# Simulate the processing of data loss in sensor networks by proposing a high speed encryption mechanism

Assist. Prof. Nada. Badr. Jarah
Statistics department / General Specialty: Computer Science
University of Basra -Collage of management and economic
Basra / Iraq
nadabadrjarah@yahoo.com

Received Dec.25, 2019. Accepted for publication Aug.31, 2020

DOI :http://dx.doi.org/10.31642/JoKMC/2018/070202

***Abstract---*** *Prepare network sensor as a context to achieve network community everywhere , it has made technological innovations sensor smaller and more efficient to use in the discovery of the ocean and gain valuable information, it can be as simple as a temperature gauge or as complicated as if used in military and dangerous areas In order to transmit information safely and without any loss, it is necessary to study a dedicated processing mechanism for calculating the encryption taking into account the reduction of power consumption of the sensor node. the network has been simulated using QualNet.*

***key words*** *: sensor networks , speed Encryption, QualNet program*

## I. INTRODUCTION

Wireless Sensors Network (WSN) is a scientific revolution in wireless communications. It has opened the door to new innovations of applications that rely on remote monitoring and control, environmental and health monitoring, weather monitoring and the restricted areas and detection of intruders. WSN consist of small-sized wireless devices called nodes and are equipped with wireless communication functions to achieve communication with each other, and in order for sensor networks to be able to function effectively, there are many challenges that must be met. The sensed nodes suffer from limited energy and low memory in addition to the average computational capacity.

The ability to deploy, direct, integrate data, process information, and reliability is some from the challenges to their using growth , when the packet is sent from the source node, it may pass through a set of intermediate nodes before the packet reaches the target node .[1]

Hence, the need for a protocol that passes packets in the network is Ad hoc On-Demand Distance Vector (AODV), in order to process data transfer without losing any part of it, we proposed in this paper a way to divide the data into multiple parts, and the use of a fast encryption mechanism for processing that encrypts parts of data from information, then procedure simulation using QualNet software is to maintain the transfer without loss or data loss.

## II. AIM OF RESEARCH

In this paper, we propose a high-speed encryption processing mechanism that can split and copy encrypted text into multiple pieces of part data and send it after performing encryption processing on environment information., we then describe the results of assessments carried out using high-speed encryption processing mechanism and QualNet network simulation to prevent the loss of environmental information by attackers.

## III. PREVIOUS STUDIES

*A. Data collection design [2]*

It eliminates excess sensor readings without encryption and maintains data confidentiality and privacy during transmission. Duplicating cases from the original readings will be grouped into a single package. In this way, the scheme is flexible to attack known as regular script, attacks with selected scripts, text-only attacks, and attacks in the middle. The proposed aggregation method has shown that it significantly reduces communication overhead and can be implemented practically on wireless sensor platforms.

*B. WiMax technology [3]*

A new technology that provides fast access to data even when they are long distances across different ways of point-to-point communication or point-to-point multiple connections.

The main objective is to make deliveries as fast as possible and efficient so that there will be no data loss during the delivery process. Through congestion in the network and there must be a quick switching to the *C. program QualNet by Scalable Net-works [4]*

In this study, QualNet was used by scalable net-works to simulate scenarios designed to communicate in more complex wireless networks, making design and testing almost impossible without a suitable software.

## IV. PROGRAM QUALNET [5]

It is an ideal simulation tool for evaluating design in research and development in communication network. It is especially useful for wireless communication and large-scale network analysis.

The biggest attraction is the QualNet equipped with a high-speed simulator engine, simulation execution time is greatly shortened by advanced technologies such as CPU load balancing and simulation model section with multi-processor support. The protocols of all layers are implemented from the application layer to the physical layer, and source code is provided. It can also handle large network models with tens of thousands of mobile nodes.

It has another advantage in supporting dual-core parallel simulations as standard and Compatible with Windows, Linux and MacOS. It also supports 64-bit operating system which is suitable for large-scale simulation.

base station taking into account many parameters such as distance, congestion, delay and signal strength. All simulations that done in a scalable network simulation through QualNet simulation. The result is in the form of total received messages, received productivity, average jitter and average end-to-end delay in a portable WiMAX cell.

Appeared program QualNet is easy to use with a clear user interface and support for distributed multiprocessor and computing systems and also provides a user-friendly command line interface.

## V. IMPORTANCE OF EVALUATING CRYPTOGRAPHIC SECURITY

With the development of networks, encryption has become a technology that supports the foundation of modern society. and the encryption technology not only maintains the confidentiality of communications on the Internet and mobile phones, but also encompasses all life facilities.

It is no exaggeration to say that the safe operation of communications, traffic and business can no longer be considered without encryption technology.

A sudden drop in security may occur due to advances in cryptographic analysis techniques. For this reason, we find ongoing the researches on assessing the integrity of encryption techniques. [5]

## VI. PROPOSED METHOD

The process of processing high-speed encryption as shown in Figure 1

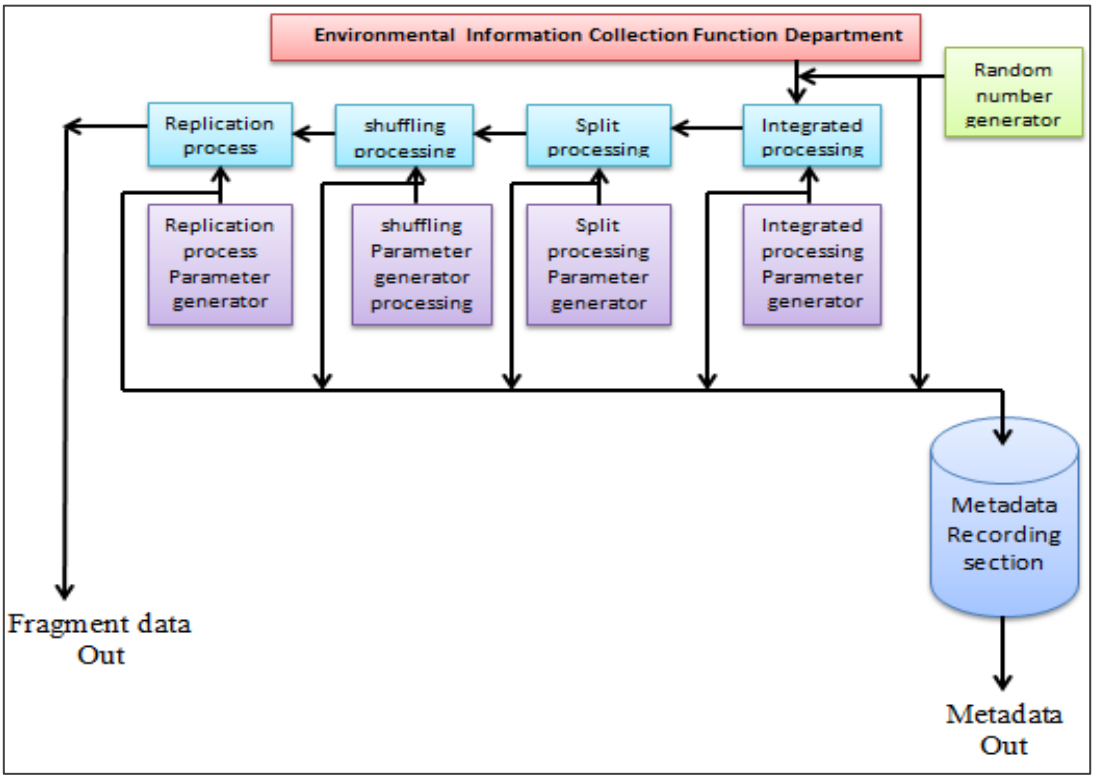


**Figure 1 high-speed processing mechanism encryption process**

In general, sensor nodes have limited computing power, and when using a high-speed encryption processing mechanism, the energy and operating cost of the sensor node must be considered.

The environmental information obtained by the sensor nodes is divided into parts of the data at high speed and the transmission of the part data is arranged independently of the order of occurrence by mixing sheets. So that part data can be copied and sent. Within.

The parameter used must correspond between the encryption key and the decryption, and then stored in the metadata recording section of the time series as decoding metadata. Then, before sending part data, it is sent to the destination node by a predefined path.

## VII. SIMULATION EXPERIENCE

In the sensor node connection system with the suggested method, the change in the data recovery rate is used when the number of nodes and the number of replicas of fragment data is used as parameters using the Qual Net network emulator.

The parameters of the simulation experiment were to determine a square area measuring 1000 × 1000 square meters.

The number of nodes spread randomly except the base station was 10,20,30,40, 50,60 nodes, the number of simulation experiments was 100 times, and the AODV routing protocol IEEE 802.15.4 was used. The size of the sensor data is 64 bytes and the number of fragmented data is 8 sections and the number of replicas of the data part is 0,1,2,3,4,5,6, where the sensor node senses every 25 seconds. After encryption, metadata and hash data are sent in 50 millisecond intervals. In Figure 2, the data loss rate of the parts for a 25-second sensor period, and Figure 3 represents the sensor data recovery rate for the same period.

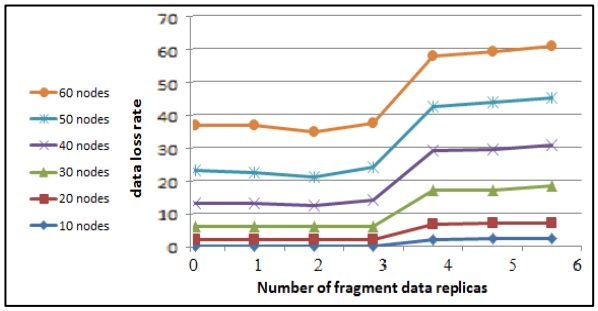


**Figure (2) data loss rate**

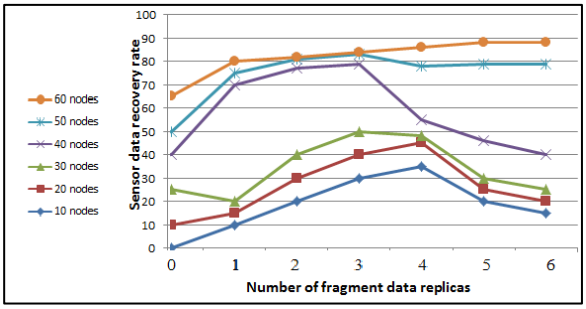


**Figure (3) Sensor data recovery rate**

As can be seen from Figures 2 and 3, when fragment data is replicated, the sensor data recovery rate is improved compared to the absence of duplication. The reason is that decryption is possible the series of processors, a random number sequence and account-related parameters are created each time environmental information is collected in the sensed nodes . using a fixed number of fragment data. When the number of iterations reaches 4 or more , the segment data loss rate and the sensor data[6] recovery rate have increased, due to the fragmented packet data size increasing with the number of copies and the effect of radio interference between terminals increasing with the segmented data transmission time.

## REFERENCES

[1] Sai Krishna Kovi , Pavankumar Jangam , Sai Kumar Goud Kosgi, wireless sensor networks and applications, Department of computer science , Frostburg state university , 20٠٩ .

[2] Shih-I Huang, Shiuhpyng Shieh, J. D. Tygar , Secure encrypted-data aggregation for wireless sensor networks, Springer Science+Business Media, LLC, 2009 .

[3] Saikat Das, Prof. Siladitya Sen, analysis of wireless network through wimax in qualnet International Research Journal of Engineering and Technology, Volume: 03 Issue: 11, 2016 .

[4] QualNet 4.5.1 Network Security Model Library, Scalable Network Technologies, Inc, july 2008.

[5] K. John Singh , Manimegalai Rajkumar, Evolution of encryption techniques and data security mechanisms, January 2015, https://www.researchgate.net/publication/305176323.

[6] Linghe Kong, Mingyuan Xia , Xiao-Yang Liu , Min-You Wu , Xue Liu, Data Loss and Reconstruction in Wireless Sensor Networks , IEEE transactions on parallel and distributed systems, 2013.