iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33752

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Ensuring the Security in WSN using a Novel Approach against Sink Hole Attacks

Santhosh J.[1], Shajila V.[2]
[1]*Assistant Professor, Department of Computer Applications and Information Technology, Sree Narayana Guru College, Coimbatore - 641 105.*
[2]*M.Phil. Research Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore - 641 105.*

***Abstract:** Wireless Sensor Network (WSN) are relatively modern technologies for the collection and transmission of information. A resource-restricted sensor network typically includes many sensor nodes. These nodes measure certain natural occurrences, analyze information and create details and submit them to a centralized data control unit called sink through multi-hop communication. In collaboration with several sensor nodes, e.g. to evaluate the relative humidity in a certain area, the collection and processing of information will be carried out according to the scenario. In a number of different scenarios, sensor networks can be used. As a result of military research, for instance sensor networks for battlefield targeting, sensor networks have become increasingly used in civil applications, such as monitoring of critical infrastructure. Security controls are extremely important for all sensor networks to ensure the functionality of the sensor network, particularly in malicious environments. In existing methods, cryptographic methods or time synchronization are used to resolve these attacks. However, the independent framework of the WSN may fail these methods. This paper provides a significant approach to mitigation of security breaches called the Hamming Method based on Residual (HMR). The findings of this study prove the approach proposed in efficient in data security.*

I. INTRODUCTION

The WSN is one of the emerging technologies of the century and is becoming an epidemic technology [1]. A variety of advances have been made in the field of wireless communication and electronic science that enable the development of low-power, low-cost and performance sensor nodes. These sensor nodes, including sensor components, data processing, and communications, allow the deployment of wireless sensor networks. The wireless sensor network consists of a large number of sensor nodes that are randomly deployed to connect through the wireless environment to monitor physical or environmental conditions such as noise, vibration, pressure, temperature, etc. Co-operative transfer to the base station. In addition, the WSN has a wide variety of applications, including agriculture, industry, health care, incident management, safety monitoring, internal, surveillance systems and nuclear power plants [2].

The location of these sensors is not necessarily predetermined. In some cases, sensors are randomly distributed in hazardous or inaccessible environments [3]. Due to its rapid development, it is used in a variety of areas such as the military, home monitoring, health care, agriculture and so on. The WSN consists of the following three elements: (i) Interface (ii) Gateway-node (GW) (iii) Sensor-Node (SN). Provides a user interface for accessing GW and SN. GW enables the communication between the U user and the SN sensor node, and the SN measures the physical environment.

Sensor nodes are capable of computing and limited storage space. They collect valuable information and send it through the bus. Users can access the data collected through the gateway. Since data is transmitted through an unsecured and unprotected channel, the transmitted data must be protected against threats such as unauthorized access, illegal eavesdropping and tampering with effective action. In the future, the sensor network will be ubiquitous to make future technologies or the environment or infrastructure more intelligent. These include health care, smart homes through sensors, environmental monitoring, and more. Figure 1 illustrate the data communication in a WSN through gateway.

Privacy, message integrity, and user authentication in such environments are crucial because enemy communications can be intercepted, deleted, or redirected. Consequently, appropriate security solutions should be used to protect communication links.

In wireless sensor structure because of resource limitation constructions, it bears several security threats, such as hardware manipulation, eavesdropping, injecting false messages, etc., hence more efficient security mechanisms that conform to specific WSN features, are transmitted to the network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

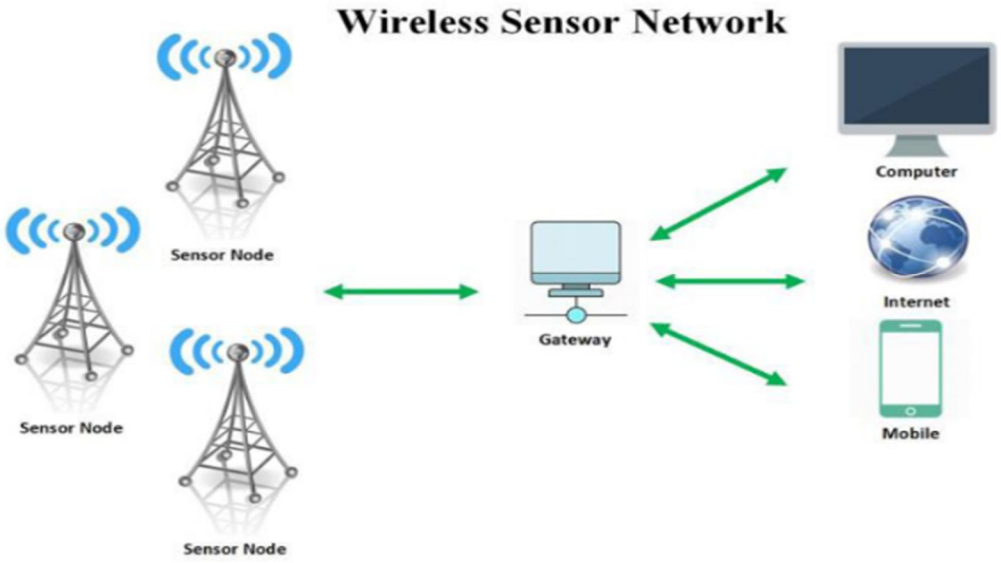


Figure 1: Data communication in a WSN through gateway

The most common security mechanism that can provide security features is symmetric cryptography [4]. In such security mechanisms, when two nodes want to communicate with each other, they use a common key for the encryption and decryption process. This symmetric key has already been selected and shared by the nodes to provide message security and authentication. The process of generating shared symmetric keys is called key management. There is some evidence that the same symmetric keys for different sessions put nodes at risk in unsupervised and protected environments [5]. Although there are systems for managing and restoring network nodes, there are still attacks that need to be identified and used to counter them.

II. RELATED WORKS

In 2016 the authors in [6] presented an authentication protocol using smart cards for a distributed cloud environment architecture. In this scheme, the registered users can access private information in safe conditions from all private cloud servers. Also, they claimed that there are two types of security flaws in existing protocol and they have the ability to cover up these security weaknesses.
In 2017 the autors in [7] proposed authenticated key agreement for multi-server architecture.In this paper, the researchers improved the chaotic map and fixed the security vulnerabilities. To improve security, a Lightweight Authentication Technique proposed for Heterogeneous Wireless Sensor Networks. Also, they review the security issues of existing schemes.
In 2018 the authors in [8] proposed an authentication scheme for multimedia communications and designed for IoT environment base on WSN. This schema provides a high efficiency.
In 2019 the authors in [9] describe the security weaknesses of existing schemes and proposed a lightweight authentication based on the three-factor technique and key agreement protocol for WSN. The proposed scheme addresses several security requirements and uses XOR and hash functions.
In 2020 the authors in [10] proposed a lightweight multiple shared key agreement for wireless sensor networks that is based on hyper elliptic curve Diffie-Hellman. the protocol decreases keys exchange overhead and increases the safety of the keys.

III. METHODOLOGIES

A. Trust And Reputation (Tr) Modeling (Existing System)

The trust and reputation of the node are represented by the beta distribution among the related trust systems, which assumes that only the cooperation and the non-cooperation in the process of interaction between nodes. Aiming at avoiding the existing states between interactions, the time interval between two adjacent collaboration is used to represent the trust and reputation of the node. Furthermore, it derive the expression of the nodes' trust and reputation according to the relationship between beta distribution and exponential distribution. In order to simplify the model of trust and reputation, it divide the behavior of nodes into two categories in two adjacent collaboration, namely, cooperation and non-cooperation. Undoubtedly, it is not adopting the potential hypothesis, because trust and reputation mainly depend on the cooperation between nodes.

B. Hamming Method Based On Residual (Hmr) Model (Proposed System)

With the implementation of confidentiality, an adversary is unable to steal the information in WSN. However, this does not automatically mean the data is safe because the adversary can maliciously change the original data in transit. Thus, data integrity ensures that the data received by the destination node in the WSN is the same as that generated by the source. In order to preserve data integrity, data modifications should be detected.

The basic concept for preserving data integrity is to add redundant information to data that can be used to determine if any change has been introduced. However, because sensor nodes have very limited energy resources, it is crucial to reduce the computational and communication overhead caused by redundant information.

The Hamming distance is a measure of the difference between two strings of characters or bits of the same length. It is defined as the number of positions at which the corresponding symbols are different. Therefore, the Hamming distance can be used as the redundant information to detect errors. For binary strings A and B, the Hamming distance is equal to the number of 1s in A XOR B. For example, the Hamming distance between A = 0100101000 and B = 1101010100 is 6, which is calculated as the number of 1 bits in A XOR B = 1001111100. The computational overhead of the XOR operation is negligible. The number of bits used to represent the Hamming distance is determined according to the size of the two strings. For b-bit strings, the Hamming distance is in the range [0, b], and thus log 2 (b + 1) bits are required for the Hamming distance. Since the Hamming distance only marginally increases the size of the transmitted data, the communication overhead is low. Therefore, the Hamming distance is used in the proposed method for the redundant information. Let N be the size of the sensor data. In order to preserve data integrity, a sensor node performs the following operations.

1) Divide sensor data into b-bit blocks (B0, B1, ..., Bn-1) where n is the number of blocks such that n is even and N = nb. If necessary, k 0s are padded at the end of the sensor data. k is the minimum value to make the size of the sensor data even with an appropriate b value.

2) Calculate the Hamming distance between two consecutive blocks: HDi = HD(B2i, B2i+1), where $0 \leq i \leq n/2 - 1$.

3) Add the binary representation of the Hamming distance HDi after the 2nd block B2i+1 of the corresponding block pair B2i and B2i+1. The Hamming distance is log2(b + 1) bits long.

4) Send the data to the base station.

Figure 2 shows an example of the process of creating redundant information at a sensor node.

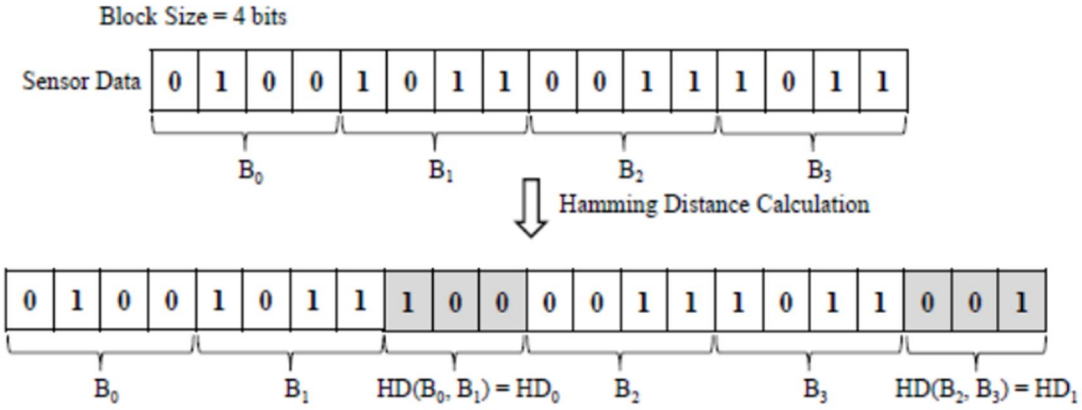


Figure 2: Creation of Redundant Information in WSN

In order to detect data modifications, the base station performs the following operations.

a) Calculate the Hamming distance between two consecutive blocks in the received data: $HDi^{\wedge} = HD(B2i, B2i+1)$, where $0 \leq i \leq n/2 - 1$

b) Compare the calculated Hamming distance $HDi^{\wedge}$ with the received Hamming distance (HDi).

- For all i, if $HDi^{\wedge} == HDi$, the data is correct.
- Otherwise, data is corrupted.

Figure 3 shows an example of data verification at the base station. For blocks B2 and B3, the calculated Hamming distance HDi^ differed from the received Hamming distance HD1. Therefore, the base station detects the modification of the received data.

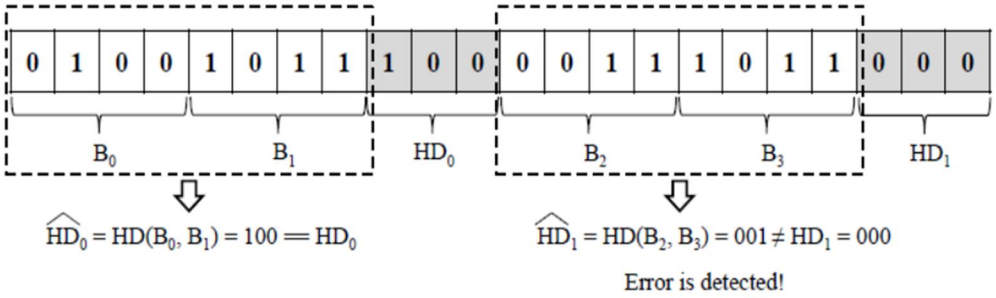


Figure 3: Verification of Data in WSN

IV. RESULTS AND DISCUSSION

To evaluate the existing and proposed models, the test scenario is designed in NS2 Environment. This scenario consists of several nodes, which are 10 meters apart from each other. One of the nodes is periodically sending an ICMPv4 echo request to the other node. When a node receives the request, it replies back the same message. Both echo request and reply are identical in length and format. Therefore, the computation time of both nodes will be the same. The communication of nodes is made using two different security protocols: TR and HMR. For each protocol the payload length of the ping message starts at 10 bytes, then, it is gradually being increased by 10 bytes, until the payload size reaches 90 bytes. In total, there are few computation per protocol. The time taken for computing is compared in milliseconds per task.

Table 1: Numerical Comparision Of Computation Time

NUMBER OF BYTES	TR	HMR
10	2.1	1.2
30	3.2	1.9
50	4.1	2.5
70	5.2	3.1
90	6.1	3.6

Table 1 and Figure 4 shows the compuation time of both existing TR model and HMR proposed model. Based on number of bytes the processing time of the models are calculated in milliseconds is the computaion time. The experimental results shows that proposed HMR model computation time is less when compared with existing TR model.

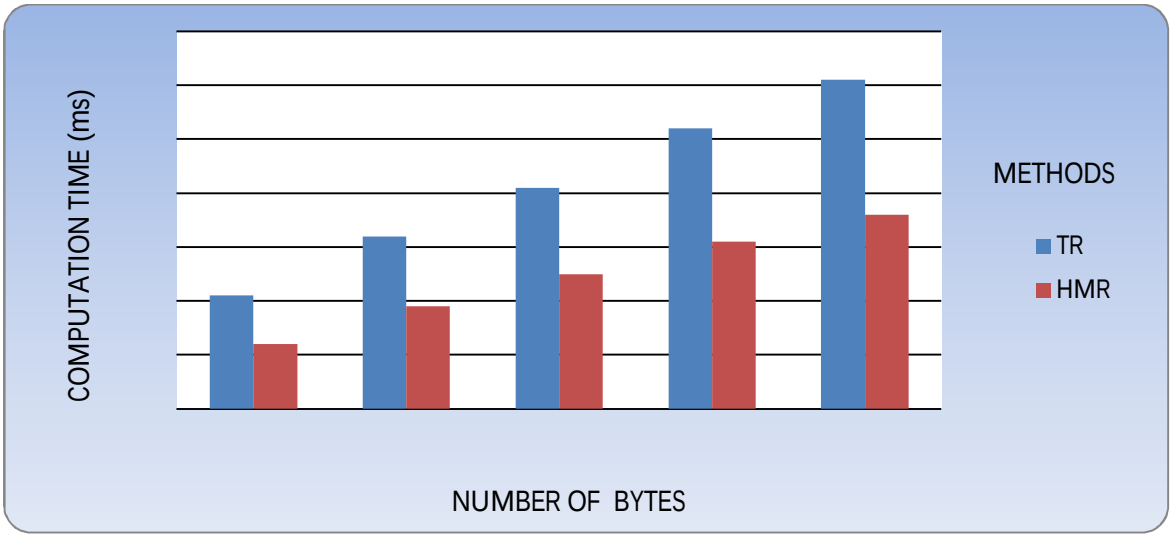


Figure 4: Graphical Comparision Of Computation Time

The next parameter is the memory usage for processing the task. Since memory is also a scarce resource for WSN nodes, we are also required to evaluate the memory usage requirements of processing the tasks. The amount of memory required to store collected time information determines the major main memory requirements of the protocols.

Table 2: Numerical Comparision Of Memory Usage

NUMBER OF BYTES	TR	HMR
10	13	7
30	25	12
50	34	15
70	42	21
90	51	26

Table 2 and Figure 5 shows the comparision of the memory usage for both existing TR and proposed HMR models. The usage of memory in WSN is a significant one, in which it directly affects the energy consumption of the model. For a better security protocol it shpuld have less compuation time and minimal memory usage. Here in this experimental analysis it shows that proposed HMR model takes minal usage of memory when compared to the existing TR model. The memory usage for different number of bytes was considered in KiloBytes (KB).

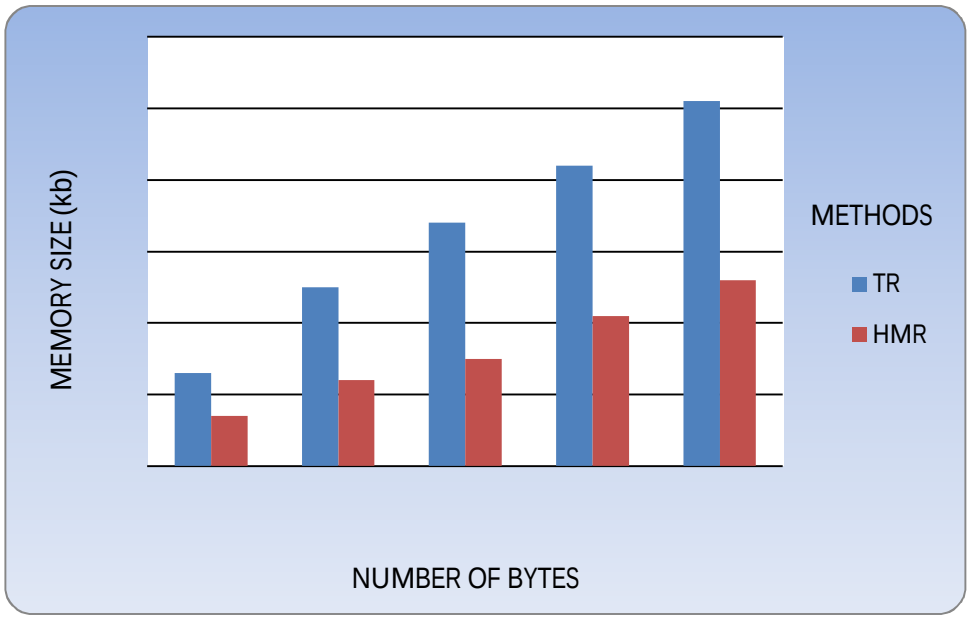


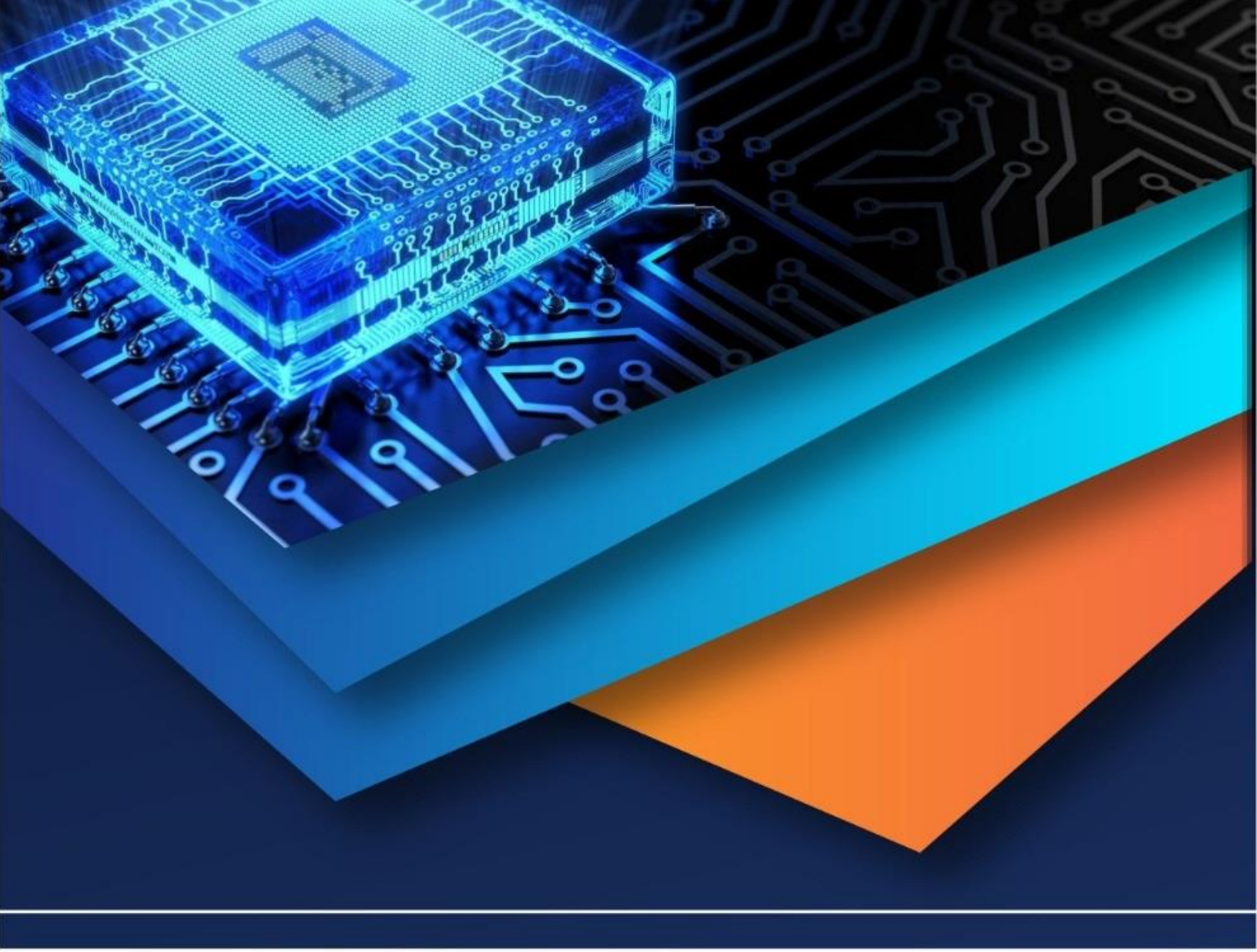
Figure 5: Graphical Comparision Of Memory Usage

V. CONCLUSION

A secure query processing framework that can preserve data confidentiality and data integrity in resource-constrained WSN is presented. For the data confidentiality preserving scheme, various simple encryption schemes are used according to a dynamic selection. The problem of deciding the selection is formulated as an integer program that maximizes security under energy constraints. In order to ensure data integrity, an error detection method based on the Hamming distance is devised. Thus the security of WSN is improved by the Hamming residue technique. The proposed approach is simple and very much effective if more number of rival nodes exists at different hops in the network. As at each node, a new security codeword is generated, which makes the proposed method more efficient, enhances the confidentiality among the nodes, and can easily detect the rival node in the network. The presented approach also reduces the mathematical complexity which in turn increases the PDR by minimizing the delay.

REFERENCES

[1] Z. Zhang, A. Mehmood, L. Shu, Z. Huo, Y. Zhang, and M. Mukherjee, ``A survey on fault diagnosis in wireless sensor networks", IEEE Access, vol. 6, pp. 11349-11364, 2018.
[2] A. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, ``Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks", Peer-Peer Netw. Appl., vol. 12, no. 1, pp. 43-59, Jan. 2019.
[3] A. H. Mohajerzadeh, H. Jahedinia, Z. Izadi-Ghodousi, D. Abbasinezhad-Mood, and M. Salehi, ``Efficient target tracking in directional sensor networks with selective target area's coverage", Telecommun. Syst., vol. 68, no. 1, pp. 47-65, May 2018.
[4] M. S. Yousefpoor and H. Barati, ``Dynamic key management algorithms in wireless sensor networks: A survey", Comput. Commun., vol. 134, pp. 52-69, Jan. 2019.
[5] S. Athmani, A. Bilami, and D. E. Boubiche, ``EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs", Future Gener. Comput. Syst., vol. 92, pp. 789-799, Mar. 2019.
[6] R. Amin and G. P. Biswas, ``A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks", Ad Hoc Netw., vol. 36, pp. 58-80, Jan. 2016.
[7] A. Irshad, ``An improved and secure chaotic-map based multi-server authentication protocol based on lu et al. and Tsai and Lo's scheme", Wireless Pers. Commun., vol. 95, no. 3, pp. 3185-3208, 2017.
[8] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, ``Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks", Multimedia Tools Appl., vol. 77, no. 14, pp. 18295-18325, Jul. 2018.
[9] S. Shin and T. Kwon, ``A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes", Sensors,vol. 19, no. 9, p. 2012, 2019.
[10] V. S. Naresh, S. Reddi, and N. V. Murthy, ``Provable secure lightweight multiple shared key agreement based on hyper elliptic curve Diffie-Hellman for wireless sensor networks" Inf. Secur. J., Global Perspective, vol. 29, no. 1, pp. 1-13, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY