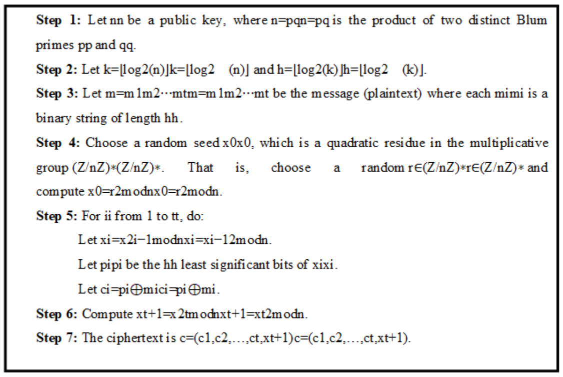
2. The Blum-Goldwasser decryption algorithm is described

INPUT:

- C – a ciphertext resulting from encrypting a plaintext using the Blum-Goldwasser encryption algorithm. The ciphertext CC must be of the form C=(c1,c2,…,ct,xt+1)C=(c1,c2,…,ct,xt+1). Each cici is a sub-block of binary string and xt+1xt+1 is the result of the t+1t+1-th iteration of the Blum-Blum-Shub algorithm.
- K – a private key (p,q,a,b)(p,q,a,b) where pp and qq are distinct Blum primes and gcd(p,q)=ap+bq=1gcd(p,q)=ap+bq=1.

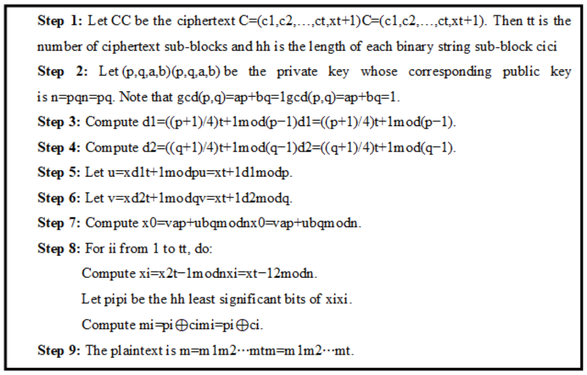
OUTPUT:

The plaintext resulting from decrypting the ciphertext C using the Blum-Goldwasser decryption algorithm.



```
Step 1: Let nn be a public key, where n=pqn=pq is the product of two distinct Blum primes pp and qq.
Step 2: Let k=⌊log2(n)⌋k=⌊log2  (n)⌋ and h=⌊log2(k)⌋h=⌊log2  (k)⌋.
Step 3: Let m=m1m2⋯mtm=m1m2⋯mt be the message (plaintext) where each mimi is a binary string of length hh.
Step 4: Choose a random seed x0x0, which is a quadratic residue in the multiplicative group (Z/nZ)∗(Z/nZ)∗. That is, choose a random r∈(Z/nZ)∗r∈(Z/nZ)∗ and compute x0=r2modnx0=r2modn.
Step 5: For ii from 1 to tt, do:
        Let xi=x2i−1modnxi=xi−12modn.
        Let pipi be the hh least significant bits of xixi.
        Let ci=pi⊕mici=pi⊕mi.
Step 6: Compute xt+1=x2tmodnxt+1=xt2modn.
Step 7: The ciphertext is c=(c1,c2,…,ct,xt+1)c=(c1,c2,…,ct,xt+1).
```

Table 1: Blum-Goldwasser Encryption Algorithm



```
Step 1: Let CC be the ciphertext C=(c1,c2,…,ct,xt+1)C=(c1,c2,…,ct,xt+1). Then tt is the number of ciphertext sub-blocks and hh is the length of each binary string sub-block cici
Step 2: Let (p,q,a,b)(p,q,a,b) be the private key whose corresponding public key is n=pqn=pq. Note that gcd(p,q)=ap+bq=1gcd(p,q)=ap+bq=1.
Step 3: Compute d1=((p+1)/4)t+1mod(p−1)d1=((p+1)/4)t+1mod(p−1).
Step 4: Compute d2=((q+1)/4)t+1mod(q−1)d2=((q+1)/4)t+1mod(q−1).
Step 5: Let u=xd1t+1modpu=xt+1d1modp.
Step 6: Let v=xd2t+1modqv=xt+1d2modq.
Step 7: Compute x0=vap+ubqmodnx0=vap+ubqmodn.
Step 8: For ii from 1 to tt, do:
        Compute xi=x2t−1modnxi=xt−12modn.
        Let pipi be the hh least significant bits of xixi.
        Compute mi=pi⊕cimi=pi⊕ci.
Step 9: The plaintext is m=m1m2⋯mtm=m1m2⋯mt.
```

Table 2: Blum-Goldwasser Decryption Algorithm

The value hh in the algorithm is the sub-block length. If the binary string representing the message cannot be divided into blocks of length hh each, then other sub-block lengths would be used instead. The sub-block lengths to fall back on are in the following order: 16, 8, 4, 2, and 1.

IV. EXPERIMENTAL RESULTS

1. Analysis of Encryption Time in Seconds

Analysis of encryption time			
	size(153)	size(118)	size(86)
RSA	4	5.3	6.5
Multi- Bit	2.3	2.7	2.9
Blum-goldwasser	8.6	9	10

Table 1: Analysis of encryption time in seconds

The comparison table 1 of analysis of encryption time of Existing and Proposed shows the different values. When comparing the Existing and Proposed the Proposed value provides the better results than the Existing value. The Existing value starts from 4 to 2.9 and the proposed values starts from 8.6 to 10. Every time the proposed value provides the better results.

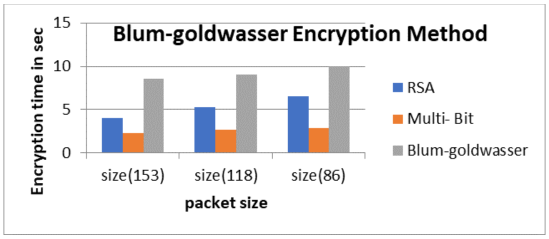


Figure 5: Blum-goldwasser Encryption Method

The comparison chart of Blum-goldwasser Encryption Method of Existing and Proposed shows the different values in figure 5. The Existing value starts from 153 to 118 and the proposed values decreased time 86 seconds. Every time the proposed value provides the better results than the Existing value.

2. Analysis of De-compiling time

Analysis of De-compiling time			
	size(153)	size(118)	size(86)
RSA	5	6.3	3.6
Multi- Bit	3.4	3.8	3.4
Blum-goldwasser	9.6	10	11

Table 2: Analysis of De-compiling time in seconds

The comparison table 2 of analysis of De-compiling time of Existing and Proposed shows the different values. When comparing the Existing and Proposed the Proposed value provides the better results than the Existing value. The Existing value starts from 5 to 3.4 and the proposed values starts from 9.6 to 11. Every time the proposed value provides the better results.

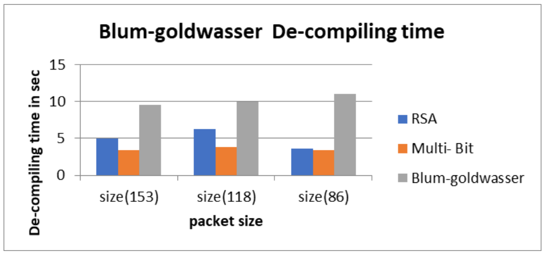


Figure 6: Blum-goldwasser De-compiling Method

The comparison chart of Blum-goldwasser De-compiling Method of Existing and Proposed shows the different values in figure 6. The Existing value starts from 153 to 118 and the proposed values decreased time 86 seconds. Every time the proposed value provides the better results than the Existing value.

3. Analysis of Decryption time

Analysis of Decryption time			
	size(153)	size(118)	size(86)
RSA	6	6.5	4.2
Multi- Bit	4.3	4.6	3.6
Blum-goldwasser	9.8	10.3	11.4

Table 3: Analysis of Decryption time in seconds

The comparison table 3 of analysis of Decryption time of Existing and Proposed shows the different values. When comparing the Existing and Proposed the Proposed value provides the better results than the Existing value. The Existing value starts from 6 to 3.6 and the proposed values starts from 9.8 to 11.4 Every time the proposed value provides the better results.

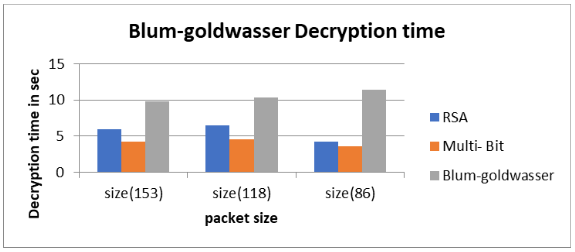


Figure 7: Blum-goldwasser Decryption Method

The comparison chart of Blum-goldwasser Decryption Method of Existing and Proposed shows the different values in figure 7. The Existing value starts from 153 to 118 and the proposed values decreased time 86 seconds. Every time the proposed value provides the better results than the Existing value.

4. Analysis of Buffer size

Analysis of Buffer size			
	size(153)	size(118)	size(86)
RSA	157	152	222
Multi- Bit	121	110	184
Blum-goldwasser	111	107	167

Table 4: Analysis of Buffer size

The comparison table 4 of analysis of Buffer size of Existing and Proposed shows the different values. When comparing the Existing and Proposed the Proposed value provides the better results than the Existing value. The Existing value starts from 157 to 184 and the proposed values starts from 111 to 167. Every time the proposed value provides the better results.

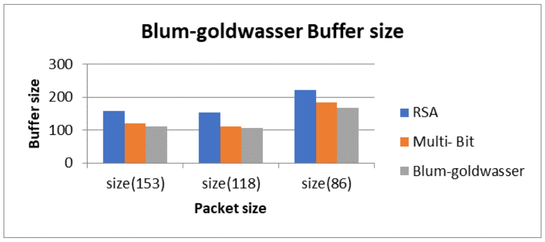


Figure 8: Blum-goldwasser Buffer size

The comparison chart of Blum-goldwasser Buffer size of Existing and Proposed shows the different values in figure 8. The Existing value starts from 153 to 118 and the proposed values decreased time 86 seconds. Every time the proposed value provides the better results than the Existing value.

CONCLUSION

This examination proposes a key circulation conspire that is reasonable for grouped Investigation on Combinatorial Asymmetric Key Cryptosystem and Hash Based Multifactor Authentication Techniques for Secured Data Communication in Wireless Sensor Networks. We exploit combinatorial plans to relate key chains to sensor hubs before organization and decreasing unpredictability of shared key disclosure calculation after arrangement. In this paper, we have featured the fundamental just as proposed calculations identified with these cryptographic techniques. In Symmetric Key Cryptography, a solitary key is for both encryption and decoding purposes. The sharing of this key turns out to be in some cases unreliable. Then again, Asymmetric Key Cryptography utilizes two separate keys to forestall any dishonest admittance to the data. The public key remaining parts public and the private key isn't shared. This strategy guarantees preferred security over the previous. In addition, the utilization of Digital Signatures if there should be an occurrence of Asymmetric Key Cryptography gives high data secrecy of Secured in Wireless Sensor Network.

REFERENCES

[1] Arun Kejariwal, " Cryptic primes", IEEE Potentials, pp. 43-45, Feb./Mar. 2004, IEEE.

[2] Minoru Kuribayashi and Hatsukazu Tanaka, "Fingerprinting Protocol for Images Based on Additive Homomorphic Property", IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2129-2139, Dec. 2005, IEEE.

[3] Subramania Sudharsanan, " Shared Key Encryption of JPEG Color Images", IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp. 1204-1211, Nov. 2005, IEEE.

[4] G. Boato, N. Conci, and V. Conotter, F.G.B. De Natale, and C. Fontanari, "Multimedia asymmetric watermarking and encryption", Electronics Letters, vol. 44 no. 9, April 2008, IEEE.

[5] K. HimaBindu, Ch. LavanyaAishani, M.Kamalakar, “A Secure Key Exchange Scheme in Wireless Sensor Networks Using Diffie Hellman,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, no 9, pp. 16338-16343, Sept 2016.

[6] D. Djenouri And L. Khelladi, A. NadjibBadache, “A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks,” IEEE Communications Surveys & Tutorials, vol. 7, no. 4, pp.2-28, Fourth Quarter 2005.

[7] MohitSaxena, “Security In Wireless Sensor Networks - A Layer Based Classification,” Cerias Tech Report 2007-04.

[8] Hirsch, Frederick J. "SSL/TLS Strong Encryption: An Introduction". Apache HTTP Server. Retrieved 17 April 2013.. The first two sections contain a very good introduction to public-key cryptography.

[9] Ferguson, Niels; Schneier, Bruce (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.

[10] Katz, Jon; Lindell, Y. (2007). Introduction to Modern Cryptography. CRC Press. ISBN 978-1-58488-551-1.

[11] Kavitha T, Sridharan D. Hybrid design of scalable key distribution for wireless sensor networks. International Journal of Engineering and Technology 2010; 2 (2): 136–141.

[12] Chong C, Kumar S. Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE 2003; 91(8): 1247–1256.

[13] Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials 2006; 8: 2–23.

[14] M. L. Das, “Two-factor user authentication in wireless sensor networks,” IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086–1090, 2009.

[15] L.-P. Zhang and Y. Wang, “An ID-based authenticated key agreement protocol for wireless sensor networks,” Journal of Communications, vol. 5, no. 8, pp. 620–626, 2010.

[16] https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/public_key/blum_goldwasser.html.