ADAPTATION OF DNA BASED CRYPTOGRAPHIC ALGORITHM IN A CLUSTERED WIRELESS SENSOR NETWORK ENVIRONMENT

Salamon P Y
Head, Department of Computer Hardware Maintenance Engineering,
Government Polytechnic College, Nedumkandam,
Idukki (Dist), Kerala (State), India – 685 553
solomonpy@gmail.com

Abstract—Wireless Sensor Networks have gained prominence in recent years due to their potential to revolutionize various segments of our life and economy. Deployed as a network of thousands wireless sensor nodes which are able to communicate with each other using radio signals, the individual nodes have limited processing speed, storage capacity, and communication bandwidth. The nature of their deployment, especially in hostile and confidential environments like in military surveillance, Body Area Networks etc., calls for better data security in Wireless Sensor Networks. Cryptography is a method used for the Data protection and Information security. A variety of encryption schemes are used, of which, DNA based encryption using the Central Dogma of Molecular Biology is relatively new. Low Energy Adaptive Clustering Hierarchy (LEACH) is a cluster based routing protocol for WSNs. In this work, one DNA Encryption Algorithm is adapted into a Clustered Wireless Sensor Network under LEACH protocol, and its various performance parameters are compared with two other most popular and widely used encryption schemes viz. Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC)

Keywords—WSN- Cryptography- LEACH Protocol- DNA Encryption- AES- ECC

I INTRODUCTION

A wireless sensor network (WSN) is a wireless network, consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocol being select depends on the application requirements. Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz [1].

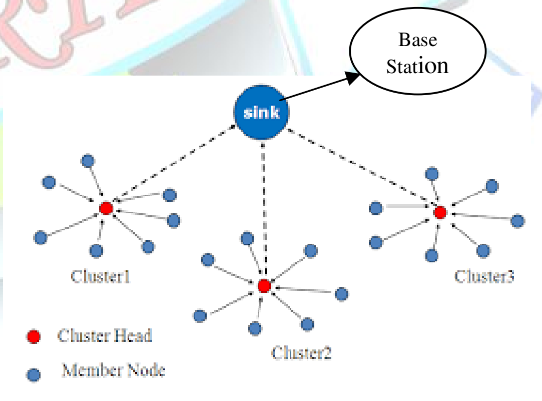

Fig.1 Schematic diagram of a Clustered W S N

A sensor network is designed to perform a set of high level information processing tasks such as detection, tracking or classification. Applications of sensor networks are wide ranging and can vary significantly, depending on the application requirements, modes of deployment, sensing modality, or means of power supply.

1.1 SENSOR NETWORK ARCHITECTURE

The design of Sensor Networks is influenced by factors such as scalability, fault tolerance, and power consumption. Two basic kinds of Sensor network Architecture are Layered architecture and Clustered architecture.[2]. Layered architecture has a single powerful Base Station (BS), and the layers of sensor nodes around it correspond to the nodes that have the same hop count to the BS. Clustered Architecture organises the sensor nodes into clusters, each governed by a Cluster Head (CH). The nodes in each cluster are involved in message exchanges with their respective Cluster Head, and these heads send messages to the Base Station which is usually an Access Point (AP), connected to a wired network.

Low-Energy Adaptive Clustering Hierarchy (LEACH) is a popular clustering based protocol that minimizes energy dissipation in WSNs. LEACH randomly selects nodes as Cluster Heads and performs periodic re-election, so that the high energy dissipation experienced by the Cluster Heads in communicating with the Base Station is spread across all nodes of the network. Computation is performed locally to reduce the amount of transmitted data, network configuration and operation is done using local control, and media access control (MAC) and routing protocols enable low-energy networking, and detailed in[3].

1.2 CRYPTOGRAPHY

Cryptography is defined as the practice and study of techniques for secure communication in the presence of third parties called adversaries [4][5]. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are also central to modern cryptography.

Cryptographic systems are characterized along three independent dimensions: Based on the type of operations used for transforming plaintext to ciphertext, they are classified as a substitution or transposition, or a product system. Based on the number of keys used, they are called symmetric encryption. Symmetric models include the most known DES (Data Encryption Scheme) and its derivatives and the AES (Advanced Encryption Standard, or an asymmetric system, that uses 2 distinct keys for encryption and decryption [4]. Asymmetric systems include RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography). Based on the way in which the plaintext is processed, they are categorized as Block ciphers and stream ciphers. Christo Ananth et al. [8] proposed a system which is an innovative congestion control algorithm named FAQ-MAST TCP (Fast Active Queue Management Stability Transmission Control Protocol) is aimed for high-speed long-latency networks. Four major difficulties in FAQ-MAST TCP are highlighted at both packet and flow levels.

1.2.1 ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES replaced DES (Data Encryption Standard) which was becoming vulnerable to brute force attack. AES can be implemented in hardware and software, as well as in restricted environments like a smart card, and offer good defences against various attack techniques. Its successful use by the U.S. government led to widespread use in the private sector, leading AES to become the most popular algorithm used in symmetric key Cryptography. AES has been an ideal choice for software applications, firmware and hardware that require either low-latency or high throughput, such as firewalls and routers. It is used in many protocols such as SSL/TLS and can be found in most modern applications and devices that need encryption functionality

1.2.2 ELLIPTICAL CURVE CRYPTOGRAPHY (ECC)

Public key cryptographic algorithms (asymmetric key algorithms) play an important role in providing security services like Key management, User authentication, Digital signature etc, Public Key cryptography systems rely on the hardness of mathematical problems like the integer factorization problem (RSA), the discrete logarithm (DH) to name a few. The main problem of conventional public key cryptographic systems is that the key size has to be sufficient large in order to meet the high-level security requirement. This results in lower speed and high band width requirement. Elliptic Curve Cryptography is a better choice, which depends on another mathematical problem called Elliptic Curve Discrete Logarithm Problem (ECDLP). The greatest advantages are smaller key size, and therefore better bandwidth, faster and more efficient cryptographic keys . ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. To break ECC, one must compute an elliptic curve discrete logarithm, and it turns out that this is a significantly more difficult problem than factoring. As a result, ECC key sizes can be significantly smaller than those required by RSA yet deliver equivalent security with lower computing power and battery resource usage making it more suitable for mobile applications than RSA, and today, many manufacturers, including 3COM, Motorola, Siemens, and VeriFone have included support for ECC in their products.[6][7][8][9]

1.2.3 DNA BASED CRYPTOGRAPHY

The DNA cryptography is a new and very promising direction in cryptography research. DNA can be used in cryptography for storing and transmitting the information, as well as for computation. Although in its primitive stage, DNA cryptography is shown to be very effective. Currently, several DNA computing algorithms are proposed for cryptography, cryptanalysis and steganography problems, and they are very powerful in these areas.

Some algorithms given for DNA Cryptography have limitations that they still use modular arithmetic cryptography at some steps, or are biological laboratory experiment based, that they are not suitable for digital computing.

One algorithm seemed to be fascinating, as it follows the Central Dogma of Molecular Biology (CDMB) concept so closely, for encryption and decryption [10]. However, this algorithm was implemented in ordinary encryption environment only.

The classic view of the central dogma of biology states that "the coded genetic information hard-wired into DNA is transcribed into individual transportable cassettes, composed of messenger RNA (mRNA); each mRNA cassette contains the program for synthesis of a particular protein (or small number of proteins)."

Nucleobases are the basic building blocks of deoxyribonucleic acid (DNA) and ribonucleic acid (RNA). The primary, or canonical, nucleobases are cytosine (DNA and RNA), guanine (DNA and RNA), adenine (DNA and RNA), thymine (DNA) and uracil (RNA), abbreviated as C, G, A, T, and U, respectively. Because A, G, C, and T appear in the DNA, these molecules are called DNA-bases; A, G, C, and U are called RNA-bases. Uracil and thymine are identical except that uracil lacks the 5' methyl group. Adenine and guanine belong to the double-ringed class of molecules called purines (abbreviated as R). Cytosine, thymine, and uracil are all pyrimidines (abbreviated as Y). This Central Dogma of Molecular Biology is used for data encryption/decryption process to get a secure cryptographic system.

In this work, LEACH Protocol has been selected to implement DNA Cryptography in Wireless Sensor Network (WSN) due to their popularity, their advantages like increased life time of the Sensor Network, self-organizing and adaptive clustering that uses randomization. LEACH is also a distributed system, and does not require a global knowledge of the network. Performance parameters are compared with two other most popular Encryption Schemes (AES and ECC), to represent both Symmetric and Asymmetric Encryption Schemes respectively

II. RELATED WORKS

The encryption-decryption techniques devised for traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [11],[12], [13], [15], [15].

In their paper named “Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs”, authors states that they have implemented elliptic curve point multiplication for 160-bit, 192-bit, and 224-bit NIST/SECG curves over GF (p) and RSA-1024 and RSA-2048 on two 8-bit microcontrollers, breaking the common belief that Strong public-key cryptography is often considered to be too computationally expensive for small devices if not accelerated by cryptographic hardware.[16]

AES implementation in WSN is documented in [17], and this paper presents a performance and energy consumption analysis of three AES implementations: (1) exclusively software AES using the original Rijndael algorithm, (2) exclusively software AES using an optimized table lookup AES and (3) hardware supported AES using the Chipcon CC2420 RF transceiver chip.

Following the land mark paper published by Adelman in the Science Journal in 1994, by solving an instance of the directed Hamiltonian path problem [18], many Cryptographic algorithms also were suggested, with varying degree of closeness to the “Central Dogma of Molecular Biology (CDMB).[19][20][21][22][23][24][25]

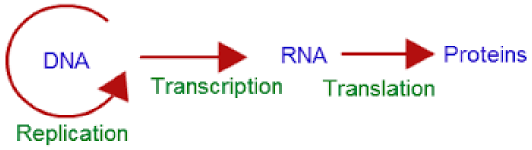

Fig. 2 Schematic diagram of Central Dogma of Molecular Biology

In [10] Noorul Hussain et,al had articulated few criteria to be satisfied by a DNA Encryption algorithm. An algorithm based on the Central dogma of Molecular Biology was also proposed in the same paper. However, this algorithm was implemented in ordinary text files only. This particular Algorithm has been implemented in this work, and compared with both AES and ECC Encryption schemes in WSN under LEACH Protocol.

III. PROPOSED SYSTEM

The Hardware limitations, and the application areas of Wireless Sensor Networks pause different kinds of security issues in WSN. Cryptography has been a powerful tool to address some of these. Both Symmetric Key Algorithms and Asymmetric Key Algorithms have been used in WSN.[26][27]

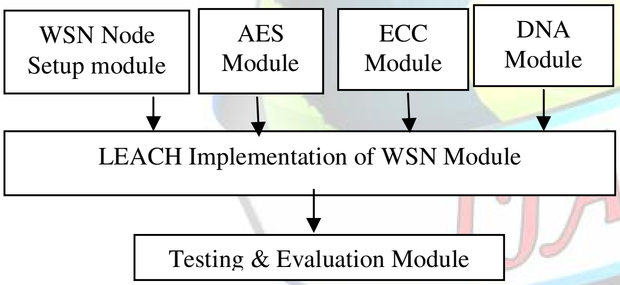
WSN Node Setup module
AES Module
ECC Module
DNA Module
LEACH Implementation of WSN Module
Testing & Evaluation Module

Figure 3. System Architecture

3.1 SYSTEM ARCHITECTURE

The proposed system consists of 4 Modules having 1. A LEACH Clustering module, 2. An AES module,3. An ECC Module and 4. A DNA Encryption Module. A data structure for String matrix has been presented in [28] as the basis for the DNA decoding, encryption and decryption algorithm proposed in [10] is implemented in C++

IV. SYSTEM IMPLEMENTATION

4.1 Hardware/Software requirements and tools

Coding and testing was done on an Intel i5 6200U CPU@2.3GHz based Desktop with 8GB RAM & 4GB NVIDIA GEFORCE Graphics Card with 4GB RAM, Running VMWare Workstation9 under 64Bit Windows 10., with Red Hat Enterprise Linux 6 with 1GB RAM. Implementation of the system was done with Network Simulator-2 version 2.34. NAM (Network Animator) is used for viewing network simulation traces and real world packet trace data. During an NS-2 simulation, we can produce topology configurations, layout information, and packet traces using tracing events in NS2.

When a trace file is generated, it can be animated by NAM [29]. XGRAPH in ns2 is used to plot the network parameter characteristics like throughput, delay, jitter, latency etc. AWK, which is another programming language designed for text processing, is typically used as a data extraction and reporting tool. It is a standard feature of most Unix-like operating systems. After the Installation of NS-2 (ns-allinone-2.34) [30]. Installation of LEACH Protocol in NS-2 with MIT Patches, [31]. Installation of DNA Encryption/Decryption Patches, Coding and Testing & Evaluation is done [32].

V. RESULT ANALYSIS

The DNA based Cryptographic Algorithm has been adapted into the Clustered (LEACH) Wireless Sensor Network environment with 75 Nodes and 5 Clusters. Performance of this DNA based encryption scheme has been compared with Advanced Encryption System (AES), and Elliptic Curve Cryptography (ECC), which is also implemented in the same LEACH Protocol with 75 Nodes, under the identical test conditions.

Performance of a Cryptographic Algorithm can be measured by analyzing the following characteristics of an algorithm under study.

1. Encryption time
2. Decryption time
3. Energy Consumption

A.Encryption Time:

In this, encryption time with varying file size has been computed and the result is tabulated as shown in Table1

It shows an improvement of 5 to 11% when compared to ECC and 8 to 17% improvement when compared to AES, depending on various file sizes.

S No	File Size in KB	Encryption Time in micro seconds		
		AES	*ECC*	*DNA*
1	1	256	267	232
2	10	2854	2634	2334
3	50	12721	11502	10592
4	100	21331	20561	19531

Table 1. Comparison of Encryption time of AES, ECC & DNA under LEACH

B. Decryption time:

In this, decryption time with varying file size has been computed and the result is tabulated as shown in Table 2

It shows an improvement of 3 to 8% when compared to ECC and 4 to 14% improvement when compared to AES, depending on various file sizes

S No	File Size in KB	Decryption Time in micro seconds		
		AES	*ECC*	*DNA*
1	1	189	189	173
2	10	1721	1712	1652
3	50	8932	7932	7653
4	100	15908	15526	14356

Table 2. Comparison of Decryption time of AES, ECC & DNA under LEACH

C. Average Energy Consumption

Energy consumption in a wireless network environment is very crucial, as each node is limited in its power. Low power consumption by a network implies higher residual energy, and a longer life for the nodes. Table 3 shows the comparison

S No	File Size in KB	Energy Consumption in in joules		
		AES	*ECC*	*DNA*
1	20	6.23563	6.12343	6.02343
2	30	7.12233	7.04335	6.94335
3	40	8.13921	8.04521	7.64521
4	50	8.92432	8.75323	8.45323
5	60	9.27892	9.07452	8.87452

Table 3. Comparison of Average Energy Consumption AES, ECC & DNA under LEACH

VI. CONCLUSION AND FUTURE WORK

DNA based Cryptography is adapted and simulated in a Clustered Wireless Sensor Network under LEACH protocol. Performance evaluation in terms of Encryption time, Decryption time, and average energy consumption are compared and the results are tabulated with two other popular encryption schemes: AES, ECC and DNA Encryption Schemes, as a representatives of both Symmetric and Asymmetric key encryption methods, with a total of 75 Nodes. The work has been implemented in NS-2 under Linux Operating System.

In terms of the Encryption time, irrespective of file sizes, better encryption time is obtained for the DNA decryption, followed by ECC, and AES.

In terms of the Decryption time better result obtained for the DNA decryption, followed by ECC, and AES.

In the case of Energy Consumption, which is another very crucial parameter in a Wireless Sensor network environment, again, the AES system consumed much more energy than ECC, while DNA scheme consumed the least, with a significant variation from AES.

This work, therefore shows that DNA Encryption/Decryption algorithm outperforms both ECC and AES Encryption/Decryption algorithms, in a Clustered Wireless Sensor Network under LEACH Protocol.

However, this work is limited in the sense that it is done in a simulated environment with NS-2 only. As a future work, this work has to be implemented in real time environment with Hardware to see the actual performance, and its viability in real life applications.

References

[1] White paper on Wireless Sensor Networks by National Instruments available @ http://www.ni.com/white-paper/7142/en J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] C Siva ram Murthy, B S Manoj, "AdHoc Wireless Networks – Architectures and Protocols". Pearson Education, Inc.2014, Pages 650 – 655

[3] Wendi B. Heinzelman, Anantha P. Chandrakasan, and Hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks, IEEE Transactions on Wireless Communications", Vol. 1, No.4, October 2002. Page 660 -669

[4] Mark S Merkow, Jim Breithaupt, "Information security – Principles and practices" Pearson Education, Inc. 2011. Pages 264 – 269

[5] Bruce Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C", Wiley Computer Publishing, John

[6] William Stallings "Cryptography and Network Security- Principles andpractice" 5e Pearson Education Inc. 2011, chapters 2-5

[7] Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall PTR 2003, Chapters: 7-10

[8] Christo Ananth, S.Esakki Rajavel, I.AnnaDurai, A.Mydeen@SyedAli, C.Sudalai@UtchiMahali, M.Ruban Kingston, "FAQ-MAST TCP for Secure Download", International Journal of Communication and Computer Technologies (IJCCTS), Volume 02 – No.13 Issue: 01 , Mar 2014, pp 78-85

[9] William Stallings "Network Security Essentials- Applications and Standards" 4e Pearson Education Inc.2013 Chapters 2, 3.

[10] Noorul Hussain Ubaidur Rehman ,Chithralekha Balamurugan, Rajapandian M, "A Novel DNA Computing based Encryption and Decryption Algorithm" International Conference on Information and Commn. Technologies 2014, Elsevier

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges"ICACT 2006, ISBN 89-5519-129-4

[12] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS:Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534

[13] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534Wiley & Sons, Inc.1996Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[14] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets,M.,and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 – 201.

[15] Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

[16] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, Sheueling Chang Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs" Sun Microsystems Laboratories, http://www.research.sun.com/projects/crypto

[17] Fan Zhang, Reiner Dojen, Tom Coffey, "Comparative performance and energy consumption analysis of different AES implementations on a Wireless Sensor network Node

[18] Leonard M Adleman, "Molecular Computation of Solutions to Combinatorial Problems", Science, vol. 266, pp. 1021-1024, 1994.

[19] Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang. An encryption scheme using DNA technology. In: Proceedings of the 3rd International Conference on Bio-Inspired Computing: Theories and Applications; 2008 Sep 28 – Oct 1; United States. IEEE; 2008. P. 37-42.

[20] Kang Ning. A Pseudo DNA Cryptography Method. http://arxiv.org/abs/0903.269; 2009

[21] Qiang Zhang, Ling Guo, Xianglian Xue, Xiaopeng Wei. "An image encryption algorithm based on DNA sequence addition operation". Proceedings of 4th International Conference on Bio-Inspired Computing: Theories and Applications. IEEE; 2009; 16-19.

[22] Souhila Sadeg, Mohamed Gougache, Mansouri N, Drias H. "An encryption algorithm inspired from DNA". Proceedings of the International Conference on Machine and Web Intelligence. IEEE; 2010; p.344-349

[23] Sherif T Amin, MagdySaeb, Salah El Gindi. "A DNA-based Implementation of YAEA Encryption Algorithm". Proceedings of the International Conference on Computational Intelligence. IASTED; 2006; p.120-125.

[24] Xing Wang, Qiang Zhang, 'DNA computing- based cryptography',IEEE.2009, pp. 67-69.

[25] Zhang, Qiang, Wang, Qian, Wei, Xiaopeng. "A Novel Image Encryption Scheme based on DNA Coding and Multi-Chaotic Map". Advanced Science Letters; 2010; 3:447-451.

[26] Xueying Zhang,Howard M Heys, and Cheng Li "Energy Efficiency of Symmetric key Cryptographic Algorithms in Wireless Sensor Networks", 25th Biennial symposium on Communications IEEE, pp168-172,2010

[27] Gustavo S. Quirino, Admilson R. L. Ribeiro, and Edward David Moreno, "Asymmetric Encryption in Wireless Sensor Networks" http://www.intechopen.com/books/wireless-sensor-networks-technology-and-protocols/asymmetric-encryption-in-wireless-sensor-networks.

[28] Noorul Hussain Ubaidur Rehman ,Chithralekha Balamurugan, ,Rajapandian M, "A Novel String Matrix Data Structure for DNA Encoding Algorithm" International Conference on Information and Communication Technologies 2014, Elsevier

[29] Kevin Fall, Kannan Varadhan Editors, "The ns Manual", the VINT Project, 2011

[30] https://en.wikipedia.org/wiki/AWK

[31] Dale Dougherty & Arnold Robbins; "SED & AWK Programing", 2e,1997, Oreilly

[32] Arnold Robbins, "Effective awk Programming", 3e, 2001, Oreilly