Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AERP: AGGREGATED ENCRYPTING ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS (WSN)

OMAR KHALID SALIH ALHAFIDH[1] , YOUNIS SAMIR YOUNIS [2] , SADOON HUSSEIN ABDULLAH[3]

[1]Associate Lecturer, College of Education for Human Sciences, Mosul University, Mosul, Iraq

[2] PhD in Computer Science, Lecturer. Nineveh Education Directorate, Ministry of Education, Nineveh, Iraq

[3]PhD in Computer Science, Associate Professor. Department of Physics, Collage of Science, Mosul University, Mosul, Iraq

E-mail: [1]omaralhafidh@uomosul.edu.iq, [2]fajirnet@gmail.com, [3]sadosbio113@uompsul.edu.iq

ABSTRACT

The data harvested of the sensor nodes in Wireless Sensor Networks (WSNs) have to be secured. However, the power consumption constraint of these networks makes the normal encryption technique an issue. Moreover, the routing process and clustering in WANs create data aggregation in some nodes. This aggregation increases the complexity of encryption. To mitigate the encryption issue, this work addresses the critical challenge of securing data aggregation in WANs under strict energy constraints. The main contribution of this paper is proposing an aggregated encryption routing protocol (AERP), which introduces a lightweight encryption and routing mechanism that minimizes power and memory consumption while maintaining data security. The proposed protocol covers three main folds. In the first fold, a semi-clustering routing protocol can be implemented easily without the complex setup and cluster formatting phase. Second, the protocol proposes a new key distribution and exchanging method for the encryption process. This method depends on regenerating the encryption key from the data collected from different number of nodes. The third fold, the encryption algorithm, Playfair, has been adopted to be modified to encrypt the data and to round over the encrypted data in the aggregating nodes. This work integrates lightweight encryption, dynamic key generation, and encrypted data aggregation without requiring decryption at intermediate nodes. To evaluate AERP, a sensor node has been constructed and Advanced Encryption Standard (AES) and the modified Playfair have been written to show the power usage of these algorithms. In addition, AERP has been written in simulation environment to show the power usage of data routing. Our results showed that the protocol reduced the encryption power usage of AES with 50% and memory usage with 50% of the microcontroller. On the other hand, the encryption power consumption has reduced the network life time with less than 4%.

Keywords: *Three Diminution (3D), Wireless sensor Networks (WSNs), Advance Encryption Standard (AES), Multi-hops Routing, Semi-clustering Internet of Things (IoT)*

1. INTRODUCTION

Internet of things (IoT) era is the era of connecting intelligent devices to make decisions based on data harvested from different distributed locations [1]. Wireless sensor networks (WSNs) are one of the applications that covered under the IoT umbrella. In these networks, massive number of sensor nodes that consists of a transceiver, processing unit, sensors and batteries are distributed over a sensed field to harvest data. This data are routed to center points, named sink nodes, for farther processing, visualization or rerouting to other locations over the Internet. WSNs applications are used by many areas such as agriculture, military, mining, under-oceans [2] studies and health applications [3].

WSNs became one of the hot research areas in communication and networking in the past decade. 2D and 3D WSNs have been investigated in [8-9]. Holes detection [4], clustering [5] and routing [6] have been also addressed. Many issues have been revealed [7], and many proposed methods have been published. Among the revealed issues, power consumption dominated. To reduce power consumption, researchers attempted to tackle the

communication and routing issues of these networks. However, the power consumption of the computation part of the sensor nodes has not been considered an issue since the microprocessor of these nodes does not execute a massive or complex algorithms to consume power. However, the data of these sensors nodes are routed over the network as plaintext without any protection. With the emergence of IoT and their massive applications, the data that is sensed and routed in WSN should be protected if it is a sensitive data. Moreover, the sink node should be protected from malicious nodes that may embed bad data to the network. To do this, encryption and data integrity should be introduced to the network. However, encryption and integrity should be performed over the sensor node itself. This consumes power and reduces the network life time. Moreover, the routing process in WSN depends on data aggregation before routing the data even in cluster routing protocol or in semi-cluster protocols. This reveals another issue in how to aggregate encrypted data with other data in gateway nodes. A third issue is how to distribute the encryption keys in these networks. These networks are dynamic and created in random manner. Many nodes die over the time and new nodes maybe introduced dynamically.

The core concern of this research stems from the critical trade-off between security and energy efficiency in WSNs. While securing sensed data has become essential due to the rapid expansion of IoT applications, existing security mechanisms often rely on computationally intensive encryption techniques that significantly increase power consumption. This creates a fundamental challenge, as sensor nodes are resource constrained devices with limited battery life, memory, and processing capabilities. Therefore, selecting an appropriate encryption and routing strategy that balances security and resource utilization is a crucial research problem that requires further investigation.

Motivated by this gap, this work aims to develop a lightweight, aggregation-aware encryption routing protocol that minimizes energy consumption while preserving data confidentiality in WSN environments.

In this work, a new Aggregated Encrypting Routing Protocol (AERP) is proposed. This protocol aims to encrypt the data harvested from the sensor nodes to reduce resource usage, such as, memory, computation and power consumption. The protocol allows the nodes to aggregate the encrypted data and re-encrypt them in new packets without the requirement of decrypting the data. AERP is established based on symmetric encryption methodology. The utilized algorithm is a new version of play-fair cypher. This algorithm has been utilized for three main reasons. First, the computational process is small which will not consume power. Moreover, the data size that will be encrypted is simple, which are sensors readings. Second, the memory requirement of this method is small unlike other symmetric encryption algorithms, such as, AES and Data Encryption Standard (DES) that require the processor to keep big S-tables in the memory all the time for the encryption process. Finally, the key size required in this method varies from 1 character into infant number of characters. Our contribution in this work can be summarized as follows:

- Proposing a modified Play-fair encryption algorithm with multi-hybrid rounds. In each round the routing nodes aggregates other nodes encrypted data and encrypt all the data in new packets. In this way, the data of remote nodes will be encrypted in multiple rounds
- Proposing AERP that utilizes Play-fair and data aggregation to route the data with minimum power consumption
- Proposing a new method for encrypting key generating. This method depends on the neighbors lists, gateway addresses and the distance from the sink nodes in waves.

The rest of this paper is organized as follows. In the next section the related works that have been conducted in the area of WSN routing and data encryption detection. Section 3, overviews the proposed protocol. Section 4, introduces the conducted simulation experiment and discusses the results. We conclude this paper in section 5

2. RELATED WORKS

In the past decade, routing the data in WSN and its impact on power consumption and the network life time has dominated [10, 11]. However, power consumption in data routing revealed the security issues and data breaching in this process. Many surveys have been written to show the security prospective of routing protocols in WSN [12]. These studies have motivated researchers to propose different security and data encryption protocols for the proposed routing protocols.

It started with SLEACH protocol [13] that proposed to secure the LEACH clustering routing protocol. Based on SLEACH, SecLeach [14] was

an enhancement of the availability issues in SLEACH and introduced the symmetric encryption process to the protocol. In [15], the author introduced the Asymmetric encrypting algorithm utilizing elliptic curve for data aggregation security issue in WSN. In [16], elliptic curve has been utilized also to generate encrypting key for the nodes to utilize in WSN. In [17], trust-cluster head algorithm has been proposed to solve WSN application in vehicles network. In [18], the author proposed a secure routing protocol for WSN. The protocol has been proposed to reduce power consumption in multi-hop routing network. Shard key encryption system has been utilized to secure the data and to reduce the number of hops between nodes in the network. In [19], elliptic curve has been adopted for key management and distribution in WSN. This algorithm has been adoptive to reduce the effort of key distribution since it is asymmetric encryption algorithm with the generation of two keys one for the encryption process and the other for the decrypting process.

Despite the extensive research on secure routing and encryption in WSNs, existing approaches suffer from significant limitations. Many solutions depend on computationally intensive cryptographic techniques such as AES or elliptic curve cryptography, which increase energy consumption and reduce network lifetime. Moreover, current methods do not efficiently support encrypted data aggregation without requiring decryption at intermediate nodes, which introduces additional overhead and security risks. Ther is a need for lightweight encrypt-efficient encryption and routing protocol that supports secure data aggregation while minimizing computational and memory requirements in WSN environments.

3. AGGREGATED ENCRYPTED ROUTING PROTOCOL (AERP)

Before introducing the proposed key generating and encryption method, the AERP protocol is a semi-clustering routing protocol. This protocol does not adopt the clustering method of LEACH and its descendants; it adopts the semi-clustering behavior in [4] since the semi-clustering process is more viable. The following subsections overview the adopted power model, the semi-clustering method and data aggregating. Finally, the key generating and the modified Playfair algorithms will be introduced.

3.1 Power Model 1

Figure 1 shows the structure of sensor nodes in the environment. The figure shows a microcontroller with a built-in memory, RAMs and I/O interfacing pins for analog and digital sensors. A transceiver model connects to the microcontroller serially using the universal asynchronous receiver transmitter (UART) interface. Finally, the node structure has a batter to power the controller, sensors and communication model. The power model of the Atmega328 microcontroller was utilized for the computation, and the IEEE802.15.1 Zigbee protocol was leveraged in Xbee kits for the communication power model. Equ.1 shows the power model of the communication part. Equ.2 shows the power model of the computational part. The power model of the sensors have been neglected since that changed according to the application of the WSN. Table 1 defines the variables used in these equations.

$$En = \frac{Vc * ic * L}{b} \quad (1)$$

$$Ec = \frac{V*I*CPI*i}{f} \quad (2)$$

As observed from the equ.1, the transceiver power model does not depend on node distances as in LEACH and its descendants clustering protocol. It only depends on the packet size, bit rate and the power usage of the transceiver module to transmit one bit. It is worth mentioning that the current usage of receiving data and transmitting data differs in this module.

Table 1: Experiment Parameters

Variable	Definition
En	Energy usage of the transceiver module
Ec	Computational energy usage of the microcontroller
Vc	Voltage of the transceiver module
ic	Current of the transceiver module
L	Packet size in bits
CPI	Is the cycles per instruction which is the average number of execution cycle of instructions in the processor. For ATmega328 it is 1
i	Number of instruction
I	Current of the microcontroller per execution cycle
V	Voltage of the microcontroller
f	Oscillation frequency of the controller

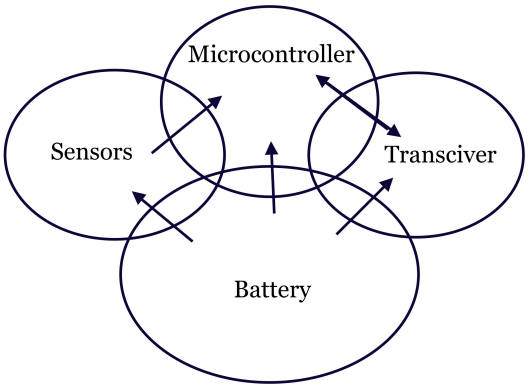

Figure 1: Sensor Node Structure

3.2 The Semi-Clustering Setup

To route the data between the sensors and the sink node, the sink nodes convert the network into number of multi-sized donates shapes. Each donate is identified by a unique id that shows its distance from the sink node. The first donate is the area around the sink node. Each node in this area can communicate directly with the sink node. In other words, they can hear sinks node broadcasts directly without gateways or routers. The second donate is located around the first one. The nodes in this donate can communicate directly with at least one node in the first donate. In other words, the size of this area is bigger than the first one which is located in the hole of this area. The network will be converted into n number of donates inside each other. The data will be aggregated and forwarded from each area to the inner areas until reaching the sink node. Each node will have a list, called gateway list, of all nodes that can communicate with from another inner donate. In addition, each node will have a list, called neighbors list, of all nodes in its range with the same donate id. To construct these lists, the following steps are utilized in the network.

1. The sink node broadcasts a hello message with ID of zero. Any node hears the broadcasts increments the ID of the message and save it as its donate ID. All of these nodes are located in the first donate
2. Each node in the first area broadcasts the message after incrementing the zero ID inside the message body. This means that other nodes will receive this message.
3. Upon receiving this message, any node has three actions to perform. First, if the node has no ID saved, the node increments the ID in the message, record it and rebroadcast the message with the new ID. Second, if the ID in the message equals the ID saved in the node, the node adds the address of the sender to its neighbor list and neglects the message "no broadcasting". Third, if the node receives a message with an ID less than its ID with one, the address of the sender is added to its gateways list and the message will be broadcasted after incrementing the ID field. Finally, if the ID is higher than the ID of the node, the node adds the sender ID to its neighbor list and the message will be neglected.

In this way, each node can construct the neighbor list and the gateway list. These lists will be used in key generating process in the following sections. Finally, each node calculates its distance to the sink node with the number of donates between it and the sink node which equals to the donate id that have been saved in each node. Figure 2. shows the network after conversion. Figure 3 shows the flowchart of the setup phase.

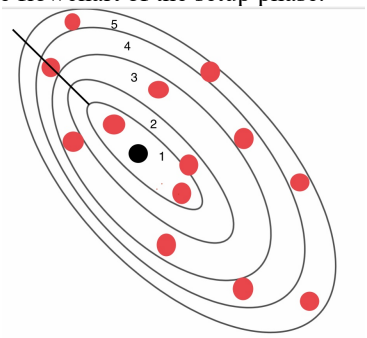

Figure 2: The network conversion, the black node is the sink node and the red nodes are the sensor nodes

3.3 Encryption Key Generating and Distributing

In below Figure 3 shows that contain three phases, in first phase starting with insert ID, Gateway and Neighbor parameter, second phase insert ID and Broadcast, in third phase for Algorithm showing the output, this illustrate in Figure 3. Setup Phase Flowchart.

AERP depends on symmetric encryption. In this encryption, only one key is used for data encryption and decryption. This reveals a security issue in the network of how to exchange the key between the encryption and decryption nodes. Sensor nodes are responsible of encrypting their data and the sink node is responsible of decrypting the data. In computer networks, different algorithms have been proposed for key distribution and exchanging between computers such as Diffe-Hellman and asymmetric encryption. However, these methods consumes power in the computation process since they depends on complex

mathematical operations such as primary key extracting and modular operations.

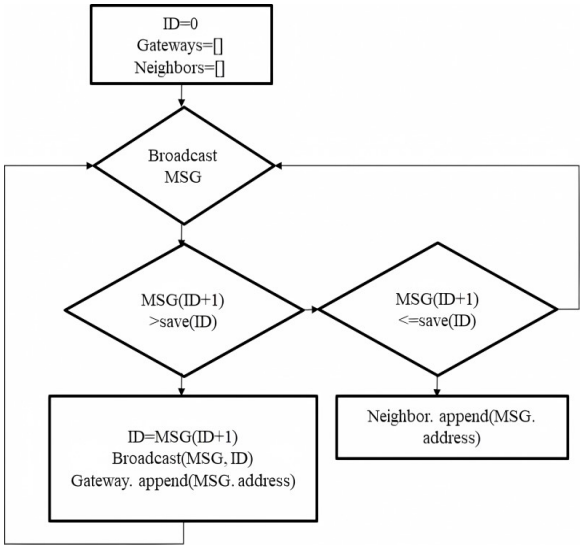

Figure 3: Setup Phase Flowchart

To generate the cipher key, each node after constructing its neighbor list and gateway list sends a small part of these lists to the sink node. Subsequently, each node select one of the nodes' IDs that has not been transmitted to the sink node and select gateway ID from the list that have been sent to the sink node with its ID to construct a onetime key to encrypt a well-known word and send the encrypted data with the partial lists to the sink node.

Upon the reception of the encrypted data, the partial lists from all nodes, the sink node attempts to construct the full list of neighbors and gateways of each node. Subsequently, the sink node attempts to decrypt the message from the constructed lists of each node. Two options will be encountered. First, the sink node will decrypt the message; using the extracted key to encrypt the key of the encryption that this node will utilize to send data to the sink node. Second, the sink node will fail in extracting the key since the sink node will attempt the construct the neighbor list of each node from messages received from all nodes in the network. If the constructed list did not contain the ID that the node utilized in constructing the encryption key, the sink will fail in regenerating the key. In this case, the sink will select another neighbor ID from the nodes neighbor list to generate a key, encrypt the well-known word and send it to the node.

To crack this method, a cracker node has to listen to all messages around the node to construct its neighbor list. Moreover, it has to construct its gateway list. This means that beaning in the transmission range of a node is not enough to construct these lists. Moreover, the donates IDs of the node and its neighbor is also utilized in generating the key, the number has to be collected from the nodes to reconstruct the encryption key

It worth mentioning that the generated key contains the nodes ID, one of its neighbors ID, one of its gateways ID, its donate ID, and its neighbors donates ID.

3.4 Data Aggregating

To aggregate the encrypted data, the gateway nodes will receive the encrypted data. However, the forwarded packet of the gateway node will consist of its sensed encrypted data and other nodes data. To aggregate the data and enhance the security of the Play-fair, the received encrypted data will be added to the data of the gateway and both of them will be encrypted with the key of the gateway node. The process looks like the rounds in DES or AES encryption methods. However, before the re-encrypting of the data, the gateway will add the address of the node in front of its encrypted data. This means that if the node is in the fourth donate, its data will be encrypted 4 times in the way to the sink node, or we have four rounds play-fair with different keys.

3.5 The modified Playfair Algorithm

Play-fair algorithm has been selected for three reasons. First, it is simple and light weighted encryption algorithm, which does not require massive computational power. Second, it works like streaming ciphers. The message size ranges from two bytes to any number of bits. Unlike the block ciphers that requires the data to be with a fixed size, padding is used if the data is smaller than this size. Third, the key size of Play-fair starts from one byte to any number of bytes. However, it has one issue; the data should be arranged in a square matrix. All the possible data output and input of the algorithm must be arranged in a square matrix. In [20], they exhibited an example of the original Plat-fair with English letters that the letters I and J have been considered as one character to generate a 5x5 English letters matrix.

For current data in the WSN, the data are sensed numbers from multiple of sensors. Each value should consist of the sensor name or type and its sensed value. This means that the data input consists of two parts a number part and a character part. Table 2 shows the generated 4x4 matrix of the data in the proposed algorithm. Digits and the dot should be included since the second part of the data is a floating number. The characters are used to

name the sensors in each node in the network. In such way, they can decode the first part of the data. Finally the # value is used in two locations; first to separate two sensors data from each other, and second to separate two equal digits follow each other.

Table 2: Modified Play-fair Encryption Matrix

0	1	2	3
4	5	6	7
8	9	.	#
A	B	C	D

So, it is necessary to know how Play-fair works and review the concepts. The following steps describe how the algorithm works:

1. The password or passphrase is written in the matrix after duplication is eliminated.
2. The matrix is completed with the missing elements
3. The data is divided into two characters, and a search starts in the matrix for these two characters.

When they are found, the characters are replaced with other two characters according to their location in the matrix.

- If they are in the same row, each one is replaced with the left element.
- If they are in the same column, each one is replaced with the below element.
- If they are in two separated columns and rows, they create a square and each one is replaced with the opposite angle of the square.

4. EXPERIMENT

To evaluate AERP, two main methods have been leveraged; hardware construction and simulation.

4.1 Sensor Node Construction

In the first method, a sensor node has been constructed utilizing Xbee S2, Arduino nano kit with ATmega328p microcontroller with 3.3v. The frequency oscillator of the controller has been dropped to 8MHz. The microcontroller has been programmed by AES algorithm "AESLib [21]" with 128bit key and the lightweight Playfair algorithm. Only the encryption part of these algorithms has been written for the microcontroller. Random data has been generated in each microcontroller for the encryption and decryption process. The generated data varied between 10 bytes and 200 bytes. The power consumption of the kit has been measured using a USB multi-meter that can be connected between the Arduino kit and the power supply. The circuit encrypts the data 100 times to obtain the record of the power usage of the device before putting it in sleep mode. Table 3 shows the comparison between the AES and the modified Playfair in the computation part of the encryption only without the sensing, ADC, or data transmission.

TABLE 3: POWER CONSUMPTION COMPARISON

Data size	Playfair	AES
50 byte	0.0009J	0.0016J
100 byte	0.0012J	0.0051J
200byte	0.0029J	0.009J

The memory of the device is another issue. The real AES encryption algorithm requires the device to save one S-BOX that consists of 256byte. The RAM of this device is only 2Kbyte which means that 1/8 of the memory is utilized before defining and saving any variable from the sensed data of the network. According to the Xbee s2c data sheet, the module has 250Kbps bit rate with a usage voltage of 3.3 and usage current of 33mA in transmitting, and 28mA in receiving or listening state. This means that to transmit 200byte data without any overhead, it requires 0.69mJ. However to encrypt these data, 0.029mJ is required in Playfair and 0.09mJ in AES. This means that each transmission requires 4% increasing in power usage for the new algorithm and around 13% for the AES encryption. These numbers have been utilized in the second evaluation method of this work in the simulation part.

4.2 Simulation

The semi-clustering part of AERP has been written in MATLAB using the descriptions in [4]. A 3D sensing field has been constructed as a cube. The diminutions of the field are 500x500x500m. The sink node has been located at the upper corner <0, 0, 0>. 1000 nodes have been distributed randomly in the field with a transmission range of 90 m as in the data sheet of Xbee s2c [22]. The nodes have been equipped with a battery of 1J. Table 4 summarizes the experiment parameters.

TABLE 4: EXPERIMENT PARAMETERS

Variable	Value
Number of Nodes	1000
Transmitting Current Xbee s2c	33mA
Receiving Current "listening"	28mA
Operating Voltage of Xbee s2c	3.3v
Packet Size "with overheads"	200 byte
Bit rate	250,000bps
Field Size	500x500x500
Nodes energy	1J
Transmitting range	90m

Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. RESULTS

To evaluate the protocol, we have iterated the simulation 30 times and obtained the average results of these 30 iterations. An overview of power consumption and the network life time will be shown first. Three protocols will be compared; semi-clustering without encryption, AES and AERP. Subsequently, the key management and distribution results will be overviewed.

5.1 Power Consumption and Network Life Time

Figure 4 displays network round-by-round power use. A round is the time each node needs to deliver one packet to the sink node. Semi-clustering protocol has no cluster heads. AES uses more power each round than other protocols. This reduced network life, as demonstrated. AERP has increased the utilized power in each round since the encryption calculation is aggregated across the communication power. However, network life has decreased 4%. AES cuts almost 30%.

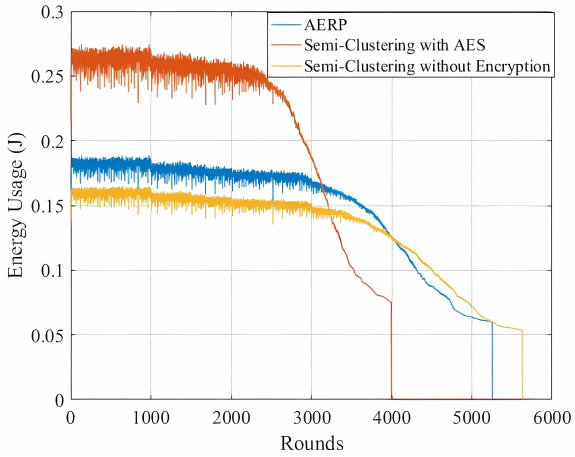

Figure 4: Energy usage each round

Figure 5 displays the CDF value of the network's deceased nodes. 50% of AES nodes perished before 3000 cycles. 50% of AERP nodes lasted 4000 rounds, while the secure-less version lasted 4200. AES network life duration is 4000 rounds, which is the same amount of rounds 50% of nodes perished at AERP.

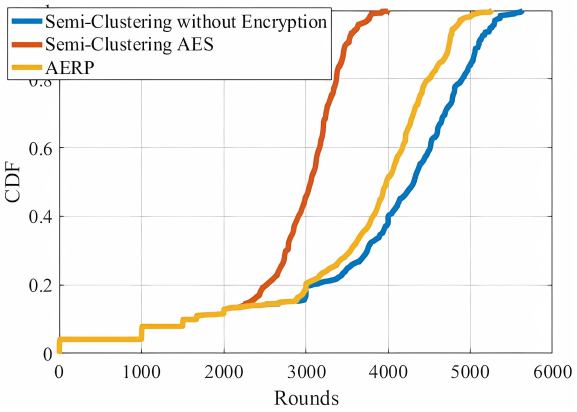

Figure 5: Network life time

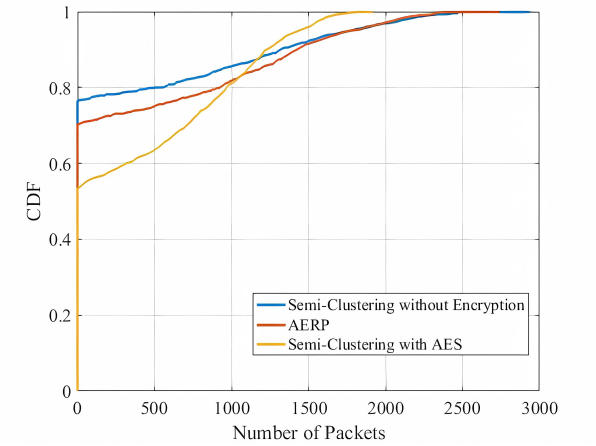

Figure 6: Packet Lost in the network

Figure 6 illustrates lost packet CDF. The network handled 75% of AERP packets without loss. Many gateway nodes died and unplugged from the network, thus losses accumulated. The secure protocol has 78% less packets. However, AES protocol is below 58%. To minimize lost packets, disconnect network graphs.

5.2 Key Distribution Evaluating

In AERP, each node sends a partial neighbor and gateway lists to the sink node. The sink node aggregates these lists to generate the complete lists of each node to regenerate the encryption key. Figure 7. shows number of nodes that the sink could not generate with its full neighbor list and gateway list compared with the percentage of neighbors that have been sent to the sink node. We can observe from the figure that with 45% of the neighbor list, the sink node generated the full neighbor lists of each node in the network with an accuracy of 100%. This accuracy drops with the reduction of the size of the list. However,

even though this reduction, the number of nodes that have to reselect new node IDs as keys in the network is less than 20% in the worst case "200 nodes in current case". Figure 8 re-computes the same values in figure 7 however with extending the transmitting range of the nodes from 90m to 150m. We can observe that the accuracy is 100% for 35% part of the real list of each node since the number of neighbors of each node has increased with the new transmitting range. These figures show that the process of distributing the key proposed in AERP is usable. However, to hack the proposed method, the hacker has to collect the lists of all the nodes around the target node to reconstruct the list. This process is out of the scope of this work. However, in future works, different attacks will be presented to show the efficiency of the AERP.

6. DIFFERENCES

This study assumes that integrating lightweight encryption with aggregation aware routing can reduce power consumption while maintaining acceptable security level in WANs. It is also assumes that modifying simple encryption algorithms such as Playfair can provide an efficient trade off between security and resource utilization compared to conventional encryption methods.

Unlike existing approaches that depend on complex encryption algorithms such as AES, the proposed AERS protocol is based on a lightweight algorithm (Modified Playfair), which reduces energy consumption and memory usage. Furthermore, most previous studies do not support the aggregation of encrypted data without decryption, whereas AERS provides this feature, thereby enhancing both efficiency and security. However, the security level provided by lightweight algorithms such as the modified Playfair, may be lower than that of standard algorithms such as AES. Additionally, the dynamic key generation mechanism may introduce synchronization challenges in highly dynamic network environments. Finaly AERP has been evaluated in limited simulation and hardware setup, it may not fully represent large scale real word deployments These factors represent potential limitations of this work.

This work differs from all of the above related algorithms in terms of three folds. First, asymmetric algorithm has not been utilized since it requires complex mathematical operations that require intensive computation and memory of the nodes' controller. Moreover, this requires more power for the computation process of the protocol. Second, we proposed a new key management and distribution process unlike the two keys asymmetric encryption. Finally, this protocol attempted to modify one of the simplest encryption algorithms since it requires less computational operation unlike the massive operations in the commercial block ciphering algorithms.

7. CONCLUSION

This work presented AERP, a lightweight aggregated encryption routing protocol to address the trade-off between security and energy consumption in WSNs, a new data aggregation and semi-clustering routing protocol has been proposed. The protocol utilized a new modified Playfair encryption algorithm to encrypt the sensed data before transmitting the data. The gateway nodes that reroute the data re-encrypt all the received data in one packet and resend them to the sink node. The aggregated encrypted data is re-encrypted in each gateway node in the network. The modified version of Playfair is lightweighted and consumes less energy than other block ciphering techniques. AERP proposes a new key distribution and exchanging process that depends on sending partial parts of neighbor lists to the sink node and allows the sink node to regenerate these lists to generate the encryption key. To evaluate AERP, hardware design and simulation have been leveraged. In the hardware design, ATmega328p and Xbee kits have been leveraged to write AERP and AES encryption to measure their power consumption. Playfair utilized less 15% power than AES encryption. In the simulation AERP with playfair and AES has been written. The results confirm the research hypothesis, demonstrating that lightweight encryption combined with aggregation-aware routing can reduce power and memory usage compared to traditional methods such as AES. This work contributes a practical solution for secure and energy efficient data routing in resource constrained WSN environments. It has been shown that AERP consumes more power than secure-less routing protocol with 4%.

8. FUTURE RECOMMENDATIONS

In this work and after finish paper, recommend that AREP must be developed to improving QoS quality of service in Wireless Networks, and also recommend to using AERP in WANs to help and enhancing data safety. On other hand, should be making balancing between encryption power consumption and network life time. In addition, by creating AERP this is help to utilizes Play-fair and data aggregation to route the data with minimum power consumption, and

recommend to generating new method for encrypting key generating. This method depends on the neighbors lists, gateway addresses and the distance from the sink nodes in waves.

REFERENCES:

[1] Masoud, Mohammad, Yousef Jaradat, Ahmad Manasrah, and Ismael Jannoud. "Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts." Journal of Sensors 2019 (2019). https://doi.org/10.1155/2019/6514520

[2] Shah, Syed Bilal Hussain, Chen Zhe, Syed Hassan Ahmed, Yin Fuliang, Muhammad Faheem, and Seema Begum. "Depth based routing protocol using smart clustered sensor nodes in underwater WSN." In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems ICFNDS'18, pp. 1-7. 2018. http://dx.doi.org/10.1145/3231053.3231119

[3] Adame, Toni, Albert Bel, Anna Carreras, Joan Melia-Segui, Miquel Oliver, and Rafael Pous. "CUIDATS: An RFID–WSN hybrid monitoring system for smart health care environments." Future Generation Computer Systems 78 (2018): 602-615. https://doi.org/10.1016/j.future.2016.12.023

[4] Masoud, Mohammad Z., Yousef Jaradat, Ismael Jannoud, and Mustafa A. Al Sibahee. "A hybrid clustering routing protocol based on machine learning and graph theory for energy conservation and hole detection in wireless sensor network." International Journal of Distributed Sensor Networks 15, no. 6 (2019): 1550147719858231. http://dx.doi.org/10.1177/1550147719858231

[5] Masoud, Mohammad Z., Yousef Jaradat, Dema Zaidan, and Ismael Jannoud. "To Cluster or Not to Cluster: A Hybrid Clustering Protocol for WSN." In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 678-682. IEEE, 2019. http://dx.doi.org/10.1109/JEEIT.2019.8717524

[6] Al Sibahee, Mustafa A., Songfeng Lu, Mohammad Z. Masoud, Zaid Alaa Hussien, Mohammed Abdulridha Hussain, and Zaid Ameen Abduljabbar. "LEACH-T: LEACH clustering protocol based on three layers." In 2016 International Conference on Network and Information Systems for Computers (ICNISC), pp. 36-40. IEEE, 2016. DOI 10.1109/ICNISC.2016.59

[7] Jaradat, Yousef, Mohammad Masoud, Ismael Jannoud, and Dema Zaidan. "The Impact of Nodes Distribution on Energy Consumption in WSN." In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 590-595. IEEE, 2019. https://doi.org/10.1109/JEEIT.2019.8717473

[8] Jaradat, Yousef, Mohammad Masoud, and Ismael Jannoud. "A mathematical framework of optimal number of clusters in 3d noise-prone wsn environment." IEEE Sensors Journal 19, no. 6 (2018): 2378-2388. http://dx.doi.org/10.1109/JSEN.2018.2885927

[9] Yousef Jaradat, Mohammad Masoud, Saleh Al-Jazzar. "A Comparative Study of the Effect of Node Distributions on 2D and 3D Heterogeneous WSN", International Journal of Sensor Networks, 2020. https://doi.org/10.1504/IJSNET.2020.109187

[10] Maizate, A., El Kamoun, N., "A New Metric Based Cluster Head Selection Technique for Prolonged Lifetime in Wireless Sensor Networks", (2013) International Journal on Communications Antenna and Propagation (IRECAP), 3 (4), pp. 227-236. https://www.praiseworthyprize.org/jsm/index.php?journal=irecap&page=article&op=view&path%5B%5D=12990b

[11] Bani Yassein, M., Khamayseh, Y., Hmeidi, I., Al-Dubai, A., Al-Maolegi, M., "A New Energy-Efficient Hybrid and Clustering Routing for Wireless Sensor Networks", (2017) International Journal on Communications Antenna and Propagation (IRECAP), 7 (3), pp. 176-187. https://doi.org/10.15866/irecap.v7i3.11484

[12] Ali Idarous Adnan, Zurina M. Hanapi, "Geographic Routing Protocols for Wireless Sensor Networks: Design and Security Perspectives", International Journal on Communications Antenna and Propagation (IRECAP), (2015) , 7 (3), pp. 176-187. DOI:10.15866/irecap.v5i4.6252

[13] Xiao-yun, Wang, Yang Li-zhen, and Chen Ke-fei. "Sleach: Secure low-energy adaptive clustering hierarchy protocol for wireless sensor networks." Wuhan University Journal of Natural Sciences 10, no. 1 (2005): 127-131. http://dx.doi.org/10.1007/BF02828633

[14] Oliveira, Leonardo B., Adrian Ferreira, Marco A. Vilaça, Hao Chi Wong, Marshall Bern, Ricardo Dahab, and Antonio AF Loureiro. "SecLEACH—On the security of clustered sensor networks." Signal Processing 87, no.

12 (2007): 2882-2895. http://dx.doi.org/10.1016/j.sigpro.2007.05.016

[15] Zhou, Qiang, Geng Yang, and Liwen He. "A secure-enhanced data aggregation based on ECC in wireless sensor networks." Sensors 14, no. 4 (2014): 6701-6721. https://doi.org/10.3390/s140406701

[16] Elhoseny, Mohamed, Hamdy Elminir, Alaa Riad, and Xiaohui Yuan. "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption." Journal of King Saud University-Computer and Information Sciences 28, no. 3 (2016): 262-275. http://dx.doi.org/10.1016/j.jksuci.2015.11.001

[17] Gaber, Tarek, Sarah Abdelwahab, Mohamed Elhoseny, and Aboul Ella Hassanien. "Trust-based secure clustering in WSN-based intelligent transportation systems." Computer Networks 146 (2018): 151-158. http://dx.doi.org/10.1016/j.comnet.2018.09.015

[18] Haseeb, Khalid, Naveed Islam, Ahmad Almogren, Ikram Ud Din, Hisham N. Almajed, and Nadra Guizani. "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs." IEEE Access 7 (2019): 79980-79988. http://dx.doi.org/10.1109/ACCESS.2019.2922971

[19] Qazi, Rosheen, Kashif Naseer Qureshi, Faisal Bashir, Najam Ul Islam, Saleem Iqbal, and Arsalan Arshad. "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks.", journal of Ambient Intelligence and Humanized Computing , (2020). https://link.springer.com/article/10.1007/s12652-020-02020-z

[20] Forouzan, Behrouz A. "Cryptography & network security". McGraw-Hill, Inc., 2007.

[21] AESLib, https://www.arduino.cc/reference/en/libraries/aeslib/

[22] Horvat, Goran, Damir Šoštarić, and Drago Žagar. "Power consumption and RF propagation analysis on ZigBee XBee modules for ATPC." 2012 35th International Conference on Telecommunications and Signal Processing (TSP). IEEE, 2012. http://dx.doi.org/10.1109/TSP.2012.6256286

[23] Anitha, R., & Nawaz, G. (2014). "Development of a secure, energy efficient and reliable routing protocol for mobile wireless sensor networks". International Review on Computers and Software.(IRECOS), 9(3), 487-494. https://www.praiseworthyprize.org/jsm/index.php?journal=irecos&page=article&op=view&path%5B%5D=15017

[24] Faheem, M., Ngadi, A. B., Ali, S., Shahid, M. A., & Sakar, L. (2013). "Energy based efficiency evaluation of cluster-based routing protocols for wireless sensor networks (WSNs)". International Journal of Software Engineering and Its Applications, 7(6), 249-264. http://dx.doi.org/10.14257/ijseia.2013.7.6.21

[25] Smys, S. (2019). "Energy-aware security routing protocol for WSN in big-data applications". Journal of ISMAC, 1(01), 38-55. http://dx.doi.org/10.36548/jismac.2019.1.004

[26] Vinitha, A., & Rukmini, M. S. S. (2019). "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm". Journal of King Saud University-Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2019.11.009

[27] Zhou, J. (2013). "Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks". International Journal of Distributed Sensor Networks, 9(4), 108968. https://doi.org/10.1155/2013/108968

[28] Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks". Ad Hoc Networks, 115, 102448. https://doi.org/10.1016/j.adhoc.2021.102448

[29] Deebak, B. D., & Al-Turjman, F. (2020). "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks". Ad Hoc Networks, 97, 102022. https://doi.org/10.1016/j.adhoc.2019.102022