JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Review Paper on Cryptography Algorithms Used in Wireless Sensor Networks

H. Kaur[1*], K. Kaur[2]

[1,2]Computer Science Engineering, Patiala Institute of Engineering and Technology for Women, Maharaja Ranjit Singh Punjab Technical University, Patiala, India

[*]*Corresponding Author: kaurhk0019@gmail.com , Tel.: +79-8668-1861*

Available online at: www.ijcseonline.org

Accepted: 13/Aug/2018, Published: 31/Aug/2018

***Abstract*—**Wireless sensor network are autonomous nodes which monitor and communicate the sensor data to central unit through wireless network. There devices are installed in the remote areas and used for communicate sensitive information in different application such as smart grids, MANET. The attackers attack on these nodes to extract information or modify. In this paper, various attacks and its countermeasure technique such as cryptography algorithms are studied and comparative analysis is done for the wireless sensor network. From, the analysis found that symmetric and asymmetric ciphers are hybrid which provide authentication and confidentiality but increased the resources requirement. But, the wireless sensor nodes are battery operated and low memory available. Therefore, we recommend in the future work preferred lightweight cipher and different modes of authentication such as CCM, counter mode to enhance the performance on wireless sensor network.

***Keywords*—**Cryptography, Wireless SensorNetwork,Attacks,AES,RSA.

I. INTRODUCTION

The wireless sensors deployment in the various applications such as smart grids, E-healthcare, MANET networks is increased exponentially in the last few decades to improve performance and maintain the network reliability. The wireless sensor network includes large number of sensors placed in the harsh environment [1]. The sensor nodes are wireless connected and no physical protection is provided. Hence, more prone to the various attacks. These attacks are briefly explained below [2].

- Flooding Attack

In this attack, the attacker sends continuously sending request to the sensor nodes. On each request, node assign some resources to one request and continuously assigned resources complete the memory stack.

- Black Hole Attack

The attacker places the malicious node in the network which shows the shortest/ optimize path for data routing and number of adjacent nodes tries to communicate data through this node, this result message captured.

- Node Replication Attack

In the wireless sensor network, each node has unique ID through message is communicated in the optimized way. The attacker designed the sensor node device with same unique IDs which disturb the whole routing in the network.

To overcome these attacks, various cryptography encryption and authentication algorithms are used in the wireless sensor network for secure routing, data integrity, and freshness of the data [3]. The cryptography algorithms are separated into symmetric and asymmetric algorithms. The symmetric algorithms provide encryption and used for large amount of data encryption. On the other side, asymmetric algorithms are used for data authentication and mostly deployed in securing the symmetric keys in the sensor network. Further, the symmetric and asymmetric algorithms are hybrid to provide encryption as well as authentication in the network [4,5].

The cryptography algorithms are used in wireless sensor network are studied and reviewed in this paper. Next, the comparative analysis of various algorithms is done on the basis of block size, key size, and remarks. In last, the conclusion is drawn and some future direction is defined which helps other authors to contribute their work in the field of wireless sensor network security.

The next sections of the paper are defined as follows. Section II defined the literature survey on wireless sensor network security algorithms, section III defined the comparative of various algorithms is drawn, Section IV explained conclusion and future work.

II. LITERATURE SURVEY

The various cryptography algorithms used in wireless sensor network are reviewed and analyze in this section. The review is sub-divided into three parts.

A) Symmetric Cipher for Wireless Sensor Network

Prathamesh, et al. [6], used the 3DES algorithm with honey encryption to resolve malware attack in the wireless sensor network.

Cristina Panait and Dan Dragomir [7], used AES algorithm for wireless sensor security. They have done various modes of implementation for AES algorithm and optimized it for ATmega128RFA1 microcontroller. In last, they have shown that their design is fast and more energy efficient as compared to other software implementation.

Priyadharshini, et al. [8], for data confidentiality in the wireless sensor network using the Blowfish algorithm. The algorithm is simulated in Proteus software.

Kumar, et al. [9], designed 128-bit NLFSR (non-linear feedback shift register) stream cipher for wireless sensor data security. The designed hardware implementation is done on FPGA virtex board and synthesize result show its consume 144 slices.

Toru Akishita and HarunagaHiwatari [10], developed CLEFIA for resource constraint device such as wireless sensor nodes. Their architecture hardware efficient and for encryption/decryption same architecture used.

B) Asymmetric Ciphers for Wireless Sensor Network

Abduvaliev, et al. [11], deployed the lost cost authentication and integrity algorithm for wireless sensor security due to less memory and computation required as compared to other ciphers. They used the Hash and Diffie Hellman algorithm for authentication and pre-sharing the secret key between transmitter and receiver.

Sreevidya, et al. [12], deployed RSA algorithm for wireless sensor network to resolve false data injection attack. The algorithm is simulated in NS-2 simulator.

Verma, et al. [13], have done the performance analysis of cryptography asymmetric algorithms such as RSA and ECC for wireless sensor network. Next, designed the code in the MATLAB.

Eldefrawt, et al. [14], designed a protocol which authenticate the broadcast messages in the wireless sensor network. They have used the nested hash and Chinese reminder theorem(CRT) for this purpose. The nested hash function which provide seed point generation and key generation in the logic then further CRT employed. There are number of advantages of their technique such as no time synchronization required and non-restricted key generation.

Liu, et al. [15], due to precise constraint area and memory of wireless sensor network lightweight cryptography algorithms are required. Hence, they deployed Elliptic Curve Cryptography algorithm for wireless sensor network and implemented on 8-bit AVR processor. Their proposed technique support Montgomery multiplier and various key sizes 160, 192, 224, and 256 bits.

C) Hybrid of Symmetric and Asymmetric Ciphers

Parrilla, et al. [4], designed an ECC-AES co-processor key support algorithm which provide security and privacy in the wireless sensor network. The algorithm is hardware implemented on Spartan 6 device and consume very less resources in terms of 2101 LUTs.

RawyaRizk and Yasmin Alkady [16], designed 2 phase hybrid security algorithms. In the first phase data is encrypted using AES and ECC algorithm. In the second phase to provide authentication and integrity RSA and MD5 algorithm are used. The algorithm is simulated on NS-2 software and their proposed technique is robust to different attacks.

Bisht, et al. [5], to provide confidentiality, integrity, and authentication hybrid the AES and RSA algorithm. In the AES algorithm the initialization key is generated using Arnold algorithm. The hybridization is provided double layer of security.

M. Senthil Murugan and Dr. T. Sasilatha [17], to provide maximum key lifetime, reduced power level and improve security used the AES and stream cipher RC-4 algorithm for data encryption. The input stream is divided into two half. On the left half, AES algorithm and in the right half, RC-4 algorithms are used.

R. Sharmila and V. Vijayalakshmi [18], proposed hybrid key management scheme by hybrid the genetic and hyper-elliptic curve cryptography (HECC) algorithm. In their proposed work, the genetic algorithm generates the symmetric keys and their key seed point is generated using HECC. Their technique provides energy efficiency, key refreshment and less resources.

Tzonelih Hwang and ProsantaGope [19], designed robust stream cipher mode of authentication using PFC-CTR and PFC-OCB. In their algorithm the key is generated using block cipher AES. They have resolved number of attacks such as chosen plaintext attack, known plaintext attacks. In last, they have shown that their design provide less computational head as compared to other encryption authentication scheme.

III. COMPARATIVE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS FOR WIRELESS SENSOR NETWORK

In this section, various cryptography algorithms used in the wireless sensor network are compared as shown in Table 1-3.

Table 1 Comparative Analysis of Symmetric Cryptography Algorithms for Wireless Sensor Network

Reference	Algorithm	Structure	Block Size	Key Size	Remark
[6]	DES	Substitution-Permutation Network	64	56	Small Key size so easy to break.

[7]	AES	Substitution-Permutation Network	128	128,192.256	Fast Encryption, NIST Recommended Large number of S-boxes required.
[8]	Blowfish	Feistel Network	64	32 to 448bits	Same architecture used for encryption/decryption
[9]	NLFSR	---		128	Simple operations
[10]	CLEFIA	Feistel Network	128	128,192.256	Same architecture for encryption/decryption Less Number of Rounds

Table 2 Comparative Analysis of Asymmetric Cryptography Algorithms for Wireless Sensor Network

Reference	Algorithm	Key Size	Remarks
[11]	Hash	32,64,128,256	Same mathematical function applied between transmitter and receiver for authentication purposes.
[12]	RSA	512,1024,2048 bit	Large size key required for data security.
[13]	RSA & ECC		Lightweight authentication algorithm and its key size 163 bit provide same security as compared to RSA 1024bits.
[14]	Hash and Chinese Reminder Theorem		
[15]	ECC	160,224,256, 384,521	Used for authentication and key generation

Table 3 Comparative Analysis of Hybrid of Symmetric-Asymmetric Cryptography Algorithms for Wireless Sensor Network

References	Algorithm	Remarks	
[4]	AES_ECC	Hybrid of Symmetric and Asymmetric provide confidentiality and authentication but increased the computation and resource requirement.	
[16]	AES_ECC_RSA_MD5		
[5]	AES_RSA		
[17]	AES_RC4		
[18]	Genetic Algorithm_HECC		
[19]	PFC-CTR and PFC-OCB, AES	Provide encryption and authentication without any overhead on resources and computation.	

IV. Conclusion and Future Research Directions

In this paper, various symmetric and asymmetric cipher and their hybridization analysis is done for the wireless sensor network. The Table 1 analysis show that symmetric cipher are fast for data encryption and preferred for bulk amount of data encryption and provide confidentiality. Further, conventional symmetric ciphers such as AES, Blowfish provide security but required large memory. In the Table 2, asymmetric algorithms are used for data authentication but consume large amount of resource because of large key sizes. In the asymmetric, RSA and ECC is most preferred algorithm. ECC algorithm provide same level of security in small key size as compared to RSA. In the last Table 3, to provide confidentiality and authentication, symmetric and asymmetric ciphers are hybrid which consume maximum resources. We have also defined some future work on which further work can be done.

- Prefer lightweight cipher for wireless sensor network which consume less memory.
- As defined, to provide confidentiality and authentication, symmetric and asymmetric algorithm is preferred which increased memory required. Therefore, in place of hybridization various modes such as counter modes, CCM modes prefer in symmetric cipher.

REFERENCES

[1] Cheikhrouhou, Omar, "*Secure group communication in wireless sensor networks: a survey*," Journal of Network and Computer Applications, vol. 61, pp. 115-132, 2016.

[2] Pawar, M., & Agarwal, J.,"*A literature survey on security issues of WSN and different types of attacks in network,*" Indian Journal of Computer Science and Engineering, vol. 8, issue 2, pp. 80-83, 2017.

[3] Faquih, A., Kadam, P., &Saquib, Z.,."*Cryptographic techniques for wireless sensor networks: A survey*," In Bombay Section Symposium (IBSS),pp. 1-6, 2015.

[4] Parrilla, L., Castillo, E., López-Ramos, J. A., Álvarez-Bermejo, J. A., García, A., & Morales, D. P. "*Unified Compact ECC-AES Co-Processor with Group-Key Support for IoT Devices in Wireless Sensor Networks,"* Sensors, vol. 18, issue 1,pp. 251, 2018.

[5] Bisht, N., Thomas, J., &Thanikaiselvan, V. "*Implementation of*

security algorithm for wireless sensor networks over multimedia images," International Conference onin Communication and Electronics Systems (ICCES), ,pp. 1-6, 2016.

[6] Prathamesh, G., Sanket, G., Yogeshwar, K., & Aniket, N..“*Secure Data Transmission in WSN Using 3 DES with Honey Encryption,”* IJARIIE, vol.1, issue 4, pp.455-461, 2015.

[7] Panait, C., & Dragomir, D.,“*Measuring the performance and energy consumption of AES in wireless sensor networks*,”2015 Federated Conference onin Computer Science and Information Systems (FedCSIS), ,pp. 1261-1266, 2015.

[8] Priyadharshini, S. P., Arumuagam, N., &SangeethaAnanthamani, K. “*Implementation of Security in Wireless Sensor Network using Blowfish Algorithm*,”International Journal of Computer Applications, pp. 33-37, 2014.

[9] Kumar, K. J., Reddy, K. C. K., Salivahanan, S., Karthik, S. D., & Praveen, V.,*“Exclusive-128 Bit NLFSR Stream Cipher for Wireless Sensor Network Applications*,” International Journal of Engineering and Technology, vol. 5, issue 5, pp. 3668-3675, 2013.

[10] Akishita, T., &Hiwatari, H. “*Very compact hardware implementations of the blockcipher CLEFIA,”* In International Workshop on Selected Areas in Cryptography, Springer, Berlin, Heidelberg, pp. 278-292, 2011.

[11] Abduvaliev, A., Lee, S., & Lee, Y. K..“*Simple hash based message authentication scheme for wireless sensor networks,”*In 9th International Symposium on Communications and Information Technology,(ISCIT), Icheon, pp. 982-986, 2009.

[12] Sreevidya, B., Rajesh, M., & Mamatha, T. M..“*Design and Development of an Enhanced Security Scheme Using RSA for Preventing False Data Injection in Wireless Sensor Networks,”* In Ambient Communications and Computer Systems, pp. 225-236, 2018.

[13] Verma, D., Jain, R., & Shrivastava, A. “*Performance analysis of cryptographic algorithms RSA and ECC in wireless sensor networks*,” IUP Journal of Telecommunications, vol. 7, issue 3, pp. 51, 2015.

[14] Eldefrawy, M. H., Khan, M. K., Alghathbar, K., & Cho, E. S. “*Broadcast authentication for wireless sensor networks using nested hashing and the Chinese remainder theorem,”*. Sensors,vol. 10, issue 9, pp.8683-8695, 2010

[15] Liu, Z., Wenger, E., &Großschädl, J. “*MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks*,” In International Conference on Applied Cryptography and Network Security, pp. 361-379, 2014.

[16] Rizk, R., &Alkady, Y. “*Two-phase hybrid cryptography algorithm for wireless sensor networks,”* Journal of Electrical Systems and Information Technology, vol. 2, issue 3, pp. 296-313, 2015.

[17] Murugan, M. S., Sasilatha, T., & Dean, A. M. E. T. “*Design of Hybrid Model Cryptographic Algorithm for Wireless Sensor Network*,”International Journal of Pure and Applied Mathematics, vol. 117, pp.171-177, 2017.

[18] Sharmila, R., & Vijayalakshmi, V.,“*Hybrid Key Management Scheme for Wireless Sensor Networks*,” International Journal of Security and Its Applications, vol. 9, issue 11, pp. 125-132, 2015.

[19] Hwang, T., &Gope, P.,“*Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network,”* Security and Communication Networks, vol. 9, issue 7, pp. 667-679, 2016.

Authors Profile

Harpreet kaur pursed Bachelor of Science from Punjabi University Patiala campus Yadwinder college of engineering in 2014 and pursing Master of Science from PIET college.

Kavneet kaur in pursed Bachelor of Science and Master of Science from PTU Jalandhar in 2007 and 2010. He has published more than 10 research papers in reputed international and national journals. His main research work focuses on Cryptography Algorithms, Network Security based education. He has more than 3 years of teaching experience.