Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 83-95
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.002

The Robust Routing Protocol with Authentication for Wireless Adhoc Networks

Dr. Subarna Shakya
Professor, Department of Electronics and Computer Engineering,
Central Campus, Institute of Engineering, Pulchowk,
Tribhuvan University,
Pulchowk, Lalitpur Nepal.
Email: drss@ioe.edu.np.

Abstract: The adhoc networks are the platforms formed for specific reason to attain a specific purpose. It is a communication strategy followed by the wireless devices when or while the actual communication setup is not possible. Any portable device communicating in the wireless medium in a decentralized manner is termed to be a wireless adhoc network. One such device is the wireless-sensors that imitate the aforementioned procedures to send the information from the source to the target falls under the category of the wireless adhoc network, as it communicates through the air in a wireless medium. The rapid proliferation of sensors and growing demand for applications and services from the network formed using such wireless-sensors generate unrivaled appeals for routing data packets on infrastructure of the network formed using the wireless-sensors. Such sensors lays as the fundamental devices in a wide range application and are even more predominant in the internet of things paradigm. Numerous of such devices are used in the internet of things to gather enormous amount of data from a broad range of applications. The sensors used in the internet of thing usually performs the sensed data transmission to the gateway-nodes through the public channel that are insecure for conversing the confidential data. So the routing with authentication becomes essential, to make the routing robust and long lasting it is necessary to develop a light weight authentication scheme that does not consume too much of the energy of the network of the wireless-sensors. To handle this problem the paper concatenates the unique key generation technique the mid-square (Mid-S) with the Beziers curve based authentication (UKHA) to secure and authenticate the routing between the wireless-sensor networks framed in adhoc manner and the gate way nodes of the internet of things platform. The proposed protocol for routing is develop in the MATLAB and simulated in it to manifest the proficiency of the developed protocol on the terms of the energy consumption, packet deliver rate, percentage of losses incurred and running time.

Keywords: Wireless-Sensors, Internet of things, unique key Generation, Bezier Curve Authentication, Mid-Square Hash

1. Introduction

The world striving to have a rapid and a swift way of communication expects more technological development in the communication, leading to seamless way of information sharing. The wireless adhoc networks also contribute major portion to satisfy the communication needs of the public. WANET-Wireless Adhoc network is a sort of local area network, constructed spontaneously with the motive of providing an uninterrupted communication among the two or more devices that are homogenous or heterogeneous. The devices connected communicate in the decentralized fashion as the devices involved are capable of accessing the resources of the any other device in the network through a fundamental point to point wireless communication directly.

The devices in the adhoc communicate using the network adapter that assist the network that is hosted. Every wireless adapter are set up in the adhoc mode, and not in the infrastructure mode and uses the service set identifier and the channel number that is the same. The network set up is usually temporary, this type of network model are more useful when and where the infrastructure mode of communication set up is not possible. Wireless- sensors that lay as the most essential and the primary source of data collection in a broad range of application in many circumstances sends data by forming a adhoc manner network, since they are deployed even in areas where human existence is impossible and most probably engaged in disaster management where the resuming of actual infrastructure communication would take few hours or days.

Since wireless sensors use the network formed in decentralized manner to communicate the collected information a routing becomes necessary to begin the messaging, in case of IoT the information's from the very fundamental source, the wireless-sensors are routed to the nearby gateways through the public channel that is vulnerable to al kind of security breaches. So it becomes requisite to develop a robust routing protocol with authentication to secure the confidential data's flowing from the sensors to the gateway.

Multiple of researchers came up with many type of routing with multi-objective optimization, addressing the issue of the energy consumption in the wireless-sensors as it is battery powered and failed to concentrate in providing a trustworthy routing, one such type of routing was developed by the author Raj, Jennifer S. et al [1] who focused mainly on developing a routing taking into consideration the energy consumption and the network utilization , and used the fuzzy and the CNN in make a proper route discovery but failed to focus on the security of the data sent from the sensor to the internet of things platform and Manshahia, et al [2] conducted a same energy efficient data transmission, but by utilizing the swarm intelligence , the author conducted the routing for the wireless-sensor and the actuator network of the smart cities to virtualize the internet of things in the smart cities.

Further G. Josemin Bala et al [5] designed a balanced data communication method for the adhoc type of network formed using the mobile devices to establish a balanced routing. Many authors like Celesti et al [6] conducted the experiments using the mobile adhoc networks and attempted to develop application like safe-transportation with comfort ability using the computing capability of the mobile sensors.

In the aim of developing an secured routing the author Smys, S. et al [7] in his paper used the cryptographic techniques to address the issue related to safety in the wireless sensors, he managed to optimize the energy consumption by developing a routing taking into consideration the distance between the nodes and utilized the nodes with minimum distance from the destination in the process. But the cryptographic method employed caused major energy consumption in key generation, encrypting and decrypting process. Kumar, et al [8] performed an "A green routing algorithm for IoT-enabled software defined wireless sensor network." Using the “fork and join adaptive PSO” the author Kuo, et al [9] developed a routing to elude the congestion in the network. Praveena, A., et al [10] and S. Smys et al [11] followed the "Efficient cryptographic approach for data security in wireless sensor networks using MES VU" and the "Prevention of inference attacks for private information in social networking sites" to mitigate the security threats in the wireless networks.

Secure data conveyance in the IoT was developed by the Harbi, et al [11] for securing the overall data flow in the Iot and not specifically the date conveyance from the wireless –sensors to the gate ways. The author used the ECC to secure data, this caused heightened energy consumption in the basic components involved affecting the network’s quality of service.

Jyothirmai, Pondi, et al [12] performed a "Secured self-organizing network architecture in wireless personal networks." Khalid et al [13] developed a “smart home and ambient assisted living”. Wazid, et al [14] discussed the developed measure addressing the security issues of the generic internet of things by designing a “user authenticated key management protocol” and further the authors Smys, S., and Jennifer S. Raj et al [15] incorporated the authentication scheme with optimized performance for the ad hoc network formed using the wireless devices.

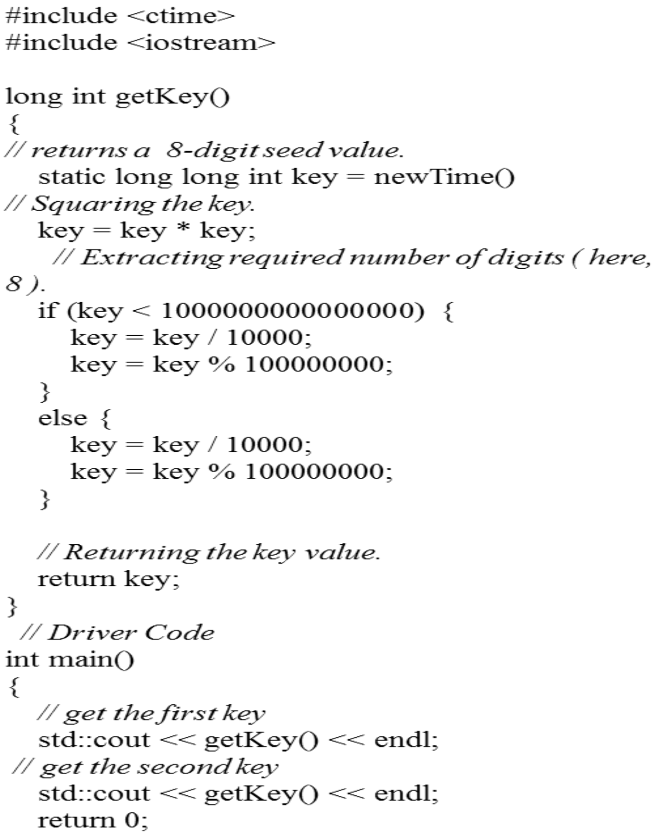
The proposed focused in enhancing the performance of the existing method, that concentrated either in security or the energy consumption by addressing both the issues related to the security and the energy consumption. So the procedure /protocol developed used the secure the data flow with unique key hashing and authentication concatenating the mid square hashing and Bezier authentication. The light weight security measure is employed to make the routing robust and energy efficient.

The remaining paper proceeds with the technique involved in 2, the detailed design description of the authentication and robust routing development in 3, the results evaluation in 4 and Conclusion in 5.

2. Technology Used

2.1. Mid Square Hashing [3]

It is process through which the unique key generation are done, the technique performs by taking a value (seed-value) and squaring it. The procedure further does the extraction of the digits from the middle to assign it to be the next new seed value. The randomness of the keys are proportional to the size of the value assigned as seed. The process also abides by certain limitations, for instance for an six digit value the squared value would be 12, as the squared value exceeds the integer data type, the over flow occurred is managed by the long inter data type or the string as multiplication. During the chances of collision the hash map manages the collision taken place. The implementation of the hashing algorithm using the C++ is displayed below in figure .1



```
#include <ctime>
#include <iostream>

long int getKey()
{
// returns a  8-digit seed value.
   static long long int key = newTime()
// Squaring the key.
   key = key * key;
     // Extracting required number of digits ( here,
8 ).
   if (key < 1000000000000000)  {
      key = key / 10000;
      key = key % 100000000;
   }
   else {
      key = key / 10000;
      key = key % 100000000;
   }

   // Returning the key value.
   return key;
}
 // Driver Code
int main()
{
   // get the first key
   std::cout << getKey() << endl;
 // get the second key
   std::cout << getKey() << endl;
   return 0;
```

Figure.2 Implementation of Mid –Square [3]

2.2. Bezier Curve Authentication [4]

Beziers curve is the commonly used procedure to sketch the arc in the computer graphics, very smooth curves are acquired using the algorithm of Beziers curves and are capable of being scale indefinitely. “The curve moves along the velocity over the time with the controlling points”, and compatible for the authentication. The smooth curve is obtained without any deformation and the regulating points determine the alignment of the curve, the formula below in equation 1 is framed in regard of Bezier curve “BC”.

$$BC = (1-t)^3\, Cp_0 + 3t(1-)^2\, IP_c + 3t^2(1-t)\, Cp_1 + t^3 EP_c \text{ While } t\epsilon[0,1] \qquad (1)$$

Where the Cp_0 and Cp_1 is the controlling points, and IP_c and the EP_c are the initial and the end points of the curve.

3. Authentication Scheme for Robust Routing Protocol

The proposed system concatenates the mid square and Beziers and develops a unique key generation and a authentication (UKHA) for the routing of the data from the sensors to the gate ways, the network model follows a clustering type routing and energy model based on the multipath fading, measuring the Euclidean distance between the source the destination, the energy consumption in the transmission (ET) and the reception (ER) of the single bit at a distance “D” is estimated for a single node as shown in equation 2 and 3 given below.

$$ET = ET - Elec(l) \qquad (2)$$

$$ER = ER - Elec(l) \qquad (3)$$

To devise the routing, the particulars of the traffic flow in the network is collected in the initial stage followed by the registration process and the unique key generation process by the Mid-Square and finally performs the authentication process using he Beziers. The accuracy of the authentication is stimulated by the requisition that initiated to IoT and responded by the Iot and the reply that stops the data routing. The step below provide the detailed explanation of the each phase involve in the proposed process.

The architecture is encompassed with multitudes of the wireless sensors with resources limitations and many gateway nodes. The mid square used collects the information of the network traffic flow of the IoT

Step1: The Mid –square filters TCP, selects the protocols, IP address, frame length , labels and the frame number. Then extracts features.

Step2: For every gateway node, senor and the head of the cluster the Euclidean distance is measured, across the transmitter and the receiver using the formula $distance = \sqrt{(t_x - t_y)^2 + (r_x - r_y)^2 \ldots\ldots}$, where the ‘t and r’ are transmitter (x) and the receiver (y) nodes co-ordinates.

Step 3: Measure the transmission and the reception energy, using equation 2 and 3

Step4: Acquire key across the gateway and the sensors with the equation$key = Midsquarehash\ (password\ (gateway)|Identification\ of\ sensors)$.

Step 5: Perform the registration process among the client the gateway utilizing the key generated and, the registration route request by the user is performed. The user and the gateway node communicates via the cluster head. The co-ordinates of the nodes, the key generated and the time duration are gathered.

Step 6: Selects the identification (ID) and unique identification (UID) and uses the public channel (Pc) to transmit the message through the head in the cluster.

Step 7: Gateway processes the parameters of the users and both the gateway and the users generate the private key. After completion of the registration of both the gate way and the users through the head in the cluster.

Step 8: Bezier Authentication is developed to sort out the accurate nodes that would afford to provide a robust routing that is authenticated.

Step 9: The control points are fed as input, and for all registered users obtain the Bezier curve using the equation 1

Step 10: Estimate the area of control with $Cp\ area\ = \frac{radius\ ^2\beta\pi}{360}$ while β is the point linking the sensors along with the gateway nodes.

Step 11: Determine the area across the two circles overlapping (sensor and the gateway nodes) with (πR^2) and determines the "progressive distance", the complete response duration and the cost of the authentication, by calculating the secure route area by subtracting the distance for the gateway to the sensors from the $Cp\ area$, and further calculating the progressive distance as shown in equation 4

$$progressive\ distance = \frac{dist\ (s \rightarrow gateway) - dist\ (neighbornode \rightarrow gateway)}{dist\ (s \rightarrow gateway)} * \text{ secure area} \qquad (4)$$

The time taken to complete the route response is calculated using the equation 5

$$Route\ Response\ time = \frac{Response\ time\ of\ neigbor\ node}{dist\ (s \rightarrow gateway)} \qquad (5)$$

And the cost of the authentication is acquired using the equation 6

$$Authentication\ cost = \ progressive\ distance + \ Route\ Response\ time \qquad (6)$$

4. Results Evaluation

The protocol developed with the concatenation of the UKHA is designed using the C++ and evaluated in the MATLAB to manifest the proficiency of the developed protocol on the terms of the energy consumption, packet deliver rate, percentage of losses incurred and running time. The content of table .1 list the parameter employed in the simulation process.

Parameters	Values
Number of Sensors	500
Simulation Time	100 s
Pause Duration	10 s
Mobility Model	Random Way Point
Range of Transmission	500 m
Simulation area	2500m*2500m
Data Packets	200
Number of Runs	10

Table.1 Simulation Parameters

The Analysis is deeply performed and compared with the existing state of art algorithms such as the SDTS [12] and the FPSO [9] the analysis is done over the packet delivery rate, consumption of the energy, the running time and the loss in the data.

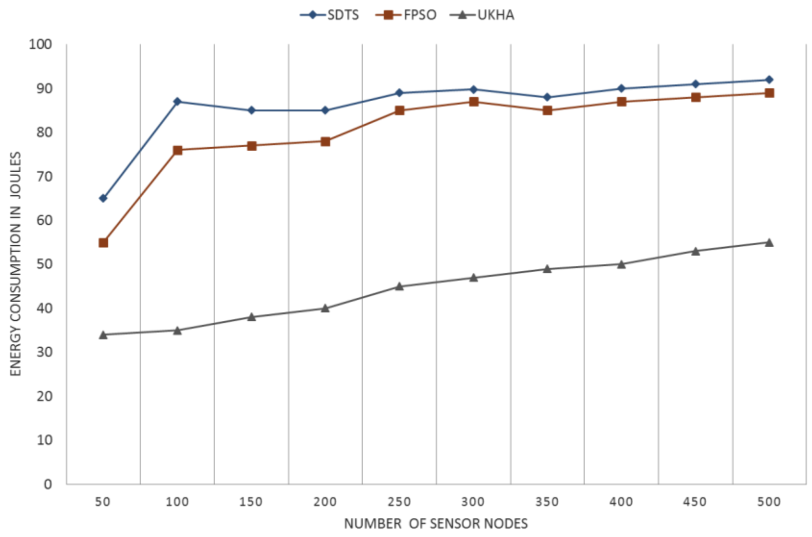


Figure.2 Energy Consumption

The energy used in producing the key is measured taking the product of the energy utilized by the one sensor for producing key and the total number of sensors. The results observed over the energy utilization in producing the keys is depicted in fig.2 the results observed is further compared with the other exiting methods SDTS [12] and the FPSO [9] to manifest its performance improvement.

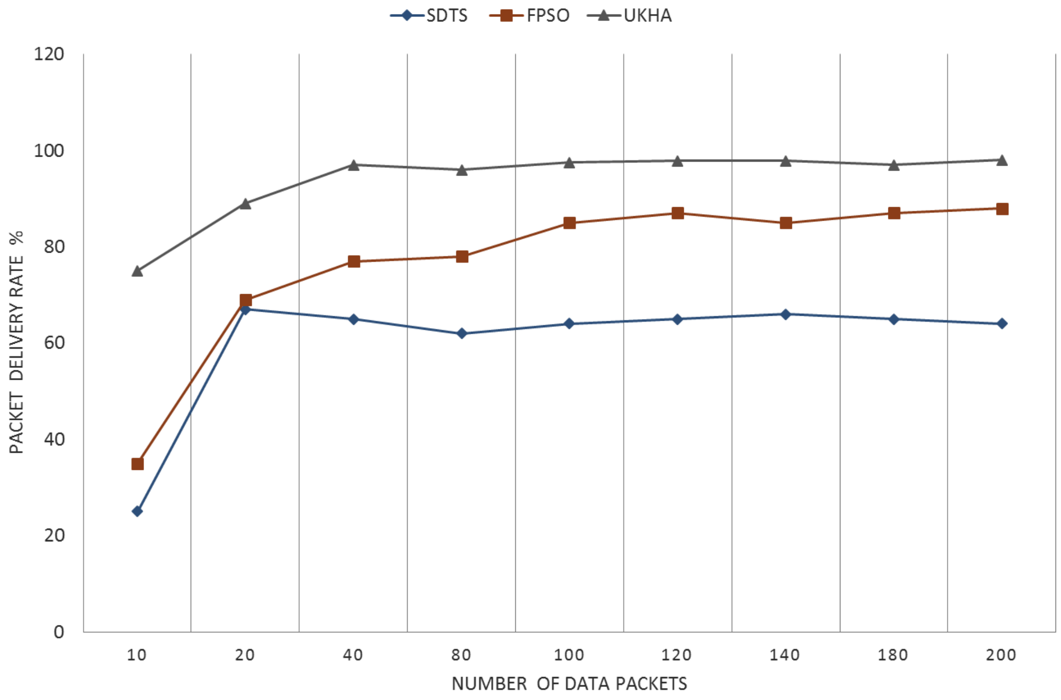


Figure.3 Packet Delivery Rate

The fig.3 shows the Packet Delivery Rate that is calculated by "averaging the number of packets produced at the source and packets received at the target" the results observed is further compared with the other exiting methods SDTS [12] and the FPSO [9] to manifest its performance improvement in the PDR.

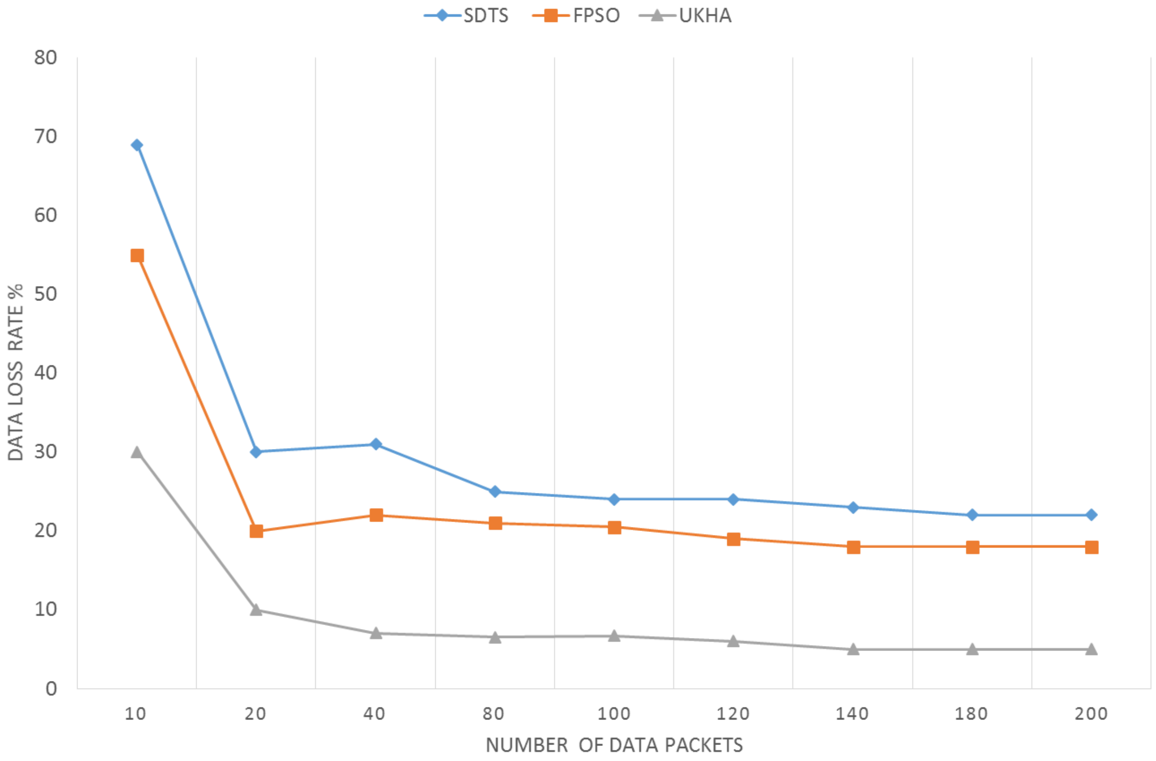


Figure.4 Data Loss Rate

The Data loss rate is depicted in the figure.4 is measured using the following equation (7), the measured drop loss rate of the proposed protocol is compared with the prevailing methods. The proposed method showed lesser data drop rate compared to the prevailing methods SDTS [12] and the FPSO [9].

$$Data\ Loss\ Rate\ =\ data\ drop\ rate\ in\ destination/data\ sent\ from\ the\ source \qquad (7)$$

Further the time of utilized by the sensors for generating the key to have a secured transmission of data is presented in the figure .5 this is analyzed by comparing it with the existing method , the results observed proves the betterment achieved in the proposed method over the other.

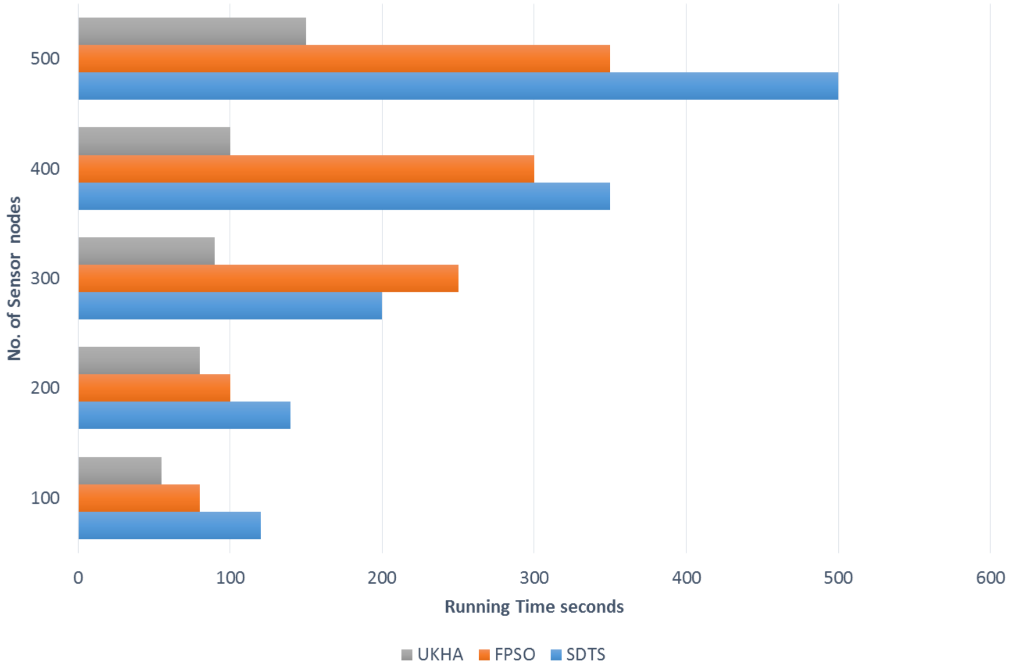


Figure.5 Running Time

$$Running\ Time\ = \sum\ sensor\ nodes * time\ taken\ in\ \ producing\ key \qquad (8)$$

The equation 8 is used in measuring the running time. The experiments is completely done on the 5th generation i9 processor with 16 GB RAM and the 120 GB SSD and HDD of 1 TB the process was repeated with varying number of sensors and the packets of data, to identify the behavior of the proposed work, it was further compared with other state art methods and the performance was evinced.

5. Conclusion

The proposed method concatenates the unique key generation with the authentication UKHA by integrating the mid square and Bezier curve to develop a robust routing that is secure for the data flowing from the sensors to the gate ways of the IoT. The process engages the mid square in the collection of the network traffic and unique key generation and does the authentication using the Bezier to form a path with the nodes that are accurately capable of performing a secure robust routing. The calculations done and the results observed on the energy consumption , PDR, data loss and the time of execution ensures the capability of the proposed method over the prevailing state of art methods such as SDTS and FPSO.

References

[1] Raj, Jennifer S. "QoS optimization of energy efficient routing in IoT wireless sensor networks." *Journal of ISMAC* 1, no. 01 (2019): 12-23.

[2] Manshahia, Mukhdeep Singh. "Swarm intelligence-based energy-efficient data delivery in WSAN to virtualise IoT in smart cities." IET Wireless Sensor Systems 8, no. 6 (2018): 256-259.

[3] https://www.geeksforgeeks.org/mid-square-hashing/

[4] https://www.hindawi.com/journals/mpe/2014/928039/

[5] Smys, S., and G. Josemin Bala. "K-connection Maintenance algorithm for Balanced Routing in Mobile Ad Hoc Networks." International Journal of Computer Networks and Communications (IJCNC) 1, no. 3 (2009): 105-111.

[6] Celesti, Antonio, Antonino Galletta, Lorenzo Carnevale, Maria Fazio, Aime Ĺay-Ekuakille, and Massimo Villari. "An IoT cloud system for traffic monitoring and vehicular accidents prevention based on mobile sensor data processing." IEEE Sensors Journal 18, no. 12 (2017): 4795-4802.

[7] Smys, S. "Energy-Aware Security Routing Protocol For Wsn In Big-Data Applications." *Journal of ISMAC* 1, no. 01 (2019): 38-55.

[8] Kumar, Neetesh, and Deo Prakash Vidyarthi. "A green routing algorithm for IoT-enabled software defined wireless sensor network." IEEE Sensors Journal 18, no. 22 (2018): 9449-9460.

[9] Kuo, Yaw-Wen, 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, no. 12 (2018): 5187-5197.

[10] Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In 2016 10th international conference on intelligent systems and control (ISCO), pp. 1-6. IEEE, 2016.

[11] Praveena, A., and S. Smys. "Prevention of inference attacks for private information in social networking sites." In 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1-7. IEEE, 2017.

[12] Harbi, Yasmine, Zibouda Aliouat, Saad Harous, and Abdelhak Bentaleb. "Secure data transmission scheme based on elliptic curve cryptography for internet of things." In International Symposium on Modelling and Implementation of Complex Systems, pp. 34-46. Springer, Cham, 2018.

[13] Jyothirmai, Pondi, Jennifer S. Raj, and S. Smys. "Secured self-organizing network architecture in wireless personal networks." Wireless Personal Communications 96, no. 4 (2017): 5603-5620.

[14] Khalid, Zubair, Norsheila Fisal, Hashim Safdar, Rahat Ullah, and Wajahat Maqbool. "System design in sensor network virtualization for SHAAL." In 2014 5th International Conference on Intelligent Systems, Modelling and Simulation, pp. 636-641. IEEE, 2014.

[15] Wazid, Mohammad, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, and Minho Jo. "Design of secure user authenticated key management protocol for generic IoT networks." IEEE Internet of Things Journal 5, no. 1 (2017): 269-282.

[16] Smys, S., and Jennifer S. Raj. "Performance Optimization of Wireless Adhoc Networks with Authentication." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1, no. 02 (2019): 64-75.

Biography: Dr. Prof. Subarna Shakya is currently a Professor of Computer Engineering, Department of Electronics and Computer Engineering, Central Campus, Institute of Engineering, Pulchowk, Tribhuvan University, Coordinator (IOE) , LEADER Project (Links in Europe and Asia for engineering, education, Enterprise and Research exchanges), ERASMUS MUNDUS. She received MSc and PhD degrees in Computer Engineering from the Lviv Polytechnic National University, Ukraine, 1996 and 2000 respectively. Her research area includes E-Government system, Computer Systems & Simulation, Distributed & Cloud computing, Software Engineering & Information System, Computer Architecture, Information Security for E-Government, Multimedia system