Time Execution Constraints using Intricate Encryption and Decryption Process for Secure Data Transmission

M. Laxmi Jeevani
PG Scholar
Jawaharlal Nehru Technical University, Jagitial

Kuldeep Chouhan, Ph.D.
Associate Professor, Department of CSE
Medak College of Engineering and Technology

ABSTRACT
The encryption and decryption process is widely investigated and developed for a robust data security which is challenging to crack. Many researchers proposed different types of encryption and decryption algorithms such as DES, AES, RSA, etc., the proposed algorithms are encountered such as deficiency of stoutness and significant amount of time added to packet delay and to maintain the node data security in the network. The data security is the process which protects its privacy, integrity and availability. In this work, text data makes secure using encryption to decryption process while the secret key does not match and produce ambiguous message to the user during execution. The results demonstrate the efficiency of the encryption and decryption process in the measurement of time execution variations are presented.

Keywords
Wireless Network Security, Data Encryption and Data Decryption Technique, Time Execution.

1. INTRODUCTION
The wireless network is the emergent technique in area of data processing and communication networks which can consensus the environment to complete specified tasks efficiently and independently due to the vast potential of wireless networks to enable requests that connect the to the cybernetic world. Each node data involves multiple types of memory which have transceiver, power source and accommodate various sensors and actuators [7]. The wireless network security is based on different frame formats, protection level and properties [8,10]. The key appraisal metrics for wireless networks are lifetime, coverage, cost and ease of deployment, security, response time, effective sample rate and temporal accuracy. The wireless network security includes the obstacles and requirements in the data security, organize the attacks and their corresponding defensive measures [11,14]. However, the data protocol should have resilient against false data inoculated into the network by malicious node data and bootstrap secure data communication via use of decrypted key establishment mechanisms. The encoding of data is used secure routing, cryptography, access control protocol and dynamic energy to protect node based data and makes robust transmission. The node network interconnection of systems allow the people to do many shared transactions and highly sensitive information is placed over the network which is necessary to protect the information from hackers. The objectives of node network security include, but not limited to are,

(i) ***Availability*****:** Information and systems accessible are usable upon demand by an authorized entity.

(ii) ***Integrity*****:** Safeguarding the information accuracy and completeness of assets.

(iii) ***Confidentiality*****:** It is not disclosed to unauthorized individuals, entities or processes.

(iv) ***Authentication*** - Ensures the reliability of the message by identifying its origin. By authenticating other nodes, cluster heads and base stations are granting a limited resource or revealing information.

Data security issues in homogeneous sensor networks for key management which is an essential cryptographic primitive upon which other node data security primitives are raised. Probabilistic encrypted key distribution is an auspicious scheme for key management in wireless networks which ensure the probability that each sensor has at least one shared key with a neighbor node data (as encrypted key-sharing probability) should be high.

1.1 Significance of Encryption in Wireless Networks
Wireless network increasing wide variety of applications such as climate change, environmental monitoring, traffic monitoring, etc. it provides security through by the symmetric key techniques, asymmetric key techniques and hash function. It constrained in terms of computing, communication and battery power. Secret-key cryptography uses a single secret key for both encryption and decryption as shown in Figure 1.

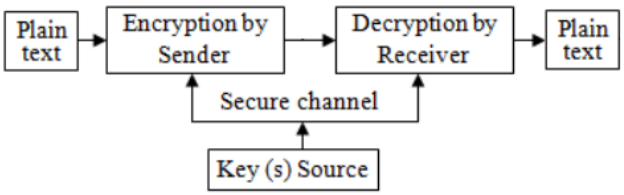

Fig. 1 Secure data communication model

The wireless networks require protection against eavesdropping and modification of propagated data packets [5]. It implies a consistently varying level of overhead in the form of increased code size, packet size, processor usage and effect on the quality of service (QoS) etc. [13]. However, the decision depends on the computation and communication capability of the wireless node data. Since, the node data typically have asymmetric cryptography for many applications and also affect the QoS of the network. It is extremely important to ensure that all known attacks are defended against when designing a security system for a WSN.

1.2 Encryption of Node Data Systems
The node data encryption system works secure and efficient mechanisms to encrypt or decrypt data to provide a level of data privacy that goes elsewhere simple access control. It should be integrated with the operating system for ease of use and flexibility. A storage security framework include immunity from attacks that privileged entities, enabling legitimate remote access to shared encrypted volumes and providing a scalable [2] and transparent encrypted key management scheme.

1.3 Advance Cryptography Algorithm for Data Security Improvement

The encryption/decryption schemes are protecting confidential information then cryptography and provide high level of privacy of individuals and clusters. It allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information node data.

2. PREVIOUS WORK

Vishwa Gupta, et al., [2012] proposed a new cryptography algorithm which is based on block cipher concept. Obaida, et al., [2013] proposed a new approach for complex encrypting and decrypting data which maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme. H. Mohan and R. Raji [2011] proposed an algorithm to improve the security level and increase the performance by minimizing a significant amount of delay time to maintain the data security. Obaida [2012] proposed to increase the security level for real-time application using new key management solution in wireless network. Kocarev, L. and La Jolla [2001] presented chaos-based cryptography which is faster to the spirit of both cryptography and chaos theory. Shih-I Huang et al., [2010] presented a secure encrypted-data aggregation scheme for wireless sensor networks. Li, T., et al., [2006] proposed an efficient scheme for encrypted data aggregation on sensor networks. Uma, G and Sriram [2014] proposed robust encryption algorithm based SHT in wireless sensor networks. Yu Zhang [2012] presented a public key infrastructure for WSN to solve the problem of data security for ensuring the authenticity of the base station. Gurjot Singh and Sandeep [2014] presented the cryptographic schemes that evaluated the different metrics like throughput, jitter, end-to-end delay and energy consumption. N. Li, et al., [2009] proposed a constrained optimization problem and develop heuristics for an efficient privacy algorithm. Bhavin, et al., [2013] presented to explore design of cost efficient secure network protocol which reduces number of key transmission required in symmetric key encryption for rekeying task. Madhumita [2014] presented wireless sensor networks continues to grow and become vulnerable to attacks and hence need for effective security mechanisms.

3. SECURE ENCRYPTED DATA TRANSMISSION

The secure data mechanism includes server, client, embedded mote, transmission medium and cryptographic algorithm. In this work authentication (i.e. prevention of untrusted node data), encryption and decryption module and reacting to dynamic changes, where the node data validates and contains the mechanism to prevent to untrustworthy nodes to the particular client.

3.1 Nodes Dependability

The node dependability of the node data is significant for applications in wireless network. Conventionally, when a node has a failure, it (i.e. data from that node) is usually discarded and the network is simplified with faultless nodes to continue with the normal operation without a tradeoff with the functional coverage of the networks. The physical layer contains the node details and identifies all legitimate hosts accessing the data server and subsequently performs in network. The node data metrics include,

(i) Latency

(ii) Throughput

(iii) Number of collisions among the broadcasting nodes

3.2 Collision-less Multiple Node Interconnections

The multiple nodes interconnected through the node switch, where one node performs as the node station and accepts information from the other node data. Each and every node is assigned with a particular time slot to send/receive data. The node station sends the beep to any one of the nodes connected together indicates that it is ready to accept the information from the particular node within the allotted time slot and after the arrival of beep sound from the station node data, the client node data get ready to sends the data to the station node data. The nodes having data to send will transfer the data to the station in their respective slots using encryption/decryption process is shown in Figure 2.

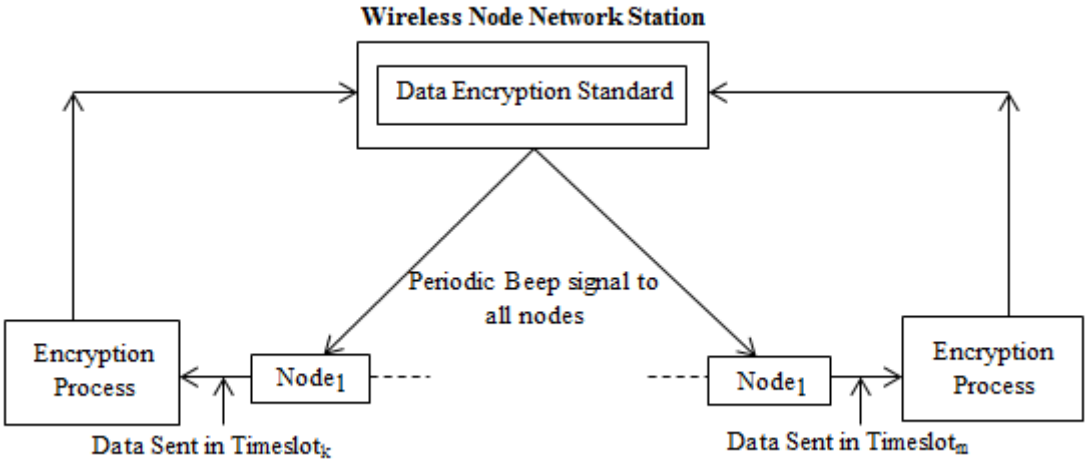

Fig. 2 Transmission of Node Data using DES in Wireless Node Network Station

4. PERFORMANCE ANALYSIS FOR ENCRYPTION AND DECRYPTION

The speed of the performance is required time analysis where the parameters are experimented and measured for both encryption and decryption scheme. The node data security test level is analyzed and performed on the key length algorithm which is given in Table 1.

Table 1 Speed for Encryption and Decryption in different key lengths

Algorithm	Key Length			
Analysis	Proposed Technique	Encryption scheme	Proposed Technique	Decryption scheme
128-bits	0.1815438	0.5402353	0.2490837	0.5207581
256-bits	0.2265183	0.6936481	0.2709861	0.6709456
512-bits	0.2876384	0.8619085	0.2912970	0.7184742

4.1 Correlation Analysis for Secure Data

The correlation analysis generates an isolated position based on the secret value from public key infrastructure. It analyzes the correlations between the public and the private positions, where the correlation coefficients test is used. The correlation coefficients (CC) rules are described by a pseudo-code is as,

if (CC=0)
then
private key table ≠ public key table
else
private key table = public key table

In *CC* analysis indicate different values in the public and private positions. The public and the private key positions are calculated all in the directions (vertical, horizontal and diagonal directions) where the *CC* for the three dimensions has different positions which indicates the public and private positions are not correlated. The positions are,

Private positions - close to 0 and

Public positions - close to 1.

4.2 Node Data Information Entropy

To calculate the entropy $M(Z)$, where

$$M(Z) = \sum_{a-1}^{n} q_a log_2 \left(\frac{1}{q_a}\right) \quad \ldots (1)$$

The entropy $M(Z)$ directed by a pseudo-code as entropy information which is very close to the theoretical value, where

'n' indicates number of attacks and

'a' indicates the entropy attacks that indicates the encryption algorithm is secure upon the different entropy attack.

The procedures of information entropy are shown in Figure 3.

```
if (M(Z) > ideally close to n)
then
    no predictability which threatens the security occurs
else
    if (M(Z) < n
then
    exists a predictability which threatens the security
```

Fig. 3 Procedures of Information Entropy

5. NODE DATA ENCODING FOR SEQUENTIAL TRANSMISSION

The node data from client via server node generates packet data and converts into bytes in wireless network. The data search network location checks the errors then decodes the data for a safe transmission. The data transmission sequence of an encoded packet is transmitted from a node along with the data encoding process as a flowchart is shown in Figure 4.

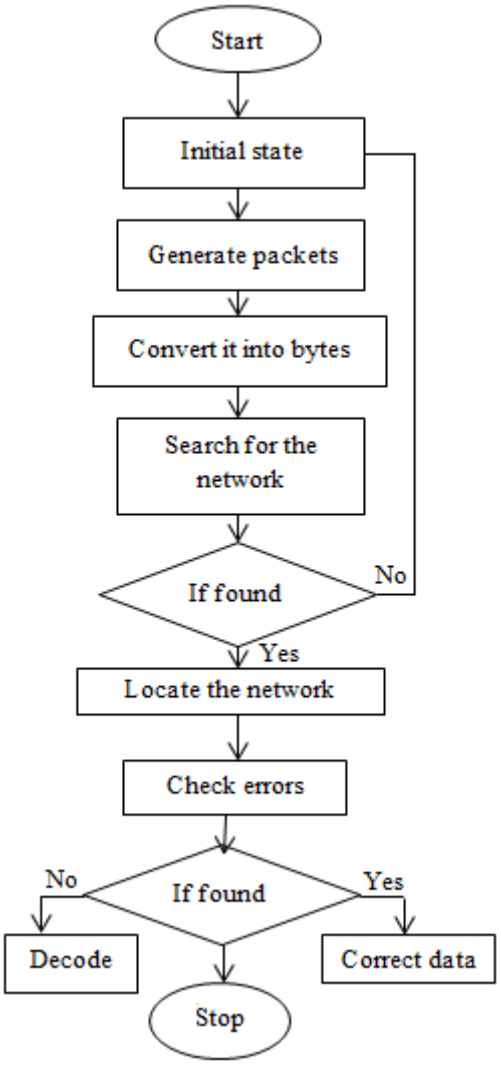

Fig. 4 Node data transmission sequence in packet data encoding

6. IMPLEMENTATION OF DATA TRANSMISSION WITH COMPARISON STUDY

The data performance improvement achieved due to time delay reduction in transmission scheme using encryption to encryption technique is studied (i.e. in Figure 2). The nodes are capable of transmitting packets continuously whenever sufficient node data energy exists. In conventional scheme, when the node data energy of a particular node is poor, the i^{th} packet transmitted by that node cannot reach the next node and thereby goes into a state of repeated timeout/deadlock. This undesirable situation is handled in this work, by generous the self-opts out by a node whenever its node data energy drops and gains energy enough to joins the node network back and continues data transmission from where it left. It is

analogous to the back-off solution used for collision prevention among node data station is shown in Figure 5.

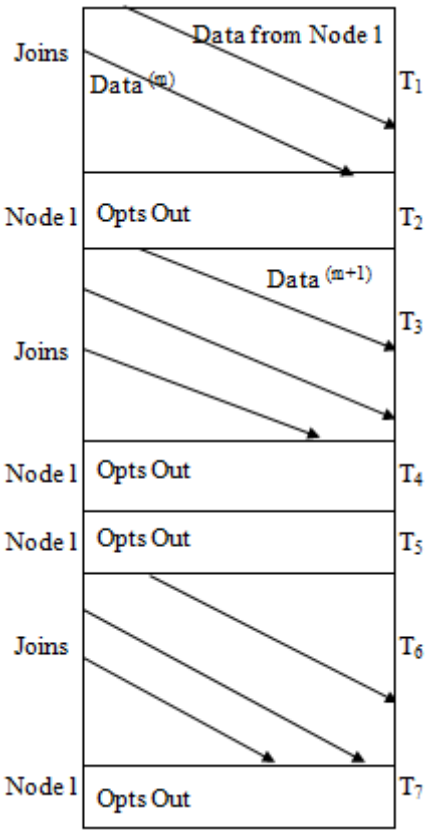

Fig. 5 Node data transmission flow process

7. RESULTS AND DISCUSSION

In this work, the encryption and decryption output is shown the plain text as input which is converted to cipher text through the process of encryption and decrypted the message through the decryption method is shown in Figure 6.

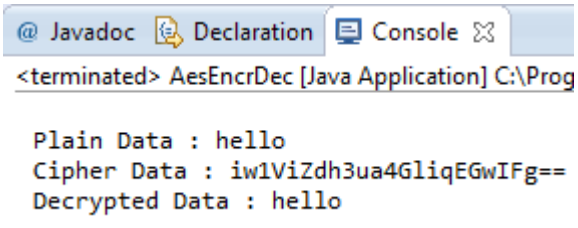

Fig. 6 Text data conversion using DES process

The plane text is converted as cipher text after decryption and make data secure which is shown in Figure 7.

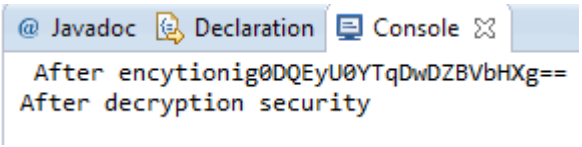

Fig. 7 Secure data after encryption to decryption of data

The secret key is used for encryption to decryption process for conversion of text data, when the secret key does not match and generates error during execution of output is shown in Figure 8.

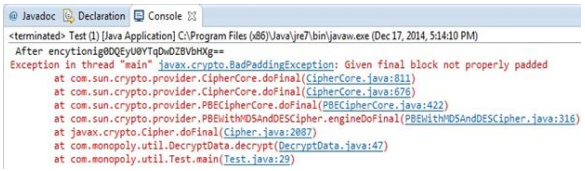

Fig. 8 Thread as error generated in output during execution

7.1 Encryption Time Comparisons of Node Data Security

The node data parameters for data encryption and data decryption time consumption as improved time for data transmission and reduced time delay between node network is experimented as shown in Figure 9 and Figure 10.

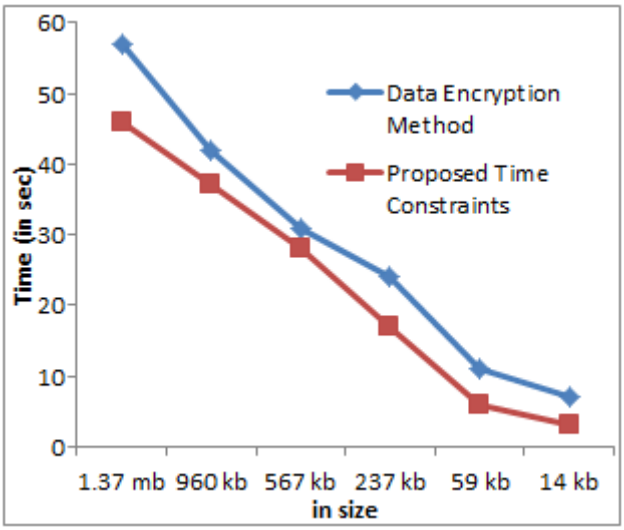

Fig. 9 Data Transmission time comparisons with encryption method

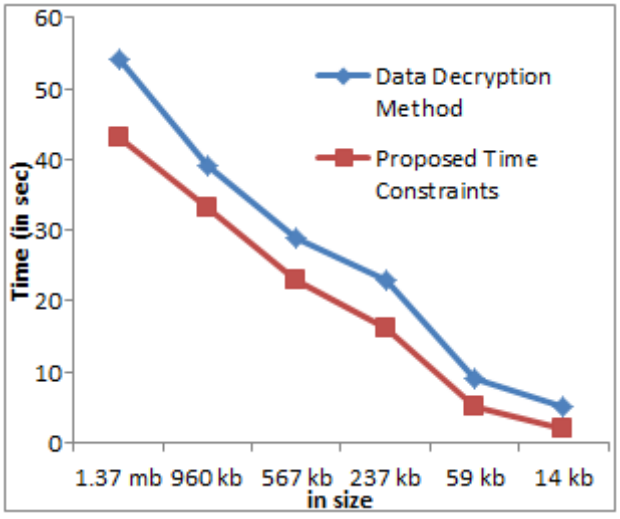

Fig. 10 Data Transmission time comparisons with decryption method

8. CONCLUSION

In this work, the wireless networks continuous grow and widely used in encryption and decryption to consume time to elude unpredicted delay in network. However, it suffers from many constraints such as limited node data energy, data processing capability and data loading capacity, etc. The

approach for intricate encrypting and decrypting node data security is introduced where the proposed algorithm is checked the network location and detect the errors to be securing data against unauthenticated node network is demonstrated. The results are demonstrated the time comparisons between proposed time constraints and data encryption/decryption technique to consume less time and provide enhanced data transmission. To reduce error rate and time consumption hardware implementation is to be used which is possible in embedded linux system in future and deliver robustness security.

9. ACKNOWLEDGEMENT

I thanks to my research supervisor Mr. Uday Kumar and co-supervisor Dr. Kuldeep Chouhan who have been carried out my research work successfully.

10. REFERENCES

[1] Vishwa Gupta, Gajendra Singh and Ravindra Gupta. 2012. Advance cryptography algorithm for improving data security. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, No. 1.

[2] Dripto Chatterjee, Joyshree Nath, Suvadeep Das Gupta and Asoke Nath. 2011. A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm. IEEE International Conference on Communication Systems and Network Technologies.

[3] Obaida Mohammad and Awad Al-Hazaimeh. 2013. A new approach for complex encrypting and decrypting data. International Journal of Computer Networks and Communications. Vol. 5, No. 2.

[4] Mohan, H. and Raji, R. 2011. Performance Analysis of AES and MARS Encryption Algorithms. International Journal of Computer Science Issues. Vol. 8, No. 4.

[5] Obaida Al-Hazaimeh. 2012. Increase the Security Level for Real-Time Application Using New Key Management Solution. International Journal of Computer Science Issues. Vol. 9, No. 3.

[6] Kocarev, L. and La Jolla. 2001. Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine. Vol. 1, No. 3, pp. 6-21.

[7] Shih-I. Huang, E. Shiuhpyng Shieh, E.J.D. Tygar. 2010. Secure encrypted-data aggregation for Wireless Sensor Networks. In Wireless Networks. Vol. 16, No. 4, pp. 915-927.

[8] Li, T., Wu, Y. and Zhu, H. 2006. An efficient scheme for encrypted data aggregation on sensor networks. In proceedings of Vehicular Technology Conference, pp. 831–835.

[9] Uma, G. and Sriram, G. 2014. "Robust encryption algorithm based SHT in Wireless Sensor Networks", International Journal of Distributed and Parallel Systems. Vol. 5, No. 1/2/3.

[10] N. Li, N. Zhang, S. Das and B. Thuraisingham. 2009. Privacy Preservation in Wireless Sensor Networks (WSN): A State-of-the-Art Survey. Elsevier Journal Ad-Hoc Networks. Vol. 7, No. 8, pp. 1501-1514.

[11] Madhumita Panda. 2014. Security in Wireless Sensor Networks using Cryptographic Techniques. American Journal of Engineering Research. Vol. 3, No. 1, pp. 50-56.

[12] Yu Zhang. 2012. The Scheme of Public Key Infrastructure for Improving Wireless Sensor Networks Security. IEEE Conference, pp. 626-629.

[13] Gurjot Singh and Sandeep Kaur Dhanda. 2014. Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes. International Journal of Information Technology and Computer Science. Vol. 8, pp. 32-42.

[14] Bhavin, N. Patel and Neha Pandya. 2013. Secure Data Transfer using Cryptography with Virtual Energy for Wireless Sensor Network. International Journal of Engineering Trends and Technology. Vol. 4, No. 8, pp. 3468-3473.

11. AUTHOR'S PROFILE

M. Laxmi Jeevani was born on July 11th 1992 and got her B.Tech. Information Technology in the year 2013 from St. Martins Engineering College affiliated to JNTU, Hyderabad and pursuing M.Tech in CSE from JNTU, Jagitial. Her area of interest is Network Security and Linux Networking Security.

Kuldeep Chouhan was born on November 12th 1984 and got his M.Tech. and Ph.D. degree in Computer Science and Engineering in the year 2009 and 2014 respectively from Dr. MGR Educational and Research Institute University, Chennai. He has been published Ten International Publications and presented Two International conferences. His area of research is Wireless Network Security, Embedded Linux Networking and Android Apps Security.