International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 3157-3164
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

AN HONEY ENCRYPTION BASED EFFICIENT SECURITY MECHANISM FOR WIRELESS SENSOR NETWORKS

P. Lourdu Gracy, D. Venkatesan

Department of Computer Science and Engineering, SASTRA Deemed to be University, India

ABSTRACT

The Wireless Sensor Networks (WSN) security has a major issue in the current era. The data need to be transmitted in a secure way between two nodes,for that each node information need to be encrypted. Hence the Honey Encryption (HE) algorithm is used in WSN. Here seeds are used, contains various words in it. While attackers encrypt the data using a wrong cipher key, HE will return a honey message (i.e. fake plain-text). This text may seem like legitimate but they are actually not. So attacker may end up witha wrong message. Our experimental results,shows that Honey Encryption gives better performance when compared with other algorithms.

Keywords: WirelessSensor Network, Honey Encryption, Seeds, Distribution Transforming Encoders, cipher key.

1. INTRODUCTION

Wireless Sensor Networks (WSN) iscome up with both a significantly advanced category in the IT ecosystem and it is also a rich territory of an effective research on networking, distributed algorithms, data management, social factors and security [4]. The primitive notion of Sensor networks indicates a heterogeneous structure incorporate with teeny sensors and actuators with general-purpose computing aspect. The network basically consists of thousands of low power, economical and self-organizing sensor nodes set up to monitor and its influence on the situation [1][4]. Nowadays sensors are used for tracking pressure, humidity, temperature, noise levels, vehicular movement etc. [4].

The characteristic of sensor networks is restricted power supplies, restraint energy, low bandwidth and limited memory sizes. In case of WSN, the transmission of signals sends from one sensor to another via wireless transceivers. Hence manipulating of signals are much easier for an intruder. So securing that data needs encryption algorithm [4]. The main target of security functionalities in WSN is to preserve the resource and information from attacks. The security obligation in WSNcomprises:Confidentiality, Authentication, Integrity,and Availability [1]. Even though security is also a mandatory but we have to consider about an energy required for generating. Wireless networks are liable to attacks due to the broadcast situation of the transmission intermedia [3].

In WSN, data transferred from one sensor to another sensor need to securely transfer. Hence security-related algorithms are mandatory. In computer environment they are various algorithms are presented for securing the data. An encryption algorithm is majorly classified as Symmetric - key algorithms (e.g. AES, DES, RC_3, RC_4) and Asymmetric-key algorithms (e.g. RSA, DSS, Rabin). In a symmetric-key algorithm,both sides use the same key for encryption and decryption. But for an asymmetric-key algorithm,two types of keys used the namely private key and public key to secure the data.If the keys used for encryption was secured then the data must be immensely secured. Both symmetric-key and asymmetric-key algorithms are needed to satisfy that the generated keys must be secure [6].

Symmetric-key encryption algorithms are the most powerful cryptographic solution for an application. So this paper addresses an encryption using symmetric-key. Based on that an encryption is done via Honey Encryption algorithm to secure the data. Our schema shows that even though an attacker may found out the key they will end up with a wrong data. An alternate word chooses for a correct word that is incorporate in seeds. This makes the system more secure and efficient.

This paper is discussed in the following sections. Related works are explained in section 2. The proposed methodology is explained in section 3. In section 4, experimental results and analysis are explained and conclusion of the proposed system in section 5.

2.RELATED WORKS

The proposed methodology uses a honey encryption and dynamic prime number to secure the data collected from the sensor nodes.These related works indicate various techniques that are relevant to the proposed system.

To authenticate the message is pivotal to avoid a false response that may be invoked by a message. A strong cryptographic system needs to ensure security. For that, a Multivariate Cryptographic Schema is used to enhance throughput, reduce the average delay and diminish the memory consumption and [5]. To construct an effective key generation a chaotic encryptionis used, visor an information from attackers. It against brute force, phishing, man-in-middle, fault attack and reduce logical complexityin WSN [8].

To preserve data integrity and data privacy an AI tree (Authenticity and Integrity tree) and OPSE (Order-Preserving Symmetric Encryption) is used. But for a stored data an authentication pattern may leak and makes the system vulnerable. Hence an Order Encryption Mechanisms used to resists DOS attack on the storage nodes via a wireless channel. For that SER mechanism is used to resists attackers from gaining the information that stored in the storage nodes[9].HRES (Homomorphic Re-Encryption Scheme)the system is used to preserve both data confidentiality and data privacy.To achieve this various operation done over the ciphertexts and have flexible control access over the ciphertext. This makes the system more efficient, effective and secure [11]. The Cryptographic Tools are also used to protect both data confidentiality and data integrity among the nodes. It is used in a military application because there the BS (Base Station) continuously gather compatible data from each node around the environment [13].

3. PROPOSED METHOD

Even though today various solutions for security comes across but confidentiality and integrity faces some challenges. In order to improve the confidentiality and integrity of a system,a honey encryption algorithm is used for this problem. And also it improves the efficiency and security of the system.

3.1 HONEY ENCRYPTION

By using the honey encryption algorithm, an attackers prediction goes wrong but it produces the same result as a real one. Because each faulty hypothesis brings about a plausible-looking outcome, hence the attacker is confused by honey encryption [7].

3.1.1 DISTRIBUTION TRANSFORMING ENCODERS (DTE)

The Distribution Transforming Encoders (DTE) is the preeminent idea behind a classic honey encryption approach. By using DTE honey encryption maintain the space of plaintext. For message *M*, the probability distribution for the message space is*p*.

The DTE divides the message *M* as an*N* bit seed $S \in \{0, 1\}^N$ anddecodesby using inverse DTE mechanism *decode (S) =M*. The internal architecture of the honey encryption incorporates DTE encryption and decryption. The following algorithms describe the flow of honey encryption.

Honey Encryption Algorithm

$H \leftarrow \text{Enc}(K, M)$
$S \leftarrow \$\ encode\ (M)$
$R \leftarrow \$\ \{0, 1\}\ n$
$S' \leftarrow H(R, K)$
$C \leftarrow S' \oplus S$

Honey Decryption Algorithm

$H \leftarrow \text{Dec}(K, (R, C))$
$S' \leftarrow H(R, K)$
$S \leftarrow C \oplus S'$
$M \leftarrow decode(S)$
Return M

H is a cryptographic hash function, *K* is a key, *M* is a message, *C* is a ciphertext,*R*is a random string,*S*is a seed and ←$ indicates Honey Encryption algorithm may use some number of uniform random bits.For encrypting the plaintext message *M*, the honey encryption encodes the plaintext *M* to *S* finally *S* is encrypted by a key value *K*via proper symmetric encryption algorithm. The steps given in the honey encryption clearly shows high message resumption security is provided. The above method is described by a favorite's fruits example. It contains

three fruits namely Banana, Jackfruit,and Mango. These fruits are encrypted in a form of two-bit strings like {00, 01, 10, 11} etc.

This example is explained via honey encryption in fig.1. Let's assume Alice need to encrypt his cherished fruits *M*=Jackfruit, it needs to be sent to Bob using a secret key *K*=0000 is also shared with Bob. Then Alice constructs the DTE for his favorite fruits that map with the message *M*intostring space of 2 bits {00, 01, 10, 11}. For example, the Alice encoded the message Jackfruit, having 01 as a value. Before that Banana have 00 as a value and Mangohave either 10 or 11 as a value which may be chosen randomly.

A random number *R* is selected by Aliceand calculates$S=H(R,K)$. Based on *K* value the equation is$S'=(R, 0000) =11$ and he computes$C=11\oplus01=10$. That *C* value is sent to Bob.

In another end, Bob decrypts*C*value by the key value sends from Alice (i.e. *K*=0000). Hence $S'=(R, 0000) =11$ and $S=C\oplus S' =10\oplus11=01$ = Jackfruit and it is successfully retrieved by Bob. If an attacker Eve attempts to decrypt the message, he actually doesn't know what key value is used by Alice while encrypting. So he infers the key value as 1432, $H=(R, 1432)=00$ then $S''=C\oplus S'=10$,by using S'''' value an attacker decrypts(10) = Mango. By this, the attacker ends up in a wrong data.

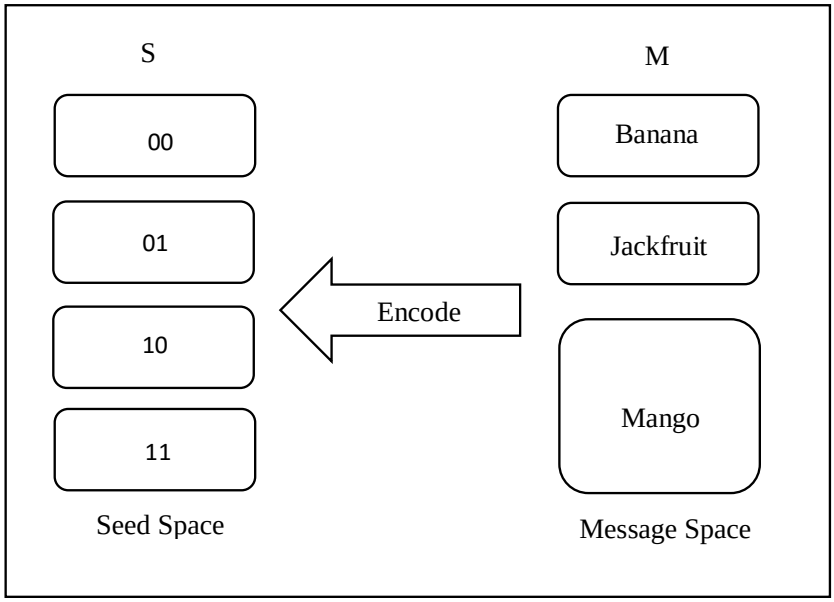


Fig. 1. DTE Mapping

Finally the message "Banana" (withp_m= 1/4) maps to 00, "Jackfruit" (with p_m = 1/4) maps to 01, and"Mango" (withp_m= 1/2) maps to {10, 11}; p_m is a probability distribution for the message space.

4.EXPERIMENTAL RESULTS AND ANALYSIS

The proposed honey encryption schema is plausible in Wireless Sensor Network. Here, the efficiency of the proposed schema is evaluated for each data transfer. To evaluate our schema a COOJA simulation environment is used for node deployment in Wireless Sensor Network.

4.1 SENSOR NODE PERFORMANCE

The sensor node performance is calculated via COOJA simulator in Contiki OS. For an experimental analysis sky mote sensor node is chosen. An open source OS (Operating System) is used for calculating node performance in WSN via Contiki [10]. COOJA simulator shows a network simulation with the real-time features.

The overall node data transfer is shown in fig.2 in the radio environment. Here, how the data transfer from one node to another node is shown via radio traffic. Overall power consumption for a sky mote while generating keys is shown in fig 3 for average sensor nodes.The battery consumption of average sky mote is also reduced while generating the key and data exchange between the sensor nodes when power consumption is decreased.

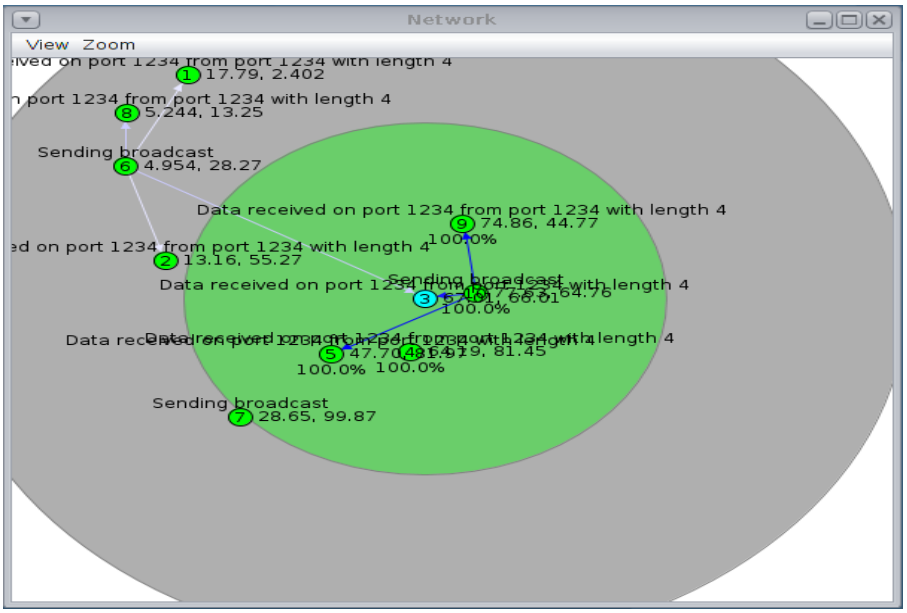


Fig. 2. Data Transfer

The data transfer among the nodes is based on port number and IP address ofeach node. Both power consumption and battery consumption of sensor nodes is average of five sky mote nodes.

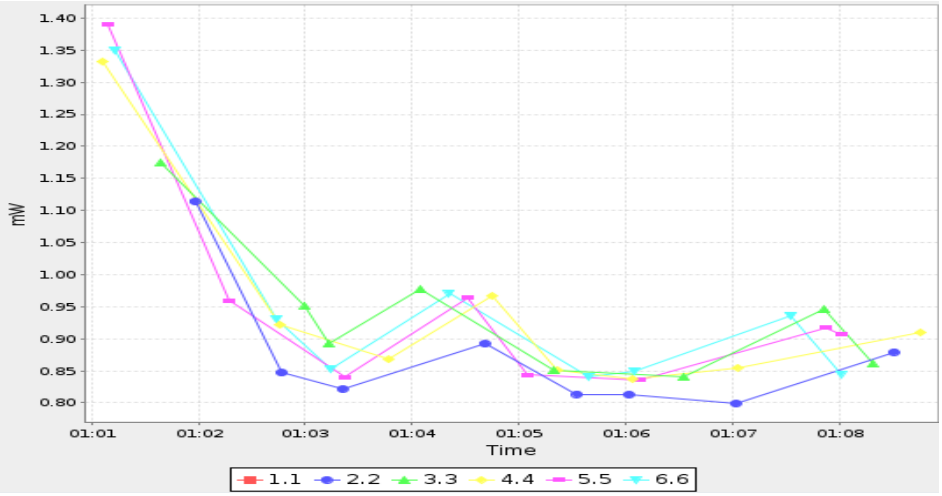


Fig. 3. Power Consumption

The power consumption is reduced because of nodes are in the inactive state (i.e. while data transfer nodes are an inactive state). In fig 4. Shows a comparison of various security algorithms. The performance is better when compared with DPBSV [12] and AES [2] algorithm.

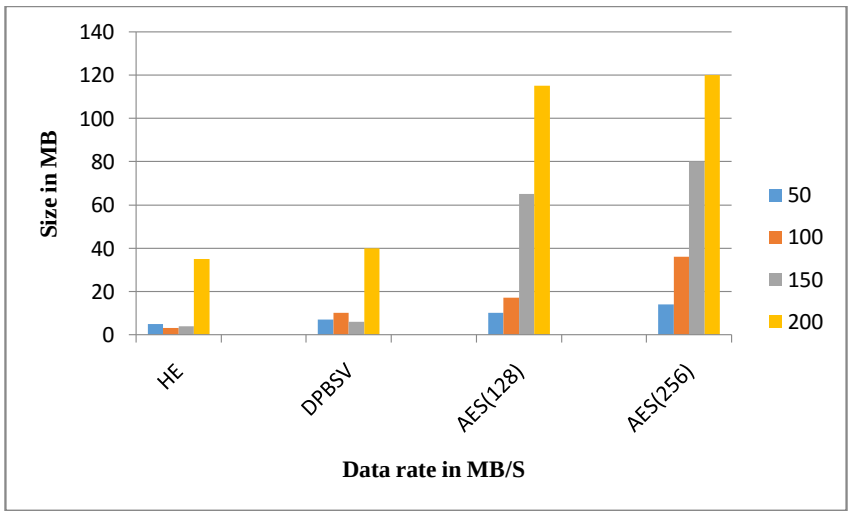


Fig. 4. Performance Comparison of various algorithm

5. CONCLUSION

The main issue in WSN (Wireless Sensor Network) is the security of the data. In the proposed work, the security of the data is enhanced and defends brute force attack. Here, seed space is used for encoding the data via bit strengthen the encryption is done for the message space using seed space. By using this, confidentiality, integrity is maintained in the system. While compared

to other algorithms, honey encryption gives a better result. In future, this technique can be used in the Internet of Things for secure data communication.

REFERENCES

[1]Madhumita Panda,Security in Wireless Sensor Networks using Cryptographic Techniques, American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936.
[2] PUB, NIST FIPS, 197: advanced encryption standard (AES), in: Fed. Inf. Process. Stand. Publ., vol.197, 2001, 441-0311.
[3] Abhishek Jain, Kamal Kant, M. R. TripathySecurity Solutions for Wireless Sensor Networks 2012 Second International Conference on Advanced Computing & Communication Technologies978-0-7695-4640-7/12 $26.00 © 2012 IEEE
[4] Al-Sakib Khan Pathan,Hyung-Woo Lee, ChoongSeon Hong, Security in Wireless Sensor Networks: Issues and Challenges, in: International Conference on Advanced Communications Technology,ISBN 89-5519-129-4, 2006,pp.1043-1048.
[5] Pradheepkumar Singaravelu , Shekhar Verma, Performance analysis of multivariate cryptosystemschemesfor wireless sensor network, Computers and Electrical Engineering 39 (2013) 1880–1893.
[6] D. Puthal, S. Nepal, R. Ranjan, J. Chen DPBSV, An efficient and secure scheme for big sensingdata stream, in: Proceedings of 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE TrustCom-15, 2015,pp.246–253.
[7] NahriSyeda Noorunnisa1, Dr. Khan RahatAfreen, Review on Honey Encryption Technique, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.
[8]Priyanka K. Babar, Vishal P. Bhope, Design and Implement Dynamic Key Generation to Enhance DES Algorithm, www.ijraset.com Volume 4 Issue VII, July 2016IC Value: 13.98, ISSN: 2321-9653.
[9] Yao-Tung Tsou , Chun-Shien Lu,Sy-Yen Kuo, SER: Secure and efficient retrieval for anonymous range query in wireless sensor networks, Computer Communications 108 (2017) 1–16.
[10] Contiki operating system official website, http://www.contiki-os.org/(accessed on: 04.08.2017).
[11] Wenxiu Ding, Zheng Yan, Robert H. Deng,Encrypted data processing with Homomorphic Re-Encryption, Information Sciences 409–410 (2017) 35–55.
[12] N. Penchalaiah, R. Seshadri, Effective comparison and evaluation of DES and rijndael algorithm (AES), Int. J. Comput. Sci. Eng. 2(5) (2010) 1641–1645
[13] Omar Rafik Merad Boudia, Sidi Mohammed Senouci, Mohammed Feham, A novel secure aggregation scheme for wireless sensor networksusingstateful public key cryptography, Ad Hoc Networks 32 (2015) 98–113.