Research Article
Volume 9:1, 2020

International Journal of
Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Mid Square Hash Bezier Secured Routing for IoT Enabled Wireless Sensor Networks

Renuka Mohanraj*

Department of Computer Science, Maharishi International University, Fairfield, Iowa, USA

Abstract

The swift uptake of sensors and the increasing demand of Wireless Sensor Network (WSN) applications and services create unmatched appeals for routing data packets on WSN infrastructure. In the era of Internet of Things (IoT), an immense number of sensing devices collect numerous sensor data over time for an extensive span of fields. For IoT-enabled devices routing through WSN, sensor nodes transmit confidential data to the gateway nodes via public channels. In such an environment, secured routing remains a serious issue that has to be addressed. To address this issue, in this work, a robust method using Mid Square Hash-based Bezier Authentication (MSH-BA) is designed to secure the routing for IoT-enabled WSNs. First, a Mid Square Hashing Data Collection algorithm is proposed to minimize the energy consumption through unique key generation. To minimize the running time of IoT sensor network, discrete registration is performed between user and gateway nodes. Finally, the proof of correctness of mutual authentication is performed using the Bezier Authentication method via progressive distance, therefore ensuring packet delivery ratio. The robust authentication method is analyzed comprehensively and compared against the similar authentication methods and the results showed that it is efficient and robust than earlier methods.

Keywords: Wireless sensor network • Internet of things • Mid Square Hash • Data collection • Bezier authentication

Introduction

The Internet of Things (IoT) is evenly voyaging from an Internet of people concerning IoT. Based on the finding of Cisco [1], in 2020, to an extent of 50 billion things are linked to the Internet, thus concealing the data originated by humans. According to the characteristics, the things to be connected to Internet heavily differ. This difference ranges from very small and static devices to large and mobile devices. Such changes persuade complication and specify the presence of an advanced middleware used for concealing this heterogeneity and boost clarity.

In specific, WSNs are linking things to Internet via gateway node that interfaces WSN to the Internet. Unlike other networks, like, Ad hoc network, MANET, WSNs possess specific characteristic of collecting the sensed data like, temperature, pressure, fire detection, etc., and forwarding it to the gateway via single or two-way communication and react accordingly. However, secure routing in IoT-enabled WSN still remains challenging.

To provide solution to this issue, a Secure Data Transmission Scheme (SDTS) was designed in [2] with the objective of improving the communication security in WSNs. The SDTS was designed based on Elliptic Curve Cryptography (ECC) as it ensures higher level of security. Also, confidentiality, integrity and authentication were said to be achieved via separate encryption and decryption. With the application of SDTS using ECC, security aspects such as confidentiality, integrity, and authentication were said to be ensured. However, with increase in volume of data in WSN, by expansion of IoT and its increasing popularity, necessity to maintain secured routing has become a demanding task to be addressed.

In [3], a green routing algorithm using Fork and Join Adaptive Particle Swarm Optimization (FJAPSO) was presented to increase the sensor network lifetime via selecting optimal number of control nodes and optimal clustering of control nodes. However, with billions of smart objects communicating with each other, routing gets yet complicated and again security becomes a major concern.

To ensure secure transmission for long range, a LoRa mesh networking system was designed in [4] that transmitted packets of different buffers via multiple channels. With the swift implementation and expansion of the Internet of things (IoT) energy-efficient routing in WSN for IoT have emerged as a crucial area of research in the current years. Particle swarm optimization (PSO) algorithm was designed in [5] to address issues related to congestion with energy-efficient routing. Yet overview of WSN towards IoT was presented in [6]. The unanticipated traffic deceleration specifically in fast scrolling highways designated by a scanty visibility is one of the crucial causes of accidents among motorized vehicles. A probable alternate solution to address this issue by installing mobile traffic sensors using IoT cloud system was designed in [7].

The Internet of things (IoT) that combines different set of devices into networks assists in providing advanced and intelligent services. In [8], IoT security solutions depends on machine-learning (ML) techniques were reviewed using supervised learning, unsupervised learning, and reinforcement learning (RL). Yet another monitoring of open-field livestock and poultry breeding environment based on IOT were designed in [9]. With the distinguished potential of IoT, there comes an extensive range of problems.

In [10], different routing protocols and security challenges were

***Address for Correspondence:** Dr. Renuka Mohanraj, Department of Computer Science, Maharishi International University, 1000 N 4th St, Fairfield, Iowa, 52557, USA; E-mail: rmohanraj@mum.edu/mr.renuka@gmail.com*

Received 23 December, 2020; **Accepted** 04 February 04, 2020; **Published** February 11, 2020

addressed based on secure loading routing protocol. However, energy efficiency remained unsolved. In [11], an energy-efficient transmission scheme using secrecy outrage probability and secure energy efficiency was designed. To improve security, strong authentication mechanisms are required. With this objective, a mutual authentication mechanism using BAN logic model was investigated in [12].

A wearable Internet of Things aimed at ensuring safety with low power consumption was presented in [13]. During packet broadcasting, identifying route between source and destinations were found to be time consuming and complex process. If not handled properly, results in congestion. In [14], a routing scheme to avoid links possessing higher congestion, therefore addressing conflicts in routing was designed. With the swift increase in the area of Internet of Things (IoT) results in immense formation of sensors, hence requiring automatically reconfigurable complex WSN.

A WSN based IoT platform was designed in [15] for heterogeneous sensing applications. Using Fork and Join Adaptive Particle Swarm Optimization (FJAPSO), a reliable connection between sensors and database on the Internet was said to be established. Due to this TSCH protocol, multi-hop transmission, collision-free transmission, and high energy efficiency was also said to be achieved. Furthermore, to minimize the energy consumption, a novel synchronization scheme and a burst transmission feature was also presented, therefore, fulfilling high throughput requirement for high-rate applications and long battery life for low-rate applications at the same time. However, with the resource constrained IoT devices, secure transmission was not said to be ensured.

To address this issue, in [16], multipath load balancing routing was designed to estimate future load, therefore resulting in lower packet loss and better routing connectivity. In modern years, Internet of Things (IoT) has made exceptional advancement in human beings from healthcare applications [17] to day to day task. This is because the IoT warrants everyday object to be associated to the Internet. However, in Smart Home and Ambient Assisted Living (SHAAL) is heavily based on the aggregation and resource allocation, where virtualization of sensor network plays a major role. In [18], a secure and energy aware middleware framework was designed for ensuring both sensor and network virtualization. Yet another secure block chain technology was designed in [19], addressing both integrity and authentication.

This paper endeavors to propose three novel composite modules to ensure secure routing for IoT-enabled WSNs. With the objective of providing secured routing for IoT-enabled WSNs, first, Mid Square Hashing Data Collection algorithm is designed which involves IoT device filtering by applying Mid Square Hashing. Next, discrete registration is performed between the user and the gateway node by applying two step processes to generate unique secret key. Finally, Progressive Bezier Authentication is employed to differentiate the malicious and non-malicious route and perform secured routing ensuring smooth data transmission accordingly by applying Progressive Distance.

This paper is ordered as follows. In this paper Section 2 details the system model that includes network model and energy model in detail. Section 3 presents the methodology. Section 4 introduces the modeling and simulation parameters along with the detailed discussion involving comparison with the state-of-the-art methods. Section 5 presents the conclusion.

The System Model

In this section, the network model and energy model used for the design of energy efficient secured routing in IoT for WSN based on Progressive Bezier Authentication by applying Progressive Distance is presented. To start with, the network model is designed for IoT. Followed by which, the energy consumption model applying multipath fading is presented.

Network model

A network model [20] illustrated in Figure 1 is followed in this work for providing secured routing in IoT for WSN. Figure 1 shows the network model. Figure 1 consists of a Gateway Node 'GN' with resource constrained sensors 's_i' and resource rich cluster head nodes 'CH_j'. In this work, numerous sensors are employed in different disjoint clusters. A sensor node 's_i' in a specific cluster 'cl_k' send its sensed information to its own cluster head 'CH_j', followed by which the cluster head 'CH_j' forwards the information to the gateway node 'GN'. Here, cluster only refers to group where similar data are sensed and placed. For example, data pertaining to temperature is sensed and positioned in 'cl_1', data pertaining to pressure is sensed and positioned in 'cl_2'.

As illustrated in the Figure 1, the communication between sensors and their corresponding cluster heads and the Gateway Node are performed and accessed via the wireless channels.

Energy model

In this work, a widely adopted energy consumption model based on multipath fading 'E_{mf}' is adopted. The multipath fading energy consumption model is designed based on distance among two nodes, the transmitter and the receiver node. Let '(p_i, p_j)' and '(q_i, q_j)' represents the coordinates of the transmitter and receiver 'i' and 'j' respectively, then the Euclidean distance is measured as given below.

$$Dis = \sqrt{(p_i - p_j)^2 + (q_i - q_j)^2} \text{ ----------} \quad (1)$$

To transmit a '1-bit' message with a distance 'Dis', the required transmission energy consumption for a sensor node 's_i' is calculated as given below.

$$E_{TX\_S_i}(l, Dis) = E_{TX} - elec(l) \text{ ----------} \quad -(2)$$

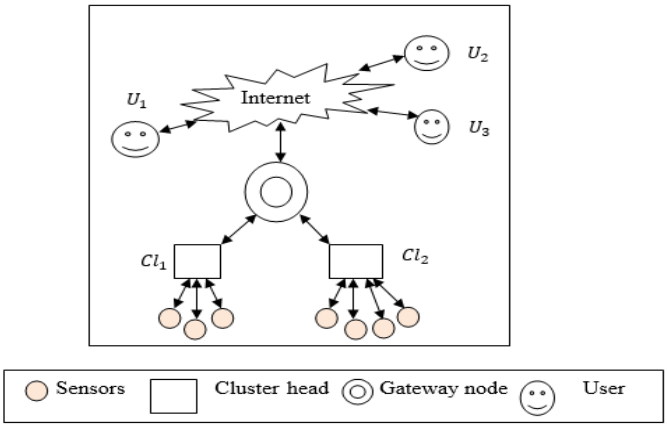

Figure 1. Network model.

To measure the energy transmission for receiving a $'l-bit'$ message for a sensor node 'S_i' is calculated as given below.

$$E_{RX_{S_i}}(l) = \mathrm{E}_{RX} - elec(l) \text{ ----------} \quad (3)$$

With the above network and energy model, a Mid Square Hash-based Bezier Authentication method is designed in this work for providing secured routing in IoT-enabled WSNs.

Mid square hash-based bezier authentication

Routing algorithms were designed by several researchers with the objective of optimizing the energy being consumed by automatically adjusting the number of clusters [3]. However, security aspects for IoT enabled WSN were not focused. This is an overhead in FJAPSO [3] which may affect the packet delivery ratio. Besides, as IoT devices such as sensors generally possess resource and computation constraints, secured routing challenges usually have degraded performance in IoT system. Therefore, Secure Region-based Routing in WSN using Bezier Curves is designed that assist in building light-weight access control protocols to minimize energy consumption and therefore reducing the running time and subsequently improving the network lifetime with higher packet delivery ratio of IoT systems. This section presents overall workflow. Figure 2 illustrates the experiment workflow structure of Mid Square Hash-based Bezier Authentication (MSH-BA) for secured routing consisting of three modules.

As illustrated in the Figure 2, the first module is data collection where the cluster head captures the network traffic and transmits the network traffic data collected to the next part. This stage is performed by Mid Square Hashing Data Collection algorithm. In the second module, which is the actual registration phase, registration is performed between the user and gateway node using discrete registration. The Progressive Bezier Authentication entails the final module, whereby the IoT devices respond to the routing initiation via route request '**RREQ**' and routing termination via route reply '**RREP**' to stimulate the authentication accuracy. The following sections communicate each module in detail.

Network traffic data collection

To start with, IoT architecture comprises networked things, i.e., the wireless sensors. Here, the network traffic pertaining to IoT architecture is analyzed by applying Mid Square Hashing Data Collection algorithm. WSN comprises several resource constrained sensors 's_i' that are limited in memory, energy, and processing capacity, and a proportional number of Gateway Nodes 'GN'.

As shown in the Figure 2, the IoT device (i.e., the cluster head) filter the TCP packets and selects the features among several features like, the IP address, protocols, file type, frame number, frame length, labels them and extracts these features, therefore ensuring multipath fading. By filtering the TCP packets vial multipath fading, this phase (i.e. the cluster head) also collects the WSNs network traffic data like, the identification of each sensor 's_i', 's_i(ID)' and authentication key between the gateway node and the sensor node ID, 'AK_i' using the Algorithm 1 Mid Square Hashing Data Collection algorithm.

As given in the above Mid Square Hashing Data Collection algorithm, for each gateway node with different sensors, the cluster head performs three different tasks. They are, measuring the distance among transmitter and receiver. Followed by which, the transmission and receiver energy consumption is measured. Finally, with the resultant values obtained, the authentication key 'AK_i' between the gateway node and the sensor node ID is generated and is mathematically formulated as given below.

$$\mathrm{AK}_i = Mid\_Square\_H(\mathrm{P}_{GN} \mid s_i(\mathrm{ID})) \text{ ----------} \quad (4)$$

From the above equation (4), the authentication key 'AK_i' is obtained by mid square hashing via cluster head. This is performed via identification of sensor node 's_i(ID)', randomly generated password by gateway node 'P_{GN}'. With these two measures, unique keys are generated. The obtained 's_i(ID)' and 'AK_i' for each IoT devices are obtained that possess the advantages of generating unique keys.

Two user discrete registration phase

Along with the collected data and unique authentication key generated by the cluster head, registration between the user 'U_i' and the gateway node 'GN' is performed. In this registration phase, the user 'U_i' registers his/her self for route request. This two-user discrete registration is also performed by the cluster head. Figure 3 illustrates the Two User Discrete Registration phase, corresponding to two users, user 'U_i' and gateway node 'GN' via the cluster head 'CH'.

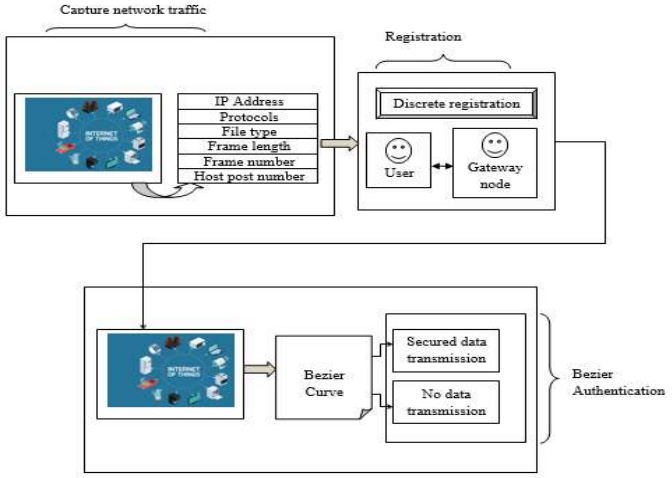

Figure 2. Mid square hash-based Bezier authentication.

Input: Gateway Node 'GN', Sensors 'S_i', Cluster Head 'CH_j'
Output: Unique authentication key generation
1: **Begin**
2: **For** each Gateway Node 'GN' with Sensors 'S_i' and Cluster Head 'CH_j'
3: Measure Euclidean distance between coordinates of the transmitter and receiver using (1)
4: Measure transmission energy consumption using (2)
5: Measure receiver energy consumption using (3)
6: Obtain authentication key between Gateway Node 'GN' and Sensors 'S_i' using (4)
7: **End for**
8: **End**

Algorithm 1. Mid square hashing data collection algorithm.

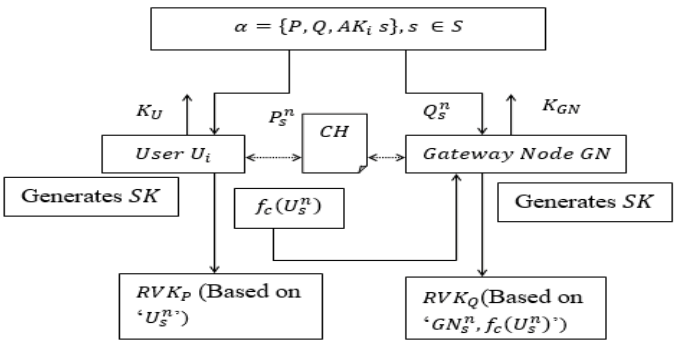

Figure 3. Two user discrete registration phase.

As illustrated in the Figure 3, the Two User Discrete Registration is used for registration between the user and the gateway node via cluster head. Two users, user U_i and the gateway node GN, observes a compound $\alpha = \{P, Q, AK_i, s\}, s \in S$ for time duration $n \in N$. User U_i, and the gateway node GN has the goal to generate a shared $SKK_U = K_{GN}$. Hence, $K_U, K_{GN}, P_s^n, Q_s^n$ represent their initial representation for the source state $s \in S$. Then, the two-user discrete registration with source $\alpha = \{P, Q, AK_i, s\} s \in S$ consists of the following two steps.

The first step is after observing $'P_s^n'$, the user chooses its ID 'U_iID' and transmits a message $'f_c(P_s^n)'$ to the gateway node over the public secured wireless channel via cluster head. Here, 'f_c' is referred to as the public communication function. The first step is mathematically formulated as given below.

$$RVK_P : U_s^n \rightarrow (f_c(P_s^n), U_i ID : GN) \text{ ----------} \quad (5)$$

Next, the gateway node computes the parameters for user. The user generates a secret key 'SK', represented by an arbitrary variable 'AV', 'AV K_U'. The gateway node generates a secret key 'SK', represented by a 'AV K_{GN}'. This is mathematically formulated as given below.

$$RVK_Q : GN_s^n \rightarrow SK, Q_s^n, fc(P_s^n) \text{ ----------} \quad (6)$$

From the above two equations (5) and (6), the gateway node 'GN' saves all the parameters $'SK, Q_s^n, fc(P_s^n)'$ and sends them to the user 'U_i' via a secure channel. So, whenever the user makes route request, it sends the data to sensors using the parameters and only upon successful comparison of the parameters, successful route reply is said to be accomplished, ensuring smooth data transmission. The detailed process is elaborated as given below.

In Algorithm 2, for each Gateway Node '**GN**' with user 'U_i' and generated Authentication Key 'AK_i' the objective of the above algorithm is to perform registration between the user and gateway node to ensure secured routing. This is performed using two steps. The first step involved is the registration by the user via cluster head. The second step involved is the registration by the gateway node via cluster head. By these two steps, two user's discrete registration, route request is placed. Only upon successful route reply, smooth transmission is said to take place. The proposed method uses a combination of energy aware metrics and control points via Bezier curve to select an appropriate node for routing. This is elaborated in the forthcoming section.

Progressive bezier authentication

In this section, finally, the authentication is performed so that either secure routing is ensured, or no routing is said to take place. This is performed by applying the Bezier Authentication method via control points using progressive distance. In order to establish robust secure routing process while ensuring soft guarantees regarding the timely delivery of data-packets, Progressive Bezier Authentication method is used. Figure 4 shows the block diagram of Progressive Bezier Authentication.

As shown in the Figure 4, a family of four Bezier curves is used as alternate routes for a given source, gateway node 'S, GN', in addition to the direct line segment between the source and the gateway node.

Each of these curves as illustrated in the Figure 4 involves a coherent polynomial of a third degree possessing four control points 'CP' to establish it. Besides, the coordinates of these four control points represent the only overhead in terms of transmission cost.

Input: Gateway Node '*GN*', Authentication Key 'AK_i', User 'U_i', Arbitrary Variable '*AV*'
Output: Computational efficient registration
1: **Begin**
2: **For** each Gateway Node '*GN*' with user 'U_i' and generated Authentication Key 'AK_i'
3: Perform registration between users and gateway node using (5) and (6)
4: **End for**
6: **End**

Algorithm 2. Two users discrete registration.

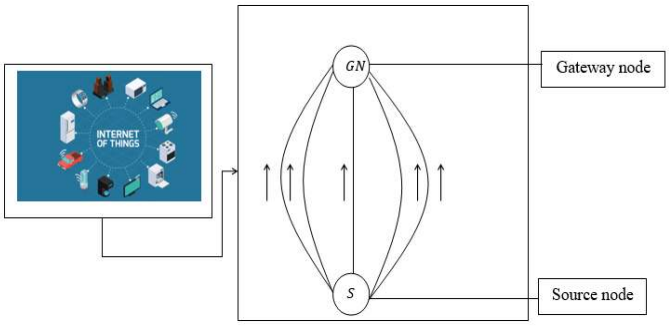

Figure 4. IoT-enabled progressive bezier authentication.

Input: Control points '$CP_0, CP_1, \ldots, CP_n$',
Output: Secured routing with minimum transmission cost
Step 1: **Begin**
Step 2: **For** registered users (i.e. gateway node and sender) with Control Points 'CP_i'
Step 3: Obtain Bezier curve using equation (7)
Step 4: Evaluate area of control point using equation (8)
Step 5: Measure area between two overlapping circles (i.e. gateway node and sender) using equation (9)
Step 6: Measure progressive distance '*PD*' using equation (11)
Step 7: Evaluate overall route response time using equation (12)
Step 8: Measure authentication cost using equation (13)
Step 9: **End for**
Step 10: **End**

Algorithm 3. Progressive Bezier authentication algorithm.

This is because of the reason that every sensor node decides restricted in a dispersed manner, whether it should in the routing process or not. The pseudo code representation of Progressive Bezier Authentication is given below.

As given in the Algorithm 3, let us consider a Bezier curve over a set of 'CP_0, CP_1,...,CP_n' control points (i.e. with four control points) with a parameter $'P \in \{0,1\}'$ and is mathematically formulated as given below.

$$\overrightarrow{CP(P)} = B_{i,n}(P).\overrightarrow{C(P_l)} \text{ ----------} \quad (7)$$

Then, the area of control point is mathematically formulated as given below

$$AREA_{CP} = \frac{r^2 \beta \pi}{360} \text{ ----------} \quad (8)$$

From the above equation (8), $'\beta'$ refers to the portion connecting the sender 'S' and the gateway node 'GN', with 'r' referring to the transmission range of sender 'S'. The area among two overlapping circles (i.e. gateway node and sender) is formulated as given below.

$$Dis_{GN-S} = [\pi(R^2 - r^2)] \text{ ----------} \quad -(9)$$

From the above equation (9), 'R' refers to the radius of distance from gateway node 'GN' to the sender 'S'. Unlike the previous routing protocol, in the proposed routing protocol using Bezier Authentication method, a secure area is laid based on the radius of transmission range of the sender and the distance from gateway node to the sender 'Dis_{GN-S}' subtracting the area of allocated area '$AREA_{CP}$'. It is mathematically formulated as given below

$$SEC_{Route} = AREA_{CP} - Dis_{GN-S} \text{ ----------} \quad (10)$$

Finally, the secured routing is said to be ensured between the source and the gateway node. Besides, with the objective of minimizing the transmission cost, progressive distance PD formulation is used. It is formulated based on the distance between the source and gateway node '$Dist_{S\to GN}$', distance between neighboring node and gateway node '$Dist_{NN\to GN}$' as given below.

$$PD = SEC_{Route} * [\frac{Dist_{S\to GN} - Dist_{NN\to GN}}{Dist_{S\to GN}}] \text{ ----------} \quad (11)$$

Then the ratio of overall route response time 'RRES [T]' of the nodes is mathematically formulated as given below.

$$\text{RRES}[T] = \frac{RRES_t[\text{NN}]}{RRES_t[\text{N}]} \text{ ---------} \quad (12)$$

From the above equation, '$RRES_t$ [NN]' refers to the route response time of neighboring nodes and '$RRES_t$' refers to the route response time of the total '[N]' nodes. Finally, the authentication cost 'Aut_{cost}' is mathematically formulated as given below.

$$Aut_{cost} = PD + RRES\ [T] \text{----------} \quad (13)$$

To select a route through which a data packet has to be sent, the node that minimizes authentication cost 'Aut_{cost}' is selected to forward packet to the destination. The authentication cost perfectly recognizes an authenticated secured route, therefore reducing the transmission cost.

Performance Study

The Mid Square Hash-based Bezier Authentication (MSH-BA) method is designed for secured routing in IoT-enabled WSNs uses the NS-2 simulator with the network range of 2500 * 2500 m size. Sensor nodes selected for experimental purpose is 500 for MSH-BA method. To conduct experimental work, Dynamic Source Routing protocol is used for MSH-BA method. The moving speed of the sensor nodes for MSH-BA method in IoT-enabled WSN is about 20 m/s for each sensor node with a simulation rate of 20s to perform energy-efficient secured data transmission. The parametric values for performing experiments are shown in Table 1.

In order to fairly anlayze the performance of MSH-BA method, the behavior of MSH-BA method is observed with diverse parameters. The performance behavior of MSH-BA method is analyzed on average energy consumption, running time, packet delivery ratio and data loss rate. Comparative analysis is made with the state-of-the-art methods, STDS [1] and Fork and Join Adaptive Particle Swarm Optimization (FJAPSO) [3] respectively.

The energy consumption 'EC' here refers to the energy consumed while generating authentic key. Therefore, energy consumption is measured by multiplying the energy consumed by a single senor node for authentic key generation and total number of sensor nodes in IoT-enabled WSNs. It is measured in Joules (J) and formulated as given below.

$$EC = \sum_{i=1}^{n} S_i * EC(\text{AK}_i) \text{ ----------} \quad (14)$$

Table 1. NS-2 simulation parameters.

Parameters	Values
Simulator	NS2.34
Number of sensor nodes	50, 100, 150, 200, 250, 300, 350,400,500
Simulation time	100s
Pause time	20s
Mobility model	Random way point
Transmission range	300 m
Network area	2500 m * 2500 m
Data packets	15, 30, 45, 60, 75, 90, 105, 120, 135, 150
Number of runs	10

From the above equation (14), energy consumed 'EC' is determined with the aid of total number of sensor nodes in IoT-enabled WSNs 'S_i' and energy consumed for authentic key generation 'EC (AK_i)' respectively. While generating the authentic key, a stipulated amount of time is said to be consumed. Here, the time consumed for authentic key generation is referred to as the running time. The average running time refers to the running time consumed by all sensor nodes engaging in authentic key generation towards secure data transmission for IoT-enabled WSNs.

$$RT = \sum_{i=1}^{n} S_i * Time(\text{AK}_i) \text{ ----------} \quad (15)$$

From the above equation (15), the running time 'RT' refers to the product of the total sensors in IoT-enabled WSNs involving data 'S_i' and the time consumed for authentic key generation 'Time (AK_i)'. Packet delivery ratio is measured by averaging the number of packets generated at the source node 'SN' and the number of packets received at the destination node 'DN'.

$$PDR = \sum_{i=1}^{n} [\frac{D_i(\text{SN})}{D_i(DN}] * 100 \text{ ----------} \quad (16)$$

From the above equation (16), the packet delivery ratio 'PDR' is measured based on the data packets generated at the source node 'D_i(SN)' and data packets received at the destined node 'D_i (DN)'. It is measured in terms of percentage (%). In order to measure the data loss rate, data drop rate has to be obtained. Only with the aid of the data drop rate, data loss rate is obtained. Therefore, data loss rate refers to the ratio of number of data packets that are dropped to the total number of data packets considered for simulation. Hence, the data loss rate is measured as given below.

$$DLR = \frac{D_D}{D_S} * 100 \text{ ----------} \quad (17)$$

From the above equation (17), the Data Loss Rate 'DLR' is the ratio of data drop rate 'D_D' to the data sent 'D_S' in the network. It is measured in terms of percentage (%).

Comparative analysis of energy consumption

All experiments are performed on Intel 5th generation i7 processor with 8GB RAM in NS2.34 simulator. In order to effectively analyze the performance behavior of MSH-BA method, it is tested by varying various number of sensors and data packets. Further, to simulate the random behavior of the MSH-BA nodes in a geographical area, a network topology of ''S_i=500' is deployed using testing parameters as shown in Table 1. Figure 5 given below shows the performance analysis of energy consumption obtained using equation (14).

Day by day, not only number of sensors linked to internet increases, but also similar thing occurs to things connected to internet during data exchange and interaction with each other. Then, the energy consumed is also said to be proportionately increased. As illustrated in the Figure 5, with the increase in the number of IoT-enabled sensors, the energy consumed for authentic key generation is also said to be increased. However, comparative analysis shows

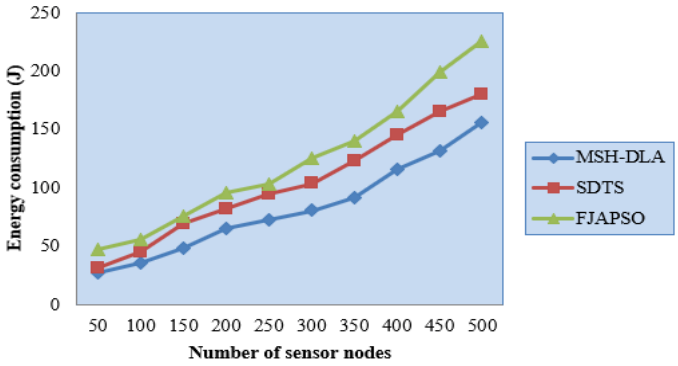

Figure 5. Performance analysis of energy consumption.

improvement by applying MSH-BA method when compared to Secure Data Transmission Scheme (SDTS) [1] and Fork and Join Adaptive Particle Swarm Optimization (FJAPSO) [3]. This is because in this work, multipath fading energy consumption model is used for collecting network traffic data.

Here, the multipath fading energy consumption model uses the distance factor while collecting the data. Based on this distance factor for transmission and reception between the sensors, data collection is said to be performed. Due to this, optimal parameter configuration is said to prevail. In other words, data collected between sensors is said to be optimal and hence consumes comparatively minimum energy for data transmission. Comparative analysis shows that the energy consumed for authentic key generation using MSH-BA method is reduced by 21% compared to SDTS [2] and 34% compared to FJAPSO [3] respectively.

Comparative analysis of running time

In order to perform secured routing, data collection or the features that has to be extracted to perform in an optimized manner. Bezier Authentication is successfully used for representing progressive distance with the purpose of minimizing the transmission cost. With this objective, Mid Square Hashing Data Collection algorithm has been applied in this work to minimize the running time. Figure 6 shows performance analysis of running time.

As illustrated in the Figure 6, running time for authentic key generation with respect to different sensors in the range of 50 to 500 are measured. From the Figure 6, it is inferred, that the number of sensor nodes is directly proportional to the running time. In other words, increasing the number of sensor nodes also increases the data being collected subsequently for each sensor node and therefore increasing the running time. However, comparative analysis shows an improvement by using MSH-BA method. This is because by using MSH-BA method, authentic keys are generated with high randomness. Besides, as unique key are said to be generated, chances of collision is said to be very less than the existing state-of-the-art methods. Therefore, as the collision is said to be less, the running time for authentic key generation is also found to be less compared to the existing state-of-the-art methods. Comparative analysis shows that the running time consumed for authentic key generation using MSH-BA method is reduced by 15% compared to SDTS [2] and 27% compared to FJAPSO [3] respectively.

Comparative analysis of packet delivery ratio

As nature and size of data is increasing, industries and organizations potentially try to find particular trajectory as close as possible in an efficient and effective manner and henceforth keeping the value of the data is among key elements in information. In this section, comparative analysis of packet delivery ratio is performed and compared with SDTS [2] and FJAPSO [3]. In order to ensure whether secure routing is ensured or not, the most important parameters is the packet delivery ratio. With higher packet delivery ratio, secure routing is said to be ensured. On the other hand, with lower packet delivery ratio, routing in IoT-enabled WSNs are not said to be ensured. Figure 7 given below shows the performance analysis of packet delivery ratio.

As clear from other explanations, energy consumption and running time given above, as data volume increases, complexity also is said to be increased, namely, the data complexity, computational complexity, and system complexity. The above graph illustrates the complexity in terms of data, or the packet delivery ratio involved in the analysis. From the Figure 7 it is inferred that with the increase in the number of data packets sent from the source side, data is said to be increasing in the IoT-enabled WSNs. Hence, the occurrence of collision is said to exist. However, by applying the Mid Square Hashing Data Collection algorithm, the collision is said to be minimized using MSH-BA method. Therefore, with minimum collision, by applying the Progressive Bezier Authentication, furthermore, using control points, not only unwanted trajectories or route of subsequent sensors are said to be minimized, but also, only few trajectories are selected via control point. This improves the packet delivery ratio. Comparative analysis shows that the packet delivery ratio is improved using MSH-BA method by 9% compared to SDTS [2] and 16% compared to FJAPSO [3] respectively.

Comparative analysis of data loss rate

As far as data for IoT-enabled WSNs are concerned, the data are different. For example, the data corresponding to each sensor may vary from information pertaining to environment, to information related to sound, image, data and even noise. Also, the velocity

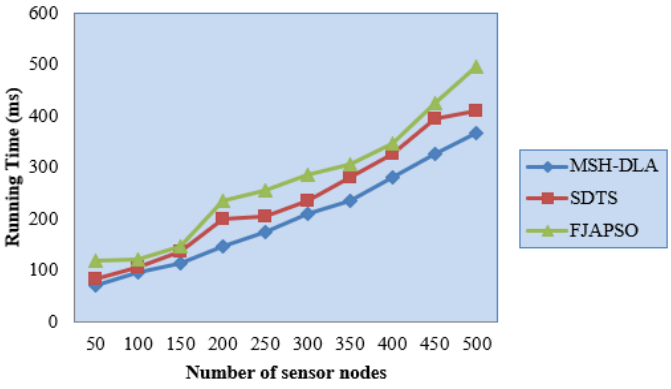

Figure 6. Performance analysis of running time.

Figure 7. Performance analysis of packet delivery ratio.

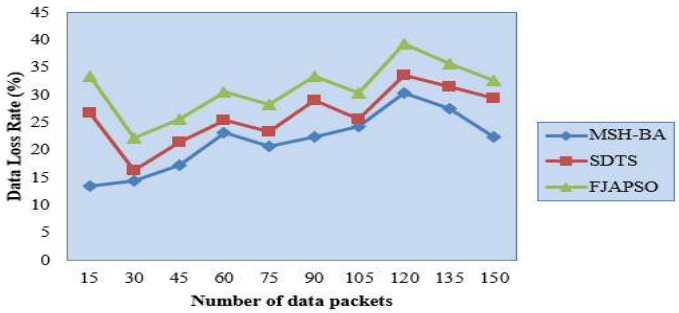

Figure 8. Performance analysis of data loss rate.

of information pointing to varied diversity and complexity of data structure, with the high speed and voluminous data being added, processing becomes a challenging task, therefore resulting in data loss. In this section, comparative analysis of MSH-BA in terms of data loss rate with respect to SDTS and FJAPSO is made. Figure 8 given below shows the comparative analysis of data loss rate for three different methods, MSH-BA, SDTS and FJAPSO respectively.

Figure 8 shows the performance analysis of data loss rate. In the Figure 8, x axis refers to the number of data packets and y axis refers to the data loss rate. For simulation purpose, data packets ranging from 15 to 150 with size in the range of 7 to 65,542 bytes are selected. Though number of data packets is said to be directly proportional to the data loss rate, the graph is not found to be linear. This is because users transmit different data and size of the data packets also differs. Also, with lower data loss rate, user data are said to be secured and hence there is less probability of malicious route having access to the sensitive information. This low data loss rate is achieved using MSH-BA method by applying Progressive Distance where the Bezier Curve uses four control points for ensuring secured routing, therefore reducing the data loss rate. Besides, by applying the computational efficient Authentication Cost, only the route that minimizes the authentication cost is selected, not all the routes are activated at the same time. Therefore, only the activated routes are used for transmission and non-activated routes are discarded, therefore no data transmission is said to be performed. On the other hand, only authenticated activated routes are used, therefore ensuring data transmission, hence reducing the data loss rate. Comparative analysis shows that the data loss rate is reduced using MSH-BA method by 18% compared to SDTS [2] and 31% compared to FJAPSO [3] respectively.

Conclusion

Secured routing in IoT-enabled WSNs is a challenging task. This paper proposed a method called Mid Square Hash-based Bezier Authentication (MSH-BA) which not only ensures security of routing being selected but also ensures minimum energy consumption with higher packet delivery ratio. To achieve this objective, three modules are designed. They are Network Traffic Data Collection, Two User Discrete Registration and IoT enabled Progressive Bezier Authentication. By applying Mid Square Hashing Data Collection algorithm with the generation of unique authentic key, packet delivery ratio is said to be improved. Next, by using Two User Discrete Registration algorithm during the registration process between the user and the gateway node, collision is said to be reduced and therefore reducing the data loss rate. Finally, by applying the Bezier authentication, only authenticated routes are selected via progressive distance. By implementing this method in IoT-enabled WSNs, secure routing is said to be ensured.

References

1. Evans, Dave. The internet of things: How the next evolution of the internet is changing everything. CISCO 1 (2011): 1-11.
2. Yasmine, Harbi, Zibouda Aliouat, Saad Harous, and Abdelhak Bentaleb. Secure Data Transmission Scheme Based on Elliptic Curve Cryptography for Internet of Things. Modelling and Implementation of Complex Systems (2018): 34-46.
3. Neetesh, Kumar, and Deo Prakash Vidyarthi. A Green Routing Algorithm for IoT enabled Software Defined Wireless Sensor Network. In: IEEE Sensors Journal 18 (2018).
4. Huang, Chen Lee, and Kai-Hsiang Ke. Monitoring of Large-Area IoT Sensors Using a LoRa Wireless Mesh Network System: Design and Evaluation. In: IEEE Transactions on Instrumentation and Measurement 67 (2018).
5. Manshahia, Mukhdeep Singh. Swarm Intelligence-Based Energy-Efficient Data Delivery in WSAN to Virtualize IoT in Smart Cities. IET Wireless Sensor Systems 8 (2018): 256-259.
6. Mustafa, Kocakulak, Ismail Butun. An Overview of Wireless Sensor Networks towards Internet of Things. IEEE 7th Annual Computing and Communication Workshop and Conference (2017).
7. Antonio, Celesti, Lorenzo Carnevale, Maria Fazio, and Massimo Villari, et al. An IoT Cloud System for Traffic Monitoring and Vehicular Accidents Prevention Based on Mobile Sensor Data Processing. IEEE Sensors 18 (2018).
8. Liang, Xiao, Xiaoyue Wan, Xiaozhen Lu, and Yanyong Zhang, et al. IoT Security Techniques Based on Machine Learning. In: Signal Processing and Internet of Things. IEEE Signal Processing Magazine 35 (2018).
9. Jianhua, Zhang, Fantao Kong, Zhifen Zhai, and Shuqing Han, et al. Design and Development of IOT Monitoring Equipment for Open Livestock Environment. IJSSST (2017).
10. Suresh, Mundru, K Meena. A Secure Loading Routing Protocol in IOT using Block Chain Technology. IJSSST (2016).
11. Xiaohui, Shang, Aijun Liu, Yida Wang, and Qing Xie, et al. Energy-Efficient Transmission Based on Direct Links: Toward Secure Cooperative Internet of Things. Wireless Communications and Mobile Computing (2018).
12. Dheerendra, Mishra, Vijayakumar P, Venkatasamy Sureshkumar, and Ruhul Amin, et al. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimedia Tools and Applications (2017).
13. Fan, Wu, Christoph Rudigery, Jean Michel Redoute and Mehmet Rasit Yuce. WE-Safe: A Wearable IoT Sensor Node for Safety Applications via LoRa. IEEE 4th World Forum on Internet of Things (2018).
14. NaziaYoussuf, Mir, Monika. Improved Survivable Path Routing in WSN for IOT Applications. International Journal of Engineering Trends and Technology 61 (2018).
15. Yaw, Wen Kuo, Cho Long Li, Jheng Han Jhang, and Sam Lin. Design of a wireless sensor network based IoT platform for wide area and heterogeneous applications. IEEE Sensors Journal 18 (2018).
16. Chinyang, Henry Tseng. Multipath Load Balancing Routing for Internet of Things. Hindawi Publishing Corporation Journal of Sensors (2016)
17. Prosanta, Gope, Tzonelih Hwang. BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network. IEEE Sensors Journal 16 (2016).
18. Zubair, Khalid, Norsheila Fisal, Hashim Safdar, and Rahat Ullah, et al. System Design in Sensor Network Virtualization for SHAAL. IEEE Fifth International Conference on Intelligent Systems, Modelling and Simulation (2014).
19. Suresh, Mundru, Meena K. A Secure Loading Routing Protocol in IOT using Block Chain Technology. IJSSST (2014).
20. Mohammad, Wazid, Ashok Kumar Das, Vanga Odelu, and Neeraj Kumar, et al. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. IEEE Internet of Things Journal 5 (2018).