The Scientific Temper (2023) Vol. 14 (4): 1404-1411

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.51

https://scientifictemper.com/

REVIEW ARTICLE

# Location-specific trusted third-party authentication model for environment monitoring using internet of things and an enhancement of quality of service

**K. Akila**

## Abstract

In the modern digital world, the internet of things (IoT) is a modern and advanced technology that interconnects many immeasurable devices. The collection of wireless sensors formed the wireless sensor network. WSN nodes are battery-powered nodes with limited power and computational capability. When using IoT-based wireless sensor networks, the nodes are used to communicate with the internet, where there is a need for more secure protocols. In this technological era where time factor plays a key role in everyone's personal busy life. The need for smart and sensor appliances that work without human intervention can be a solution to some extent for the time factor. IoT is a network where physical objects, vehicles, devices, buildings and many other smart devices are electronically embedded with hardware and software with huge network connectivity. But the communication and data exchange are not that much easy to carry out, it requires a high secured protocol for authentication as well as key encryptions. Besides focusing on secured key distribution importance for enhancing various parameters are also considered which includes, EC additions, multiplications, pairing, hash-to-point operations, security performances, and energy consumption are also considered. In this paper, focuses on "LSTTP" which authenticates the nodes based on the device finger print (DFP) with a trusted third party and proposes the algorithm for enhancing the quality of service parameters such as throughput, jitter, latency and security.

**Keywords**: Trusted third party, Physical unclonable function, Wireless sensor network, Internet of things, Cluster node, Device fingerprint, X-OR operation.

## Introduction

To have a green cool environment, throws a confront with reverence to pure form of water, good quality of air, and radiation-less atmosphere, where these things are difficult to achieve. Society with healthiness can be achieved and maintained with permanent environmental monitoring. EM can be maintained with the acquirement of data for a long time, to achieve this both WSN and IoT play an important role. Several factors contribute as sources of pollution, some from nature while the majority are man-made. The effective and precise role of EM has emerged here while addressing these challenges. There are several factors that effect the environmental growth of the entire world which include, agriculture, economy, quality education, industries and many more, but among them the key role is played by the environment is very important to be considered but as a fact it is completely neglected. For the sustainable growth of a country and mankind hygiene and health are major components that are obtained only when one has pollution-free, hazardous free and clean and cool environment. EM becomes important in order to ensure a healthy life to be led by citizen of ay nations. It can be achieved with proper management and planning of various disasters controlling pollution besides proper addressing of raised challenges which has emerged due to various external unhealthy conditions. AI took the working of sensors to next level, where controlling and monitoring methods of these devices can be achieved accurately even from the palaces where human presence is not possible. Tracking of vehicles, temperature

Department of Computer Applications, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Trichy, India

***Corresponding Author:** K. Akila, Department of Computer Applications, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Trichy, India, E-Mail: akilak.ca@cauverycollege.ac.in

**How to cite this article:** Akila, K. (2023). Location-specific trusted third-party authentication model for environment monitoring using internet of things and an enhancement of quality of service. The Scientific Temper, **14**(4):1404-1411.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.51

**Source of support:** Nil

**Conflict of interest:** None.



**Received:** 16/09/2023 **Accepted:** 10/11/2023 **Published:**27/12/2023

controlling in large furnaces, and management of waste effectively, controlling pollution all such kind of things can be achieved while proper embedding of IoT devices in WSNs. This kind of effective managing environment through smart devices has increased the scope of research for SEM. In deep forest tracing the exact location of fire by considering satellite images as source, monitoring mobile health systems (Cicala *et al*., 2018), assessing the damage on crops (Pathak *et al*., 2019), monitoring water quality and its controlling (Pavithra.G *et al*., 2018), weather forecasting (Kamal *et al*.,2017), SIAEM (K.Akila *et al*., 2019), method proposed two functional blocks of customized clustering of IoT-WSN nodes (CCIN) and energy aware state change routing protocol (EASCRP). The method of CCIN classified the sensor nodes as low, medium and high power nodes based on their energy. EASCRP suggested an alternate path for the communication between base station to cluster head and cluster head to member nodes. (Anandhavalli *et al*., 2023) proposed the method to exchange the new authentication key between the IoT devices with security based on Dual Rosenberg pairing location masker and Fuzzy Miller's elliptic curve.

### *Literature Survey*

*Reliable PUF-based authentication protocol for IoT devices (RPUFAP)*

The main highlights of this approach are. two-level finite state machine IBE, PUF key-based hash functions are effectively used for keyless authentication protocol (Lao *et al*., 2017) (Chatterjee *et al*., 2017). A video surveillance attack was utterly overcome in this approach. The drawback of this approach is unable to detect attacks of side channel, frame work encryption optimizations are not achieved properly.

*Pairing Free certificate-based proxy re-encryption method (PFCPEM)*

Repudiation and identity authentication are main highlights of this approach, where instead of using generally paring operations are replaced with unique additions and multiplications which are based on elliptic curve and encryption schemes (Braeken *et al*., 2017). Many important attacks referring to man in the middle, impersonation, and relay is among the one which are addressed here. Main drawback of this approach is that during the communication to locate the address of node with 64 bits was a bit difficult.

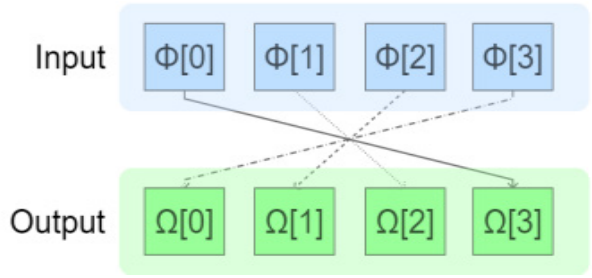


**Figure 1:** Static shuffling

*Dynamic security scheme manager (DSSM)*

The random memory shuffling method (Akila *et al*., 2019) is based on static shuffling and shuffles first four bytes of data and remaining data shuffled dynamically. RMS swaps the first, fourth and second, third. The following diagram 2.1 shows the static shuffling.

*Uniform distribution of energy between cluster head nodes and members (UDECHN)*

Distribution of energy among the available cluster nodes are carried out uniforms by categorizing the sensor nodes into normal, advanced and moderate level. The main highlight of this approach lies at uniform distribution of energy between the active members of cluster nodes. An enhanced version of stable election protocol algorithm is used, helpful for environment monitoring for air pollution (Dhingra *et al*., 2019) (Wang Braeken with the help of which uniform population at the cluster nodes are being maintained (Dutt *et al*., 2018). Its main drawback lies at the failure of constant speed node in a network between two given points.

### *A Lightweight Three-Factor Authentication and Key Agreement Scheme for Multigateway WSNs in IoT (LTFA)*

LFTA (Sooyeon *et al*., 2019) proposed three types of entities and five phases such as system setup, user registration, login, authentication and password change and three types of entities are user (Ui), home gateway (HG) and sensor nodes (Sj). In the phase of system setup, home gateway (HG) creates sensor ID using hash function and sensor nodes register itself with ID and password and biometrics using X-OR operation and hash function. Users can register themselves by using the ID, password and biometrics with trusted third party (TTP), users can able to change the password by its bio metrices. LFTA proposed the algorithm of BAN and oracle model for achieving security. During the registration phase, the sensor nodes register itself with ID, password and biometrics at home gateway (HGWN). The Figure 1 shows the registration phase. After registration, the FGWN provides the authentication to the sensors. The following Figure 2 shows the registration phase.

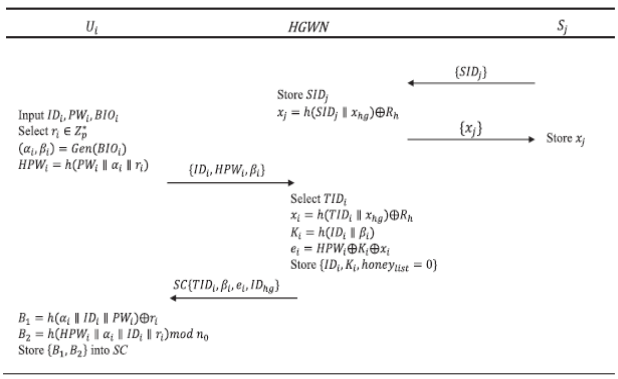


**Figure 2:** Registration phase

### *Registration Phase*

- *Blockchain-based secured access control in an IoT system (BBSAC)*

BBSAC (Sultan Algarni *et al*., 2021) (Behera *et al*., 2020) proposed the hierarchical blockchain architecture for access control of iot devices (Figure 3). The architecture consists of local block chain manager (LBCM) and core fog block chain manager (CFBCM) cloud blockchain managar (CBCM). The architecture met the needs of confidentiality, Integrity and availability. BCM is responsible for assigning access control policy for each node.

Securing environmental IoT data using masked authentication messaging protocol in a DAG-Based Blockchain: IOTA Tangle (MAM)

MAM (Pranav Gangwani *et al*.,2021) proposed the approach based on the distributed ledger technology of IOTA for overcoming the issues in blockchain and masked, secured authenticated communication among the IoT nodes. MAM aims to deliver an environmental monitoring application by masked authenticated messaging (MAM) protocol. This application intentions to guarantee the security and privacy of the sensor data, as well as to control and avert various protection issues and hazards such as air pollution and green house emissions. MAM used the methodology of the Merkle Hashing technique, MH concentrated the nodes upward. The approach is called as wherein the leaves of the tree embody the hash of the values of the data or the ordered elements of a set. Let this reliable ordered set of elements for MHT bex0,0,x0,1,x0,2,. . .,x0,n; therefore, the leaf node of the element x0,I will be the hash of that element. Let this leaf node be epitomized by x1,i, where x1,i=H(x0,i) and H() is a function that is cryptographically hashed one way. A node in the MHT contains multiple incoming edges; the value of a node is the shared or concatenated hash

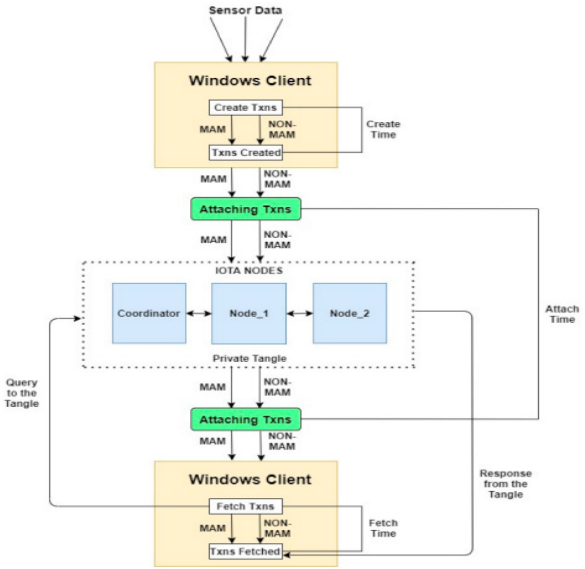


**Figure 3:** System architecture

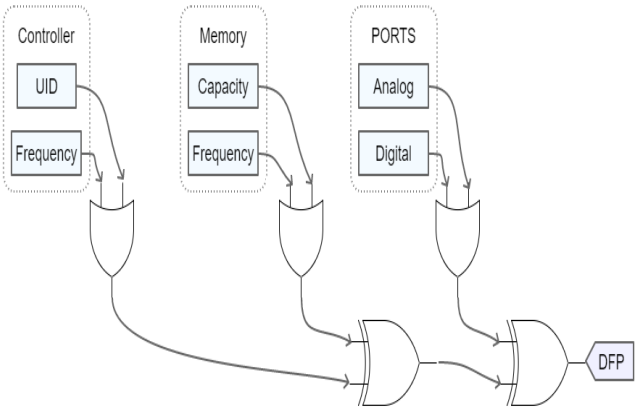


**Figure 4:** LSTTP device finger print generation architecture

(Brogan *et al*.,2018) of it preceding nodes, also known as Sub nodes, where the sequence of the nodes is preserved. An internal node or a non- leaf node x2,0 with Sub nodes x1,0 and x1,1 hence contains the value x2,0 = H(x1,0x1,1). The MHT and a verification object that contains a set of nodes can be used to establish the existence of an element. The root of the MHT (Zhang *et al*., 2017) can be recomputed by the verifier by using the verification object and a set of nodes that are contained within it. The verifier compares there computed root using the verification object, with the public known root that the tree generates. For instance, consider the element x0,0 in the MHT; the verification object consists of the values of the nodes x0,0, x1,1, and x2,1. x1,0 = H(x0,0),x2,0 = H(x1,0x1,1) and conclusively, root = H(y2,0 x 2,1) is constructed by the verifier. Once this verification object is constructed, the verifier can compare the computed root with the public known root and verify the value. MAM method includes a digital signature based on RSA algorithm for secure communication which provides one time signature. Based on the OTS security of the nodes ensured. Figure 3 represents the system architecture.

### *Proposed System*

Proposed 'Location specific trusted third-party authentication method' is based on physical clonable function based signature. The objective of this approach is indented to provide mobility without compromising the security level (Table 1).

*Location specific trusted third-party authentication model (LSTTP)*

As the target of the proposed method is environment sensing IoT devices, LSTTP model takes advantage of the built-in hardware components of the nodes to generate keys. Every IoT node is equipped with a processing unit which includes a tiny microprocessor or a microcontroller, some amount of random access memory (RAM), flash memory, and input output ports. The hardware fingerprint otherwise called as the device fingerprint which is generated by combining multiple features such as hardware IDs,

specifications, embedded software versions, driver versions, memory configurations and input output characteristics. The device fingerprint (DFP) generation architecture of LSTTP is given in Figure 4.

The physically unclonable function based signature (PUFS) generation process of LSTTP uses internal noise generated by the processing unit and the external noise sensed by the inbuilt or connected add-on sensors. The external noises are processes with an adder and then sent to the X-OR operation with internal noise to improve the key perplexity. LSTTP uses a dedicated hash function to generate the node key by blending device fingerprint, PUF signature, node ID and a random key.

*Algorithm: LSTTP Hash Algorithm*

Input: $IB$ Input Byte
Output: $OB$ Output Byte

Step 1: Get $IB$ from buffer
Step 2: Extract $IB$ into separate bits as $Ib_0, Ib_1, \ldots Ib_7$
Step 3: Allocate 8-bits in memory for $Ob_0, Ob_1 \ldots Ob_7$ to form $OB$
Step4:

$$\forall i = 0 \rightarrow 7 := \{Ob_{\left(\frac{i}{2}\right)+4} = Ib_i \; if \; i \; is \; EVEN \; Ob_{\left(\frac{i}{2}\right)-0.5} = Ib_i \; if \; i \; is \; ODD$$

Step 5: return $OB$

LSTTP hash architecture is illustrated in Figure 5.

LSTTP uses environmental parameters along with device signatures to produce a PUF based signature to generate the key as illustrated in Figure 3.

### *Registration Phase*

TTPs public key encryption plays the major role in the registration phase. All the authorized nodes are fed with the TTPs public key. Every IoT node generates LSTTP node key and encrypts it using TTPs public key and sends the crypted value to the TTP (Figure 6). The TTP is aware of the device fingerprint and Node ID. TTP decrypts the encrypted registration packet received form the IoT node using the private key. Then the TTP can compute the value of PUFS and random number generated by the IoT node applying LSTTP reverse hash (Equation 1) to the MSBs and LSBs of the 16-bit node key, respectively. TTP stores this information for all member nodes of the IoT network for future use.

$$\forall i = 0 \rightarrow 7 := \{OB_{(i\times 2)+1} = IB_i \; if (i < 4) \; OB_{(i-4)\times 2} = IB_i \; otherwise$$

Equation (1)

Where $IB$ is the input and $OB$ is the output

*Authentication and communication establishment phase*

Let $DFP_1$, $PUFS_1$, $K_1$, $R_1$, $NID_1$ are the device finger print, PUF signature, node key, random number and node ID of IoT node 1 (Sender). Similarly, $DFP_2$, $PUFS_2$, $K_2$, $R_2$, $NID_2$ are the device finger print, PUF signature, node key, random number and node ID of IoT node 2 which is referred to the receiver. Initially both sender and receiver send their keys to the TPP. TPP computes $NID_2 \oplus K_1$ and sends it to sender.

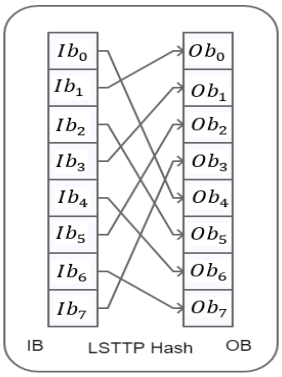


**Figure 5:** LSTTP hash

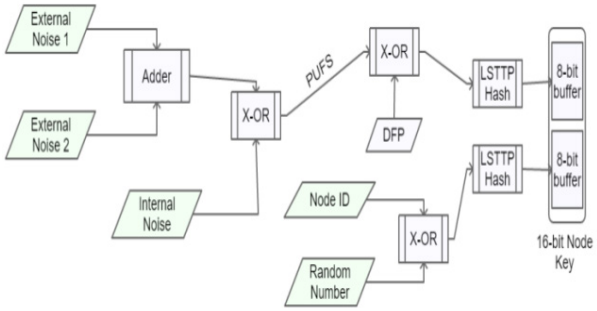


**Figure 6:** LSTTP node key generation algorithm

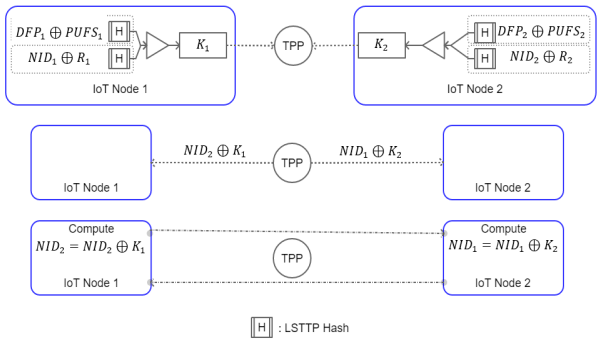


**Figure 7:** Establishment of communication between sender and receiver

Similarly, TPP computes $NID_1 \oplus K_2$ and sends to the receiver After than the sender and receiver can compute each other's keys and use them to establish the communication directly. Then the key agreement and communication establishment between the sender and the receiver through TTP takes place as given in Figure 7.

### *Experimental Setup*

OPNET from riverbed technology which is considered as the network simulator from recent years, it is supported by a fine state of art network simulation support. The freedom to design any kind of protocols and network architecture is provided by the scripting provision and graphical interface of OPNET (Zheng *et al*., 2012) (Table 1).

**Table 1:** Experimental setup

| *S. No.* | *Entity* | *Details* |
|---|---|---|
| 1 | Simulation Area | 10000 Sq. Meters |
| 2 | Number of nodes | 100 to 1000 in steps of 100 |
| 3 | IoT Node type | ESP-32, ESP-8266, LoRa (Uniform Distribution) |
| 4 | Number of Routers | Automatic selection |
| 5 | Node Placement | Random distribution |
| 6 | Network Density | Default |
| 7 | RF Range of IoT-WSN Nodes | Based on the type of 100 to 1000 meters |
| 8 | Frequency Band | Auto-select |
| 9 | Simulation Time | 168 Real-World hours |

**Table 2:** Throughput (Kbps)

| *Time stamp* | *LTFA* | *BBSAC* | *MAM* | *LSTTP* |
|---|---|---|---|---|
| 1 | 35519 | 35063 | 35278 | 37108 |
| 2 | 34248 | 33800 | 34054 | 36027 |
| 3 | 32892 | 32528 | 32862 | 34873 |
| 4 | 31516 | 31240 | 31606 | 33811 |
| 5 | 30142 | 29957 | 30379 | 32651 |
| 6 | 28787 | 28613 | 29207 | 31593 |
| 7 | 27466 | 27395 | 28014 | 30481 |
| 8 | 26114 | 26101 | 26730 | 29329 |
| 9 | 24729 | 24762 | 25594 | 28167 |
| 10 | 23375 | 23553 | 24360 | 27099 |

**Table 3:** Latency (ms)

| *Time stamp* | *LTFA* | *BBSAC* | *MAM* | *LSTTP* |
|---|---|---|---|---|
| 1 | 28 | 32 | 31 | 15 |
| 2 | 39 | 43 | 41 | 24 |
| 3 | 51 | 54 | 51 | 34 |
| 4 | 62 | 64 | 61 | 43 |
| 5 | 74 | 75 | 71 | 53 |
| 6 | 85 | 86 | 81 | 61 |
| 7 | 96 | 97 | 91 | 71 |
| 8 | 107 | 107 | 102 | 80 |
| 9 | 119 | 119 | 112 | 90 |
| 10 | 130 | 129 | 122 | 99 |

## Results and Analysis

For measuring the nature of a standard network among many some of the important parameters which are considered as throughput, latency, end-to-end delay, packet delivery ratio, security and energy. The results with the above parameters were collected while conducting the experiments in OPNET simulation environment at 10 different Simulations from 100 to 1000 nodes. The performance of all the parameters were observed in trending methods such as LFTA, BBSAC, MAM, along with LSTTP the proposed , for the obtained results the values and corresponding graphs.

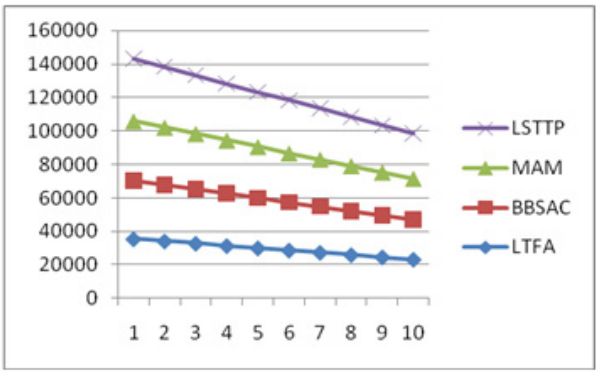


**Figure 8:** Throughput

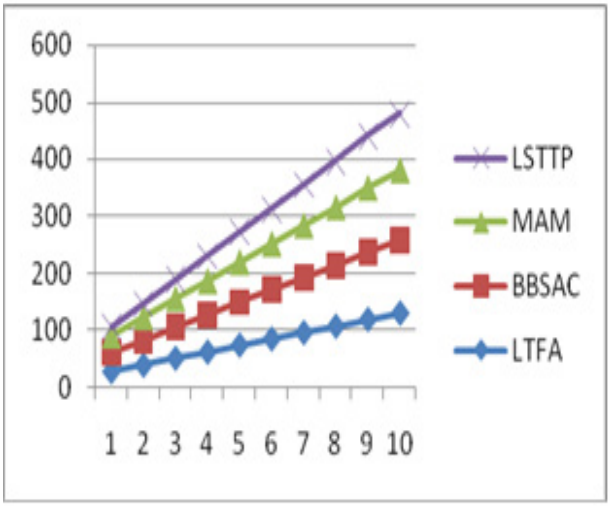


**Figure 9:** Latency (ms)

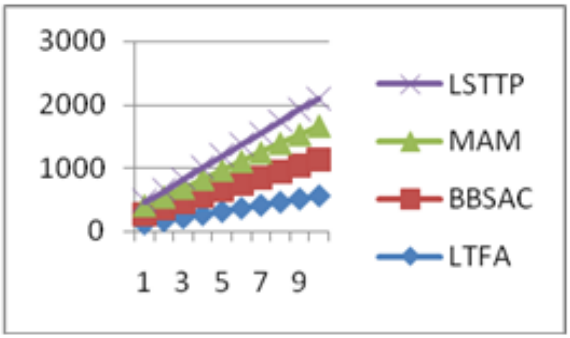


**Figure 10:** End-to-end delay (ms)

### *Throughput*

For a given communication channel the rate of data flow is termed as throughput. Throughput is an important factor which needs a continuous collection of data during environment monitoring. Higher the quality of the

**Table 4:** End-to-end delay (ms)

| *Time stamp* | *LTFA* | *BBSAC* | *MAM* | *LSTTP* |
|---|---|---|---|---|
| 1 | 126 | 143 | 135 | 68 |
| 2 | 172 | 189 | 180 | 108 |
| 3 | 222 | 235 | 223 | 150 |
| 4 | 272 | 282 | 269 | 188 |
| 5 | 322 | 329 | 313 | 231 |
| 6 | 371 | 378 | 356 | 269 |
| 7 | 419 | 422 | 399 | 310 |
| 8 | 469 | 469 | 446 | 352 |
| 9 | 519 | 518 | 487 | 394 |
| 10 | 568 | 562 | 532 | 433 |

**Table 5:** Packet delivery ratio (%)

| *Time stamp* | *LTFA* | *BBSAC* | *MAM* | *LSTTP* |
|---|---|---|---|---|
| 1 | 95.70397 | 94.4753 | 95.05461 | 99.98544 |
| 2 | 92.27934 | 91.07222 | 91.75662 | 97.07275 |
| 3 | 88.62566 | 87.64489 | 88.54483 | 93.96336 |
| 4 | 84.91811 | 84.17445 | 85.16061 | 91.10186 |
| 5 | 81.21594 | 80.71748 | 81.85453 | 87.9763 |
| 6 | 77.56497 | 77.09614 | 78.69664 | 85.12558 |
| 7 | 74.00561 | 73.81431 | 75.48217 | 82.12936 |
| 8 | 70.36272 | 70.3277 | 72.0225 | 79.02536 |
| 9 | 66.63092 | 66.71983 | 68.96161 | 75.89442 |
| 10 | 62.98264 | 63.46225 | 65.63667 | 73.01675 |

throughput indicates high is the quality of the concerned network. The observed values of throughput collected from the simulation results. The highest values which are obtained from the LTFA, BBSAC, MAM, LSTTP methods are 35519 (kbps), 35063 (kbps), 35278 (kbps), 37108 (kbps). Table 2 represents the comparison of the existing and proposed methods (Figure 8). The measurement of latency and calculated by ms .

### *Latency*

Latency is defined as the response time; shorter the response time indicates higher the quality of the network (Figure 9). The latency values obtained from different nodes for the comparative methods within the simulation results are shown in the Table 3.

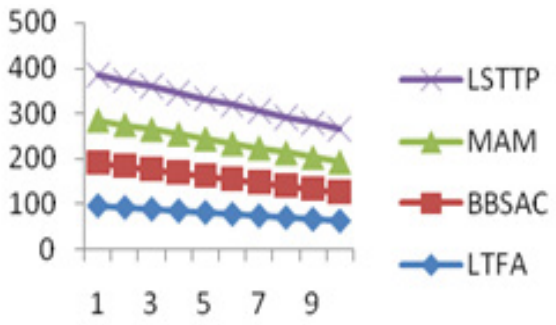


**Figure 11:** Packet delivery ratio

**Table 6:** Security (%)

| *Time stamp* | *LTFA* | *BBSAC* | *MAM* | *LSTTP* |
|---|---|---|---|---|
| 1 | 97.64 | 97.14 | 97.14 | 98.78 |
| 2 | 97.50 | 97.85 | 97 | 99.5 |
| 3 | 97.92 | 97.42 | 97.71 | 98.5 |
| 4 | 97.78 | 98.14 | 97.85 | 99.64 |
| 5 | 98.5 | 97.85 | 97.71 | 98.5 |
| 6 | 97.78 | 97.14 | 98.14 | 98.64 |
| 7 | 98.07 | 97.85 | 97.42 | 98.5 |
| 8 | 97.50 | 97.28 | 97 | 99.07 |
| 9 | 97.781 | 97.85 | 97.57 | 99.35 |
| 10 | 97.64 | 97.28 | 98.14 | 98.92 |

### *End-to-End Delay (ms)*

It is the sum of all the delay during the communication which includes Jitter, system delay and IP-delay. The travel time of a data packet from source to destination is considered. More the delay time of the packet effects the performance of the network. Various end to end delay times with respect to the proposed method are shown in the Table 4 and Figure 10.

The average end to end delay which is carried out from the proposed method LSTTP is obtained as 250.3 ms, whereas the maximum and minimum values of end to end delay are 433 ms at time stamp 10 and 68 ms at time stamp 1, respectively.

### *Packet Delivery Ratio (%)*

It is calculated as the ratio of the number of packets which are transmitted from the source to the number of packets which are received at the destination, higher its values indicate lower is the data loss and hence resembling a strong architecture of the network. Packet delivery ratio obtained values for the comparative and proposed method in OPNET simulation environments are as shown in the Table 5.

The following Figure 11 shows the parameter of packet delivery ratio in (%) between the existing and proposed methodologies

The average PDR value of the proposed method is 86.19% and higher and lower PDR values are 99 and 73% which are obtained at time stamp of 1 and 10.

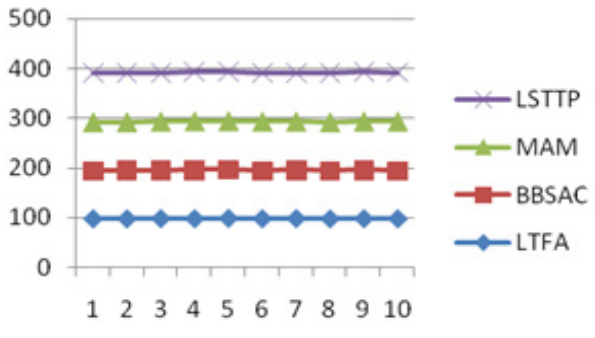


**Figure 12:** Security

**Table 7:** Energy (uJ)

| *Time stamp* | *LTFA* | *BBSAC* | *MAM* | *LSTTP* |
|---|---|---|---|---|
| 1 | 343 | 331 | 333 | 320 |
| 2 | 355 | 346 | 343 | 335 |
| 3 | 378 | 369 | 353 | 340 |
| 4 | 381 | 381 | 374 | 359 |
| 5 | 400 | 391 | 386 | 374 |
| 6 | 429 | 398 | 384 | 368 |
| 7 | 441 | 400 | 403 | 387 |
| 8 | 464 | 417 | 422 | 404 |
| 9 | 479 | 440 | 438 | 405 |
| 10 | 503 | 436 | 435 | 421 |

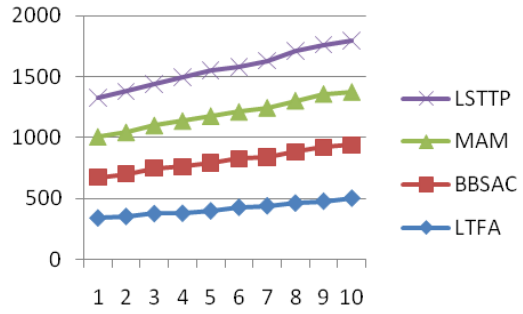


**Figure 13:** Energy

### *Security*

Security plays an important role in any field, more the security, and resembling strangeness of the architecture of the network. Measuring continuous data values is the basic thing for IoT-WSN environment monitoring devices depending on which required and necessary decisions has to be taken, to achieve this they are always kept at remote locations where there is more probability of hackers to hack the devices. The Table 6 represents the compared results of security.

The following Figure 12 shows the parameter of security in (%) between the existing and proposed methodologies

The average security value obtained from the proposed method is 98.4% which is more when compared with that of other existing methods, even the lowest security level is 98% and the highest security levels is 99%.

### *Energy*

Consumption of energy plays an important role in IoT-WSN dependent environment monitoring. Less amount of energy consumed by the packet during its transmission is best and indicates a strong architecture of the model. Simulation environment carried out by OPNET the average amount of energy spent during the data transmission is noted which are labeled in the Table 7.

The following Figure 13 shows the parameter of security in (%) between the existing and proposed methodologies

## Conclusion

Using the architecture of LSTTP, the security among the IoT devices with respect of optimized energy is achieved. Based on the algorithm of LSTTP, the trusted third party authenticates the sensor nodes and establishes the communication between the nodes. When optimal parameters such as latency, throughput, end-to-end delay, throughput, packet delivery ratio along with energy and security are considered then these parameters are reached with satisfiable values from the proposed method when compared with that of the existing methods which is observed from the simulation tool. The obtained results of the proposed method indicate that it will sustain with the current requirements of IoT based monitoring systems.

## Acknowledgement

We are grateful to the Management and Principal for their motivation and constant support. This research has been supported by the grant obtained under the scheme of seed money for research projects from Cauvery College for Women (Autonomous), Tiruchirappalli- 620 018.

## References

Anandhavalli.A, Dr.A.Bhuvaneswari, "Masked Location based Key Exchange Mechanism for IoT Nodes", in International Journal of Intelligent Engineering & Systems, Vol:16, No:1, 2023

Braeken, P. Shabisha, A. Touhafi and K. Steenhaut, "PAIRING FREE AND IMPLICIT CERTIFICATE BASED SIGNCRYPTION SCHEME WITH PROXY RE-ENCRYPTION FOR SECURE CLOUD DATA STORAGE," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, 2017,pp.1-7,doi: 0.1109/CloudTech.2017.8284701.

Behera, T. & Mohapatra, S K & Samal, U.C. & Khan, Mohammad Shoeb & Daneshmand, Mahmoud & Gandomi, Amir. "I-SEP: AN IMPROVED ROUTING PROTOCOL FOR HETEROGENEOUS WSN FOR IOT BASED ENVIRONMENTAL MONITORING", 2020, PP 710-717, doi: 10.1109/JIOT.2019.2940988.

Brogan, J.; Baskaran, I.; Ramachandran, N. "AUTHENTICATING HEALTH ACTIVITY DATA USING DISTRIBUTED LEDGER TECHNOLOGIES. COMPUT. STRUCT. BIOTECHNOL. J. 2018, 16, 257–266. [CrossRef] [PubMed].

Cicala, L.; Angelino, C.V.; Parrilli, S. Fiscante (2018), "UNSUPERVISED POST-FIRE ASSESSMENT OF BURNED AREAS WITH FREE AND OPEN MULTISPECTRAL DATA USING OBIA ", Conference: IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, pp. 1–21. Available online: https://hal.univ-reunion.fr/hal-01957184

Kamal, R. " INTERNET CONNECTED ENVIRONMENT (WEATHER, AIR POLLUTION AND FOREST FIRE) MONITORING". 2017, Available online: https://www.dauniv.ac.in/ public/ front assets/ course material/ Internet of Things /IoT Ch 12L11.PP 1–41

K.Akila, Dr.D.J.Evanjaline "STRENGTHENING IOT-WSN ARCHITECTURE FOR ENVIRONMENTAL MONITORING" in International journal of Innovative technology and Exploring Engineering, ISSN:2278-3075, Volume-8, Issue-11, September 2019.

K.Akila, Dr.D.J.Evanjaline "SECURED IOT-WSN ARCHITECTURE FOR MONITORING ENVIRONMENTAL POLLUTION" in International journal of Scientific & Technology Research, ISSN: 2277-8616,

Volume-8, Issue-12, December 2019.

Y. Lao, B. Yuan, C. H. Kim and K. K. Parhi, "Reliable PUF-Based Local Authentication With Self- Correction," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 2, pp. 201-213, Feb. 2017, doi: 10.1109/TCAD.2016.2569581.

Pranav Gangwani, Alexander Perez-Pons, "SECURING ENVIRONMENTAL IOT DATA USING MASKED AUTHENTICATION MESSAGING PROTOCOL IN A DAG-BASED BLOCKCHAIN: IOTA TANGLE' IN FUTURE INTERNET, 2021, *13*(12), 312; https://doi.org/10.3390/fi13120312.

Pavithra, G., "INTELLIGENT MONITORING DEVICE FOR AGRICULTURAL GREENHOUSE USING IOT," 2018, Journal of Agricultural Science and Food Research. PP 1-4

Pathak, A., AmazUddin, M., Abedin, M.J., Andersson, K., Mustafa, R. and Hossain, M.S., " IOT BASED SMART SYSTEM TO SUPPORT AGRICULTURAL PARAMETERS: A CASE STUDY". Procedia Computer Science, 155, pp.648- 653.

Sooyeon Shin, Taekyoung Kwon "A LIGHTWEIGHT THREE-FACTOR AUTHENTICATION AND KEY AGREEMENT SCHEME IN WIRELESS SENSOR NETWORKS FOR SMART HOMES" in Sensors ,www.mdpi.com/journal/sensors, April 2019.

S. Dhingra, R. B. Madda, A. H. Gandomi, R. Patan and M. Daneshmand, "INTERNET OF THINGS MOBILE– AIR POLLUTION MONITORING SYSTEM (IOT-MOBAIR)," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5577- 5584, June 2019, doi: 10.1109/JIOT.2019.2903821.

S. Wang, J. Yu, M. Atiquzzaman, H. Chen, and L. Ni, "CRPD: A NOVEL CLUSTERING ROUTING PROTOCOL FOR DYNAMIC WIRELESS SENSOR NETWORKS," 2018, Pers. Ubiquitous Computer, vol. 22, no. 3, pp. 545–559.

S. Dutt, S. Agrawal, and R. Vig, "CLUSTER-HEAD RESTRICTED ENERGY EFFICIENT PROTOCOL (CREEP) FOR ROUTING IN HETEROGENEOUS WIRELESS SENSOR NETWORKS ," 2018 Wireless. Pers. Communication., vol. 100, no. 4, pp. 1477–1497.

Sultan Algarni, Fathy Eassa, Khalid Almarhabi, "BLOCKCHAIN-BASED SECURED ACCESS CONTROL IN AN IOT SYSTEM", in Applied Science, Febrary 2021, https://doi.org/10.3390/app11041772.

U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF -BASED SECURE COMMUNICATION PROTOCOL FOR IOT," 2017 ACM Trans. Embedded Computer. Syst., vol. 16, no. 3, pp. 67:1–67

Zhang, Y.; Wu, S.; Jin, B.; Du, J. "A BLOCKCHAIN-BASED PROCESS PROVENANCE FOR CLOUD FORENSICS". In Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 13–16 December 2017; pp. 2470–2473.

Zheng Lu and Hongji Yang, "UNLOCKING THE POWER OF OPNET MODELER". In Cambridge University Press.