International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Lightweight Security Algorithm on PMIPV6 Protocol for IOT Based Wireless Sensor Networks

A. Anandhavalli, A. Bhuvaneswari

Abstract: ***Nowadays Wireless Sensor Networks are using Internet-of-Thing (IoT) technology-based nodes because of the wide usance and cost effectiveness. Many of the Wireless sensor nodes are battery powered devices with limited computational and communication resources. The algorithm of the conventional wireless sensor networks are designed for small closed group network communications with better power management and reasonable security strategies. When using IoT based Wireless sensor networks, the nodes are used to communicate with the internet, where there is a need for more secured algorithm. The internet protocols are having powerful security authentication systems those require more computational resources, thus they can drain a battery operated little wireless sensor node. This work is indented to introduce a legacy power-security balanced algorithm to use in the IoT based Wireless Sensor Network environments. Proxy Mobile Internet Protocol version 6 (PMIPv6) is selected as the base protocol in which the proposed security authentication mechanism is used instead of inbuilt Diffie-Hellman authentication scheme. A customized Media Access Control (MAC) address-based session key initialization procedure along with seed based random number session key update mechanism is proposed and verified in this work.***

Keywords: Internet-of-Things (IoT), Wireless Sensor Networks (WSN), Communication Protocols, PMIPv6, Security schemes, Authentication mechanisms

I. INTRODUCTION

Wireless sensor networks are used to collect and monitor environmental data which is mandatory for several applications such as healthcare, natural resource management, industrial monitoring and natural calamity detections / predictions. Recent advancements in communication science introduced Internet-of-Things (IoT) makes it possible to connect merely all electronic devices with the internet. Present Wireless sensor networks are using IoT to communicate between the nodes and with the internet. Since internet is public and highly vulnerable to intruder attacks, the standard internet communication protocols follow a strong resource consuming high security authentication schemes to initialize, clustering and the routing processes[1][2].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Ms.A.Anandhavalli*, Assistant Professor, Department of Computer Science, Cauverycollege for Women, Trichy,Tamilnadu
Dr A. Bhuvaneswari, Cauvery College for Women (under the affiliation of Bharathidasan University), Trichy, Tamil Nadu, India.

Security protocols developed for conventional wireless sensor networks are targeted in power management rather than security because of the closed nature of the network. The energy efficiency of these protocols is used to extend the battery dependent nodes life and so as the network. Security is compromised here to provide better power management [3].

The challenging part of the protocol design for IoT based wireless sensor network is to assert a balance between Power consumption and Security. The complexity is significantly increased while there are different types of nodes involved in the heterogeneous network environments [4][5].The prominent part of designing a Power-Security balanced algorithm for heterogeneous wireless sensor network relies on its security authentication system. The key generation and session key update process is vital for the authentication procedure.

There are several keys involved such as private signature key, Public signature verification key, Symmetric Authentication Key, Private Authentication Key, Public Authentication Key, Symmetric Data Encryption Key, Symmetric Key Wrapping Key, Symmetric and Asymmetric Random Number Generation Keys, Symmetric Master Key, Private Key Transport Key, Public Key Transport Key, Symmetric Key Agreement Key, Private Static Key Agreement Key, Private Ephemeral Key Agreement Key, Public Ephemeral Key Agreement Key and Symmetric Authorization Key are used in existing Wireless authentication schemes such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access version 2 (WPA2). These authentication keys are used widely in IEEE 801.xx standards. Since the IoT technology is relatively new, the developers are drafting new standards labeled as IEEE P2413, IEEE 804.15.4 and IEEE 1451-99 [6].

Most recent advancement in the communication technology is the invention of LoRa – the Long-Range Wireless IoT Protocol which can cover 15 to 20 kilometers range seamlessly. The contribution of IoT in making the smart world by constructing smart cities will be enormous in the near future [7]. A dedicated power-security balanced communication algorithm is proposed in this work to enhance the quality of the IoT based Heterogeneous Wireless Sensor Network.

II. EXISTING METHODS

There are many developments in-progress in the IoT field. Several attempts are performed by the researchers to ameliorate in IoT based wireless sensor network experiences.

Many of them are commercial success and already used widely in resource monitoring and management. A crisp analysis of some of the renowned methods are analyzed here to compare the performance with the proposed method. The existing methods taken for analysis are Aggregated-Proof based Hierarchical Authentication Scheme for the Internet-of-Things (APHA) [8], Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Thing (DIIOT) [9], Graph Theory Applications in Network Security (GTANS) [10], Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Network (SEPRP-SHIOT) [11], An Ultra-lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet-of-Things (ULASHWSN) [12] and A New Security Authentication Method in the Internet of Things based on PID and Design Impedance Mismatch Physical Unclonable Functions for IoT security (SAMPID) [13].

A. *Aggregated-proof based Hierarchical Authentication Scheme for the Internet-of-Things (APHA)*

This work defines two new protocols to cover Homomorphism function-based System Initialization, Authentication protocol in Unit IoT, Backward aggregated proof challenge, Forward aggregated proof response, The authentication protocol in Ubiquitous IoT, Data confidentiality, Data integrity, Hierarchical access control, Mutual Authentication, Privacy Preservation. The APHA procedure is analyzed by the Burrows-Abadi-Needham (BAN) logic. The work concentrates only on security and other important network quality assessment metrics such as Throughput, Communication delays, Packet Delivery Ratio and Power consumption are not included in the study. The proposed method is not tested with any Network Simulator or with Protocol Definition Language (PDL).

B. *Edge Mesh: A* ***New*** *Paradigm to Enable Distributed Intelligence in Internet of Things (DIIOT)*

Edge devices are capable of processing the data which pass through it. The distribution nature of Edge technology shares the computational load among the devices. The process distribution sagely avoids overloading of specific nodes in the network. DIIOT work is referred here due to this load distribution nature which prevents power supply drains in specific nodes. Energy saving is the only motive of the work DIIOT and other essential network metrics are not discussed in this work. The challenges of applying DIIOT in IoT real-time environments are heterogeneous node connectivity, frequent packet loss, communication stability in low data rates and random channel variations[14].

C. *Graph Theory Application in Network Security (GTANS)*

Four Color Graph Theorem is used as the base of this GTANS work. GTANS is created to create the least possible communication traffic and high-speed execution. The challenges in Four color graph theorem such as Elimination of no-coverage spots and Allocation of different channel in overlapping spots are well handled in GTANSusing a node coloring algorithm. GTANS is a coarse procedure that is applicable for Cellular Relay Networks, Mobile ad-hoc Networks, Wireless Mesh Networks wireless sensor networks. GTANS is added here due to its less traffic operation in wireless sensor network environments. The traffic reduction mechanism is used to improve the throughput and packet delivery ratio by reducing the data congestion and packet loss. Energy, Time and Resource optimizations are achieved by GTANS but security is not discussed. A proof-of-concept by simulation or implementation results are not carried out in this work.

D. *Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Network (SEPRP-SHIOT)*

SEPRP-SHIOT is developed to provide security and performance enhancements for Smart Home Internet of Things (SH-IoT). SEPRP-SHIOT has the ability to handle heterogeneous nodes in a Smart Home Network Environment. PMIPv6 is selected as the base protocol in SEPRP-SHIOT. The security of SEPRP-SHIOT is proved by using BAN Logic. Standard performance metrics such as Throughput, End-to-End Delay, Transmission Rate and Packet loss are analyzed in this work using Network Simulator-2 and AVISPA – an automated tool which can analyze a communication protocol defined in High-Level Protocol Specification Language (HLPSL). SEPRP-SHIOT achieved better results in terms of stand metrics. The power consumptions of nodes in different network conditions are not covered in SEPRP-SHIOT.

E. *An Ultra-lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet-of-Things (ULASHWSN)*

ULASHWSN work is about to achieve secured communication in wireless sensor network with low power consumption. It takes part in user-to-sensor node authentication. ULASHWSN defines a clear authentication scheme for different phases of communication such as registration phase, authentication phase between sensor nodes and gateway and key establishment between nodes and users. ULASHWSN protects wireless sensor from various attacks such as Replay attack, Impersonation attack and Denial of Service attack. A clear energy consumption analysis is performed theoretically in ULASHWSN. Network performance metrics such as throughput and communication delays are not discussed in ULASHWSN. The energy efficient authentication scheme of ULASHWSN makes it inevitable in the comparison.

F. *A New Security Authentication Method in the Internet of Things based on PID and Design Impedance Mismatch Physical Unclonable Functions for IoT security (SAMPID)*

SAMPID introduced a new Pseudo Identifier to annihilate security problem during data transfer between tags and servers in IoT environment. The legal ID of tag is saved in the protocol to provide authentication between database server and IoT tag. Anonymity of the Tags, Position trailing attacks, Forward security, Mutual authentication, Relay attack, DoS and Synchronization
problems are analyzed in this work. SAMPID is tested in the RFID tag authentication where the throughput and communication delays are bearable to certain amount. The security is analyzed with the BAN logic and there is no simulation or implementation results provided in the work. SAMPID is brought here for comparison due to its simple authentication scheme, faster performance than hash-based protocolsand the Pseudo ID requires lesser storage space in IoT environment.

The advantages and limitations of the existing methods are given below in Table 1.

Author	Work	Method	Advantages	Limitations
Huansheng Ning et.al.	Aggregated-proof based Hierarchical Authentication Scheme for the Internet-of-Things	U2IoT Authentication	High Security	Moderate Performance and High energy consumption
Yuvraj Sahni et.al.	Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things	EDGE Distribution	Load Balance and Energy efficient	Lagging heterogeneous node connectivity
Jonathan Webb et.al.	Graph Theory Application in Network Security	Four Color Theorem	High Performance	Low Security
Daemin Shin et.al.	Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Network	PMIPv6 Authentication	High performance with high security	High Power and resource demand
Hamza Khemissa et.al.	An Ultra-lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet-of-Things	User to sensor node Authentication	High Security with Low Power Consumption	Low Performance
Jinsha Yuan et.al.	A New Security Authentication Method in the Internet of Things based on PID and Design Impedance Mismatch Physical Unclonable Functions for IoT security	Pseudo Identifier based Authentication	Moderate Security with High performance	High Power consumption

Table 1: Advantages and Limitations of Existing Methods

II. RELATED WORKS

Understanding Key exchange procedures and Random Number Generation are cardinal for proposed Lightweight PMIPv6 based Security Algorithm for IoT Wireless Sensor Networks (LPSAIW). Diffie-Hellman Key Exchange procedure is used the standard PMIPv6 protocol. Random number generation is widely used in many key exchange methods to select the initial keys or prime numbers.

A. Diffie-Hellman Key Exchange (DHKE)

Diffie-Hellman Key exchange procedure is one of the quondam procedures used to establish a shared secret key secured communication in the public communication channels. The steps involved in exchanging keys in DHKE are given below

Step 1. Both Sender and Receiver are agreed to use a finite cyclic group G with the generating element g in Order n

Step 2. Sender selects a random number a which satisfies the condition $1 \leq a < n$ and sends g^a to Receiver

Step 3. Similarly, Receiver selects a random number b and sends g^b to the Sender

Step 4. Sender computes the shared secret key g^{ab} as $(g^b)^a$

Step 5. Receiver computes the shared secret key g^{ab} as $(g^a)^b$

This five-step simple and straight-forward method is famed in the shared secret key based public channel communications. A simple pictorial representation DHKE is given below as Figure 1 for the betterment of understanding.

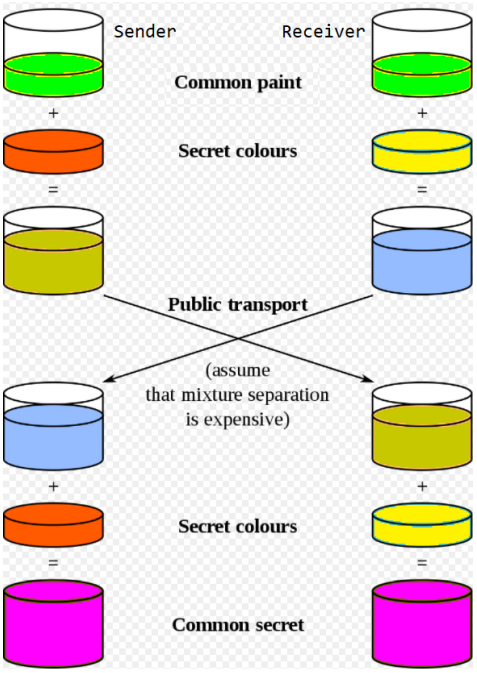


Figure 1: Pictorial Representation of DHKE

Though the DHKE procedure seems simple, calculating prime numbers and exponential values are complicated for the limited computational resource devices such as wireless sensor network. Therefore, selecting a low-computational complexity key exchange procedure is required in the IoT based Wireless sensor networks Nodes.

B. Random Number Generation

Random Number Generation is an important process in cryptography and security key generation. There are many random number generation procedures are used currently in security key management process. Some procedures require a prime random number whereas other methods are just fine with any random integer. Repeatability and randomness are required as the vital characteristics of a random number generation procedure un security schemes. Repeatability refers the ability of generating same sequence for same initial seeds. This property is used for debugging and in mutual key authentication systems. Randomness refers that the generated random numbers should be uniformly distributed independent numbers which can pass randomness statistical tests.

Linear Congruential Method is widely used to generate random numbers for many applications. It produces a sequence of random numbers between 0 and $max - 1$ such as$\gamma_1, \gamma_2, \ldots max - 1$ based on the equation $\gamma_{i+1} = (a\gamma_i + c)\, mod\, max\,, i = 1,2\ldots.$ Here the initial value γ_0 is the seed of the sequence, a is a constant multiplier, c is the increment and max is the modulus. If $c \neq 0$ then the method is called mixed congruential method. Otherwise it is called as Multiplicative congruential method. Combined Linear Congruential Method is introduced to extend the cyclic length of the random number repetitive sequences. It also increases the prediction complexity which is achieved by combining more than one multiplicative congruential generator. The Equation for Combined Linear Congruential Method is $\gamma_{i+1,j} = (a_j\gamma_i + c_j)\, mod\, max_j$.

Hardware random number generators are more powerful and can make complex random number sequences than the arithmetic algorithm based random number generators. Hardware random number generators use Real-Time-Clock (RTC), Environmental Temperature, Environmental Noise or accumulated values from random scratchpad memory as their seeds which provides complete unpredictable randomness. Some Hardware random number generators are using light intensity as the source of seeds [15]. The operating model of hardware random number generator is explained in Figure 2.

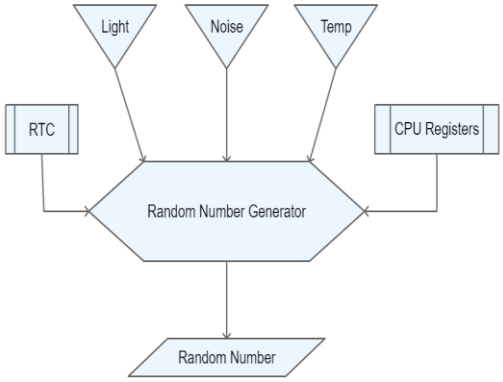


Figure 2: Hardware Random Number Generator

III. PROJECTED WORK

A. Lightweight Security Algorithm on PMIPv6 protocol for IoT based Wireless Sensor Networks (LSA)

LSA consists of two primary functional modules. The first module MAC Address XOR key exchange authentication (MAXOR) is used to initialize the communication session between the nodes. The second module Legacy Random number Generator (LRG) is used for key annihilation of session keys and key updates. These two modules combined together to form the LSA for IoT based Wireless sensor networks.

a. MAC Address XOR Key exchange authentication (MAXOR)

MAC address is an unique identifier for the communication devices. MAC-48 is the latest addressing scheme which can point 281474976710656 different devices. IPv6 protocol treats MAC-48 as EUI-48 (Extended Unique Identifier) which is represented in six 2-digit hexadecimal numbers noted as 00:00:00:00:00:00. Since these addresses are unique for all communication devices, MAXOR uses it as the base in initial authentications.

Let MAC_g is the MAC address of the gateway, $MAC_{N1}$is the MAC address of IoT Node 1 and MAC_{N2} is the MAC address of IoT Node 2. When Node 1 and Node 2 want to communicate each other, they should share the same secret key. Gateway takes place in initializing the communication and to share the keys between the nodes. Node 1 selects a random number γ_{N1} and calculates $MAC'_{N1} = MAC_{N1} \oplus \gamma_{N1}$. Then Node 1 sends MAC'_{N1} to the gateway.

Gateway recognize the Node 1 since its MAC address is already registered and calculates the value of γ_{N1} using the following equation.

$\gamma_{N1} = MAC'_{N1} \oplus MAC_{N1}$ Equation(1)

Similarly, the random number γ_{N2} which is selected by Node 2 can be calculated using the following Equation

$\gamma_{N2} = MAC'_{N2} \oplus MAC_{N2}$ Equation(2)

Here MAC'_{N2} is received by a ping request sent by gateway to Node 2 and MAC_{N2} is already available to gateway since Node 2 is also registered in the same network.

Then the gateway calculates K_{N1} as $\gamma_{N2} \oplus MAC_{N1}$ and K_{N2} as $\gamma_{N1} \oplus MAC_{N2}$. Then K_{N1} is sent to Node 1 and K_{N2} is sent to Node 2 by the gateway.

Now it is possible to know the secret key of Node 2 to Node 1 using Equation 3 given below

$\gamma_{N2} = K_{N1} \oplus MAC_{N1}$ Equation(3)

Similarly, Node 2 can calculate the secret key of Node 1 using the following Equation

$\gamma_{N1} = K_{N2} \oplus MAC_{N2}$ Equation (4)

Now Node 1 and Node 2 can calculate the shared secret key δ_{N1N2} by using following equation

$\delta_{N1N2} = \gamma_{N1} \oplus \gamma_{N2}$ Equation(5)

The justness of the above equations is explained using the following illustration

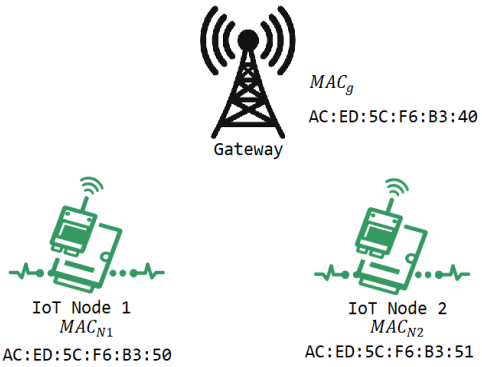


Figure 3: MAXOR – Gateway and Nodes information

Let MAC_g = AC:ED:5C:F6:B3:40 = [10101100:11101101:1011100:11110110:10110011:1000000]b

Let MAC_{N1} = AC:ED:5C:F6:B3:50 = [10101100:11101101:1011100:11110110:10110011:1010000]b

Let MAC_{N2} = AC:ED:5C:F6:B3:51 = [10101100:11101101:1011100:11110110:10110011:1010001]b

The Secret Key of Node 1 γ_{N1}= 0x45 = 1000101 b

MAC'_{N1}= E9:A8:19:B3:F6:15

Gateway receives MAC'_{N1} from Node 1 and calculates γ_{N1} by Equation 1

γ_{N1}= [E9:A8:19:B3:F6:15] $\oplus$ [AC:ED:5C:F6:B3:50] = [45:45:45:45:45:45] := 0x45

Node 2 selects its secret key γ_{N2} = 0x34 = 110100 b

Node 2 Calculates MAC'_{N2} = 98:D9:68:C2:87:65 after getting the ping request from gateway

Gateway receives MAC'_{N2} from Node 2 and calculates γ_{N2} by Equation 2

γ_{N2} = [98:D9:68:C2:87:65] $\oplus$ AC:ED:5C:F6:B3:51 = [34:34:34:34:34:34] := 0x34

Now gateway can calculate K_{N1} = [98:D9:68:C2:87:64],K_{N2}= [E9:A8:19:B3:F6:14] and sends them to Node 1 & 2 respectively.

Node 1 calculates γ_{N2} as follows by Equation 3

γ_{N2} = [98:D9:68:C2:87:64] $\oplus$ [AC:ED:5C:F6:B3:50] = [34:34:34:34:34:34] := 0x34

Similarly, Node 2 can calculate the secret key γ_{N1} of Node 1 using Equation 4

γ_{N2}= [E9:A8:19:B3:F6:15] $\oplus$ [AC:ED:5C:F6:B3:50] = [45:45:45:45:45:45] := 0x45

Now Node 1 and Node 2 calculates the shared secret key as follows by Equation 5

$$\delta 0_{N1N2} = [45:45:45:45:45:45] \oplus [34:34:34:34:34:34] = [71:71:71:71:71:71]$$

By this way the Session key initialization process is performed in proposed LSA without power starving exponential operation and complicated calculations. Since the logical XOR operation is inbuilt in the processors architecture itself, the session initializations start seamlessly.

B. Legacy Random number Generator (LRG)

Generating random numbers with complete randomness is an important task in security procedures. Generating same random number in different devices is also a crucial task in a network environment. When two nodes are communicating each other, they have to generate random numbers in same order to maintain the harmony in session key updates. Session key update is required in situations such as end of session timing, long jitter or latency, too much of packet drops and during intruder attacks. Session key update during the intruder attacks ensure the security of the network.

LRG uses Combined Linear Congruential Method with legacy seeds. When two nodes - Node 1 and Node 2 are in the communication with the shared secret key $\delta 0_{N1N2}$ with the value [71:71:71:71:71:71] the next secret key $\delta 1_{N1N2}$ will be generated using existing key and new session time stamp as follows

Let the synchronized network session time is $t_h : t_m : t_s : t_i$ in Hour : Minute : Second : Millisecond sequence

The seed ξ for random number generation is calculated as $\xi = (t_n + t_m + t_s) \times t_i$

Then a set of 6 random numbers $\Gamma = \{\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Gamma_5\}$ is generated using the Combined Linear Congruential Method

The for any new session $n + 1$, the session key will be calculated as follows

$\delta 1_{N1N2} = \delta 0_{N1N2} \oplus \Gamma$ Equation (6)

For the existing key $\delta 0_{N1N2} = [71:71:71:71:71:71]$, new session key $\delta 1_{N1N2}$ is calculated as

$$[71 \oplus \Gamma_0 : 71 \oplus \Gamma_1 : 71 \oplus \Gamma_2 : 71 \oplus \Gamma_3 : 71 \oplus \Gamma_4 : 71 \oplus \Gamma_5]$$

The main purpose of introducing LRG is to obscure the random number seed generation process from the intruders to ensure security.

IV. EXPERIMENTAL SETUP

OPNET – one of the best network simulation and evaluation tools of the decade which is developed by OPNET Technologies Inc. and acquired by Riverbed Technology. OPNET uses graphical representations of different network nodes and network environments[16][17]. It has the provision to inherit the real-world network environments by defining the latitude and longitude details.

Table 2: Simulation Parameters

S.No	Entity	Details
1	Simulation Area	10000 Square meters
2	Number of Nodes	100 to 1000 in step 100
3	IoT-Node types	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 from 100 meters to 1000 meters
8	Frequency bands	Auto-select
9	Simulation Time	168 real-world hours

OPNET permits to define and override the default network node types, protocols and network communication strategies. OPNET has an advanced property of processing C++ codes to define the network strategies such as in Automatic Validation of Internet Security Protocols and Applications (AVISPA) [18]with High Level Protocol Specification Language (HLPSL).

Experiments are carried out in OPNET repeatedly with different number of nodes for existing and proposed methods. The Simulation world details are provided in Table 2.

Visual Studio is one of the Industry leading Integrated Development Environments (IDE) from Microsoft. Visual Studio[19]is used to code the Network scripts and a dedicated UI is designed to perform repeated OPNET simulations, acquire results and to plot the comparison graphs. User Interface screen image is given in Figure 4.

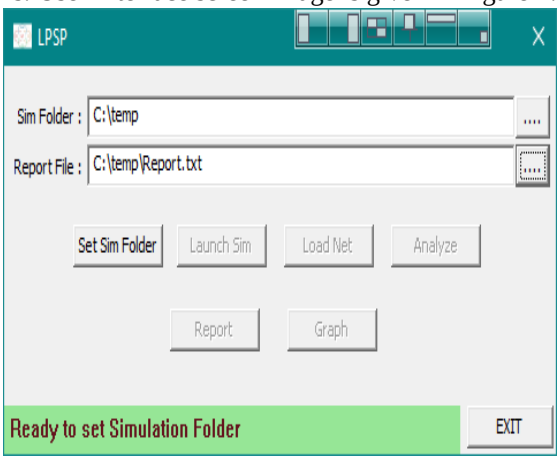


Figure 4: Dedicated User Interface

Network node placement in OPNET Simulator is given in Figure 5.

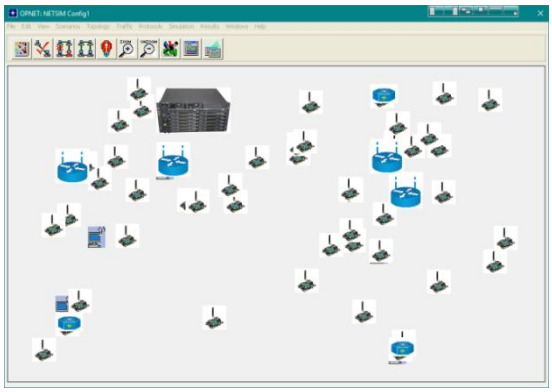


Figure 5: Node placements OPNET

V. RESULT AND ANALYSIS

Standard network evaluation metrics such as Throughput, Communication Delays, Packet Delivery Ratio, Security and Energy consumption are measured through the OPNET Simulation. Observed values are given as tables and graphs below.

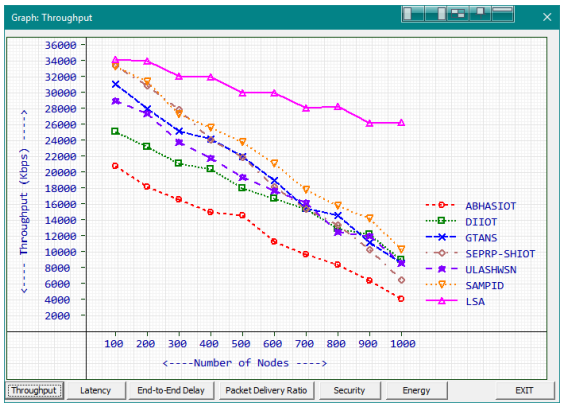
A. Throughput

Throughput refers the successful data communication in a network channel. Throughput is measured in bits-per-second (bps) units which represents how fast the communication occurs in the channel. In general, IoT wireless sensor nodes are communicating little pieces of information over the network whereas, broadened use of IoT devices such as healthcare monitors continuously streaming data to the network. The tremendous increase of individual healthcare devices causes plenty of data flow over the network, so it is important to measure the throughput and to find the maximum data transfer capacity of the network. Throughput values are measured for 100 to 1000 number of nodes with different methods are given in Table 3 and plotted as graph in figure 6.

Table 3 : Throughput (Kbps)

Throughput (Kbps)							
Nodes	**ABHASIOT**	**DIIOT**	**GTANS**	**SEPRP-SHIOT**	**ULASHWSN**	**SAMPID**	**LSA**
100	20963	25985	31013	33151	29578	32636	34248
200	18317	23574	28206	31072	26958	30152	34438
300	17143	21995	26657	26304	25108	27511	32344
400	15809	20068	22671	24314	22816	25545	32398
500	14446	18057	21474	21722	20337	23541	30100
600	12886	17178	18454	19313	18438	20704	30342
700	9920	15377	17078	15571	16619	19353	28239
800	8319	12221	13140	13295	13918	17049	28198
900	5784	11603	11970	10417	11700	13929	26465
1000	4505	9803	7981	7027	8714	12219	26373

Figure 6: Throughput (Kbps)



It is observed that the increase in node count causes a decrement in the throughput. While observing the slope, proposed LSA has a shallow slope than the other methods. SEPRP-SHIOT scored the throughput value of 33151 kbps for 100 nodes and 7027 kbps for 1000 nodes – causes a deep slope. Proposed LPSP scored higher throughput values in all experiments with different node counts.

B. Latency

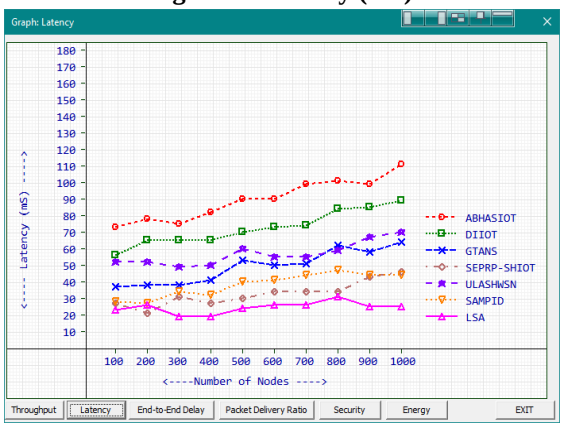
Latency is the duration between a data transfer request and the beginning of the data transfer. If the latency is higher, then the overall response time of the network will be high. Therefore, a good communication protocol should take fewer latency values. Latency values are measured for existing and proposed methods and given in Table 4.

Table 4: Latency (mS)

Latency (mS)							
Nodes	**ABHASIOT**	**DIIOT**	**GTANS**	**SEPRP-SHIOT**	**ULASHWSN**	**SAMPID**	**LSA**
100	76	61	34	21	45	25	24
200	72	68	45	24	47	32	20
300	84	64	42	30	57	32	20
400	81	66	46	34	54	34	29
500	92	70	45	34	54	33	30
600	91	74	54	39	61	40	31
700	93	78	54	32	62	39	23
800	104	79	58	40	64	48	27
900	109	89	64	36	65	45	26
1000	109	90	61	46	69	46	32

From the table, it is understood that the latency slightly increases with the increase in number of nodes. Table values are plotted as graph and given in the following Figure 7.

Figure 7: Latency (mS)



Latency is measured in Milliseconds (mS). While number of nodes is more than 100, LSA gets lower latency values than the other methods.

It is 24 mS for 100 number of nodes and 32 mS for 1000 number of nodes. SEPRP-SHIOT gets the lowest latency of 21 mS for 100 nodes, but it takes higher latency than LSA for more than 100 number of nodes. Therefore, LSA is recommended to use where there are more than 100 number of IoT nodes in a network.

C. End-to-End delay

End-to-End delay is the time duration between the beginning of a data packet transfer from the source node and ending in the destination node. It consists of all communication delays such as latency, IP delay, system delay and jitter. End-to-End delay also should be kept in control to design a better network protocol. End-to-End delay is measured in Milliseconds. Since End-to-End delay is the accumulated value of all communication delays, it is also increasing when the number of nodes is increased. Measured values and Comparison graph of End-to-End delay values are given in Table 5 and Figure 8.

Table 5: End-to-End delay(mS)

End-to-End Delay (mS)							
Nodes	**ABHASIOT**	**DIIOT**	**GTANS**	**SEPRP-SHIOT**	**ULASHWSN**	**SAMPID**	**LSA**
100	186	178	150	125	158	145	102
200	222	207	178	136	191	166	102
300	244	237	196	152	223	180	112
400	282	266	226	160	252	210	114
500	307	301	257	176	279	230	118
600	334	323	280	190	301	244	119
700	367	353	313	200	331	268	125
800	395	387	333	211	362	293	128
900	426	417	361	223	397	315	123
1000	457	448	388	232	420	334	131

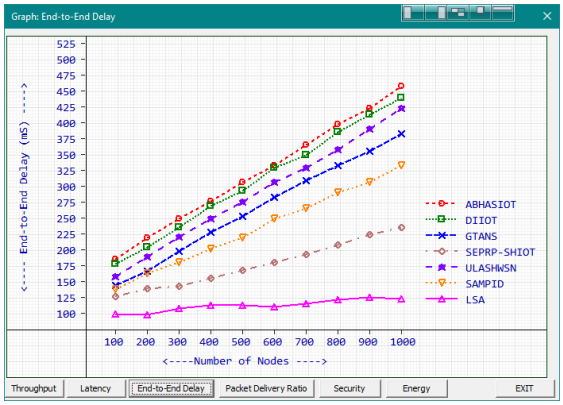


Figure 8: End-to-End delay (mS)

D. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the ratio between number of transmitted data packets from the source node and number of successfully received data packets by the destination node. Higher value of PDR refers low number data collisions and packet drops. Measured PDR values are given in table 6 and plotted as graph in Figure 9 – given below.

Table 6: Packet Delivery Ratio (%)

Packet Delivery Ratio (%)							
Nodes	**ABHASIOT**	**DIIOT**	**GTANS**	**SEPRP-SHIOT**	**ULASHWSN**	**SAMPID**	**LSA**
100	94	94	97	98	96	97	99
200	91	90	95	97	92	96	98
300	88	88	92	97	90	95	98
400	87	88	91	96	90	92	96
500	84	84	87	95	86	89	95
600	83	83	87	93	84	87	95
700	79	81	85	92	84	87	94
800	77	78	82	91	81	83	92
900	73	75	80	90	80	83	92
1000	73	73	79	90	78	79	90

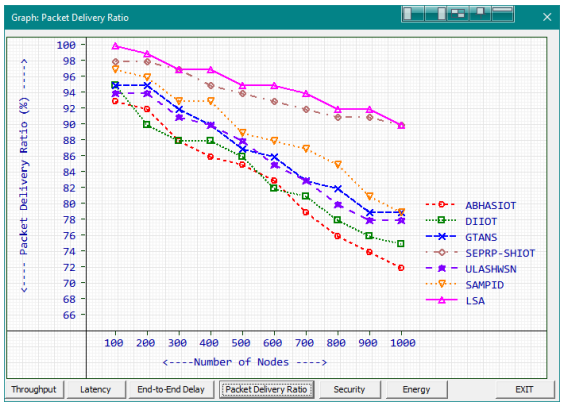


Figure 9: Packet Delivery Ratio (%)

Based on the PDR results, SEPRP-SHIOT is the close competitor for the proposed LSA – which has the highest PDR Value 99% for 100 number of nodes. For 1000 number of nodes, both LSA and SEPRP-SHIOT are scoring 90% PDR.

E. Security

Security is one of the important metrics in network communication. The entire network can be in vulnerable situation if security is compromised. IoT-WSN are used in several sensitive area such as healthcare and industrial automations, security is the prime aspect taken in to consideration. OPNET has the facility to measure the security in a network architecture by introducing random intruder attacks. The measured security values of existing and proposed methods are given in Table 7.

Table 7: Security (%)

Security (%)							
Nodes	**ABHASIOT**	**DIIOT**	**GTANS**	**SEPRP-SHIOT**	**ULASHWSN**	**SAMPID**	**LSA**
100	98	93	91	98	96	94	99
200	98	94	91	98	97	94	98
300	97	94	92	98	97	94	98
400	98	93	91	97	96	95	99
500	98	93	91	98	97	94	98
600	98	93	92	97	97	94	98
700	97	94	92	98	97	95	98
800	98	93	91	98	96	95	99
900	97	93	91	98	96	94	99
1000	97	93	92	97	96	95	98

Security levels of procedures are plotted as graph in figure 10.

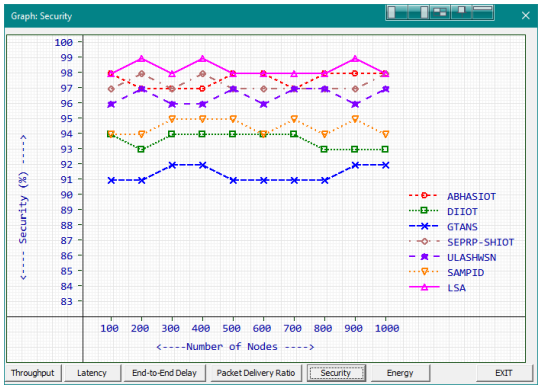


Figure 10: Security (%)

LSA manages the security level between 98% to 99% for the number of nodes from 100 to 1000. ABHASIOT and SEPRP-SHIOT are closely following with their security range from 97% to 98% for 100 to 1000 number of nodes.

F. Energy

Energy consumption is one of the prime factors where there are a notable number of battery-powered network nodes. As the IoT based wireless sensor network nodes are primarily battery-operated devices, Energy consumption is a vital parameter here. Energy is measured in Micro-Joules (uJ), The energy consumption values are given in Table 8.

Energy (uJ)							
Nodes	**ABHASIOT**	**DIIOT**	**GTANS**	**SEPRP-SHIOT**	**ULASHWSN**	**SAMPID**	**LSA**
100	984	1157	1119	901	403	907	378
200	1005	1159	1128	918	442	942	373
300	1015	1183	1165	941	471	978	397
400	1044	1223	1181	979	489	997	391
500	1062	1231	1229	1029	514	1006	424
600	1078	1250	1227	1037	543	1049	420
700	1074	1254	1271	1075	552	1059	467
800	1114	1272	1272	1090	588	1082	445
900	1116	1280	1293	1138	607	1113	476
1000	1127	1297	1333	1180	619	1126	487

The energy consumed to complete successful network transactions are calculated and the average value is calculated. The average energy consumption represents the requirement to complete a network transaction from source to destination. The table values are plotted as graph in Figure 11.

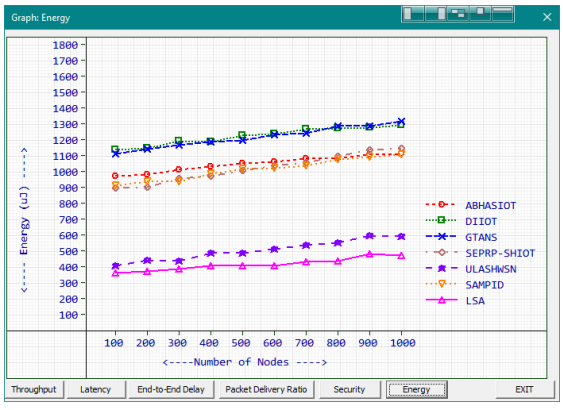


Figure 11: Energy (uJ)

Based on the observed results, proposed LSA consumes an average of 378 uJ while the number of nodes is 100 and 487 uJ while the number of nodes is 1000. ULASHWSN consumes a little more energy of 403 uJ for 100 nodes and 619 uJ for 1000 nodes.

VI. CONCLUSION

Network performance, Security and Energy efficiency are the vital deciding factors in the evaluation of a communication protocol. While analyzing the existing communication protocols for this research work, it is understood that many of the procedures breaks in either one or two key factors while trying to improve one key factor. Improving or sustaining one key factor while improving the another is a challenging task. In this proposed work LSA, a Lightweight security algorithm is designed and evaluated which shows improved results in Network performance, Security and Energy efficiency. Therefore, the proposed work will support upcoming IoT based wireless sensor network applications from constructing Smart home to Smart city. On account of its property of improved security and energy efficiency without compromising the network performance, LSA is desirable to use with many kinds of IoT Wireless Sensor Network Applications.

REFERENCES

1. Meenakshi Munjal and Niraj Pratap Singh, "QoS and Cost-Aware Protocol Selection for Next Generation Wireless Network" in Journal of Network and Systems Management - Volume 27 issue 2, Springer 2019, pp.327-350
2. Kuinam J. Kim and Kyung-Yong Chung, "IT Convergence and Security 2012" in Lecture Notes in Electrical Engineering book serie - Volume 215, Springer 2018, pp. 685 – 693
3. Ivana Tomić and Julie A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols" in IEEE Internet of Things Journal - Volume: 4 Issue: 6, IEEE 2017, pp. 1910-1923
4. Qi Yuan, Chunguang Ma, Xiaorui Zhong, Gang Du and Jiansheng Yao, "Optimization of key predistribution protocol based on supernetworks theory in heterogeneous WSN" in Tsinghua Science and Technology - Volume: 21 Issue: 3, IEEE 2016, pp. 333 – 343
5. HyungukYoo and Taeshik Shon, "Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture" in Future Generation Computer SystemsVolume 61, Elsevier 2016, pp. 128-136
6. Marco Centenaro, Lorenzo Vangelista, Andrea Zanella and Michele Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios" in IEEE Wireless Communications Volume: 23 Issue: 5, IEEE 2016, pp. 60-67
7. Malay Bhayani, Mehul Patel and Chintan Bhatt, "Internet of Things (IoT): In a Way of Smart World" in Proceedings of the International Congress on Information and Communication Technology, Springer 2016, pp. 343-350
8. Huansheng Ning, Hong Liu and Laurence T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things" in IEEE Transactions on Parallel and Distributed Systems Volume: 26 Issue: 3, IEEE 2014, pp. 657-667
9. Yuvraj Sahni, Jiannong Cao, Shigeng Zhang and Lei Yang, "Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things" in Mobile Edge Computing for Wireless Networks - IEEE Access Volume: 5, IEEE 2017, pp. 16441-16548

10. Jonathan Webb, Fernando Docemmilli and Mikhail Bonin, "Graph Theory Applications in Network Security" in Cryptography and Security, arXiv 2015, pp. 1-7
11. Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon and Ilsun You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks" in ecurity and Privacy in Applications and Services for Future Internet of Things - IEEE Access Volume: 5, IEEE 2017, pp. 11100-11117
12. Hamza Khemissa, Djamel Tandjaoui and SamiaBouzefrane, "An Ultra-Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things' in International Conference on Mobile, Secure, and Programmable Networking, Springer 2017, pp 49-62
13. Jinsha YUAN, Yang XU and Huisheng GAO, "A New Security Authentication Method in the Internet of Things Based on PID" in International Journal of Simulation -- Systems, Science & Technology Volume 17 Issue 44, EBSCO 2016, pp. 9.1-9.6
14. Tiago P. C. de Andrade, Carlos A. Astudillo, Luiz R. Sekijima and Nelson L. S. da Fonseca, "The RandomAccess Procedure in Long Term Evolution Networks for the Internet of Things" in IEEE Communications Magazine Volume: 55 Issue: 3, IEEE 2017, pp. 124-131
15. MarialenaAkriotou, Charis Mesaritakis, EvaggelosGrivas, CharidimosChaintoutis, Alexandros Fragkos and Dimitris Syvridis, "Random Number Generation from a Secure Photonic Physical Unclonable Hardware Module" in Security in Computer and Information Sciences, Springer 2018, Pages: 28-37
16. Zheng Lu and Hongji Yang, "Unlocking the Power of OPNET Modeler" in Cambridge University Press
17. Maryam Pahlevan and Roman Obermaisser, "Evaluation of Time-Triggered Traffic in Time-Sensitive Networks Using the OPNET Simulation Framework" in Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), IEEE 2018, Pages: 283 - 287
18. David Basin, Cas CremersandCatherine Meadows, "Model Checking Security Protocols" in Handbook of Model Checking, Springer 2018, Pages: 727-762
19. Sun-Ju Kim, Ji-Hyun Min and Han-Na Kim, "The Development of an IoT-Based Educational Simulator for Dental Radiography" in Healthcare Information Technology for the Extreme and Remote Environments, IEEE 2019, Pages: 12476 - 12483

AUTHOR PROFILE

Ms.A.Anandhavalli, pursued Master of Computer Application from bharathidasan University in the year 2003. She is currently pursuing Ph.D and working as Assistant Professor in department of Computer Science, Cauverycollege for Women, Trichy,Tamilnadu, India. She is a life member ISSE. Her main research work focus on Internet of Things. She has 12 years of teaching experience.

Dr A. Bhuvaneswari, completed her Masters Degree in Computer Science and Master of Philosophy in Computer Science in the years 2002 and 2005 respectively. She has also completed his Doctorate in Computer Science in the year 2015. She has around 17 years of Academic experience and ten years of Research experience in the field of Computer Science. Currently she is working at Cauvery College for Women (under the affiliation of Bharathidasan University), Trichy, Tamil Nadu, India. She has published several papers in International Journals and Conferences related to Computer Science. Her area of interest is Mobile Communication and Internet of Things.