Asymmetrical Encryption for Wireless Sensor Networks: A Comparative Study

Heena Dogra[1], Jyoti Kohil[2]

[1]Student, M-Tech, Electronics and Communication Engineering, Jalandhar, Punjab, India
[2]Assistant Professor, Department of Electronics and Electrical Engineering, Jalandhar, Punjab, India

---***---

Abstract - *In wireless sensor networks use of nodes which serves as the communicating devices in the networks. The use of such nodes comes with the security issues like data confidently, data availability, authentication, data integrity. All these issues should be solved by using cryptography techniques to provide efficient and reliable security for secure data transmission. This paper speaks to a review over the utilization of cryptography procedures in WSNs. The primary concentration of this paper is utilization of public key cryptography procedures over the symmetrical one and giving a solid and secure information transmission.*

***Key Words*: Wireless Sensor Networks (WSNs), Efficient and Reliable Security, Security Issues, Cryptography.**

1. INTRODUCTION

The first section of this paper provides the introductory concepts of WSN, security issues and requirements. The section II reviews the various cryptographic techniques. In section III the reviews for the types of cryptography with key management ideas. Section IV contains the current and future work in asymmetrical cryptography and section V provides the general views of our work on the concluded comparison between cryptography techniques and at last this paper is finished up with section VI.

1.1 WIRELESS SENSOR NETWORKS.

A remote sensor system has a storage facility of capacity, handling, detecting and transmission as principle electronic parts in a conveyed way. It contains countless, self-coordinated and, low controlled gadgets called sensor hubs which are utilized to detect the nearness of wanted application like temperature control, fire cautions, development location, and so forth. In WSNs an extensive number of haphazardly disseminated, battery-worked, inserted gadgets that are utilized to gather, prepare, and pass on information to the clients as a matter of course as its fundamentals of operation [1]. Every hub is intended for performing errands like gathering information, detecting, preparing and speaking with different hubs [2]. For some ongoing applications the sensor hubs are performing distinctive diverse undertakings like distinguishing the neighbor hubs, savvy detecting, putting away of information and handling of put away information, information total, following of target, control and observing, hub restriction, synchronization and proficient steering amongst hubs and base station [3]. As appeared in figure 1 the WSN contains a detecting unit, a handling unit and an imparting unit every one of these units are controlled by a power unit used to give the working of WSNs by utilizing these critical units to give dependable and productive working of conveying between the hubs and for secure information transmission imparting between the hubs ought to be solid and effective.

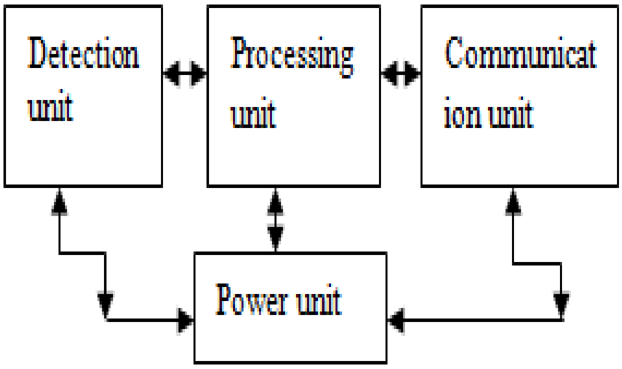

Fig- 1: Block Diagram of Wireless Sensor Network

WSNs couldn't give a solid and an effective working model because of the dangers of systems administration. These dangers are influencing distinctive layers of imparting conventions essentially, transport layer, organize layer, session and application layers. Before actualizing information uprightness, information secrecy, and information validation we should manage these dangers and ought to discover some approaches to maintain a strategic distance from them.

1.2 THREATS IN WSNs.

The following threats in wireless sensor network includes basically security issues of the secure data transmission in WSNs during node communication includes some of the basic communication threats and some advance threats which affects the wireless sensor network's working model [4]. The following table shows the basic threats involvement in WSNs.

Table -1: Threats in WSNs.

Threaets	Description
False node insertion	Flow false data and prevents the true data to flow.
Routing attack	Changes the routing path causing Sinkhole, Warm hole.
Malicious data	False observations.
Subversion of node	Node misbehavior causes extraction of data.

1.3 SECURITY REQUIREMENTS.

When managing security in WSNs, mostly the issue is accomplishing the security amid transmission of information over the communication system which includes a few or all security issues portrayed beneath. There are different security issues in WSN as takes after [5].

1. ***Data Integrity***: It is the ability to confirm the message has not been changed while it was on the network i.e. messaging authentication.

2. ***Data Freshness***: Ensures that the information is later, and no old messages have been sending again i.e. stays away from replay of messages.

3. ***Data Availability***: Determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate i.e. node availability is there or not.

4. ***Data Confidentiality***: It is the ability to hide message from a passive attacker i.e. data encryption or data authentication.

5. ***Self-Organization***: A remote sensor arrange requires each sensor hub to be autonomous and sufficiently adaptable to act naturally sorting out and self-recuperating as indicated by various circumstances i.e. long life time ought to be there for a hub in a system.

6. ***Authentication****:* Ensures that the communication from one node to another node is authorized i.e. authenticated users are communicating in a network to avoid attacker's forgery.

2. CRYPTOGRAPHY TECHNIQUES.

Cryptography plans are created to meet the fundamental security prerequisites of secrecy and honesty in systems to give dependable and productive secure information transmission i.e. security of information and client's character over an uncertain system. Cryptography is basically encryption techniques used for encryption of data or information into some secured data packets of coded data words i.e. raw data is converted into a secure coded data packets, which is being transmitted over the network instead of direct original data packets transmission in an insecure format. Encrypted data is basically a set of some extra bits along with the data bits for securing the original data from being accessed by the unauthorized users' means the original data is encrypted into some data bits in a coded form by changing its actual sequence into some random occurrence. During transmission encrypted data which is secured and compatible to the existing protocols over the network operating as a layered model of network i.e. compatible for transmission over the physical, data link, transport, and network and application layers in a secure way without being affected by threats of protocols layered architecture as original sequence of data is randomized using encryption techniques.

Cryptography is basically of two types: Symmetric Cryptography (secret key) and Asymmetrical Cryptography (public key) [6].

1. Symmetrical cryptography / Symmetric encryption / secret-key cryptography:

Most referred earlier technique and uses only a single secret key for both encryption and decryption of the data packets in a communicating network which is kept as secret in a network as shown in Figure 2. This technique makes use of only a single key called secret key which is shared between the communicating parties over the network, thus this process of sharing the key is much threat prone. The further classification of Symmetric key algorithms is i) block ciphers for fixed transformations i.e. when data transmission is considered to be of fixed size as every time the sequence of data bits and their size is same with may be same or different content, and ii) stream ciphers for time varying transformations, where size is varied according to the length and type of data being transmitted over the network. The two subdivisions are used for comparing encryption algorithms on plain texts of the algorithm at various levels for example, the levels would be considered as various data types, battery power consumption parameters, various data block sizes, for various key sizes [14] [15] and various encryption/decryption speeds [7] [8] used as comparison basics.

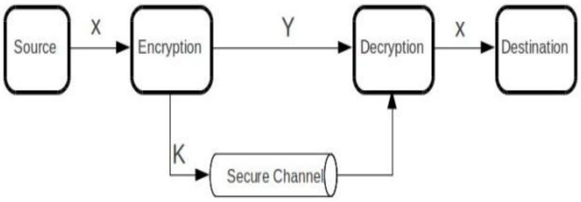

Fig- 2: Symmetric -Key Cryptography.

Keeping the key secreted in the network in the most difficult task in the network as this key more prone to threats over the insecure channel [9]. Examples of Symmetric key cryptosystems are AES, DES, RC4 CAST, RC5 algorithms used in WSN [12] [13] [14] [15] these are the algorithms employed to implement the symmetrical encryption techniques but not used mostly now as it is as the threat levels are high, they are used in combinations to provide secure data transmission.

2. Asymmetric Cryptography/Asymmetric encryption /public-key cryptography:

Being used at present time as cryptography technique in recent years due to its advantages over symmetrical techniques which were used to encrypt and decrypt the data. Asymmetrical cryptography strategy utilizes two keys public and private keys for information encryption and decryption which stays away from the danger of key partaking in a system to execute solid security needs as the general public key just shared over the uncertain system yet the unscrambling should be possible just by utilizing the private key which is accessible just to the decoding hub at goal [9] as appeared in figure 3.

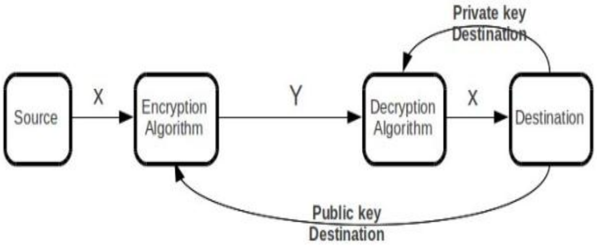

Fig- 3: Asymmetric Key Cryptography.

The keys are used as two-way security providers as the algorithm uses a pair of keys which are not same and not made for same encryption and decryption purpose, private key never makes the encrypted data publically known to every user it is only provided to the authorized users for accessing the data and by having matched private key a user can decrypt the data at the destination end comparing its public and private key with the sender's public and private key i.e. key sharing of public key could not benefits the attacker to decrypt the data as for decrypting the data private key is required and which is not shared over the network only authorized user is having private key for data decryption.

3. ASYMMETRICAL CRYPTOGRAPHY IMPLEMENTATIONS.

A public key cryptography/Asymmetrical Cryptography is basically used now as this cryptography technique avoids threats of security more efficiently then symmetrical ones. As the basic principle of public key says it consists of a pair of related and different keys i) public: provided publically to all the users in a communicating network ii) private: user specified i.e. between only two secured and authorized users. The keys are related to each other but computationally different as they are two different keys, also we cannot determine our private key using our public key because of having different computation processing [10] as shown in figure 4 thus higher level attacks are avoided by using such cryptography algorithms and also degrades security complexities by avoiding known key in a network i.e. public key only used for encryption of data but not for decryption of data therefore, mostly applicable for data communication in present era [11].

3.1 PUBLIC KEY CRYPTOGRAPHY.

Asymmetric cryptography such as the Diffie-Hellman key exchange system [14] [15], ECC or RSA signatures are typically used in WSNs [12]. Mostly RSA are easy to employee thus used widely in WSNs. RSA is having easy computational capabilities but employed less as the new developments like ECC provides less hardware implementations as compared to RSA but for the software developments mostly RSA is preferred due to its easy computational processing's.

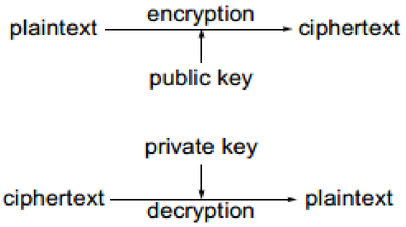

Fig- 4: Public key cryptography.

3.2 KEY MANAGEMENT.

Key administration is the most up to date scope for actualizing open key cryptography in WSNs which is generally utilized now as open key encryption system. Key administration is a fundamental security issue in remote sensor systems to set up the safe correspondence utilizing cryptographic advances between sensor hubs in a detected region over a shaky system. Key administration is the procedure by which cryptographic keys are produced, put away, secured, exchanged, stacked, utilized, and demolished in a system. There are four central issues in a key administration system:

1. **Key arrangement/pre-circulation**: How to characterize the path by which the key appropriation ought to be finished prior to the hubs are sent and what number of keys are required for arrangement in entire system?

2. **Key foundation**: How a gathering of hubs could build up any protected session in the imparting system over an uncertain channel or system for secure information

transmission in WSNs and being not influenced by the dangers in the system layers?

3. **Part/hub option**: How ought to a hub could be added to the system to such an extent that it ought to have the capacity to set up secure sessions with existing hubs in the system, while not having the capacity to make issues for pervious information stream in the system?

4. **Part/hub expulsion**: How ought to a hub could be expelled from the system to such an extent that it won't again have the capacity to build up secure sessions with any of the current hubs in the system, and not have the capacity to interpret next information stream in the system?

4. CURRENT AND FUTURE WORK.

In WSNs Symmetrical cryptography are more prone to security issues while the stronger asymmetrical cryptography still seems to be applicable one in providing security for secure data transmission needs. The Public key cryptosystems are used presently for solving security issues of WSNs currently mostly ECC, RSA, LPKC (large size PKC), MQ-PKC (multivariate quadratic PKC) [12] [13] [14] [15] are used along with key generation techniques either using static key generation or by using group key generation providing number of WSNs applications successful implementations [14] [15]. The key generation is the basic of new work being deployed in WSNs while are implementing public key cryptography in today's scenario as with key generation the problems regarding key exchange and key sharing are being solved easily.

4.1 WORK BEING DONE.

The study of key management schemes are based on the review of some research papers defining some works done on cryptography for solving security issues on data transmission over the network.

1. Wenliang Du. Jing Deng. Yunghsidng S. Hant. Shigang ChenT. also, Prainod K. Varshney (2004): "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge"- this paper concentrates on the ideas based to accomplish security in remote sensor systems for which it is essential to encode messages sent among sensor hubs. Keys for encryption purposes must be settled upon by conveying hubs.

2. Examination of cryptography for remote sensor arrange security by F. Amin, A. H. Jahangir, and H. Rasifard (2008): According to their review RSA is not a productive method for information encryption in WSNs. For this they have Compared ECC-160 and RSA-1024.Results demonstrates that execution of RSA cryptography devours more endeavors for actualizing security prerequisites when contrasted with ECC-224 which gives more plausible, time and power utilization arrangements.

3. Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, Ahlem Bencheikh (2010): "An Efficient and Highly Resilient Key Management Scheme for Wireless Sensor Networks"- portrays the assets constraint of WSNs makes the general population key based arrangements, which offer more proficient key administration administrations, inadmissible for remote sensor systems. In this paper, a novel effective tree-based probabilistic key administration conspire which is exceedingly flexible against hub catch assaults. Arrangement depends on symmetric cryptography with a probabilistic key pre-dispersion.

4. Unforgiving Kupwade Patil, Joseph Camp, Stephen A. Szygenda (2012): In this paper, proposed an area and vitality productive directing plan utilizing character bases cryptography. Explored the established particular sending assault on WSN and perceive how a personality based cryptographic plan utilizing a cross-layer configuration approach is useful in evading such an assault. Also, demonstrated that a personality based cryptographic way to deal with steering in WSN is more down to business then the conventional open key framework (PKI) based plans.

5. Kun Mu, Qingmin Cui (2012): This paper depends on "An Efficient Pairwise Key Establishment Scheme for Wireless Sensor Networks" portraying about the Wireless Sensor Networks (WSNs) and Security in WSNs which is basic when there are potential foes. In this paper, novel key administration conspire for remote sensor systems are assessed. The plan depends on EG plan and utilize one-way hash capacity to produce another key pool from a given key pool. Contrasted with leaving key pre conveyance conspires, this plans is generously more strength against sensor hubs catch.

6. Information security utilizing open key cryptography in WSNs by Amin Reza Sedghi, Mohammad Reza Kaghazgaran (June 2013): The utilization of open key cryptography on little remote gadgets is given unraveling to solid and effective verification and key trade conventions prerequisites.

7. PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks by Daehee Kim, Sunshin An (April 15, 2016): PKC-based cryptography resistance plans regard dodge DoS assaults and are vitality proficient and dependably holds information bundles under acknowledged limit constrains regardless of the possibility that vast number of false parcels are being produced by neighboring cells.

8. Open Key Cryptographic Primitives in Wireless Sensor Networks by Kyung-Ah Shim (2016): For information correspondence and transmission PKC primitives are

productive arrangement suppliers in settling on choices and outlining security conspires on WSN systems which are straightforwardly material for WSNs applications without much adjustment.

9. Key eras from remote channels by Junqing zhang, Trung q. Duong, Alan marshall, and Roger woods (2016): For simple and proficient reasonable working of key era with cryptography calculations in WSNs arbitrary key era for remote correspondence channels are utilized.

5. COMAPARISION RESULTS.

The following results are obtained by applying the concluded work.

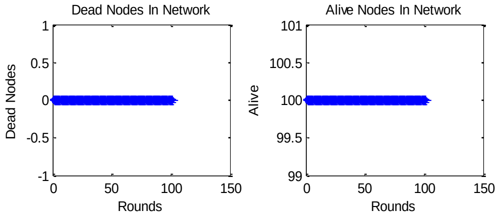

Fig- 4: Node formation and comparision of dead and alive nodes.

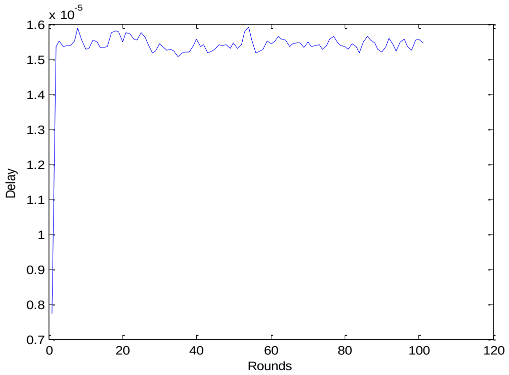

Fig- 5: Dealy graph.

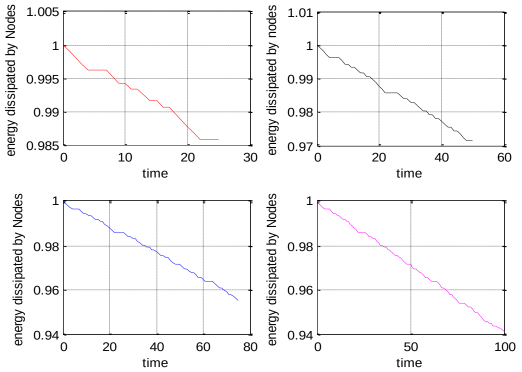

Fig- 6: Energy dissipation graphs based on asymmetrical techniques.

6. CONCLUSIONS

In this way finished up data proposes that the Public key cryptography is more useful as a result of its low memory utilization, low CPU utilization, and little key size over symmetrical plans. These plans give positive vitality benefits than doing irregular drops as in key administration plans. The time calculations are more dependable with variable key administration era procedures giving proficient security objectives as the key size is indistinguishable and differed at each progression without being in need to make them known to all hubs in a system as key calculation for key calculation for computing open key and private key is not same and not indistinguishable keys are utilized for encryption and decryption. The symmetrical cryptography is not appropriate for WSNs when contrasted with asymmetrical cryptography as symmetrical cryptosystems because of maintain a strategic distance from security dangers effectively. Notwithstanding key administration and security, public key cryptography can be the effective and dependable plan for number of WSNs applications as key administration scopes the general public key cryptosystems more solid and productive type of key era and trade handle. Likewise the public cryptosystems are more proficient in security objectives accomplishment when contrasted with symmetrical ones as symmetrical ones needs to give the connection keys publically which causes unapproved assaults and client's information security absconds while public cryptosystems does not have to publically profit their key era as public key is utilized for encryption is promptly accessible yet the private key utilized for unscrambling is not made accessible in this manner security dangers decreases as assailant have no learning in regards to the private key which can decode the information hence information respectability, information secrecy, and validation could be accomplished which gives the fundamental secure transmission needs achievement.

REFERENCES

[1] K. Akkaya and M. Younis, "A Survey on steering conventions for remote sensor systems, Ad Hoc arranges", 3 (2005), pp 325-349.

[2] Gustavo S. Quirino, Admilson R. L. Riberio and Edward David Moreno "Hilter kilter Encryption in remote sensor systems", 8(2012), http;// dx.doi.org/10.5772/48464.

[3] E. Shi and A. Perrig, "Outlining secure sensor systems". Remote correspondence magazine, 11 (6), pp 37-43, 2004.

[4] Y. Wang, G. Attebeery, and B. Ramamurthy, "A Survey of security issues in remote sensor systems", IEEE correspondence overviews and instructional exercises, 8(2): pp 2-23, 2006.

[5] Y. Wang, W. Hmm, S. Chellappan, Dong Xuan, and Ten H. Laii, "Seek based physical assaults in sensor systems: Modeling and Defense, specialized report, bureau of

software engineering and designing, Ohio state college, 2005.

[6] Shish Ahmad, Mohamad Rizwan ask, and Qamar Abbas, " Energy sparing secure structure for sensor arrange utilizing circular bend cryptography Mobile Adhoc systems", pp 167-172, 2012.

[7] R. Ahlswede and I. Csiszar,"Common irregularity in data hypothesis and cryptography I. mystery sharing" , vol. 39, no.4, pp 1121-1132, July.1993.

[8] D. Han Kerson, A. Meneres, S. Vanstone, "Manual for Elliptical bend cryptography", Springer-Verlag New York, Inc. 2004.

[9] A. J. Menezes, P.C. Van oorschot, S.A. Vanstone, "Handbook of connected cryptography", 1997.

[10] G. Gaubtaz, J. P. Kaps, and B. Sunar, "Open key cryptography in sensor systems returned to", pp 1-17, 2004.

[11] A. S. Meander, N. Gura, H. Eberle, V. Gupta and S.C. Shantz, "Vitality examination of open key cryptography for remote sensor arrange", pp 324-328, 2005.

[12] Zhang Yu, "The Scheme of open key foundation for enhancing remote sensor systems security", pp 167-172, 2003

[13] W. Du, J. Deny, Y. S. Han, Shigang Chen, P. K. Varshney, "A key administration conspire for remote sensor organize utilizing arrangement learning", 2004.

[14] O. Gungor, F. Chen, C. E. Koksal, "Emit key era through restriction and portability", vol. 6, no. 6, pp 2214-2230, Jun. 2015.

[15] H. Liu, J. Yang, Y. Wang, Y. Chen and C. E. Koksal, "Gather key era", vol. 13, no. 12, pp 2820-2835, Dec 2014.

BIOGRAPHY

HEENA DOGRA
Student, M-Tech, Electronics and Communication Engineering, Jalandhar, Punjab, India