Improved Blowfish Algorithm based Secure Routing Technique in IoT based WSN

Majid Alotaibi
Department of Computer Engineering
College of Computer and Information Systems
Umm Al-Qura University, Makkah, Saudi Arabia.
EMAIL-mmgethami@uqu.edu.sa

ABSTRACT
Internet of Things (IoT) has gained popularity with the growth and prospects of smart networks. It is intended to exploit the network edges, which enables smart service and assessment for IoT. Moreover, this exploitation not only improves the user experiences but also provides service resiliencies at any catastrophe. The IoT appliances deploy distributed structure and proximity of end-users to offer quicker responses and improved quality of service (QoS). Nevertheless, security is mainly considered to resist the susceptibility of attacks. This work aims to introduce a novel secure routing model by carrying out optimal path selection and encryption. Initially, optimal link-state multipath routing takes place, where optimal paths or nodes are chosen for secure transmission. For optimal path selection destination and source, a Crossover Mutated Marriage in Honey Bee (CM-MH) algorithm is developed and proposed in this work. Next, encryption takes place that ensures secure transmission. In this research, an Improved Blowfish algorithm (IBFA) is proposed for secured authentication. Finally, the updates are monitored. At last, the supremacy of the developed approach is examined via evaluation over numerous existing techniques.

INDEX TERMS
Internet of Things, Optimal path, QoS, Improved Blowfish, CM-MH Algorithm

Nomenclature

| Abbreviation | Description                  |
|--------------|------------------------------|
| AES          | Advanced Encryption Standard |
| ATE          | Authentication and Encryption Model |
| API          | Application Programming Interface |
| CPA          | Chosen-Plaintext Attack       |
| CM-MH        | Crossover Mutated Marriage in Honey Bee |
| CCA          | Chosen-Ciphertext Attack      |
| CWOA         | CrowWhale optimization algorithm |
| CrowWhale-ETR| Crow Whale-energy trust routing |
| EE           | Energy Efficiency             |
| ETR          | Crow Whale-energy trust routing |
| FF           | Firefly                       |
| GA           | Genetic Algorithm             |
| IBFA         | Improved Blowfish algorithm   |
| IoT          | Internet of Things            |
| IDS          | Intrusion Detection System    |
| MHBRO        | Marriage in Honey Bee Optimization |
| PSO          | Particle Swarm Optimization   |
| PDE          | Perceptron Detection with Enhancement |
| PDR          | Packet Drop Rate              |
| QCMMR        | QoS-based Cross-layer Multichannel Multi-sink Routing protocol |
| QoS          | Quality Of Service            |
| RPL          | Routing Protocol for Low-Power and Loss Network |
| RSA          | Rivest–Shamir–Adleman         |
| SARF         | Secure and Scalable Routing Protocol |
| TP           | Two-Fish                      |
| TMG          | Trusted Multipath Graph       |
| TSS          | Threshold Secret Sharing      |
| VANETs       | Vehicular Adhoc Networks      |
| WSNs         | Wireless Sensor Networks      |

I. INTRODUCTION

“IoT refers to the rapidly growing network of connected objects that are able to collect and exchange data in real time using embedded sensors” [1-2]. The modelling of IoT should pay attention to multiple issues regarding communication and interconnection. There are numerous appliances in day-to-day life, where we employ sensors, laptops, mobile phones and household equipment namely, fridge, air conditioner, coffee maker, washing machines and microwave oven, which are gathered with IoT for carrying out a lot of activities [3-5]. In addition, IoT can be utilized together with vehicles using VANETs and it could be deployed for data collection routing [6-8].

The use of IoT devices has expanded tremendously as information and communication technologies have advanced. WSNs play an important role in the growth of the Internet of Things, and they are made up of low-cost smart devices that collect data. On the other hand, smart gadgets have limitations in terms of computing, processing, memory, and energy.
resources. Along with these limits, one of the most important problems for WSN is to accomplish reliability while maintaining data security in a vulnerable environment against malicious nodes. In IoT, WSNs is a significant element, which has concerned IoT and networking communities [9-12] [41-44]. Offering securities with optimal energy is a tough task in WSNs while nodes are mobile, as controlling nodes’ movement and moving adversaries is crucial regarding security. There are different types of attacks formed by adversaries [13]. A WSN with satisfactory software and hardware could seize the transferring data in an unauthentic manner [14-17].

To overcome such susceptible attacks or activities, IDS is deployed practically. IDS [18-19] is chiefly deployed in wired systems with the exploitation of h/w systems among nodes or servers to observe the network’s activities. Conventionally, IDS-oriented learning schemes were considered for evaluating existing networks i.e. not particularly for IoT systems [20]. Hence, it is essential to model the WSN nodes with EE, to formulate the associated protocols to enhance entire network quality with security while routing [20-24].

The major contributions are as follows.

1. As a novelty, this work proposes a new Crossover Mutated Marriage in Honey Bee model for optimal path selection between destination and source.
2. Also, it introduces an improved blowfish approach for secure data transmission.

The paper is organized as follows: Section II reviews the work. The developed Secure Routing Model in IoT-based WSN is illustrated in Section III. Link state multipath routing via optimal path selection is portrayed in Section IV. Section V portrays secure transmission via an improved blowfish model. Section VI and Section VII explain the results and conclusion.

II. LITERATURE REVIEW

A. RELATED WORKS

In 2019, Thangaramya et al. [8] have focused on enhancing the network using intellectual schemes, by which proficient routing decisions were made. Eventually, analysis was carried out and the accomplished outcomes have proved the efficacy of the proposed scheme about delay, lifetime, and PDR.

In 2020, Deebak and Fadi [24] established a new secure routing protocol via TF symmetric key model for recognizing and avoiding the challenges in the overall WSN. At last, the results accomplished using the adopted model have revealed its superiority over other models; and thereby, the multipath delivery was assured.

In 2020, Mauro et al. [25] have established a new scheme termed as SARP that resulted in effective routing in IoT networks. In addition, the adopted scheme helped in reducing the delay ratio, overhead and energy utilization, thus enhancing the effectiveness of the system performance.

In 2019, David et al. [26] have introduced a routing model termed as SecTrust-RPL for safeguarding the IoT from various types of attacks. Further, the efficacy of the adopted scheme was computed over another protocol, and its enhancement was established regarding robustness and efficiency.

In 2019, Lake et al. [27] adopted a robust and secure technique that facilitated the transmission of private information in IoT networks. Furthermore, the adopted scheme has assured the integrity and privacy of data even if there were more collusive and sophisticated attackers who could hijack the device.

In 2019, Liu et al. [28] have implemented a technique, which exploited both “K-means and perceptron” approaches for evaluating the trust values of IoT nodes and it also detected various malevolent nodes. To enhance the detection accuracy, the routing network was optimized via the PDE model. In the end, the accomplished resultants illustrated the superiority of the implemented scheme in detecting the malevolent node and eliminating it efficiently.

In 2020, Waqas et al. [29] have presented a novel QCM2R technique for WSNs. Accordingly, for verifying the enhancement of “QCM2R protocol”, implementations were done that demonstrated the superiority of the adopted model with regard to various measures like reliability, throughput, delay and life span.

In 2020, Badis et al. [30] adopted a “secured trust management and multipath routing model”, which were adapted to various scenarios in IoT networks. Finally, the simulated outcomes exposed the supremacy of the presented approach regarding scalability, efficiency and security.

In 2020, Shende, D.K. and Sonavane [39] have presented an energy-aware multicast routing protocol using the CrowWhale-ETR on the basis of objective function designed with the energy as well as trust factors of the nodes. To establish the routes that are chosen optimally utilizing CWOA, the nodes’ confidence and energy are first examined. This ideally chosen path is utilized for data transmission, in which the energy and trust of each node are updated at the end of each individual transmission, allowing for the selection of secure nodes and improving network security. From the analysis, it can be noticed that the proposed method attains minimal delay, maximal detection rate, energy and throughput in the presence and absence of attacks.

In 2020, Rahim [40] have suggested a Taylor-based Grey Wolf Optimization algorithm (TGWOA) to overcome the energy issue in WSN. The introduced method is the integration of the Taylor series with Grey Wolf Optimization, which helps in finding optimal hops to attain multi-hop routing. The aim of this method is to secure routing for conserving energy efficiently during routing. The presented method attains better performance of 23.8% of energy and...
53.2% of network lifetime. Table I illustrates the review on secure routing in IoT-based WSNs.

Table I. Review on existing secure routing in IoT based WSN systems

| Author             | Method            | Features                                      | Challenges                                                                 |
|--------------------|-------------------|-----------------------------------------------|-----------------------------------------------------------------------------|
| Tangaramya et al.  | Neuro-Fuzzy Rule  | High throughput, Minimal delay                | Becomes complex in terms of local path repair.                              |
| Deebak and Fadi    | TF model          | Multipath delivery, Increased security        | Real-time analysis is not carried out.                                      |
| Mauro et al.       | SARP method       | Reduced energy utilization, Minimal overhead   | Robustness is not evaluated.                                                |
| David et al.       | SecTrust-RPL      | Highly reliable Reduced packet loss           | Problems occur due to depleted battery power.                               |
| Bu et al.          | TSS method        | Ensures privacy, Resilient scheme             | Templates need to be adjusted                                              |
| Liu et al.         | PDE scheme        | Improved accuracy, Reduced error rate         | Attacks have to be detected collaboratively.                                |
| Waqas et al.       | QCME2R scheme     | Offers improved reliability, Extended lifetime| Becomes complex for local path repairs.                                     |
| Badis et al.       | TMG               | High delivery probability, Much appropriate   | Becomes non-operational under high dynamic ad hoc network.                  |
| Shende, D.K. and   | CWOA              | Maximum throughput                            | There is a need to determine the optimal routes to enable effective routing|
| Sonavane [39]     |                   |                                               |                                                                             |
| Rahim [40]         | TGWOA             | Improved scalability                          | The lifetime of the network is very low                                     |

B. RESEARCH GAP

- Numerous approaches have been focused on IoT-based WSN systems.
- However, the presented approaches are complex in terms of local path repair and issues due to depleted battery power and so on.
- Hence there is a need to propose a new secure routing model.
- This work aims to introduce a novel secure routing model.
- This is done by the optimal path selection and encryption using the CM-MH algorithm.
- In addition, an improved blowfish approach is introduced to secure data transmission.

III. DEVELOPED SECURE ROUTING MODEL IN IOT BASED WSN

Fig. 1 demonstrates the adopted secure routing in IoT-based WSN. The IoT-based WSN is an innovatory scheme for smart monitoring. This allows the development of grid sharing for maintaining power quality. The IoT data transfer is done via the Thingspeak application. Thingspeak is a web-based open (API) IoT source information platform that can store sensor data from a variety of "IoT applications" and display it in graphical form on the web. Thingspeak communicates with the host microcontroller via an internet connection that acts as a "data packet" carrier between the connected "things" and the Thingspeak cloud, which retrieves, saves/stores, analyses, observes, and works on the sensed data from the associated sensor to the host microcontroller.

The presented approach includes two stages, namely: (a) Link state multipath routing via optimal path selection and (b) secured transmission by Improved Blowfish algorithm. Initially, the network is generated. Further, optimal path selection is carried out, in which the optimal paths are chosen for data transmission. Here, optimal path selection is carried out by considering the constraints such as energy, delay, distance and trust. The use of energy is regarded as an essential concern in the WSN. In reality, if the battery in the WSN is employed, there will be no way to re-energize it, and there will be no power supply. In general, as the network performs multiple operations such as receiving, transmission, aggregation, and sensing, it consumes more energy. In this work, the energy is calculated by taking the mean of energy of nodes in the path. The trust is determined by the mean of trust of nodes in the path. Further, the distance is the distance among the nodes. After selecting the optimal paths for multipath routing, it is necessary to transmit the data securely through the paths. For secure transmission, this work deploys an improved blowfish algorithm. In addition, optimal path selection is carried out by exploiting the CM-MH model that aids in attaining the defined objective function precisely with optimal training.
FIGURE 1. Pictorial demonstration of the proposed technique

IV. LINK STATE MULTIPATH ROUTING VIA OPTIMAL PATH SELECTION

A. NETWORK GENERATION

Herein, the node counts are assigned for three variations, namely, 50, 100 and 150. The network area is fixed as 100 × 100. Moreover, each node is allocated with energy, distance, delay and trust.

(a) Energy

The energy consumption model declares the network model, which decreases energy in different operations such as transmission, reception, sensing, and idle state [48]. The energy is defined as the mean of energy of nodes in the path.

(b) Distance

The Euclidean distance is evaluated based on the distance computed between the nodes in the paths [49].

(c) Delay

The delay is termed as the time spent for the data packet to arrive at the destination [49].

(d) Trust

In this paradigm, trust is an important metric since it is preferable to choose a trusted node with lower power levels than an unreliable node with higher power levels. Furthermore, when determining the weights of nodes, the trusted node is given a higher priority. Trust is calculated by taking the mean of trust nodes in the path [50].

B. OPTIMAL PATH SELECTION

Here, the optimal path selection is carried out by determining the minimum distance, delay, and assigned trust of the node. Then, the transmission of data can be done by selecting the optimal path between source and destination. Here, a multipath selection process can be done. The
forwarding nodes from multi-channels are selected. The multi-paths are selected using the CM-MH algorithm.

C. OBJECTIVE FUNCTION AND SOLUTION ENCODING FOR OPTIMAL PATH SELECTION

In this work, the paths are optimally chosen for carrying out the data transmission. For this, a new CM-MH approach is introduced. The input solution to the proposed algorithm is shown in Fig. 2, wherein the paths with 0 values are dropped and the paths with 1’s are chosen as optimal paths. The chromosome length will be equivalent to the count of nodes in each path. The objective function of the developed model denoted by Obj is given in Eq. (1), wherein \( w \) signifies the weights that are randomly generated among 0 and 1 (i.e., \( w_1 + w_2 + w_3 + w_4 = 1 \)), \( D_e \) refers to delay, \( E \) refers to energy and \( T \) refers to trust.

\[
Obj = \min \left[ w_1 \times (1 - E) + w_2 \times (D_e) + w_3 \times (D_s) + w_4 \times (1 - T) \right]
\]

![Solution encoding](image)

**FIGURE 2.** Solution encoding

D. PROPOSED CM-MH MODEL

The existing MHBO model [21] reveals optimal solutions; however, it endures from low precision. To overcome the disadvantages of traditional MHBO, certain improvements are performed in the adopted algorithm. Self-improvements are established to be promising in existing optimization algorithms [13] [16-17] [22-23] [31-33]. MHBO tends to design the marrying behaviour of honey-bee in a bee-hive colony. A colony of honey bees usually is made of drones, queen(s), broods, and workers. Each member includes a definite task to perform in the colonies. The queen will be the mother of every other bee in colonies. The principal purpose of the queen is laying eggs to generate offspring. The drone is the father of a colony. The only job of the drone is to situate and are capable of catching her. After mating, the drone normally mate with the drones, which flutter the maximum flying far away from hives with the intention of mating with drones.

The mating flight count, count of prospective broods, drone count, and queen’s spermatheca dimension. The subsequent stage is the mating procedure. Before the mating flight, both the speed and energy of every queen are arbitrarily assigned with values in the ranges among [0.5, 1].

All through the mating flights, queens mate with a drone, including the higher marriage probability as shown in Eq. (2).

\[
\Pr(o(d_n, q_p)) = e^{-\Delta(f)}
\]

In Eq. (2), \( \Pr(o(d_n, q_p)) \) refers to the probability of a victorious mating among the queen \( q_p \) and drone \( d_n \); \( \Delta(f) \) refers to absolute divergence among fitness value of \( d_n \) and fitness value of \( q_p \). The mating probability is higher whilst the speed of the queen is higher or the fitness of drones is as superior as the queen. If mating is a success, the genotype of the chosen drone is stored in the spermatheca of queen. After every conversion, the queen’s speed and energy decline based on Eq. (3) and Eq. (6). Conventionally, the speed gets updated based on \( \alpha \) and \( P(t) \). In which \( \alpha \) refers to decay factor that includes a value among 0 and 1 and \( P(t) \) refers to speed of queen at time \( t \). As per the CM-MH scheme, the update takes place based on levy as shown in Eq. (3).

\[
P(t+1) = \alpha \times P(t) \oplus Levy(\delta)
\]

The Levy flight is evaluated by Eq. (4), where \( c \) is a constant factor and \( r_1 \) and \( r_2 \) are the random numbers between [0, 1]. Further, \( \gamma \) is computed using Eq. (5), in which \( \Gamma(x) = (x-1) \).

\[
Levy(x) = 0.01 \times \frac{r_1 \times \gamma}{r_2}^{\frac{1}{\beta}}
\]

\[
\Gamma(1+c) \times \sin \left( \frac{\pi}{2} \right) \left( \frac{e^{\frac{1}{2}}}{\Gamma\left(1+\frac{c}{2}\right)} \right)^{\frac{1}{\beta}}
\]

\[
En(t+1) = En(t) - \eta
\]

In Eq. (6), \( En(t) \) refers to queen’s energy at time \( t \); \( \eta \) refers to the quantity of energy diminution following every transition, is evaluated as in Eq. (7).
\[ \eta = 0.5 \times \frac{E_n(0)}{Q} \quad (7) \]

In Eq. (7), \( Q \) refers to size of the spermatheca of the queen. The queen tends to mate with another drone till her energy gets minimized than the fixed value of \( E_{n_{min}} \) is full. Subsequently, the queen goes back to hives to start its breed.

The 3rd phase is the “breeding and feeding process”. When every queen finishes their mating flights, the breeding procedure starts. Similar to GA, the breeding procedure is depending on 3 functions of selection; mutation and crossover. In the existing model, a novel brood is produced by the crossover of queen’s genotype with chosen sperm’s genotype and then the mutation is performed to novel brood for providing better solutions. However, as per the adopted model, multi-point crossover and scramble mutation takes place. As per the proposed scramble mutation, a subset of genes is selected from the chromosome and their values are scrambled arbitrarily. Moreover, while carrying out the proposed multi-point crossover, the alternating segments are exchanged to attain novel offsprings.

Algorithm 1: Pseudocode of CM-MH method

| Operation                           | Description                                                                 |
|-------------------------------------|-----------------------------------------------------------------------------|
| Initialization of population       |                                                                           |
| Initializing of initial constraints.|                                                                           |
| Compute the objective of all individuals |                                                                  |
| Choose \( N \) optimal individuals from population and allot them as queens | |
| For a predetermined mating flight’s count |                                          |
| Assign energy for all queens as per proposed levý based updated formulation in Eq. (3) | |
| Produce a pool of drones and compute the objective | |
| While energy > \( E_{n_{min}} \) and spermatheca is not filled | |
| Choose a drone with a higher probability of marriage | |
| Add sperms of chosen drone in spermatheca | |
| Update speed and energy of queen | |
| end while | |
| Produce broods as per proposed scramble mutation and multi-point crossover | |
| Utilize workers for enhance the broods | |
| Update fitness of workers | |
| While the best brood is better than the worst queen | |
| Substitute least fit queen with better brood | |
| Eliminate the enhanced brood | |
| end while | |

end for

V. SECURE TRANSMISSION VIA IMPROVED BLOWFISH MODEL

A. IMPROVED BLOWFISH ALGORITHM (IBFA)

In 1993, Bruce modelled blowfish as a free, fast substitute to conventional encryption approaches. It is gradually attaining recognition as a stronger encryption approach.

The Blowfish approach has numerous benefits [45]. It is efficient and appropriate for hardware execution and no license is necessary [34]. The basic operators of the Blowfish approach consist of XOR, addition and table lookup.

Some stipulations of the Blowfish approach are given in the below lines:

- Contains 64 bit blocks cipher with an uneven key length.
- Contains four 32-bit \( P \)-boxes and \( S \)-array. The \( S \)-array includes 18 of 32-bit sub-keys, whereas every \( P \)-box includes 256 entries.
- The approach includes two elements: “a key-expansion part and a data-encryption part”.
- The input is a data element of 64 bits.

The \( F \) operation deploys the substitution boxes, where there are 4, every one comprising 256 32-bit entries [35]. Conventionally, if block \( XL \) is split to 8-bit blocks \( a, b, c, d \) then function \( F(XL) \) is specified by Eq. (8). As per the improved blowfish model, \( F(XL) \) is formulated as shown in Eq. (9). Moreover, 64 bits of data is separated into four blocks with 16 bits per block each. As per the developed work, 256 bits key is separated into four equal 64-bit keys, which is shown in Fig 3 and 4.

**Case 1:**

\[
F(XL) = (P_{1a} + P_{2b} \mod 2^{32}) \oplus P_{3c} + P_{4d} \mod 2^{32} \quad (8)
\]

**Case 2:**

\[
F(XL) = (P_{1a} + P_{2b} \mod 2^{32}) \oplus (P_{3c} + P_{4d} \mod 2^{32}) \quad (9)
\]

Thus, the enhanced blowfish model securely broadcasts the messages to the destination.

**FIGURE 3:** Modified blowfish for case 1
VI. RESULTS AND DISCUSSIONS

A. SIMULATION SETUP

The introduced secure routing model via CM-MH was executed in Matlab with ThingSpeak. Here, in the IoT environment data transfer is done via ThingSpeak. The analysis of the proposed model was done with respect to CCA and CPA attacks by varying the size of data bits from 3KB, 5 KB, and 7KB. Consequently, the enhancement of the developed CM-MH model was measured by evaluating it over extant schemes, namely PSO [36], FF [37], GA [38] and MHBO [21], TGWOA [39], and CWOA [40] models. Here, convergence analysis was computed for different iterations that range from 0, 5, 10, 15, 20 and 25 for three-node variations, namely, 50, 100, and 150. In addition, encryption, as well as decryption time, were examined along with throughout computation by varying the size of data bits from 3KB, 5 KB, and 7KB. The simulation parameter is illustrated in Table II.

Table II. Simulation parameters

| S.No | Parameters | Value                |
|------|------------|----------------------|
| 1    | No of Nodes | 50, 100, 150         |
| 2    | Network Area | 100*100              |
| 3    | Node Energy | Selected randomly between 0 and 1 |
| 4    | Node Trust  | Selected randomly between 0 and 1 |

B. PERFORMANCE ANALYSIS

Table III describes the total cost analysis attained by the presented approach over extant approaches for varied counts of nodes, namely, 50, 100 and 150. The total cost is calculated by considering the energy, delay, distance, and trust. Further, the analysis on distance, energy, trust and delay are summarized in Table IV, V, VI, and VII, respectively. On noticing the examination resultant, the developed CM-MH model has obtained minimal cost values for all counts of node variations compared to the existing schemes. This ensures optimal path selection and secured data transmission by the proposed model. More particularly, the adopted scheme has achieved a least-cost value of 0.3236 while the node count is 50. That is, the developed approach is 25.45%, 32.72%, 25.88%, 29.11%, 28.71% and 29.11% enhanced than extant PSO, FF, GA, MHBO, TGWOA, and CWOA models when the node count is 50. In addition, the analysis on distance attained by the presented model over extant approaches for varied counts of nodes is shown in Table IV. The distance among node has to be minimal for the improved system performances. On noticing Table IV, the adopted scheme has attained a minimal distance value (0.6533) when the count of node is 50. The adopted scheme is 25.45%, 32.72%, 28.60%, 22.43% and 28.60%, superior to traditional PSO, FF, GA, MHBO, TGWOA, and CWOA models when the node count is 150. In addition, the analysis on distance attained by the presented model over extant approaches for varied counts of nodes is shown in Table IV. The distance among node has to be minimal for the improved system performances. On noticing Table IV, the adopted scheme has attained a minimal distance value (0.6533) when the count of node is 50. The adopted scheme is 25.45%, 32.72%, 28.60%, 22.43% and 28.60%, superior to traditional PSO, FF, GA, MHBO, TGWOA, and CWOA models. Likewise, when the node count is 150, the developed scheme has attained with a high trust value of 0.58136 than the extant approaches, thus making sure about the betterment of secured transmission of the introduced model. Thus proves the betterment of the suggested scheme over other conventional models.

Table III. Total cost evaluation of developed scheme over extant schemes for varied node counts

| Node variation | PSO  | FF   | GA   | MHBO | TGWOA | CWOA | CM-MH |
|----------------|------|------|------|------|-------|------|-------|
| 50             | 0.43412 | 0.48104 | 0.43662 | 0.4565 | 0.45394 | 0.4565 | 0.3236 |
| 100            | 0.4001 | 0.43417 | 0.39298 | 0.39211 | 0.40935 | 0.42494 | 0.33037 |
| 150            | 0.3758 | 0.36555 | 0.35434 | 0.35474 | 0.35766 | 0.365 | 0.2854 |

Table IV. Distance (meter) evaluation of developed scheme over extant schemes for varied node counts

| Node variation | PSO  | FF   | GA   | MHBO | TGWOA | CWOA | CM-MH |
|----------------|------|------|------|------|-------|------|-------|
| 50             | 0.70828 | 0.90594 | 0.81197 | 0.9151 | 0.84229 | 0.9151 | 0.6533 |
| 100            | 0.58136 | 0.64483 | 0.56667 | 0.60665 | 0.58977 | 0.66313 | 0.42576 |
| 150            | 0.52702 | 0.48998 | 0.47658 | 0.49911 | 0.51688 | 0.51589 | 0.37819 |

Table V. Energy (Joule) evaluation of developed scheme over extant schemes for varied node counts

| Node variation | PSO  | FF   | GA   | MHBO | TGWOA | CWOA | CM-MH |
|----------------|------|------|------|------|-------|------|-------|
| 50             | 0.45736 | 0.47571 | 0.51965 | 0.5146 | 0.47112 | 0.5146 | 0.65701 |
| 100            | 0.30594 | 0.47772 | 0.50058 | 0.54384 | 0.46368 | 0.4880 | 0.6523 |
| 150            | 0.48423 | 0.48109 | 0.48418 | 0.51416 | 0.5061 | 0.4981 | 0.6615 |

Table VI. Trust evaluation of developed scheme over extant schemes for varied node counts
### C. THROUGHPUT ANALYSIS

The throughput analysis of the developed CM-MH model is evaluated over extant models by varying the size of data bits from 3KB, 5 KB, and 7KB. “The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm” [46]. On analyzing the graphs, the presented CM-MH model has obtained better throughput values than compared schemes. In particular, higher throughput values guarantee the enhanced performance of the model. From Fig. 3, the presented CM-MH model has achieved a better throughput value, which is 56.67%, 76.67% and 13.79% improved than AES, RSA and BFA models when the counts of data bits is 3 KB. Thus, the adopted CM-MH model offered better throughput for every bit count.

![Throughput Analysis](image1.png)

**FIGURE 5.** Throughput Analysis of developed scheme over extant schemes for secure routing

### D. CONVERGENCE ANALYSIS

Fig. 6 describes the convergence (cost) analysis of the developed model over traditional optimization schemes regarding. Here, analysis is performed for a varied number of iterations that range from 0, 5, 10, 15, 20 and 25 for three-node variations, namely, 50, 100 and 150. The three-node variations are shown in Fig. 6 (a), 6 (b) and 6 (c) correspondingly. On focusing the results, the adopted approach has obtained minimal cost values for all iterations when evaluated over the extant models. From the graph, the presented model accomplishes a reduced cost value for the 25th iteration when the node count is 150. On noticing cost function from Fig. 6 (a), the developed model has attained minimal cost value that is 0.92%, 5.54%, 4.85%, 5.54%, 2.15%, and 2.32% superior to traditional PSO, FF, GA MHBO, TGWOA, and CWOA models, when the iteration is 25. Also, from Fig. 6 (c), the adopted scheme has attained minimal cost value when the iteration is 25, which is 2.02%, 2.31%, 2.88%, 5.19%, 0.7%, and 0.35% superior to traditional PSO, FF, GA MHBO, TGWOA, and CWOA models. Thus, the overall evaluation illustrates the effectiveness of the CM-MH scheme in attaining better results.

![Convergence Analysis](image2.png)

**FIGURE 6.** Convergence Analysis of developed scheme over extant schemes for secure routing

| Node variation | PSO | FF | GA | MHBO | TGWOA | CWOA | CM-MH |
|----------------|-----|----|----|------|-------|------|-------|
| 50             | 0.514 | 0.5061 | 0.546 | 0.57449 | 0.5554 | 0.5745 | 0.6423 |
| 100            | 0.475 | 0.4304 | 0.494 | 0.48836 | 0.4887 | 0.4753 | 0.5234 |
| 150            | 0.539 | 0.5377 | 0.5751 | 0.566 | 0.5801 | 0.5578 | 0.56423 |

Table VII. Delay (meter) evaluation of developed scheme over extant schemes for varied node counts
E. ATTACK ANALYSIS

The attack analysis for proposed IBFA over conventional models is shown in Fig. 7. Fig. 7(a) and Fig. 7(b) reveal the analysis on attacks such as CPA and CCA in that order. “CCA is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key” [47]. “During the CPA, a cryptanalyst can select arbitrary plaintext data to be encrypted and then he receives the corresponding ciphertext” [47]. Here, if the correlation between both the original text and hacked text are similar, then the value ranges between 0 to 1. From the graph, it can be noticed that the proposed CM-MH algorithm attains a negative value in Fig. 7(a) and Fig. 7(b), which shows that the correlation between both the original text and hacked text is very low than the existing models like AES, RSA and BFA. Hence, it is evident that the proposed scheme cannot get hacked easily than other existing models. The attack performance of adopted CM-MH attained better outcomes than the extant schemes like AES, RSA and BFA, respectively. Moreover, the CCA performance of the developed model from Fig. 7(a) attained a minimal value of 0.08, which is 90%, 73.33% and 62.5% improved than AES, RSA and BFA models when the counts of data bits is 3 KB. This shows the betterment of the proposed CM-MH secured data transmission.

F. COMPUTATIONAL TIME ANALYSIS

The encryption, and decryption time taken by the developed IBFA model, is evaluated over extant models by varying the size of data bits from 3KB, 5 KB and 7KB. Consequently, the results for encryption time and decryption are time exposed in Fig. 8 (a) and Fig.8 (b) in that order. On analyzing the Tables, the presented IBFA model has obtained better outcomes than compared schemes. In particular, minimal time values guarantee the enhanced performance of the model with minimal computational time. From Fig. 8 (a), the presented IBFA model has achieved minimal encryption time value, which is 60%, 75% and 50% improved than AES, RSA and BFA models when the counts of data bit is 3 KB. Moreover, the presented IBFA model has achieved negligible decryption time value, which is 40%, 80.77% and 20% improved than AES, RSA and BFA models when the counts of data bit is 5 KB. These analyses have proved the supremacy of the proposed IBFA model in quicker computation on secured data transmission.
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3130005, IEEE Access

This paper introduces a new secure routing model by carrying out optimal path selection and encryption. At first, the optimal link-state multipath routing was performed in which the optimal paths or nodes were selected for secure transmission. Moreover, the CM-MH algorithm is proposed to select the optimal path. Besides, encryption takes place using improved BFA that ensures secure transmission. On noticing the results, the developed approach attained a minimal distance value (0.7933) when the count of the node is 50. That is, the adopted scheme was 2.35%, 15.35%, 6.18% and 15.35% superior to traditional PSO, FF, GA and MHBO models. Likewise, when the node count is 150, the developed scheme has attained a superior trust value of 0.58136, which was higher than the extant approaches. Moreover, the presented CM-MH model has achieved negligible decryption time value, which was 40%, 80.77% and 20% improved than AES, RSA and BFA models when the counts of data bits is 5 KB. Thus the efficacy of the developed CM-MH method was confirmed from the outcomes.

REFERENCES

[1] A. Raof, A. Matrawy and C. Lung, “Routing Attacks and Mitigation Methods for RPL-Based Internet of Things,” in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1582-1606, Secondquarter 2019.
[2] Subramanian Balaji, Enoch Golden Julie, Yesudhas Harold Robinson, Raghvendra Kumar, Le Hoang Son, “Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model”, Computer Standards & Interfaces, vol.06, October 2019, Article 103358.
[3] Nadav Schweitzer; Ariel Stulman; Roy David Margalit; Asaf Shabtai, “Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks”, IEEE Journals & Magazines, Vo.16, no.08, pp. 2174 - 2183, 2017
[4] Tong Xu; Deyun Gao; Ping Dong; Hongke Zhang; Chuan Heng Foh; Han-Chieh Chao, “ Defending Against New-Flow Attack in SDN-Based Internet of Things”, IEEE Journals & Magazines, Vol.05, pp.3431 - 3443, 2017.
[5] Richard K. Lomotey, Joseph Pry, Sumanth Sriramoju, “Wearable IoT data stream traceability in a distributed health information system”, Pervasive and Mobile Computing, 15 July 2017.
[6] S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, G. Cavone, “ LICTUS: A lightweight and standard compatible framework for securing layer-2 communications in the IoT”, Computer Networks, Vol. 108, pp. 66-77, 24 October 2016
[7] Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahman, Ethiopia Nigussie, Hannu Tenhunen, “SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways”, Procedia Computer Science, Vol. 52, pp. 452-459, 2015.
[8] K.Thangararanyam, K.Kulothungan, R.Logambigai, M.Selvi, SannaasGanapathy and A.Kannan, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT", Computer Networks, vol. 151, pp. 211-223, 14 March 2019.
[9] Bo Zhou, Qian Zhang, Qi Shi, Qiang Yang, Yinyan Yu, “Measuring web service security in the era of Internet of Things”,Computers & Electrical Engineering, 28 June 2017.
[10] Vasileios A. Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, B.B. Gupta, “An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework”, Future Generation Computer Systems, 9 May 2017.
[11] Caryntha Kharkongor, T. Chithralekha, Reena Varghese, “A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT)”, Procedia Computer Science, Vol. 89, 2016, pp. 218-227.
[12] Stefano Tedeschi, Jorn Melhem, Nikolaos Tapoglou, Rajkumar Roy, “Secure IoT Devices for the Maintenance of Machine Tools”, Procedia CIRP, Vol. 59, pp. 150-155, 2017.
[13] B. R. Rajakumar and Aloyius George, “A New Adaptive Mutation Technique for Genetic Algorithm”, In proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pages: 1-7, December 18-20, Coimbatore, India, 2012, DOI: 10.1109/ICCIC.2012.6310293.
[14] Mahmood Salehi, Azzedine Boukerche, Amir Darehshoorradeh, “Modeling and performance evaluation of security attacks on opportunistic routing protocols for multi-hop wireless networks”,Ad Hoc Networks, Vol. 50, pp. 88-101,1 November 2016.
[15] Christopher W. Badenhop, Scott R. Graham, Benjamin W. Ramsey, Barry E. Mullins, Logan O. Mailoux, “The Z-Wave routing protocol and its security implications”, Computers & Security, Vol. 68, pp. 112-129, July 2017.
[16] S. M. Swamy, B. R. Rajakumar and I. R. Valarmathi, “Design of Hybrid Wind and Photovoltaic Power System using Opposition-based Genetic Algorithm with Cauchy Mutation”, IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), Chennai, India, Dec. 2013, DOI: 10.1049/ic.2013.0361.
[17] Aloyius George and B. R. Rajakumar, “APOGA: An Adaptive Population Pool size based Genetic Algorithm”, AASRI Procedia - 2013 AASRI Conference on Intelligent Systems and Control (ISC 2013), vol. 4, pages: 288-296, 2013, DOI: https://doi.org/10.1016/j.aasri.2013.10.043.
[18] K. Sudeendra Kumar, G. Hanumanta Rao, Suvagya Sahoo, K.K. Mahapatra, “Secure split test techniques to prevent K piracy for IoT devices”, Integration, the VLSI Journal, Vol. 58, pp 390-400, June 2017.
[19] Angelo Furfaro, Luciano Argento, Andrea Parisi, Antonio Piccolo, “Using virtual environments for the assessment of cybersecurity issues

VII. CONCLUSION

FIGURE 8. Time Analysis of developed scheme over extant schemes for (a) Encryption (b) Decryption

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
in IoT scenarios”, Simulation Modelling Practice and Theory, vol. 73, pp. 43-54, April 2017.

[20] Ming Tao,Xueqiang Li,Wenhong Wei, “UAV-Aided trustworthy data collection in federated-WSN-enabled IoT applications”, Information Sciences, vol. 532 (Cover date: September 2020), pp. 155-169, 13 May 2020.

[21] Abbass, Hussein. (2001). MBO: marriage in honey bees optimization- a Haplometrosis polygynous swarming approach. Proceedings of the IEEE Conference on Evolutionary Computation, ICEC. 1. 207 - 214 vol. 1. 10.1109/ICEC.2001.934391.

[22] B. R. Rajakumar, “Impact of Static and Adaptive Mutation Techniques on Genetic Algorithm”, International Journal of Hybrid Intelligent Systems, Vol. 10, No. 1, pages: 11-22, 2013, DOI: 10.3233/HIS-120161.

[23] B. R. Rajakumar, “Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis”, International Journal of Computational Science and Engineering, Vol. 8, No. 2, pages: 180-193, 2013, DOI: 10.1504/IJCSSE.2013.053087.

[24] Deebak B.D., Fadi Al-Turjman, “A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks”, Ad Hoc Networks, vol.97, February 2020, Article 102022.

[25] Mauro Conti, Pallavi Kaliyar, Md Masoom Rabbani, Silvio Ranise, “Attestation-enabled secure and scalable routing protocol for IoT networks”, Ad Hoc Networks, vol,96, 1 March 2020, Article 102054.

[26] David Airehrour, Jairo A.Gutierrez and Sayan KumaR Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things”, Future Generation Computer Systems, vol. 93, pp. 860-876, April 2019.

[27] Lake Su, Mihailo Isakov, Michel A. Kinsy, “A secure and robust scheme for sharing confidential information in IoT systems”, Ad Hoc Networks, vol.92, September 2019, Article 101762.

[28] Liang Liu, Zuochao Ma, Weizhi Meng, “Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks”, Future Generation Computer Systems, vol.101, pp.865-879, December 2019.

[29] Waqas Rehan, Stefan Fischer, Maaz Rehan, Yasser Mawad, Shahzad Saleem, "QCM2R: A QoS-aware cross-layered multichannel multistink routing protocol for stream based wireless sensor networks", Journal of Network and Computer Applications, vol.156, 15 April 2020, Article 102552.

[30] Badis Hammi, Sherali Zeadally, Houda Labiod, Rida Khatoun, Lyes Khoukhi, “A secure multipath reactive protocol for routing in IoT and HANETs”, Ad Hoc Networks, vol. 103, 1 June 2020, Article 102118.

[31] Mukund B. Wagh and Dr. Gomathi N, "Improved GWO-CS Algorithm-Based Optimal Routing Strategy in VANET", Journal of Networking and Communication Systems, Vol.2,No.1, pp.34-42.2019.

[32] Sadashiv Halbhavi B,Kodad S F,Ambarak S K,Manjunath D, "Enhanced Invasive Weed Optimization Algorithm with Chaos Theory for Weightage based Combined Economic Emission Dispatch", Journal of Computational Mechanics, Power System and Control, Vol.2,No.3, pp.19-27.2019.

[33] Amolikumar Narayan Jadhav,Gomathi N, "DIGWO: Hybridization of Dragonfly Algorithm with Improved Grey Wolf Optimization Algorithm for Data Clustering", Multimedia Research, Vol.2,No.3, pp.1-11.2019.

[34] Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, no. 6, August 2012.

[35] Russell K. Meyers and Ahmed H. Desoky “An Implementation of the Blowfish Cryptosystem”, IEEE, 2008.

[36] Junhao Zhang, Pinqi Xia, “An improved PSO algorithm for parameter identification of nonlinear dynamic hysteretic models”, Journal of Sound and Vibration, vol. 389, pp. 153-167, 17 February 2017.

[37] Iztok Fister, Iztok Fister, Xin-She Yang, Janez Brest, "A comprehensive review of firefly algorithms", Swarm and Evorimorpution Computation, vol. 13, pp. 34-46, December 2013

[38] John McCall, “Genetic algorithms for modelling and optimisation”, Journal of Computational and Applied Mathematics, vol. 184, no. 1, pp. 205-222, 1 December 2005.

[39] Shende, D.K. and Sonavane, S.S., 2020, “Crow-Whale-ETR: Crow-Whale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications”, Wireless Networks, pp.1-19.

[40] Rahim, Robbi, S. Mutugan, S. Priya, S. Magesh, and R. Manikandan. "Taylor based grey wolf optimization algorithm (TGWOA) for energy aware secure routing protocol." International Journal of Computer Networks and Applications (IJCNA) 7, no. 4 (2020): 93-102.

[41] Deebak, B.D. and Al-Turjman, F., 2020. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Networks, 97, p.102022.

[42] Haseeb, K., Almoqren, A., Islam, N., Ud Din, I. and Jan, Z., 2019. An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. Energies, 12(21), p.4714.

[43] Haseeb, K., Islam, N., Almoqren, A. and Din, I.U., 2019. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. Ieee Access, 7, pp.185496-185505.

[44] Yang, T., Xiangyang, X., Peng, L., Tonghui, L. and Leina, P., 2018. A secure routing of wireless sensor networks based on trust evaluation model. Procedia computer science, 131, pp.1156-1163.

[45] Schneider, B., “Description of a new variable-length key, 64-bit block cipher (Blowfish)”, In International Workshop on Fast Software Encryption (pp. 191-204), Springer, Berlin, Heidelberg, 1993, December.

[46] Abd Elmainam, D.S., Abdal-Kader, H.M. and Hadhoud, M.M., 2010. Evaluating The Performance of Symmetric Encryption Algorithms. Int. J. Netw. Secur., 10(3), pp.216-222.

[47] https://en-academic.com/dic.nsf/enwiki/63077

[48] Jaganathan, V., Palanisamy, B. and Milanova, M., 2016. Recent trends and techniques in computing information intelligence.

[49] Sarma, S.K., 2020, August. Energy aware Cluster based routing for Wireless Sensor Network in IoT: Impact of Bio-inspired Algorithm. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 198-206). IEEE.

[50] Yang, T., Xiangyang, X., Peng, L., Tonghui, L. and Leina, P., 2018. A secure routing of wireless sensor networks based on trust evaluation model. Procedia computer science, 131, pp.1156-1163.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3130005, IEEE Access

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/