Secured IOT-WSN Architecture For Monitoring Environmental Pollution

K. Akila, Dr. D.J.Evanjaline

Abstract: The environment Pollution is the terrifying issue of this trendy world. A suitable requirement is needed to monitor different environmental pollutions. Many researchers and volunteers are developing and deploying Wireless Sensor Networks (WSN) for this purpose. Internet-of-Things (IoT) is one of the widely used cost-effective technologies to design wireless sensor nodes. A spanking new functional module is initiated in this work to constitute the proposed work named as 'Secured IoT-WSN Architecture for Environmental Monitoring pollution' (SIAEM) which is indented to overcome some impuissance of applying generalized wireless sensor network architecture in the field of environmental pollution monitoring. The fresh functional module introduced in this work is Dynamic Security Scheme Manager (DSSM). The aim of this projected Secured IoT-WSN architecture is to increase the Security. The impact of proposed method in the performance of Secured IoT-WSN network is measured and stated using benchmark network simulator.

Index Terms: Dynamic Security Scheme, Environment Monitoring System, Internet-of-Things (IoT), Wireless Sensor Network (WSN)

1. INTRODUCTION

Environment Pollution is spacious range of Problem around the world. Environmental safety is the burning topic circulates around the world. Global warming [1] and natural calamities tuned the heads of all nations towards them and make them to conclude their stand about protecting the nature. One side there are plenty of inventions to make the living as more comfortable and luxurious. Many awareness programs were stated during last decade to prevent the disasters. To overcome these concerns, many governments have their policies and guidelines for protecting the nature in secure manner. To monitor the environment persistently in a periodical manner, a dedicated Cost effective and secure network to connect the sensor devices is required. The low cost refers here both initial instalment cost as well as the running cost. IoT affords an easy way to connect any device with the internet. The Combination of IOT based wireless sensor nodes can be used to construct a Secured cost-effective environmental monitoring system. This work is destined to search and analyse the existing methods which serves this requirement. The analysis is performed based on one of the standard network assessment metric of Security

2 EXISTING METHODS

Many Researchers are developing new proposals to construct IOT based Wireless Sensor network. A set of communication protocols are for the purpose of connecting wireless sensor nodes and exchange the information among the nodes within network. This Analysis is based on Secured Communication between nodes .

- *K. Akila Research scholar Rajah serfoji govt arts and science college, Affiliated to Bharathidasan university Tanjore, PH-9080324155. E-mail: akilasathish2012@gmail.com*
- *Co-Author name is currently pursuing masters degree program in electric power engineering in University, Country, PH-01123456789. E-mail: author_name@mail.com*

2.1 A Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment (SPPPDRM)

SPPPDRM[2] reduced Overlapping Sensing Coverage(OSC) in mobile wireless sensor networks. This work Used the mechanisms of ID based authentication and Effective sensing Coverage rate-based procedure .SPPPDRM concentrated on Mobility, Durability, Life of battery , accuracy and Data transmission among nodes. The size of Simulation area Limited to 200X200X200 and Simulator is MATLAB R2017a. The Disadvantage of this work is security not analyzed.

2.2 Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling (EFRIWSN)

EFRIWSN [3]introduced Virtual Cluster head CH for all cluster members. Virtual Cluster improved The performance of Fault Tolerance among heterogeneous networks. The cluster head failure and data transmission acknowledgement of virtual cluster head are managed by Flow Bipartite Graph(FBG). The area of Simulation environment is 100 X 100 meters. NS2 simulator is used to measure the performance of EFRIWSN. The measure of Security is the main disadvantage of this method.

2.3 Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols (AEDMLE)

AEDMLE[4] introduced new gateway selection stratagem for load balancing in static Wireless Senser \Cluster network to use IOT device as sensor nodes. This work is based on Message Queuing Telemetry Transport Protocol (MQTT). AEDMLE can be used in the Stream of Crop Field Monioring, Industrial Plant Controlling. The disadvantage of this work is Security not analyzed properly.

2.4 Leveraging the power of the crowd and offloading urban IoT networks to extend their lifetime (LPCOUIN)

LPCOUIN[5] introduced crowd and offloading patent portrayal for Load Balancing , Mobility, Energy Model. This work achieved Power Saving. LPCOUIN Provided the theoretical Concept using assumed environment of network

with 27 Sensor nodes. The disadvantage of this work is security not discussed.

2.5 IoT-WSN security schemes

Cryptography plays a vital role in network security. Encryption takes place in source node before transferring a data packet and decryption is performed by the destination node after reception of the data packet to get meaningful information from it. Encryption algorithm and key sizes are the important factors which decide the security process. There are powerful strong mathematical based encryption procedures are there which consume lot of computational resources and there are some lightweight algorithms are also available which could provide basic security with less computational demands on the go[6][7]. There are plenty of choices in selection of encryption algorithms and key sizes are available between these two extreme categories. Selecting the right cryptography based on the requirement and environment is important to decide the security scheme of a network [8]. Since IoT-WSN nodes are heterogeneous, balancing the power and security in a safer ratio is the fundamental factor in designing network security schemes. A tri-level secure scheme is proposed in the Dynamic Security Scheme Manager (DSSM) module of this work. Existing Rivest-Shamir-Adelman (RSA) cryptographic procedure and Elliptic Curve Cryptography are used along a Random Memory Shuffle (RMS) algorithm in DSSM. RSA is selected because many IoT hardware are having this procedure inbuilt. ECC is selected for its assured safety with smaller key size[9]. A new Random Memory Shuffle cryptography is introduced to match the IoT devices with limited computational resource.

Author	Work	Methodology	Advantages	Limitations
A. S. M. S. Hosen et al.	A Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment	ID based Authentication	Better Intrusion detection	Security
J. Lin et al.	Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling	Virtual Cluster head and Flow Bipartite Graph	Better Network immovability	Security
Deepsubhra Guha Roy et al.	Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols	Gateway Load balancing solution-MQTT	Lesser Communication delay	Limited to static networks, Security
GéraldineTexier et al.	Leveraging the power of the crowd and offloading urban IoT networks to extend their lifetime	Crowd sensing based offloading procedure	Network life time	Limited to Urban area, Security

3 SECURED IOT-WSN ARCHITECTURE FOR ENVIRONMENTAL MONITORING (SIAEM)

SIAEM introduces functional block to establish an IoT-WSN dedicated for Environmental Monitoring. The functional block is Dynamic Security Scheme Manager (DSSM). This block performs the tasks of Security with low power consumption.

3.3 Dynamic Security Scheme Manager (DSSM)

RSA, ECC and RMS cryptography methods are employed to work with DSSM. The computational complexity and security of these procedures are given in Table 2.

Procedure	Complexity	Security
RMS	Low	Average
RSA	Medium	Medium
ECC	High	High

Table 2: *Cryptography Complexity and Security*

RSA and ECC are well known algorithms. The RMS cryptography method is described here. Unlike accessing Sequential storage devices, cccessing Random Access Memory (RAM) in sequential or random order will not make any difference in the performance. There are many improvements happening in the hardware industry towards memory components manufacturing. The in-memory logical operations of modern memory units work like a mathematic coprocessor for the processors[10]. Mathematical coprocessor takes care of the complicated mathematical processes such as exponential calculations or handling large numbers in high precision and the processor will get results after the calculation. This method is used to improve the user experience while multitasking. Similarly, in-memory logical process enabled memory units can perform logical operations in a large scale. RMS uses a static shuffling method for the first four bytes of the data and remaining data will be shuffled dynamically. Since the RFC8163 IoT standard packet size is 1500 Bytes, the first four bytes is not a significant size to impact the security level.The first four-byte static shuffling in a way that swap(1^{st}& 4^{th}) and swap(2^{nd}&3^{rd}) is illustrated in Figure 2.

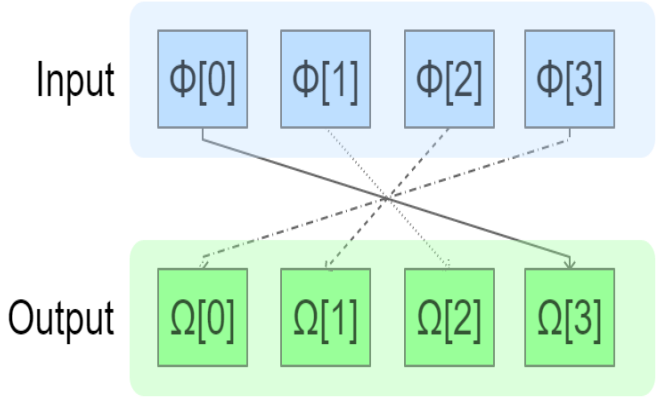

Figure 2: *First four-byte static swap*

Algorithm 4: RMS Encryption

Input: Plain Data
Output: Obfuscated data
Step 1: Let be the size of the input data
Step 2: Let [s] be the input data
Step 3: Let be the output data
Step 4: Calculate random number seed

$$\rho = \Phi[0] + \Phi[1] + \Phi[2] + \Phi[3]$$

Step 5: Assign

$$\Omega[0] \coloneqq \Phi[4],\ \Omega[1] \coloneqq \Phi[2],\ \Omega[2] \coloneqq \Phi[1], \Omega[3] \coloneqq \Phi[0]$$

as in Figure 2
M,Step 6: Generate random numbers from 4 using without redundancy and store in array
Step 7:

$$\forall i = 4 \rightarrow s: Assign\ \Omega[i] = \Phi[r[i]]$$

Step 8: Return

Since t00.alues in the destination node for decryption will not be a problem. The security scheme selects the ECC cryptography procedure for the transmission and reception nodes are from N_H category. RSA is selected when one node is of N_H type, another node is of N_I type and the value of β_x of Node $N_I x$ is below 50% of the initial value. If the communication occurs between the N_L category nodes, then RMS cryptography is assigned. The dynamic security scheme manager decides the encryption scheme in the network and the encryption algorithms are changed time-to-time based in the situation. DSSM selects the ECC procedure whenever there is a intrusion flag raised in the network to ensure the security. The intrusion flag will be reset if there is no intruder detected in the network for a while.

5. EXPERIMENTAL SETUP

OPNET Network simulator is a tool to simulate the behavior and performance of any type of network. The graphical Interface of OPNET used to design any type of legacy architecture of Network[11][12]. 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) [13]

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 al-world hours

5.1 Results and Analysis

The performance of existing SPPPDRM, EFRIWSN, AEDMLE, LPCOUIN and proposed SIAEM are measured and analyzed in this section.

5.2 Security

Security is one of the very important aspect of networking. If an intruder can penetrate into the environmental monitoring network, he can cause calamities by sending the fake values. In general, IoT-WSN nodes are to be deployed remotely, they are more prone to intruder attacks. The security measurement is performed by the inbuilt procedure of OPNET which calculates how many data packets are decoded using different network attacks. The experiment results for security is given in Table 8 and comparison graph is given in Figure 7.

Security (%)					
Nodes	SPPPDRM	EFRIWSN	AEDMLE	LPCOUIN	SIAEM
100	90	88	92	91	99
200	90	88	92	91	99
300	91	89	92	91	99
400	90	89	92	92	99
500	90	88	92	91	99
600	90	88	92	91	98
700	91	89	92	91	98
800	91	88	92	92	99
900	90	88	92	92	99
1000	91	89	93	91	99

'Table 1: *Security*

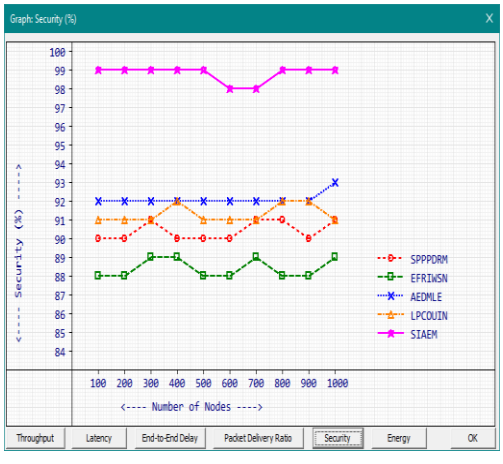

Figure1: *Security*

6. CONCLUSION

Providing security along with energy optimization is one of the challenging tasks in networking. In particular, security and energy balancing is very vital in environmental monitoring with IoT-WSN. In this work a new model is developed using the functional module Security Management. The security is properly maintained in the Projected Method SIAEM. Thus , the Projected Method is optimum solution for Environmental Monitoring for upcoming Smart city of Clean World.

7. REFERENCES:

[1] Yongyun Hu, Han Huang and Chen Zhou, "Widening and weakening of the Hadley circulation under global warming" in Science Bulletin Volume 63 Issue 10, Elsevier 2018, Pages: 640-644

[2] S. M. S. Hosen, S. Singh, V. Mariappan, M. Kaur and G. H. Cho, "A Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment," in IEEE Access vol. 7, IEEE 2019, Pages: 39702-39716

[3] J. Lin, P. R. Chelliah, M. Hsu and J. Hou, "Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling," in IEEE Access vol. 7, IEEE 2019, Pages: 14022-14034

[4] Deepsubhra Guha Roy, Bipasha Mahato, Debashis De and Rajkumar Buyya, "Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT) — MQTT-SN protocols" in Future Generation Computer Systems Volume 89, Elsevier 2018, Pages: 300-316

[5] GéraldineTexier and Valérie Issarny, "Leveraging the Power of the Crowd and Offloading Urban IoT Networks to Extend their Lifetime" in IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), IEEE 2018, Pages: 104-109

[6] S. W. Pritchard, G. P. Hancke and A. M. Abu-Mahfouz, "Cryptography Methods for Software-Defined Wireless Sensor Networks," 2018 IEEE 27th International Symposium on Industrial Electronics (ISIE), IEEE 2018, Pages: 1257-1262

[7] Pagán Alexander, Jr., Rania Baashirah and AbdelshakourAbuzneid, "Comparison and Feasibility of Various RFID Authentication Methods Using ECC" in Sesors - 2018, Pages: 1-17

[8] R. B. Gandara, G. Wang and D. N. Utama, "Hybrid Cryptography on Wireless Sensor Network: A Systematic Literature Review," International Conference on Information Management and Technology (ICIMTech), IEEE 2018, Pages: 241-245

[9] Manuel Suárez-Albela, Paula Fraga-Lamas and Tiago M. Fernández-Caramés, "A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices" in Sensors Volume 18 Issue 11, MDPI 2018, Pages: 1-26

[10] A. Agrawal, A. Jaiswal, C. Lee and K. Roy, "X-SRAM: Enabling In-Memory Boolean Computations in CMOS Static Random Access Memories," in IEEE Transactions on Circuits and Systems I: Regular Papers Volume 65 Issue 12, IEEE 2018, Pages 4219-4232

[11] Zheng Lu and Hongji Yang, "Unlocking the Power of OPNET Modeler" in Cambridge University PressMaryam 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 – 287David Basin, Cas CremersandCatherine Meadows, "Model Checking Security Protocols" in Handbook of Model Checking, Springer 2018, Pages: 727-762