ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Review on Secure Communication in Wireless Image Sensor Networks

M Deepa [1], G Ramprabu [2]

Associate Professor, Department of Electronics and Communication Engineering, Usha Rama College of Engineering and Technology, Telaprolu, Krishna District, India.[1]

Associate Professor, Department of Electronics and Communication Engineering, New Prince Shri Bhavani College of Engineering and Technology, Chennai, India.[2]

ABSTRACT: Wireless sensor networks are progressively picking up consideration. Lately, a lot of observing, control and following applications have been intended for various situations. For such networks, camera-empowered sensors can recover visual data from an observed field, giving significant data to numerous applications. All in all, those networks have asset limitations of preparing, memory, energy and transmission data transmission, forcing many plan difficulties. In any case, a gathering of utilizations may likewise have security prerequisites, which bring extra unpredictability to be taken care of. Most conventional security components for famous networks, similar to the Internet, are not appropriate for wireless sensor networks, requesting legitimate examination around there. In this paper, we study ongoing improvements in encryption and protection in wireless sensor networks conveyed for transmissions of image depictions, assessing inventive ways to deal with give distinctive dimensions of security. Promising examination headings are additionally talked about.

KEYWORDS: Wireless Sensor Networks, Watermarking, Image Monitoring, Symmetric and Asymmetric Cryptography.

I. INTRODUCTION

Wireless Sensor Networks (WSN) has rough the enthusiasm of the exploration territory, fixated by an abundance of fanciful and reasonable overcomes [1]. Groundbreaking outcomes around there have introduced a pour of collective and furnished applications. As a rule, sensor hubs have handling, stockpiling and transmission confinements beginning from their asset compelled nature. Camera-empowered sensors conveyed to recover image depictions and video streams will ordinarily request a greater number of assets than customary scalar sensors, conveying extra difficulties to the structure and activity of wireless visual sensor networks (WVSN). As of late, numerous works have proposed inventive answers for upgrade the execution of those networks, introducing promising commitments. For some of them, detecting and transmission of image previews are more practical than detecting and transmission of video streams, defining the extent of wireless image sensor networks (WISN) [2].

Numerous WISN applications will have security prerequisites. Sensor hubs might be sent in extensive and difficult to-get to territories, where the wireless channel may be gotten to by unapproved individuals. Notwithstanding natural issues when endeavoring to guarantee confidentiality, the transmission flow may likewise be liable to uprightness assaults. Finally, verification is additionally required for some applications, with the end goal to guarantee that recovered data originates from substantial source hubs. The asset compelled nature of normal WISN applications disheartens the utilization of conventional security systems as those utilized on the Internet [3,4]. Solid cryptography, for instance, may quickly exhaust the constrained energy supply of sensor hubs. As an option, a few works have proposed creative ways to deal with location these issues, utilizing improved arrangements.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

II. Related Work

Shilpy Ghai et.al [5], clarifies efficient use of energy and security has been a center region of research in wireless sensor networks. Sensor hubs utilized in a network are battery worked having low power capacities. Batteries of these hubs can't be energized regularly in the field setting, so energy advancement ends up foremost in expanding the battery-life and, thusly, the network lifetime.
Song et al [6], In request to spare energy, mostly in a thickly sent WSN, numerous proposition receive a conveyed coding approach where neighboring sensor hubs participate in performing image coding. In any case, a noteworthy trade of data, which would squander energy, might be vital.
Maniezzo et al [7], tended to the tradeoffs among registering and correspondence and demonstrate that there are an ideal number of hubs associated with a dispersed coding process which limits the aggregate energy utilization. Santha devi et.al [8], In this paper they have proposed a novel strategy to pack the image utilizing enhanced wavelet based polyomino's lossless pressure procedure which builds the quality of image at accepting end. The packed image is transmitted by Energy Efficient High Quality Image Transmission scheme (EEHQIT) to accomplish energy efficient image transmissions in Wireless Sensor Networks (WSNs). Anyway presence of clamor makes the imaging framework is a muddled undertaking. In this situation diminishing commotion utilizing channel strategy for accomplishing high quality pressure image transmission is wanted. To maintain a strategic distance from clamor in the packed image, a scheme of spatial averaging channel is exhibited and tried on the transmitted compacted image. This methodology expels the clamor from the transmitted image by method for remaking the image to acquire the first image without loss of data.

III. Symmetric/Asymmetric Cryptography

In general, secure data transmissions can be accomplished through symmetric or asymmetric cryptography. The two present points of interest and disadvantages that ought to be legitimately assessed for each sort of WSN application. For the specific instance of image detecting, the extra weight for the transmission of a lot of data ought to likewise be considered. The following subsections depict symmetric and asymmetric cryptography with regards to wireless sensor networks. In addition, the pertinent issue of key administration is additionally tended to.

Symmetric Encryption: The symmetric cryptography worldview appeared in figure 1 defines a solitary shared key for both encryption and decoding capacities. Accordingly, the procedure of cryptography is less demanding to actualize. Be that as it may, the greatest test is the means by which to securely appropriate the common key. Indeed, it's anything but a paltry assignment, since it isn't constantly conceivable to pre-send or pre-disperse keys in sensor hubs [3].

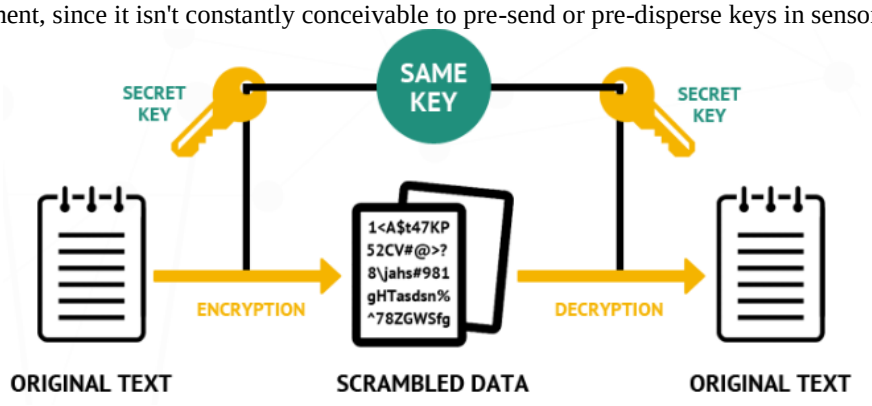

Fig. 1 Symmetric Encryption

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Asymmetric Encryption: It is otherwise called public-key cryptography (PKC), utilizes a couple of keys to perform data encryption. A public key that is known by all hubs of the network is utilized to scramble data, and a private key known just by the goal hub is utilized to decode that data. Normally, conventional asymmetric cryptography calculations have high figuring overhead, requiring additionally preparing time. In light of this supposition, as indicated by [9], most works appear to guarantee that public-key cryptography isn't practical for WSN applications. In any case, throughout the years, investigations, as directed in [10], have demonstrated something else, where efficient calculations and sensible key sizes show the practicality of asymmetric cryptography appeared in figure 2 for wireless sensor networks. In addition, sensor bits with better assets and moderate costs ought to be accessible soon.

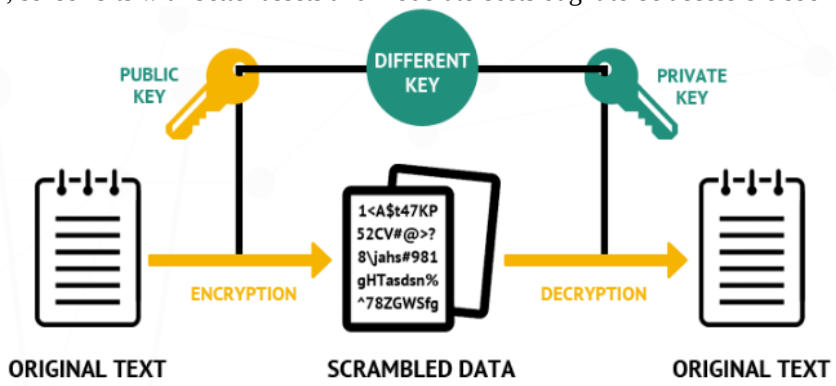

Fig. 2 Asymmetric Encryption

The comparison between two types of encryption using the following four major points:

The Basics – While Symmetric encryption makes use of a single key for both encryption and decryption, Asymmetric encryption uses different keys for encryption and decryption. It applies a public key for encryption, while a private key is used for decryption.

Algorithms – Symmetric encryption using algorithms like 3DES, DES, RC4, AES and QUAD. Whereas, asymmetric encryption uses **RSA and ECC algorithms** to create the public and private keys.

Performance – While Symmetric encryption is fast in its execution, Asymmetric encryption tends to be slower in execution as a result of more complex algorithms which come with a high computation burden.

Purpose – Symmetric encryption is utilized for bulk data transmission. Whereas, asymmetric encryption is mostly used for securely exchanging secret keys.

IV. WATERMARKING AND SECURE IMAGE MONITORING

Cryptography is a compelling method to give confidentiality, respectability and realness in various kinds of data networks. In any case, handling, memory and energy requirements in wireless sensor networks might be excessively stringent for some cryptography calculations. This setting cultivates the selection of other security components for WISN, for example, watermarking. Many image checking applications will require confirmation components. The significant test for data verification and validation is to precisely know which sensor hubs are pernicious. False visual data might be embedded into the network, and source hubs might be liable to altering assaults. In such a way, some instrument ought to be utilized to validate gotten data at the sink side. The watermarking method comes then as an approach to give a lightweight instrument to validation in wireless sensor networks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

As a rule, any image transmission over wireless sensor networks might be ensured utilizing watermarks. As a matter of fact, this strategy has been utilized in numerous visual applications on the Internet, yet it might likewise bring significant results for WISN. To put it plainly, an advanced watermark is an exceptional marker that is inserted into scalar, sound, image or video data, going for giving a system to recognize proprietorship and copyright. The watermarking procedure will shroud confirmation data in unique data, and the imprints might be unmistakable or not. In a secure setting, watermarks must not be identified or evacuated by aggressors, and there are distinctive approaches to give such insurance [11].

The watermarking procedure is made out of three general stages: age, inserting and recognition [11]. The age procedure relies upon the idea of the thought about detected data, and it might require complex calculation, where a watermarking key is for the most part utilized. The installing procedure will embed the figured watermark into the coveted data. Such a procedure might be performed abusing attributes of changes, as in discrete cosine transform (DCT), DWT, discrete fourier transform (DFT), among others. As well known image codecs depend on such changes, for example, JPEG (DCT) and JPEG2000 (DWT), image watermarking might be thought of as a successful confirmation asset for wireless sensor networks. Finally, the location procedure is in charge of identifying and extricating watermarks. Figure 7 shows a general scheme for image watermarking.

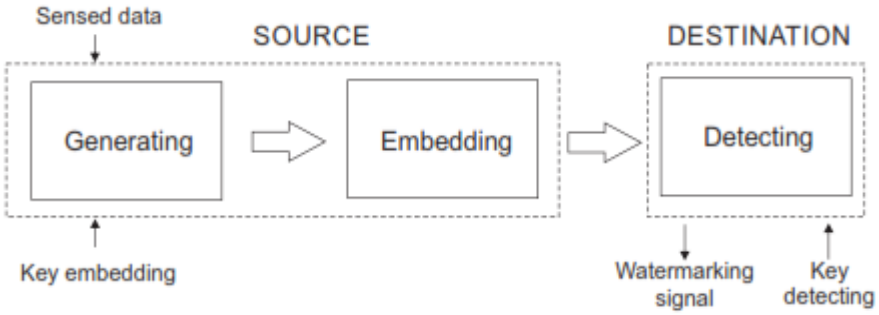

Fig. 3 Watermarking in WISN

Compression strategies and collection calculations for multimedia substance are vital in the WSN configuration with the end goal to lessen correspondence overhead, to spare preparing assets and to reduce energy utilization while diminishing the measure of transmitted data [12]. Truth be told, numerous pressure schemes have been proposed as of late [13-14]. As security systems might be excessively stringent for wireless image sensor networks, the manner in which visual data will be detected and handled might be misused to improve security. In this unique circumstance, for instance, there are techniques that consolidate pressure and encryption to lessen preparing time and processing overhead.

V. CONCLUSION

Security components might be basic in WSN plan. Late works have concentrated on creative components to give distinctive dimensions of security relying upon the accessible assets of sensor networks. In this specific circumstance, encryption is vital for WSN applications, since these networks are highly inclined to security disappointments because of their wireless and appropriated nature. Specific encryption of images is an imperative system to guarantee security in networks with asset limitations. As conventional encryption instruments might be unfeasible for WISN because of high overhead of registering and correspondence, a practical arrangement could be actually the mix of encoding calculations with cryptography. Validation performed by watermarking and secure image checking is additionally important issues that were overviewed in this work.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

REFERENCES

[1] G. Ramprabu, S. Nagarajan, "Design and Analysis of Novel Modified Cross Layer Controller for WMSN", Indian Journal of Science and Technology, Vol 8(5), pp.438–444, March 2015.
[2] Danilo de Oliveira Gonçalves, Daniel G. Costa, "A Survey of Image Security in Wireless Sensor Networks", Journal of Imaging, vol. 1, pp. 4–30, 2015.
[3] Sen, J. A Survey on Wireless Sensor Network Security. Int. J. Commun. Netw. Inf. Secur. 2009, 1, 55–78.
[4] Guerrero-Zapata, M.; Zilan, R.; Barcelo-Ordinas, J.M.; Bicakci, K.; Tavli, B. The future of security in wireless multimedia sensor networks. Telecommun. Syst. 2010, 45, 77–91.
[5] Shilpy Ghai1, Prof. V.K.Katiyar2" Energy Efficient Data Transmission Schemes in Wireless Sensor Networks" International Research Journal of Innovative Engineering Vol.1, No. 4, 2015.
[6] Akash Mittal , Prof. Ajit Kumar Shrivastava , Dr. Manish Manoria " Efficient Image transmission in Wireless Sensor Networks using Wavelet coded Preprocessing technique" IRACST – International Journal of Computer Networks and Wireless Communications IJCNWC), ISSN: 2250-3501 Vol.2, No.2, 2012.
[7] Sanghamitra Panda1, Satyanarayana Gandi2, Amarendra Kothalanka3" Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, No. 1, January 2015.
[8] Santha devi P, Sivakumar, Arthanariee A.M, "Efficient Wireless Image Transmission With Wavelet Based Polyomine Compression", International Journal of Scientific and Research Publications, Volume 3, Issue 2, 2013.
[9] Gaubatz, G.; Kaps, J.P.; Ozturk, E.; Sunar, B. State of the art in ultra-low power public key cryptography for wireless sensor networks. In Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops, Kauai Island, HI, USA, 8–12 March 2005; pp. 146–150.
[10] Lenstra, A.K.; Verhuel, E.R. Selecting cryptographic key sizes. J. Cryptol. 2001, 14, 255–293.
[11] Xiang, T.; Yu, C.; Chei, F. Fast encryption of JPEG 2000 images in wireless multimedia sensor networks. Lecture Notes Comput. Sci. 2013, 7992, 196–205.
[12] Grieco, L.A.; Boggia, G.; Sicari, S.; Colombo, P. Secure wireless multimedia sensor networks: A survey. In Proceedings of the International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Sliema, Malta, 11–16 October 2009.
[13] Misra, S.; Reisslein, M.; Guoliang, X. A survey of multimedia streaming in wireless sensor networks. IEEE Commun. Surv. Tutor. 2008, 10, 18–39.
[14] Chew, L.W.; Ang, L.M.; Seng, K.P. Survey of image compression algorithms in wireless sensor networks. In Proceedings of International Symposium on Information Technology, Kuala Lumpur, Malaysia, 26–28 August 2008.