

Hybrid security in AOMDV routing protocol with improved salp swarm algorithm in wireless sensor network

Yousif Hardan Sulaiman, Sami Abduljabbar Rashid, Mustafa Maad Hamdi, Zaid Omar

Abdulrahman Faiyadh, Abdulrahman Sabah Jaafar Sadiq, Ahmed Jamal Ahmed

Department of Computer Engineering Techniques, Al-Maarif University College, Ramadi, Iraq

Article Info

Article history:

Received Feb 13, 2022

Revised May 9, 2022

Accepted Jul 30, 2022

Keywords:

AOMDV routing protocol

Diffie-Hellman model

ECC algorithm

Gray and wormhole attacks

Hybrid security

ABSTRACT

During these years the current trends shows a fast expansion in the field of wireless sensor network (WSN) based applications. Due to this much vulnerability are created and also coverage optimization becomes essential to improve overall performance. However, maximum of the model concentrates only on security or efficiency. In order to create a highly efficient protocol both concepts need to get concerted. So, we developed a protocol namely hybrid security in ad-hoc on-demand multipath distance vector (AOMDV) routing protocol with improved salp swarm algorithm (HSA-ISSA). This model is sub-divided into three sections. They are, wormhole attack and gray hole attack construction AOMDV protocol, improved salp swarm algorithm (SSA) model is used for weighted distance position updates which leads to improve the efficiency. And to secure the network from attacks we use hybrid security with the help of Diffie-Hellman key interchange algorithm and elliptic-curve cryptography (ECC) algorithm. During performance evaluation the proposed HS-ISSA protocol provide stable results in terms of message success rate (MSR), end to end delay (E2E_Delay), network throughput (NT), and average energy efficiency (AEE). Our HAS-ISSA protocol outperformed all the other earlier works by providing hybrid security, optimized coverage as well as energy efficiency to the wireless sensor networks.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mustafa Maad Hamdi

Department of Computer Engineering Techniques, Al-Maarif University College

Ramadi, Iraq

Email: meng.mustafa@yahoo.com

1. INTRODUCTION

Wireless sensor networks (WSNs) received a lot of attention in real world applications, such as analyzing conditions, transport planning, surveillance footage, flood forecasting, health management, clinical issue, environment and climate monitoring, and tracking businesses and organizations [1]. The fundamental concern is that the assisting nodes may or may not be trustworthy, increased vulnerability to numerous attacks which have a substantial effect on data security [2]. Implementing effective routing protocol, through extending lifespan of the network, ensuring reliability and optimal path selection [3] as well as security connectivity is focused. Due to wireless transmission, security risks such as snooping are very cheap to implement. Attacker can easily inject bad messages into the network [4]. Many of the most common meta-heuristic strategies used for the optimal solution are "genetic algorithm (GA)", "particle swarm optimization (PSO)", "artificial bee colony (ABC)", firefly, "ant colony optimization (ACO)", and security concepts are implemented in [5]-[7]. Recent days security is healthcare applications are mostly concentrated. So that secure and medium access control methods are developed [8], [9].

In this paper a hybrid security in ad-hoc on-demand multipath distance vector (AOMDV) with improved salp swarm optimization algorithm is implemented. The highlights of our research work are shown in: i) the proposed system provides an effective energy model to improve the quality of service (QoS) of the network, ii) the proposed system mainly concentrated on gray hole attack and worm hole attack, iii) in our proposed model in order to overcome the attack issues hybrid security is used which is the combination of Diffie-Hellman key exchange mechanism and elliptical curve cryptography algorithm, iv) the proposed work includes the multipath routing protocol AOMDV, v) proposed system used improved weight based salp swarm optimization algorithm to provide optimization in the network which helps to improve the QoS of the network, and vi) the implementation of the proposed work is done using the software NS2. This simulation setup is created to analysis the performance of our protocol in terms of security and optimization.

2. EARLIER METHODS

The various proposed authentication solutions fail to concurrently address all known security holes. In order to retain the broadcaster's lifespan expectation while maintaining assured quality of service, the nodes energy must be properly utilized. Here a cluster head (CH) selection based on the hybrid artificial bee colony and monarchy butterfly optimization technique (HABC-MBOA) is suggested for the majority selection of CH [10]-[13]. The other optimal path selection algorithms which are used in the earlier researches are adaptive PSO [14], butterfly optimization algorithm (BOA) [15], quasi oppositional butterfly optimization algorithm (QOBOA) [16], ACO [17], grey wolf optimization (GWO) [18], the fruit fly optimization algorithm (FFOA) [19]. Some of the review works show about the security services such as confidentiality, authentication, integrity, and availableness [20], [21].

3. SYSTEM MODEL

3.1. Representation of energy

All the wireless sensor nodes are energized by battery and hence the consumption of energy by all nodes is discussed. During transmission, the energy consumption process can be categorized as: energy generated and energy absorbed and that is indicated in (1),

$$Ener(i, j) = Ener(consum)(i) + Ener(tras)(i, j) \quad (1)$$

where, $Ener(i, j)$ indicates the entire amount of energy consumed while transmitting the 'n' bits message with the distance 'D'. The notations 'i, j' indicates the energy consumed by the 'n' bits message. Basically, the distance between the source and destination may vary and hence the model will used based on the distance.

$$Ener(j) = E_{trans}(i) = j \times T_j \quad (2)$$

where, $Ener(j)$ indicates the total amount of energy consumption while transmitting the data, $E_{trans}(i)$ indicates the energy required while transmission, $j \times T_j$ indicates the time require for data transmission.

$$Residual\ Energy = Energy\ Remained - Energy\ Consumed \quad (3)$$

3.2. Channel representation

There may be occurrence of collision in the IEEE 802.11 wireless medium when there is concurrent transmission during communication. In view of this, the free space method is evident for finding the signal of every packet. Moreover, free space propagation method activates when there is possibility of ideal propagation mode with line-of-sight path accessibility among transmitter and receiver. Under free space method, transmitted message 'n' can travel throughout the distance 'D'. Hence, the total transmission energy and received energy can be represented by the (4) and (5),

$$\begin{aligned} Ener_{trans}(n, D) &= Ener_{trans-elec}(n) + Ener_{trans-amp}(n, D) \\ Ener_{trans}(n, D) &= Ener_{elec}n + \beta_{amp}nD^2 \end{aligned} \quad (4)$$

hence the consumed energy $Ener_{rec}(n)$ is,

$$\begin{aligned} Ener_{rec}(n) &= Ener_{rec-elec}(n) \\ Ener_{rec}(n) &= Ener_{elec}n \end{aligned} \quad (5)$$

where, $Ener_{trans-elec}$ indicates the total energy dissipation from the transmitter, $Ener_{trans-amp}$ indicates the transmit amplifier energy as well as $Ener_{rec-elec}$ indicates the total energy dissipation from the receiver. By utilizing (4) and (5), the distance-based energy consumption for every message can be calibrated. When comparing with receiver side energy consumption, there is more consumption of energy in transmitter side and hence it is significant to save transmitter energy. The free space method based received signal power as shown in,

$$P_{trans}(D) = \frac{P_{trans} g_{trans} g_{rec} \tau^2}{(4\pi)^2 D^2} \quad (6)$$

where, the P_{trans} indicates total transmitted power, g_{trans} indicates the transmitter gain, g_{rec} indicate the receiver gain. The gain is the ratio of the receiving power to the initial transmitting power. In this section, it is explained the results of research and at the same time is the comprehensive discussion. Results can be presented in figures, graphs, tables, and others that make the reader understand easily [14], [15]. The discussion can be made in several sub-sections.

4. HYBRID SECURITY IN AOMDV WITH IMPROVED SSA

In proposed model we introduced multi path concept in ad-hoc on-demand distance vector (AODV) protocol to overcome the drawbacks in it. And in order to reduce the energy consumption and delay we introduced improved salp swarm algorithm in multipath AODV which is AOMDV. And to secure the network malicious activities we used hybrid security model namely Diffie-Hellman key interchange algorithm and elliptic curve cryptography. By combining all these methods, we developed the new protocol namely hybrid security algorithm (HSA)-ISSA. The architecture of the proposed model is shown in the Figure 1. The major sections of our protocol are introduction for AOMDV protocol with its neighbor discovery and path selection model, introduction to SSA and the idea of improved SSA algorithm and finally the concept of hybrid security which is done using the combination of Diffie-Hellman key interchange algorithm and elliptic curve cryptography.

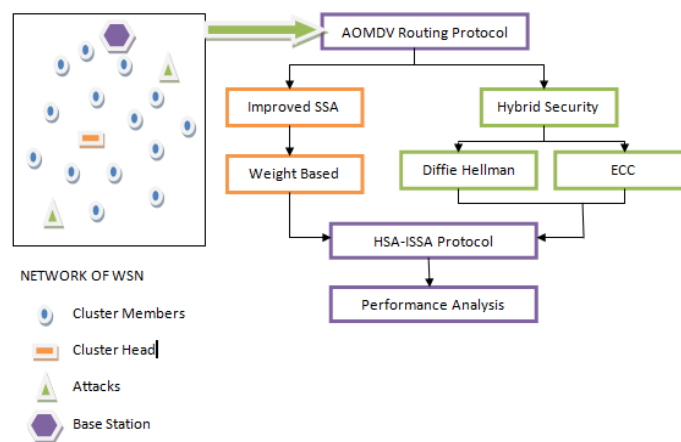


Figure 1. System architecture of the proposed hybrid security in aomdv with improved ssa (HSA-ISSA) protocol

4.1. Ad hoc on-demand multi-path distance vector routing protocol

The base for AOMDV method is route finding process. The source sends a flood of route request (RREQ) packets to the destination, which is identified by a distinct identifier. Until an intermediate node has a valid and clean path to the destination, it broadcasts both of the RREQ and route reply (RREP) messages via the initiator node and hence the replicated RREQ can be demolished by the relay node. When the initial RREQ message arrives at its destination, it rebroadcasts an RREP control messages, following the backward direction that is built during the discovery phase by relay node. Any redundant RREQ packets obtained by destination are discarded. The problem with AODV is that it only generates one path to the destination. When this one fails, a new path must be found. But AOMDV protocol is designed in the way of creating multiple paths to the destination using the same path discovery technique. The duplicate RREQ messages are exploited by AOMDV to create numerous pathways within the source and intermediary nodes. Each RREQ

message received from a different hop and it receives an RREP message from the destination node. HELLO messages are used by AOMDV to detect broken links.

The aim of AOMDV protocol is to predict the loop free manifold path of both source and destination. This process in the network may leads to discard of packets without proper delivery. Route discovery, route planning, and packet forwarding are the 3 phases of this AOMDV. In addition to this we have two more modules such as neighbor discovery and path planner which is explained.

4.1.1. Neighbor discovery

The primary aim of neighbor discovery process is to find the appropriate neighboring nodes for constructing a better network. Initially, the sensor node starts to broadcasts the HELLO packets with the assistance of network ID. At once the receiving of HELLO packets, the particular node updates its routing table with the details of ID number, distance, and received signal strength indication (RSSI). Moreover, the energy levels will be shared by nodes in the location. Finally, this phase ensures that each node has current updated values of the above-mentioned parameters about its neighborhood nodes.

4.1.2. Path planner

It is critical to install an agent that flows from the base station to the uncovered region in order to maximize coverage in a wireless sensor network. Here, we concentrate on how to plan an energy-aware path for agent nodes. For example, static nodes are power limited, and if they continue to send packets via fixed intermediate nodes, energy will be lost and network life time will be reduced. As a result, an agent node may choose a routing in which it receives packets from static nodes and forwards them to the base station, reducing the stress on the intermediary fixed node.

4.2. Salp swarm algorithm evaluations

Here, the basic key constraint is calibrated using NFL formula with the calculation of single-objective nature based objective function, which further solves the single-objective issues. The key factor of SSA is the low fitness to regulate complexities of multi level searching, as it would seem in all parameters head for the combination solution, plus deployed setting up to convert the perfections all throughout optimization process, which increases the probability of discovering an optimal global solution when solving difficult multi level issues. The amount of constants reduces the efficiency of salp swarm algorithm noticeably.

The two sections of this algorithm are leader and follower. The chain is considered as the leader and remainder indicates the followers. The role of leader is to monitor the movement of entire group and then the followers. Same as else swarm algorithm, the population notation 'P' which is mentioned in the D-dimensional space search concept. The occupancy of the salps is denoted by the matrix x , such as $xp = [xp1, xp2, xp3, \dots \dots xpD]T$, where $p = 1,2,3 \dots \dots P$. There are two bounds such as upper and lower bound, where the upper bound is being as $Ub = [Ub1, Ub2, \dots \dots UbD]$, lower bound can be denotes as $Lb = [Lb1, Lb2, Lb3 \dots \dots LbD]$, and the food is being as $f = [f1, f2, f3 \dots \dots fD]$. The entire SSA is given as three sections.

- Initialize the entire population

The initialization process is actually a casual mode as shown in,

$$x_{P \times D} = Lb + rand(P, D) \times (Ub - Lb) \quad (7)$$

- Updating the spot of leader

It is mandatory for a leader to regulate the entire group with the equation of updating in (8),

$$x_d^p = \{f_d + cp1((Ub_d - Lb_d)cp2 + Lb_d)cp3 \geq 0.5f_d - cp1((Ub_d - Lb_d)cp2 + Lb_d)cp3 < 0.5\} \quad (8)$$

where, from the above equations, x_d^p indicate the leader p (where, $p = 1,2,3, \dots \dots P1$) with d dimensional space. The note f_d indicates the food parameter in d dimensional space. The note $cp2$ and $cp3$ indicates the control parameter for the intervals $[0,1]$. The note $cp1$ indicates the convergence parameter and its depiction as shown in.

$$cp1 = 2e^{-(4e_i/i_{max})} \quad (9)$$

where, the note c_i indicates the existing iteration and i_{max} indicates the maximum iteration parameter.

- Update the position of each follower

Initially, the follower starts to make the motion of chain and hence it will be updated according to (10).

$$x_d^p = \frac{1}{2} (x_d^p + x_d^{p-1}) \quad (10)$$

By referring the movement strategy form (8), the head's position deliberates alloy the space with the centralization of food. Primarily, the value of $cp1$ is larger and it is nearby 2 and hence in the later stages, it may vary to zero range. Once this rage is reached, the leader starts to find food.

4.3. Improved salp swarm algorithm

Here, the control parameters such as $cp2$ and $cp3$ will be distributed in random manner and hence it takes much time for optimization convergence. The enhancement is made in $cp3$ control parameter for enhanced SSA which is replaces as follows,

$$D = \sqrt{(a1 - a2)^2 + (b1 - b2)^2} \quad (11)$$

where the terms $a1 = cp1 * Ub, b1 = cp1 * Lb, a2 = cp2 * Ub, b2 = cp2 * Lb$

By substituting the improved parameter for $cp3$ in the leader position with the updation of (12) can be as shown in,

$$\begin{aligned} x_d^p &= \{f_d + cp1((Ub_d - Lb_d)cp2 + Lb_d) D \\ &= \sqrt{(a1 - a2)^2 + (b1 - b2)^2} \\ &\geq 0.5f_d - cp1((Ub_d - Lb_d)cp2 + Lb_d) D \\ x_d^p &= \sqrt{(a1 - a2)^2 + (b1 - b2)^2} < 0.5 \end{aligned} \quad (12)$$

here additionally we added weights to the process which leads to improve the speed of searching and accuracy. The location update technique is altered as a weighted sum of best positions. Weights calculation is done by using the vectors $V1$; $V2$; and $V3$. The model for location updating is as follows:

$$W1 = \vec{V1} \times \vec{V2} \quad (13)$$

$$W2 = \vec{V1} \times \vec{V3} \quad (14)$$

$$x_d^p = \begin{cases} W1 * f_d + cp1((Ub_d - Lb_d)cp2 + Lb_d) cp3 \geq 0 \\ W2 * f_d + cp1((Ub_d - Lb_d)cp2 + Lb_d) cp3 < 0 \end{cases} \quad (15)$$

$$x_d^p = \frac{1}{2(W1+W2)} (W2 \times x_d^p + W1 \times x_d^{p-1}) \quad (16)$$

This weight-based technique achieves a compromise between search agents as well as global search skills. It also enhances settling time, leads to improve the performance. This approach is explained in detail in the subsequent Algorithm 1:

Algorithm 1 - ISSA:

```

1: count the total number of salps ( $P_t$ ), each salp is  $n$  and maximum iteration  $i_{max}$ 
2: while  $i_{max}$  do
3:   for  $n$  do
4:     salp fitness calculation for each one
5:   end for
6:  $f$  shows the food agent
7: update  $cp1$ 
8:   for  $n$  do
9:     if  $i==1$  then
10:      revise the leader salp location using Eq. (15)
11:     else
12:      revise the follower salp location using Eq. (16)
13:       $P_t = P_t + 1$ 
14:     end if
15:   end for
16: end while
17: revisit  $f$  as the finest result

```

4.4. Hybrid security algorithm

4.4.1. Encryption

During the encryption process, the input data is transformed into code for better security. At this point, the algorithm named Diffie-Hellman key interchange algorithm and elliptic curve cryptography can be carried out for encryption which are explained in steps:

- For developing the public keys, the algebraic expression oriented finite fields are calibrated with the addition of non-ECC cryptography least keys with the power of security equal to ECC cryptography keys. As a result, both the private and public keys are ready with encrypted format. The generic equation for elliptic curve is given as follows,

This is a technique that converts data into a code, which is used to restrict unauthorized access. At this point, data encryption can be done to use a combination of the Diffie-Hellman key exchange technique and ECC. This hybridization system's step-by-step method is as follows:

$$Y^2 = X^3 + AX + B(mod C) \quad (17)$$

where, the notations A, B , and C indicates random integers from the range 0 to $n - 1$. By alleviating the mentioned integers, the value of Y can be interchanged so that we can find the uneven points too. From the uneven points there is possibility of choosing the private key and public key as indicated in (18),

$$Pub(key) = Pri(key) \times C \quad (18)$$

where, the note $Pub(key)$ is the public key and $Pri(key)$ is the private key.

Encryption and decryption are accomplished with the help of such keys. The key agreement step is performed out in our recommended approach once picking the sender's key value. The Diffie-Hellman key exchange mechanism is used in the suggested strategy for key exchange. The Diffie-Hellman key exchange method is a method of exchanging cryptography keys. In the world of cryptography, it is the foremost way of key exchange that consists of two members, who have never met before and are establishing a shared key over an unsecured conversation. This key will subsequently be used to security systems communications using a symmetric cypher called $C_s(key)$.

4.4.2. Final encryption

As already said, encryption is the phenomenon of interchanging the data in to code with better security with the activity of producing cipher text as follows,

$$CT1 = CA * C \quad (19)$$

$$CT2 = message + CA * C_s(key) \quad (20)$$

where 'CA' indicates the coverage area from 1 to n-1, CT1 and CT2 are the cipher text keys.

4.4.3. Decryption

Decryption is just the inverse process of encryption where, the encrypted message is interchanged into normal message, where this process can be done either manually or technically by utilizing the keys. As a result, the proper message can be recovered as follows,

$$Message = CT2 - C_s(key) \times CT1 \quad (21)$$

once the unique message is found with the assistance of covert key and then it will be transmitted to the access point in optimal way. The result and discussion of the HAS-ISSA method is analyzed in the section 5.

5. RESULT AND DISCUSSION

The proposed methodology produces efficient results and it has been explained here with the help of NS2 software. The efficiency of the projected method is given throughout simulation results with the following postulation.

5.1. Simulation parameters

The evaluation providing by our HSA-ISSA protocol is mainly to improve the overall performance of the network. To analysis the betterment of our protocol it is compared with the earlier research works such

as AOMDV [22], TC-SSA [23] and society for peace and conflict management (SPACM) [24]. By using the network simulator-2 (NS-2) simulator the results were made. A protocol named AOMDV is adopted with 250 meters transmission range, two ray model, 100 numbers of nodes with 1000*1000 m, speed of 5 m/s [25]. The metrics mainly concentrated to improve the performance are message delivery rate (MDR), end to end delay (E2E-Delay), network throughput (NT) and average energy efficiency (AEE) our routing protocol evaluated the performance by calculating the following metrics:

a. MDR

MDR is defined as that it is the ratio that which are the packets received by the receiver node to the packets sent by the sender node. The unit for the calculation of MDR is percentage. The mathematical expression for MDR is shown in:

$$MDR = \frac{\sum_{x=0}^n Node_x^{receiver}}{\sum_{y=0}^m Node_y^{sender}} \tag{22}$$

b. E2E-Delay

The time duration which takes by the sender node to send all the packets to the receiver is termed as end-to-end delay calculation of the network [26]. The unit for the calculation of E2E-delay is ms. The mathematical expression for E2E-delay is shown in:

$$E2E_{Delay} = \frac{\sum_{x=0}^n (time_x^{received} - time_x^{transmitted})}{n} \tag{23}$$

c. NT

It is the calculation of the total number of data transmitted during the process of communication among the sender and the receiver for the entire network [27]. The unit for the calculation of throughput is Kbps.

d. AEE

AEE is defined as that it is amount of residual energy calculated at the end of the simulation.

5.2. Performance analysis

Figure 2 shows the performance of message success rate (MSR) for the proposed work and compared results of the earlier models such as AOMDV, TC-SSA, and SEBCS. It can be seen from the figure that the MSR of the proposed HSA-ISSA is comparatively higher than the earlier methods. The MSR rate of the proposed HSA-ISSA is around 94% whereas the earlier works are 69%, 76%, and 83%. This result is achieved by the proposed method using both hybrid security and advanced SSA optimization model. Figure 3 shows the performance of E2E_delay. The E2E_delay created by the proposed work is 191 ms where the earlier works are 348 ms, 292 ms, and 221 ms.

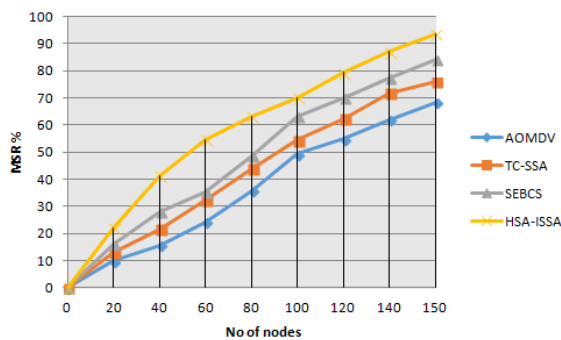


Figure 2. Message success rate calculation

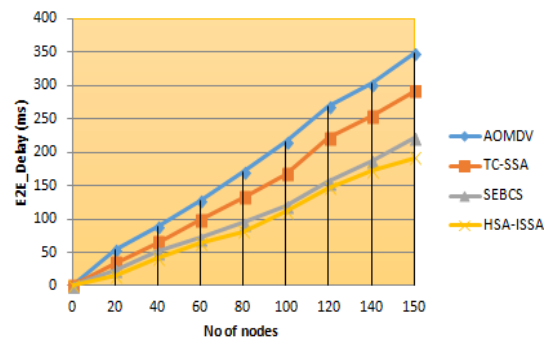


Figure 3. End to end delay calculation

Figure 4 shows the network throughput calculation of the network. Our proposed model produces very high throughput rate compared to the other work. The throughput of the proposed work is 451 kbps where the other protocols are 188 kbps, 255 kbps, and 287 kbps. Figure 5 shows the comparative analysis of AEE calculation. The AEE value received by the HSA-ISSA protocol is 89.2% where the others are 56%, 79%, and 85%. AEE is one of the core parameters to increase the QoS of the network. From this calculation

it is understood that our proposed model performed much better way when compared with the earlier methods.

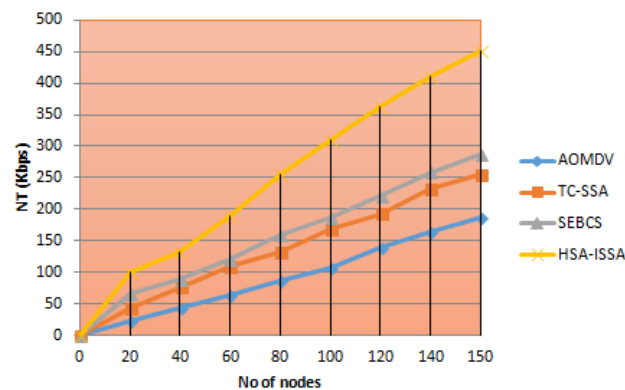


Figure 4. Network throughput calculation

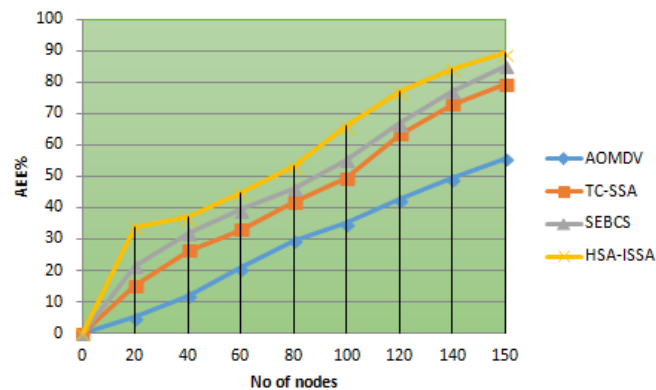


Figure 5. Average energy efficiency calculation

6. CONCLUSION

In this research work, we extended the AOMDV protocol in terms of coverage and security. Reliable and secure communication is done by using hybrid security. It combines both the Diffie-Hellman key interchange algorithm and ECC algorithm. Which helps to overcome the network from wormhole and gray hole attacks. To provide optimized coverage we used ISSA method. The results proves that our proposed HSA-ISSA provides better results in terms of MSR, E2E_delay, NT, AEE, and average energy consumption (AEC). When compared with the earlier work we can conclude that by introducing both hybrid security and ISSA in AOMDV protocol the network overall performance got better and stable. But due to the high rate of retransmitted packets during simulation the routing overhead is high that's leads to get more delay and consumption of energy. So, this research can be continued in future by concentrating in efficiency and delay during the emergency condition in WSN.





REFERENCES

- [1] A. A. Kamble and B. M. Patil, "Systematic analysis and review of path optimization techniques in WSN with mobile sink," *Computer Science Review*, vol. 41, p. 100412, 2021, doi: 10.1016/j.cosrev.2021.100412.
- [2] S. M. K. M. A. Ahmad, E. Krishnahari, and M. Y. Khan, "Neighbor node intimacy (N2i) for trust management in WSN," *Materials Today: Proceedings*, 2020, doi: 10.1016/j.matpr.2020.11.489.
- [3] E. D. Tita, Williams-Paul Nwadiugwu, and J. M. Lee, "Real-time optimizations in energy profiles and end-to-end delay in WSN using two-hop information," *Computer Communications*, vol. 172, pp. 169–182, 2021, doi: 10.1016/j.comcom.2021.02.007.
- [4] S. E. Roslin, "Data validation and integrity verification for trust based data aggregation protocol in WSN," *Microprocessors and Microsystems*, vol. 80, p. 103354, 2021, doi: 10.1016/j.micpro.2020.103354.
- [5] A. N. Rao, B. R. Naik, and L. N. Devi, "On the relay node placement in WSNs for lifetime maximization through metaheuristics," *Materials Today: Proceedings*, 2020, doi: 10.1016/j.matpr.2020.09.527.




- [6] V. Nivedhitha, A. G. Saminathan, and P. Thirumurugan, "DMEERP: A dynamic multi-hop energy efficient routing protocol for WSN," *Microprocessors and Microsystems.*, vol. 79, P. 103291, 2020, doi: 10.1016/j.micpro.2020.103291.
- [7] R. Nikouei and N. Rasouli, "A quantum-annealing-based approach to optimize the deployment cost of a multi-sink multi-controller WSN," *Procedia Computer Science*, vol. 155, pp. 250-257, 2019, doi: 10.1016/j.procs.2019.08.036.
- [8] U. Iqbal and A. H. Mir, "Secure and practical access control mechanism for WSN with node privacy," *Journal of King Saud University-Computer and Information Sciences*, 2020, doi: 10.1016/j.jksuci.2020.05.010.
- [9] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application," *Procedia computer science*, vol. 132, pp. 1243–1252, 2018, doi: 10.1016/j.procs.2018.05.040.
- [10] B. Rambabu, A. V. Reddy, and S. Janakiraman, "Hybrid artificial bee colony and monarchy butterfly optimization algorithm (HABC-MBOA)-based cluster head selection for WSNs," *Journal of King Saud University-Computer and Information Sciences*, 2019, doi: 10.1016/j.jksuci.2019.12.006.
- [11] S. Nashwan, "AAA-WSN: anonymous access authentication scheme for wireless sensor networks in big data environment," *Egyptian Informatics Journal*, vol. 21, no. 1, pp. 15-26, 2021, doi: 10.1016/j.eij.2020.02.005.
- [12] L. I. Dong, T. I. A. N Bin, and L. Shou-Shan, and Y. X. Yang, "A reliable and security method for data aggregation in WSNs," *The Journal of China Universities of Posts and Telecommunications*, vol. 18, pp. 142–146, 2018, doi: 10.1016/S1005-8885(10)60194-X.
- [13] Z. Huanan, X. Suping, and W. Jiannan, "Security and application of wireless sensor network," *Procedia Computer Science*, vol. 183, pp. 486–492, 2021, doi: 10.1016/j.procs.2021.02.088.
- [14] R. Rameke, S. Singh, and A. Malik, "Optimized routing technique for IoT enabled software-defined heterogeneous WSNs using genetic mutation based PSO," *Computer Standards & Interfaces*, vol. 79, p. 103548, 2022, doi: 10.1016/j.csi.2021.103548.
- [15] P. Maheshwari, A. K. Sharma, and K. Verma, "Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization," *Ad-hoc Networks*, vol. 110, p. 102317, 2020, doi: 10.1016/j.adhoc.2020.102317.
- [16] N. R. Maliseti and V. K. Pamula, "Performance of quasi oppositional butterfly optimization for cluster head selection in WSNs," *Procedia Computer Science*, vol. 171, pp. 1953-1960, 2020, doi: 10.1016/j.procs.2020.04.209.
- [17] M. Karpagam, P. Vinesha, D. Devi, and S. Karthika, "Reduction in information loss due to isolated and dumb nodes using ant colony optimization for WSN," *Materials Today: Proceedings*, 2020, doi: 10.1016/j.matpr.2020.10.081.
- [18] A. Lipare, D. R. Edla, and V. Kuppli, "Energy efficient load balancing approach for avoiding energy hole problem in WSN using grey wolf optimizer with novel fitness function," *Applied Soft Computing*, vol. 84, p. 105706, 2019, doi: 10.1016/j.asoc.2019.105706.
- [19] R. Bhatt, P. Maheshwary, P. Shukla, M. Shrivastava, and S. Changlani "Implementation of fruit fly optimization algorithm (FFOA) to escalate the attacking efficiency of node capture attack in wireless sensor networks (WSN)," *Computer Communications*, vol. 149, pp. 134–145, 2020, doi: 10.1016/j.comcom.2019.09.007.
- [20] M. M. Hamdi *et al.*, "A review on various security attacks in vehicular ad hoc networks," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 5, pp. 2627-2635, Oct. 2021, doi: 10.11591/eei.v10i5.3127.
- [21] M. M. Hamdi, L. Audah, S. A. Rashid, and S. Alani, "VANET-based traffic monitoring and incident detection system: A review," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 4, pp. 3193-3200, 2021, doi: 10.11591/ijece.v11i4.pp3193-3200.
- [22] H. O. B. Oloyede, M. C. Adaja, T. O. Ajiboye, and M. O. Salawu, "Human nature, the means-ends relationship, and alienation: Themes for potential EastWest collaboration," *Technology in Society*, vol. 13, no. 6, pp. 105-114, 2015, doi: 10.1016/j.techsoc.2015.03.005.
- [23] A. Vinitha, M. S. S. Rukmini, "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*, 2019, doi: 10.1016/j.jksuci.2019.11.009.
- [24] D. Thomas, R. Shankaran, M. A. Orgun, and S. C. Mukhopadhyay, "SEC2: a secure and energy efficient barrier coverage scheduling for WSN-based IoT applications," in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 622-634, June 2021, doi: 10.1109/TGCN.2021.3067606.
- [25] Z. Chen, W. Zhou, S. Wu, and L. Cheng, "An on demand load balancing multi-path routing protocol for differentiated services in MWSN," *Computer Communications*, vol. 179, pp. 296–306, 2021, doi: 10.1016/j.comcom.2021.08.020.
- [26] E. Elmahdi, Seong-Moo Yoo, and K. Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks," *Journal of Information Security and Applications*, vol. 51, p. 102425, 2020, doi: 10.1016/j.jisa.2019.102425.
- [27] V. Alappatt and P. M. J. Prathap, "Hybrid cryptographic algorithm based key management scheme in MANET," *Materials Today: Proceedings*, 2020, doi: 10.1016/j.matpr.2020.09.788.

BIOGRAPHIES OF AUTHORS






Yuosif Hardan Sulaiman     was born in Al_Anbar, Iraq. He was admitted to the degm ree of (Ph.D, Engineering Sciences)_Kharkiv National University of radio electronics Ukraine speciality: radio engineering and television systems. His research interests include meteor data transmission system. He can be contacted at email: yuosif_h_sulaiman@uoa.edu.iq.





Sami Abduljabbar Rashid    was born in Al-Anbar, Iraq. He received the B.Eng. degree in computer engineering technology from Al-Maarif University College, Iraq and the M.Sc. degree in communication and compute engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include wireless and mobile communications and VANET. He can be contacted at email: sami25.6.1989@gmail.com.




Mustafa Maad Hamdi    was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College, Iraq and the M.Sc. degree in Communication and Computer Engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include wireless and mobile communications, VANET, MANET, and satellite communication, and cryptographic. He can be contacted at email: meng.mustafa@yahoo.com.






Zaid Omar Abdulrahman Faiyadh    was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College. He can be contacted at email: zaidfaiyadh@gmail.com.



Abdulrahman Sabah Jaafar Sadiq    was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College. He can be contacted at email: hadisamir03@gmail.com.



Ahmed Jamal Ahmed    received the B.Eng. degree in Computer engineering and information Technology from Syrian International University for Science and Technology (SIUST), Syria, in 2010 and the M.S. and Ph.D. degrees in communication engineering wireless sensor network (WSN) from UTHM University Tun Hussein Onn Malaysia, Johor, Malaysia, in 2015 and 2018, respectively. Currently, he is a Senior Lecture at the Department of Computer Engineering Technique, Almaarif University college, Alramadi, Iraq. His research interests include WSN, WSN application, prolong lifetime of WSN, compression data, use compression data by WSN, power consumption of WSN, extend network of WSN, optimization WSN, Ad Hoc routing protocols, select best routing path, and distribute data throw WSN. He can be contacted at email: ahmed.jamal@uoa.edu.iq.