Secure Data Transfer using Cryptography with Virtual Energy for Wireless Sensor Network

Mr. Bhavin N Patel[#1], Ms. Neha Pandya[*2]

#PG Student, Parul Institute of Engineering and Technology, Vadodara, Gujarat, India.
**Assistant Professor in IT Department, Parul Institute of Engineering and Technology, Vadodara, Gujarat, India.*

***Abstract*: The wireless sensor network technology is one of the largest data processing and communication networks systems which continuously developed for distributed environment in field of real time application. There are so many factor associated with it's as Data security, operating speed, cost efficiency and additional sensor network constraints. Main consideration is about increase the security over existing attacks without affect the performance and complexity of overall wireless sensor network. Normally, two approach of symmetric key and asymmetric key data encryption technique is applied for it at sensor nodes. So, the proposed work is to explore design of cost efficient secure network protocol which reduces number of key transmission required in symmetric key encryption for rekeying task. In proposed algorithm mainly three steps are performed as key generation, data cryptography and data transmission. First generation of key is done by method of dynamic key approach using virtual energy value of sensor node. Then mechanism of symmetric key block cipher algorithm RC5 is performed for data cryptography. After that encrypted data packet transferred over the network using TCP/IP protocol layer in WSN. It also has performance evaluation to achieved benefit of lightweight symmetric key block cipher algorithm for proposed work in unreliable medium of wireless sensor network.**

***Keywords*: Wireless sensor network security, cryptography with virtual energy, WSN data encryption, symmetric key cryptography for WSN**.

I. INTRODUCTION

The wireless sensor networks are one of the largest growing technologies in area of data processing and communication networks today. It is a distributed intelligent network system which can accord the environment to complete assigned tasks independently and efficiently due to the vast potential of sensor networks to enable applications that connect the physical world to the virtual world. Each node consists of processing capability using one or more microcontrollers, may contain multiple types of memory, have a RF transceiver, have a power source, and accommodate various sensors and actuators [17]. There are many security schemes have been suggested for WSN, but the choice of security model based on different properties, protection level, and frame formats [10]. The key evaluation metrics for WSN are lifetime, coverage, cost and ease of deployment, response time, temporal accuracy, security, and effective sample rate. The major topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security, classify many of the current attacks, and their corresponding defensive measures. However, the protocol should be resilient against false data injected into the network by malicious nodes and bootstrap secure communication via use of key establishment mechanisms. Different security techniques are introduced for designing cost-efficient, energy efficient protocol for wireless sensor network like. Secure routing, cryptography, access control protocol and dynamic energy based encoding.

One of most important research problem in WSN is how to secure the sensor network topology and its communication procedure from potential changes that can be made by malicious nodes inside the existing network. These wireless sensor network are consisting tiny sensor that really suffer the lack of processing capability, memory requirement and battery power utilization. There are many attacks introducing on this infrastructure like Wormhole attack, Sybil attack, selective forwarding, impersonation attack and protocol specific attack on the data packet of communication network. So, design of sensor network should be efficient with different characteristics to deal with physical constrains of configuration. There are several methods that are used by many researchers, after reviewing several papers it is found that variety of technique associated with sensor network to secure data transmission like. Cryptographic algorithm, Network layer protocol, Physical MAC control and routing technique [8]. So, recent advances in technology have paved the way for the design and implementation of new generations of the security algorithms using cryptography technique with dynamic key mechanism lead to perform compatible solution for WSN.

In general term any physical system has two types of different state from which virtual state is referred as very short-lived, unobservable quantum state of system. Normally feature or operation that does not exist but appear to be so in system. Some time virtual energy of any device or sensor is known as residual energy because it's referred as minimal

level of energy store inside this system. As especially for wireless sensor network in every sensor node has certain virtual energy at time of first deployment. So, we can choose this virtual energy value for WSN to generate a secrete key for perform cryptographic algorithm procedure to convert plaintext data in to cipher text data for highly constrained sensor network. This virtual energy value computation is done in reference of transmission, data sensing, encryption, and synchronization activity of sensor mote.

The rest of the paper is organized as follows. Section 2 provides an overview of Background and Related work done in area of WSN security with existing technique. Section 3 presents proposed work scheme and implementation methodology for achieving desired characteristics of WSN system. Section 4 provides result and performance analysis process done for proposed work scheme using standard parameters evaluation. The paper then concludes in section 5, with insight to future work in the field of wireless sensor network security.

II. BACKGROUND & RELATED WORK

In this section we are presented the brief introduction about wireless sensor network and their security constraints to understand their configuration. The aim of project work is to provide an efficient and end-to-end user security mechanism for wireless sensor network and that should not affect the performance, reliability and computation task of sensor network. The whole sensor network represented using layered architecture to represent its different level security aspect. The basic functional security requirement for any WSN application can be classified in terms of Confidentiality, Availability, Integrity, Authenticity, Non-repudiation, Self Synchronization, Robustness and Survivability.

Cryptographic algorithms are an essential part of the security architecture of WSNs, using the most efficient and sufficiently secure algorithm which is an effective means of conserving resources of tiny sensors. When applying any encryption scheme, it's requires transmission of extra bits. It's very useful to provide data security using data encoding patent and compatibility with existing network layer protocols. The cryptographic algorithms used in WSNs are generally categories into two parts: symmetric-key algorithms and Asymmetric-key algorithms. Symmetric key cryptographic mechanisms use a single shared key between the two communicating host which is used both for encryption and decryption. Symmetric key algorithms can be further divided into block ciphers for fixed transformations on plain-text data, and stream ciphers for time varying transformations. It is give a comparison for those encryption algorithms at different settings such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Symmetric key cryptosystems such as the AES, DES, RC4 CAST, RC5 algorithm is used in WSN. In asymmetric public key cryptosystems each node has a public key and a private key. The public key is published, while the private key is kept secret. This asymmetric key cryptography is providing better security in terms of complexity over higher level of attacks. Asymmetric public key cryptosystems such as the Diffie-Hellman key agreement, ECC or RSA signatures are typically too conservative in their security measures but adding too much complexity and protocol overhead to be usable in WSN solutions [6]. The main drawback of this cryptography technique is that it suffers from high computational complexity and communication over head with constraints of sensor nodes.

The traditional method of wireless sensor network security applied with cryptography with two types of encryption key management scheme. There are two fundamental key management schemes as static key and dynamic key for WSN. The major drawback of key management scheme is that it increases communication overhead due to key refresh activity. This method guarantees data freshness as keys are usually kept secret. It also useful in encryption technique to prevents cryptanalysis, since the same plaintext would produce different cipher text [12]. For static key management scheme fixed numbers of key values are already loaded either prior to or shortly after network deployment. This scheme is very easy to implement but more vulnerable with advanced attacking activity. Static key is useful in WSN field where data acquisition not very critical. The dynamic key management scheme performs keying function either periodically or on demand as needed by wireless sensor network. Its provide batter attack resilient than the static key approach due to rekeying task. The disadvantage is that keys being refreshed or redistributed with time existence this increase massage transmission cost and complexity of the network infrastructure.

Here, this is the TABLE I which represents comprehensive discussion about major aspect of different literature based on security issues and counter measure approach to preventing sensor data with previously proposed schemes for WSN.

TABLE I
SUMMARY OF LITERATURE PAPERS

Topic name	Algorithm used	Description
Virtual Energy based Encryption and Keying for wireless sensor networks [1]	RC4 Encryption mechanism	Key management handles via dynamic key approach using sensor residual energy. Study of symmetric key encryption algorithm RC4 and Two operational modes to handle error data.
Implementation of Node Energy Based on Encryption Keying [2]	RC4 Encryption Algorithm	Main goal is to reduce transmission cost and complexity by reduce rekeying task. Perform permutation encryption on data block using RC4 encryption to minimize malicious data.

Potential cipher solution for security in wireless body sensor network [10]	RC5 Encryption algorithm	Implementation done over combination of ASIC hardware prototype and symmetric key encryption. Application for medical and military field
RC5 based Security in wireless sensor networks: Utilization and Performance [6]	RC5 Encryption and C-MAC Authentication	Performance and evaluation done on KLAVI platform to achieved security with lowest energy consumption. Minimum Transmission time, key expansion, encryption and decryption values achieved with various parameters.
Performance Evaluation of CAST and RC5 Encryption Algorithms [7]	CAST Protocol and RC5 Algorithm	Evaluation based on sensor Physical constraints like. Security analysis, encryption speed and power consumption. Result highlight with various data block size, variable length key and different no. of encryption round
A Low Energy Security algorithm for Exchanging Information in WSN [12]	ECC public key, Direct Diffusion Protocol,	One-way hash function applied on symmetric and public key cryptography. Results achievement done using Directed Diffusion protocol.
An Evaluation of Security Protocols on wireless sensor network [8]	LLSP, SPINS, LISP, LED and Tiny sec Protocol	All protocol working over link layer of network. It's useful to evaluate criteria of Key management, re-organization and Scalability.

Finally develop new proposed mechanism, we perform dynamic key creation via use of virtual energy (residual energy) concept of sensor node for optimize energy consumption and reduce rekeying task for symmetric key cryptography.

III. PROPOSED SCHEME & IMPLEMENTATION METHODOLOGY

This section presents the proposed scheme of new cryptographic technique for wireless sensor network using concept of virtual energy for making energy efficient communication network. This design approach directly applied with the existing symmetric key encryption algorithm for achieving efficient performance in term of security.

A. Proposed Mechanism

The objective of this section is to propose a new Advanced Virtual Energy based Encryption and keying scheme for better encryption and improve efficiency with light weight symmetric key Algorithm for WSN. Here, one significant aspect of confidentiality in WSN is entails for designing efficient key management schemes. To resolve the problem of rekeying or refreshing of key value at each transmission inside dynamic key management technique, this concept provide batter security due one key applied on data packet only one time. This is helpful to sensor network for reducing overall complexity and computational cost for it. Also, Fig. 1 VEBEK secure communication framework provides a technique to verify data inside routing network and drop false packets from malicious nodes, thus maintaining the health of the sensor network.

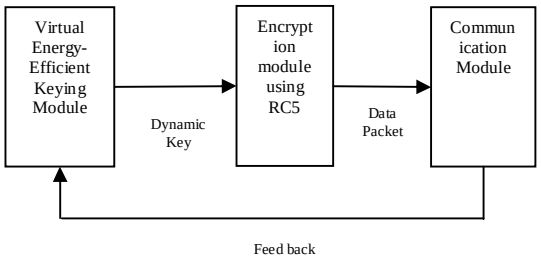

Fig. 1 Proposed scheme of VEBEK approach for WSN

The major characteristic for this VEBEK approach on encryption schema [1] given as:

1. The exchange of explicit control messages for re-keying is in dynamic route filtering mechanism not required.
2. These flexible security architecture parameters like. Authenticity, integrity, and Non-repudiation can be satisfied with it.
3. A robust secure communication framework is support over unreliable medium access control layers of wireless sensor network.

B. *Proposed Work Model Analysis*

This model is representing the object of dynamic keying approach inside the symmetric encryption schema of the wireless sensor network. The main motivation behind VEBEK is that the communication cost is the most dominant factor in a sensor's energy consumption. The module of the whole process can be explained as below:

- **VEEK Module** is handling keying approach. It produces a dynamic key that is then fed into the crypto module. It's also eliminated re-keying factor of encryption algorithm and reduces transmission overhead for sensor network. Here, it manly includes action of node state alive, packet reception, transmission, encoding and decoding. So, energy value for that node depleted after current node action. In the initial deployment all node of sensor have same energy level E_{ini} value. Each node computes and updates the transient value of its virtual energy after performing some action. The value of virtual energy for particular node can be denoted with E_{VC} which compute using equation [1],

$$E_{VC} = \text{packet size} * (E_{tx} + E_{enc}) + t * E_a + E_{syn}$$

And, for maintaining synchronization inside the overall network one concept of perceived energy [1] value taking in count using equation,

$$E_p = l * (E_{rx} + E_{dec} + E_{tx} + E_{enc}) + t * 2 * E_a$$

This module ensures that each detected packet is associated with a new unique key generated based on virtual energy of sensor node. In this activity computation cost for encryption algorithm is reduce due key value computed before encryption round activation. Here, is sample algorithm for key generation using virtual energy value of sensor node.

Algorithm for key generation:

```
Fetch Dynamic key (node energy, packet value)
  Begin
    J ← temp;
    If j → 1 then
    K← Dynamic key (node energy, packet value)
  Else
    K ← Dynamic key (k (j-1), node energy)
  End if
    Return k
  End
```

- **Crypto module** performs simple encoding operation using the permutation of bits in the packet, according to the dynamically created permutation code using concept of the RC5 encryption mechanism. The key to RC5 is created by virtual energy-based keying module. The purpose of the crypto module is to provide simple confidentiality of the packet header and payload while ensuring the authenticity and integrity of sensed data without incurring transmission overhead of existing system. The permutation code is used to encode the *(ID|TYPE|DATA)* massage and additionally include same *ID* with data packet to verify Decryption of data in side routing network. These processes involve main three task of key expansion which maintain key table in according to number of round, encryption which involve activity of integer addition, bitwise XOR operation and variable rotation round and decryption task. The benefit of simple encoding scheme is that it's not required any hash code or message digest for control sending message.

- **Communication Module** is responsible for the sending of packets initiated at the current node or received packets from other sensors along the path to the sink. The operations of the forwarding module handle using routing algorithm. These operations perform over the TCP/IP protocol layer to handle higher level of communication in wireless network. It can also include with two types of state as statistical and operation mode for tracing false data packet inside the sensor network. Here, watching mechanism is required for store node activity in accordance with perceive energy value. In this statistical mode perform activity of monitoring data packet in random manor as network configuration. On the other side operation mode perform activity of monitoring each data packet traverse from the particular node. So, these two operation state also effect with efficiency and computational parameters of wireless sensor network. These two types of working mode are more compatible with security requirement of wireless sensor network with context of symmetric key encryption technique.

IV. RESULT & PERFORMANCE ANALYSIS

This section involved result analysis for proposed model of VEBEK approach using symmetric key cryptography. This analysis is helpful to fulfil requirement of wireless sensor network constraints. Here, we performed implementation work of proposed scheme of VEBEK approach with RC5 encryption algorithm and data transfer using the TCP/IP protocol layer under the IDE of Visual Studio 2008 environment. Also, we include Simulation model of multiple sensor node network which perform data routing from source to destination using of GTNET'S simulator which provide flexibility to adopt VEBEK model for wireless sensor network.

A. Energy Consumption

The utilization of energy for wireless sensor network depends on a number of factors as node voltage, clock frequency and operation cycle. So, if we increase the security on network its affect in energy consumption for nodes. The energy consumed by node during execution using block cipher which corresponds to total running time and average power utilization. Generally, for RC5 symmetric key algorithm energy consumption values evaluated as Key setup 71.51 mJ, Encryption 34.22 mJ and Decryption 33.71 mJ [12]. Fig. 2 represents the graph of energy consumption for three approaches with RC5 using existing dynamic key, operational mode of VEBEK and statistical mode of VEBEK.

The result of graph this represents the energy values of sensor nodes consumed over different interval of symmetric key encryption. Here, comparison of these three approaches shows that the energy consumption by statistical mode of VEBEK is less. So, it's providing better energy efficiency using concept of virtual key creation for symmetric key algorithm.

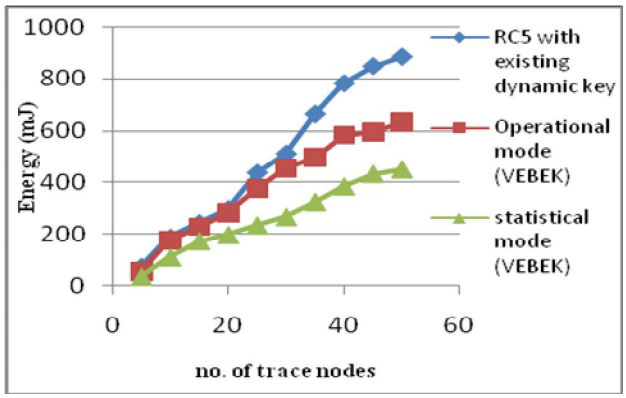

Fig. 2 Energy consumption for WSN

B. Throughput

Operation speed of algorithm is most important factor for wireless sensor network performance. From point of security aspect operation speed can be consider based on key processing, encryption and decryption. So, Throughput of a network is defined as number of information packets transmitted per second to the end node. For pure RC5 symmetric key algorithm operation time is measured as 2.33 ms for key setup, 2.01 for encryption and 2.47 for decryption using 128 bit data [5]. Fig. 3 shows the graph below for throughput of security operation with simple RC5, operational mode of VEBEK and statistical mode of VEBEK.

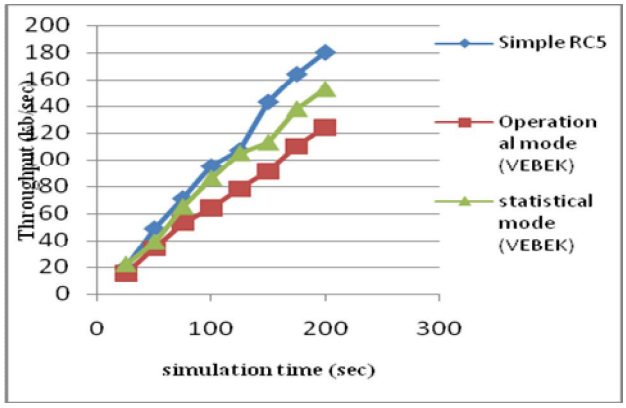

Fig. 3 Throughput of wireless sensor network

As we can see from result that the throughput of simple RC5 is higher than two other mode with some difference but in point of network scalability these two VEBEK mode is most preferable. Thus the throughput of overall network is increase with respect to time. So, it is helpful to decrease computation overhead of wireless sensor network.

C. VEBEK mode performance

VEBEK mode performance concept is useful to identify false data packet sender node inside wireless sensor network. It is helpful to identify false data packet during transmission and drop that packet to maintain sensor network reliability. Fig. 4 represents the graph of performance to handle error data packet for these two different modes.

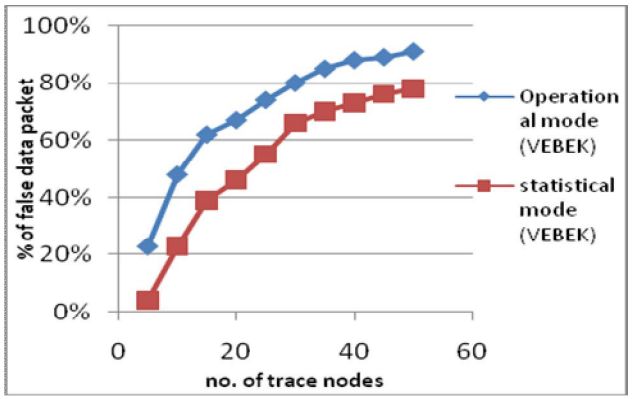

Fig. 4 VEBEK modes Performance

As we can see from the graph that the ratio of false data packet with respect to different no. of trace nodes gives batter performance with operational mode of VEBEK. Because in this mode perform authentication process at every node of transmission path. On the other hand with statistical mode it's performing authentication based on the random probability for dropping false data packet. This probability of packet drop measure using equation $p_{drop} = 1 - (1/2^{packet\ size})$ for static evaluation of WSN [1].

V. CONCLUSION

We have reviewed several security issues and countermeasure mechanism for wireless sensor network base on the existing security models which should be related to WSN constraints and security goals. We also had done comparative study of various Symmetric cryptographic algorithms which provide efficient security with main objectives of energy efficiency in the network. We proposed a concept of VEBEK mechanism to minimize massage exchanging which increase computational overhead on network. We have implemented proposed mechanism for RC5 encryption algorithm using virtual energy based dynamic key constrains for encrypt the data and transfer over reliable network using TCP/IP protocol layer with flexible modular architecture of sensor network. We have also seen result for performance of our proposed scheme through theoretically and by simulation using various factors. So, helpful to achieved benefit of work on more resilient to certain attacks with optimal computational cost.

So, future research will be to further analyse dynamic key assign cryptography mechanisms with adaptive routing to maintain dynamic path operability in WSN using varying cipher parameters.

REFERENCES

[1] S. Uluagac, R. A. Beyah, Yingshu Li, A. Copeland "VEBEK: Virtual Energy Based Encryption and Keying for wireless sensor networks " IEEE Transaction on Mobile Computing vol. 9 No 7 pp.994-1007 July 2010.

[2] S.Bhargavi, Ranjitha B.T, "Implementation of Node Energy Based On Encryption Keying" International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8, 2011.

[3] K. Ravi Chythanya, S.P.Anandaraj and S. Padmaja, "Virtual Energy Efficient Encryption and Keying for wireless sensor networks" International Journal on Computer Science and Engineering, August, 2011.

[4] H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based Encoding and Filtering in Sensor Networks," Proc. IEEE Military Comm. Conf. (MILCOM '07), Oct. 2007.

[5] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef, "Performance Evaluation of Encryption Algorithm for Wireless Sensor Networks" International Conference on Information Technology and e-Services, 2012.

[6] Juha Kukkurainen, Mikael Soini, Lauri Sydanheimo, "RC5-Based Security in Wireless Sensor Networks: Utilization and Performance" WSEAS TRANSACTIONS on COMPUTERS, ISSN: 1109-2750, Issue 10, Volume 9, October 2010.

[7] Tingyuan Nie, Yansheng Li, Chuanwang Song, "Performance Evaluation of CAST and RC5 Encryption Algorithms" International Conference on Computing, Control and Industrial Engineering, year-2010.

[8] Abu Shohel Ahmed, "An Evaluation of Security Protocols on Wireless Sensor Network" TKK T-110.5190 Seminar on Internetworking, 2009.

[9] S.Prasanna, Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[10] Dhanashri H. Gawali, Vijay M. Wadhai, "RC5 Algorithm: potential cipher solution for security in WBSN" International Journal of Advanced Smart Sensor Network Systems (IJASSN), Volume 2, No.3, July 2012.

[11] Abhishek Pandey, R.C. Tripathi, "A Survey on Wireless Sensor Networks Security" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010.

[12] Mohammad AL-Rousan, A. Rjoub and Ahmad Baset, "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks" Journal of Information Assurance and Security, Issue-4, 2009.

[13] Anu Jyothy, "Secure and Efficient Data Transfer in WSN" International Journal of Electronics & Communication Technology, ISSN: 2230-9543, Vol. 2, Issue 3, Sept. 2011.

[14] Omar Elkeelany, "Design and Analysis of Various Models of RC5-192 Embedded Information Security Algorithm", International journal of applied mathematics and informatics, Issue 1, Volume 2, 2008.

[15] Elias Ekonomou and Kate Booth, "SecRose: a data transportation layer security mechanism for Wireless Sensor Networks", International journal of computer application and security, 2006.

[16] R.L. Rivest, "The RC5 Encryption Algorithm", Proc. 2nd International Workshop on Fast Software Encryption, Leuven, Belgium, December 1994.

[17] Ganapathi Avabrath, "Some Issues of Wireless Sensor Networks", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[18] K. Naga Krishnaja, "Cryptography via Virtual Energy for Wireless Sensor Networks", International Journal of Information and Education Technology vol. 2, no. 1, pp. 51-56, 2012.

[19] Boshir Ahmed, Md. Khaled Ben Islam, Julia Rahman, "Simulation, Analysis and Performance Comparison among different Routing Protocols for Wireless Sensor Network", Computer Engineering and Intelligent Systems, *Vol. 2, No.4, 2011.*

[20] Aditya Shukla, Anurag Pandey, Saurabh Srivastava, "Virtual Energy Based Encryption & Keying on Wireless Sensor Network'', IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 9, Issue 3 (Mar. - Apr. 2013), PP 34-43.