Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks

Dr. N. Bhalaji, Associate Professor,
Department of Information Technology,
SSN College of Engineering,
Old Mahabalipuram Rd, Kalavakkam,
Tamil Nadu - 603110.
Email id: bhalajin@ssn.edu.in

Abstract: The revolution caused by the communication without wires has brought in multitudes of basic modifications in the data network and the telecommunication, making the integrated networks a reality. The further advancements in the wireless communication has enabled to set personal networks using the portable devices, and are termed as the adhoc networks. The networks formed under specific circumstances or a reason could follow any one of the topology to convey the information. W ireless mesh network is the form of such network mentioned above that organized in a mesh topology. This network formed in mesh topology contains several consumers who are arranged in the distributed manner and forward the packets in a one or more than one hop model. The protocols that help in sorting out the path for sending and receiving the information are has a vital influence over the network in mesh topology as they affect the throughput, life of established links etc. Integrating the wireless mesh topology to the internet of things has improved the way of information sharing by linking multitudes tangible things around. The mesh topology wireless networks formed using the portable devices or other –wise called as the mobile networks that are connected over internet are open to security breaches as the mesh holds few nodes that are malicious. This makes the information conveyed to be either compromised or manipulated. The article in order to ensure the reliability in the transmission of the data with the heightened confidentiality and integrity in the IOT empowered mobile networks proposes a routing strategy that is robust across the consumers in mesh, the gateway and the routers. The channels across the devices in the mesh are formed based on the efficiency of the connections for the distribution of the data. The simulation process of the proposed work using the network simulator 2 shows the performance improvement of the proposed work with respect to throughput of the network, packet loss rate, packet delivery rate, latency, energy efficiency and the computational overhead.

Keywords: Mobile Network, Iot, Adhoc Network, Wireless Mesh Network, Reliability Confidentiality and Integrity

1. Introduction

Wireless network technology has caused a serious growth of various network domains in the last two decades. It connects a large number of wireless nodes, using wireless connections to collect and transfer information to endpoints. Intermediary nodal points that are subsequent hop used as data forwarders and

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

are distributed in a multi-hop mannequin. Users may obtain the necessary information over the Internet through servers. Mesh networks that wireless are also known as wireless ad-hoc networks. It comprises a large number of mesh customers, gate way and routes systems to influence a wide region for information collecting and transmission. In the basic structure of the wireless network shown in the figure.1 every nodal point participates in the communication by initiating the transmission or being the destination point or the intermediary nodal that receive and forward the information. According network deployment the routing scheme is classified as the static and dynamic. The nodes in the deployed in the network if fixed to the same position it is static, in case of dynamic the nodal position changes even after the distribution of the node is completed and the network is set up this set up is called the mobile network. Though the mobile nodes provide an improved coverage than the nodes that are static, the selection of routes are very tedious and challenging.

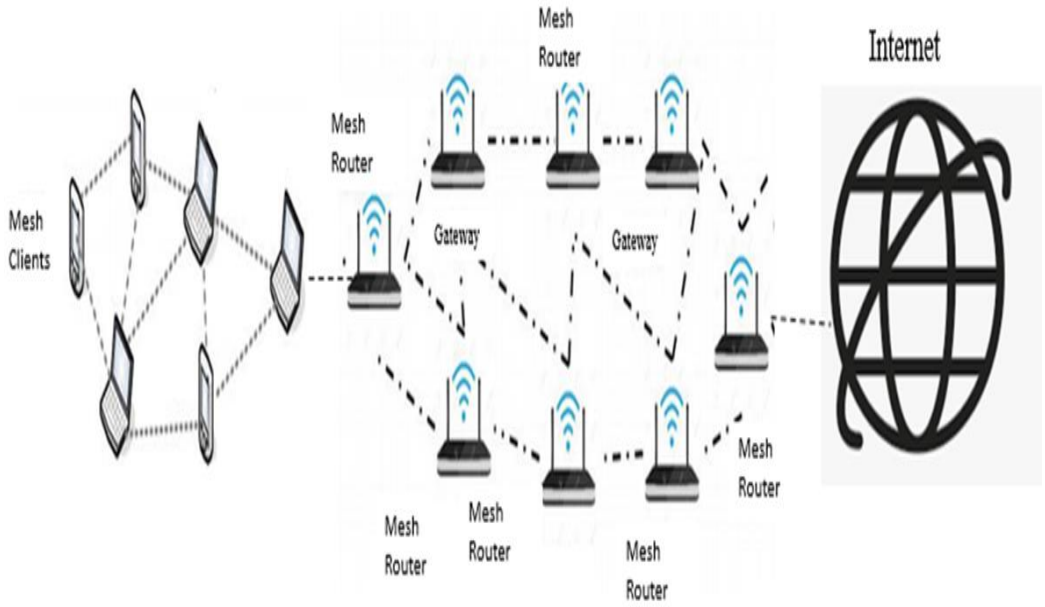

Figure.1 Basic Mesh Architecture,

“The Internet of Things (IoT) architecture links all communication devices, i.e. static or mobile, for monitoring the environment and contributes to the creation of conventional devices in various network fields IoT does not connect. The IoT enables not only the computing devices but also allows the physical objects such as the fans, electrical appliances, watches cars and other smart devices to be connected. Moreover, because of the sudden changing attributes of wireless mesh networks, they have a significant

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

impact on IoT-based applications, especially network adaptability and network coverage with improved connectivity".

Today, "various applications such as smart cities, smart health and smart farming are integrated mesh customers with data collection IoT devices that are transmitted to the central station. The key advantage of using wireless mesh networks is to connect or uninstall an existing IoT-based network mesh client without disrupting the rest of the mesh clients. Therefore, most applications developed with the integration of wireless mesh clients and IoT devices are heterogeneous for algorithms, coverage, efficiency of delivery, etc. Wireless mesh networks deliver the structures of customary ad-hoc wireless and mobile networks. Therefore, in both industrial and academic fields etc., wireless mesh network is becoming more prominent. The clients of the mesh are randomly distributed and disconnect itself from the network due to its mobile nature. However, handling data transmission through the routing chains is one of the most important research problems in mobile mesh connected wireless devices. In addition, wireless mesh offers their functionalities in an open architecture, and malicious nodes can be used as data forwarding mesh routers. Resulting in several cases reported with the denial of service this in turn compromises and interrupts the communication taking place in the network. So the paper lays out a protocol to ensure the reliability in the transmission of the data with the heightened confidentiality and integrity in the IOT empowered mobile networks proposes a routing strategy that is robust across the consumers in mesh, the gateway and the routers". The contribution of the proposed work is listed below

- The proposed strategy, develops a reliable routing across the devices, routers and the gateways in the mesh.
- Minimizes the probability in the transmission of replicated data packets, enhances the communication overhead.
- Evaluates the performance of the link established to enhance the throughput and connectivity
- Lays out a trustworthy one more hob based data transmission to enhance the security level of the data using the Asymmetric encryption and decryption based on the Paillier cryptosystem.

The paper with the protocols for reliable data transmission and the heightened confidentiality and integrity is planned with the related works in the segment 2 and proposed reliable routing strategy with the confidentiality and integrity in segment 3 Results Analysis in segment 4 and conclusion in segment 5.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

2. Related works

Smys, S. et al [1] in order to allow simultaneous transmission of huge number data packets, the author has devised an secure strategy of routing with energy efficiency for the wireless sensors engaged in the application that produce a heavy data flow. Praveena, A., et al [2] proposed the "Efficient cryptographic approach for data security in wireless sensor networks using MES VU."

Anguraj, et al [3] proffered a "Trust-based intrusion detection and clustering approach for wireless body area networks." Kumar, R. et al [4] explains the "A novel report on architecture, protocols and applications in Internet of Things (IoT)." Anand, J. V et al [5] has proposed the “Design and Development of Secure and Sustainable Software Defined Networks” Neelaveni, R. et al [6] designed a “Security Assistance for VANET Using Cloud Computing and evaluated its performance”

Mugunthan, S. R. et al [7] in his paper has performed the procedure of “Security and Privacy Preserving of Sensor Data Localization Based on Internet of Things." Sridhar, S., et al [8] devised an “intelligent security framework for iot devices cryptography based end-to-end security architecture." Bhalaji, N. et al [9] conducted an "Efficient and Secure Data Utilization in Mobile Edge Computing by Data Replication."

Rahimunnisa, K. et al [10] performed the “Hybridized Genetic-Simulated Annealing Algorithm for Performance Optimization in Wireless Adhoc Network." Shakya, Subarna et al [11] proposed the "Intelligent and Adaptive Multi-Objective Optimization in WANET Using Bio Inspired Algorithms." O’Keeffe, et al [12] elaborates the The Paillier cryptosystem." and the Das, Angsuman has put forth the "An efficient IND-CCA2 secure Paillier-based cryptosystem."

3. Proposed Work

The proposed scheme scopes in designing and developing an effective and reliable routing for the mesh wireless mobile networks. Initially the structure of the network using the mesh topology is formed and the path to transmit the information securely is identified. Since the routing is done in a proactive way. The information of the each device and its nearby device within a least distance is saved in the information table created by each device in the mesh. Every device in the network is linked in the one or more hop model as shown in figure.1. The flow chart in figure .2 provides the network formation of the mobile device in the mesh topology.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

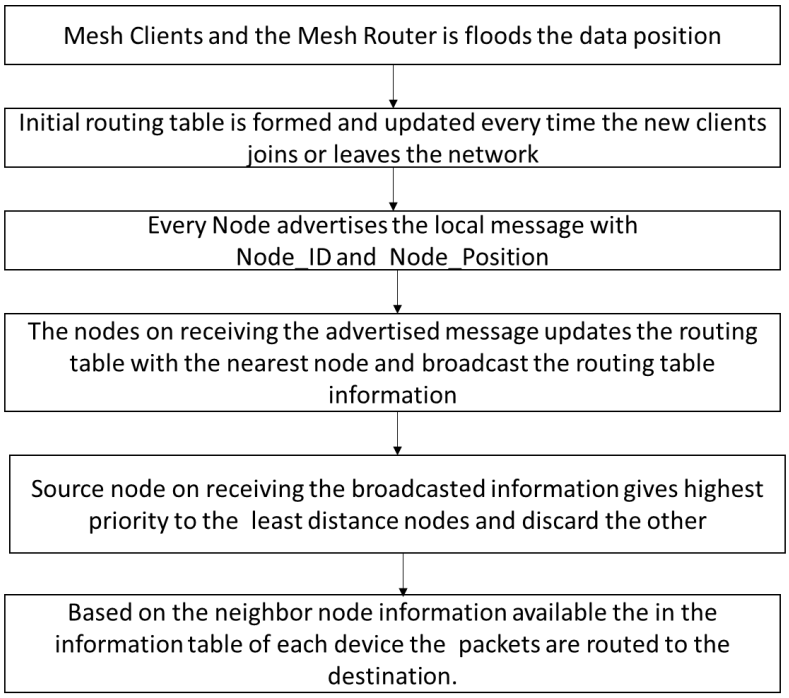

Figure .2 Flow chart of Network Formation

The current position of every node is calculated by estimating the displacement of the node form its initial position using the Euclidean Distance.

$$dispalce\ ment\ (X,Y) = \sqrt{(XI - XF)^2 + (YI - YF)^2} \quad (1)$$

To ensure the reliability in transmission the proposed method utilizes the Paillier cryptography [12] [13], to improve the data dissemination. The secret key in the Paillier is generated as shown in the flowchart in figure.3

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

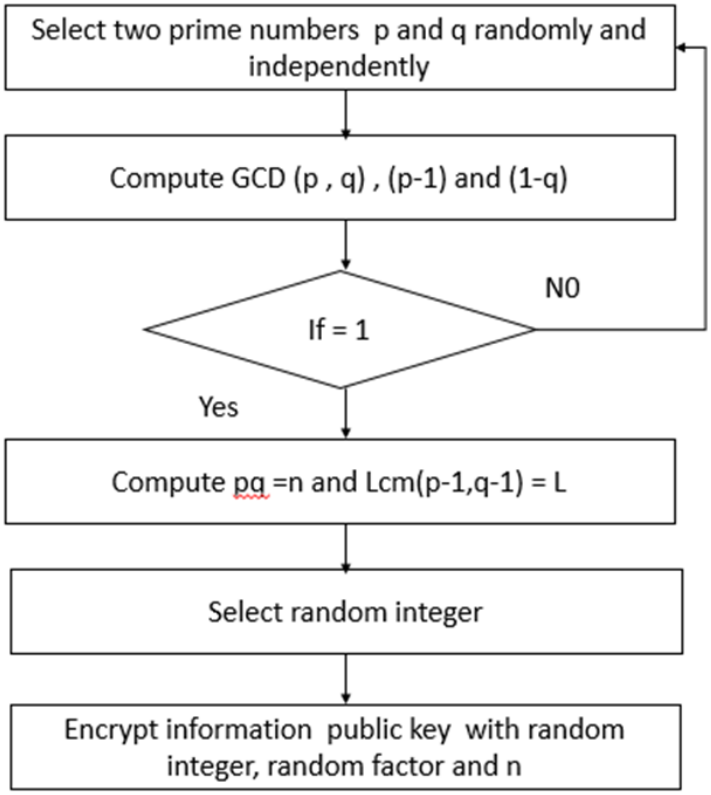

Figure.3 Paillier Cryptosystem

The decryption is done using the private key, the key is included with the each data packets from the source to destination and the authenticated destination has the secret private key to unveil the information in the packets. The equation.2 below shows the decrypted the message from the encrypted

$$plain\ text\ = \frac{ciphertext}{random\ integer^{l}\ mod\ n^{2}}\ mod\ n \qquad (2)$$

The proposed protocol with the reliable data transmission and heightened confidentiality and integrity is as shown below in figure.4

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

Input : Routing Information Table
Output : Secure Routing
For every mesh device
Enumerate displacement using equation 1
Evaluate its packet drop ratio with ($\frac{number\ of\ packets\ received}{number\ of\ packets\ transmitted}$
Deter mine the cost of connectivity with ($1 -$
$packet\ Drop\ Ratio$)
Select mesh device with
$minimum\ (packet\ drop\ ratio\ and\ cost\ of\ connectivity\ )$
Update routing table
End for
For every router of the
Deter mine the least distance and cost path to the gateway
update routing table
End for
Share public private key to routers
Attach key to the every encrypted message from source
Use private key to decrypt the message
Incoming messages are authenticated by the gateway

Figure.4 Proposed Reliable Data Transmission

4. Results Evaluation

The protocol developed is simulated using the network simulator-2 in an observation area of 1000m x1000m, the mesh devices are randomly deployed over the area. The protocol is evaluated with 100 to 400 of device connected in mesh, the network also holds 1 to 10 malicious nodes, with the packet size of 1024 bits and key size of 256 bits. The experiment is done with the transmission range fixed to be 25m and the simulation time is seta s 2500seconds. The proposed method is evaluated on the terms of throughput, packet loss rate, packet delivery rate, delay in transmission, energy efficiency.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

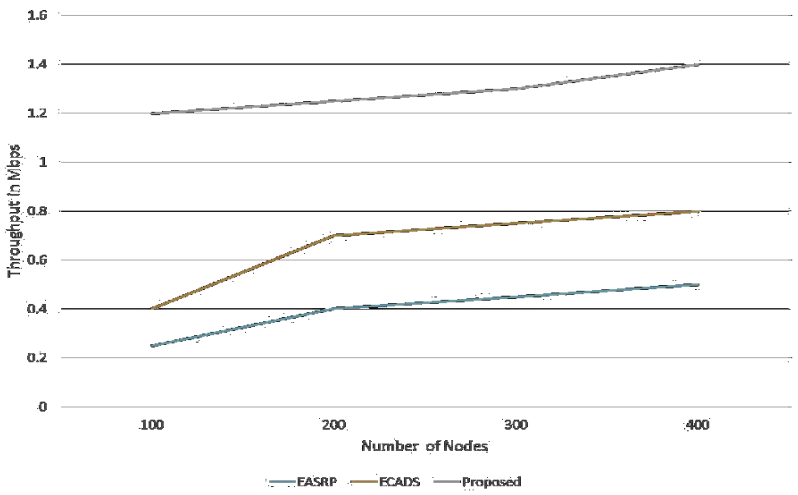

Figure.5 Throughput

The examined throughput of the proposed work is based on the number of information received for the number of information transmitted by the sender without any loss. The evaluation results shows that the throughput of the work done in the paper is reasonable and as expected compared to the other methods such as the EASRP [1] and the ECADS [2] , the cryptograph used ensures the protection of the data from any losses and the reduced communication overhead.

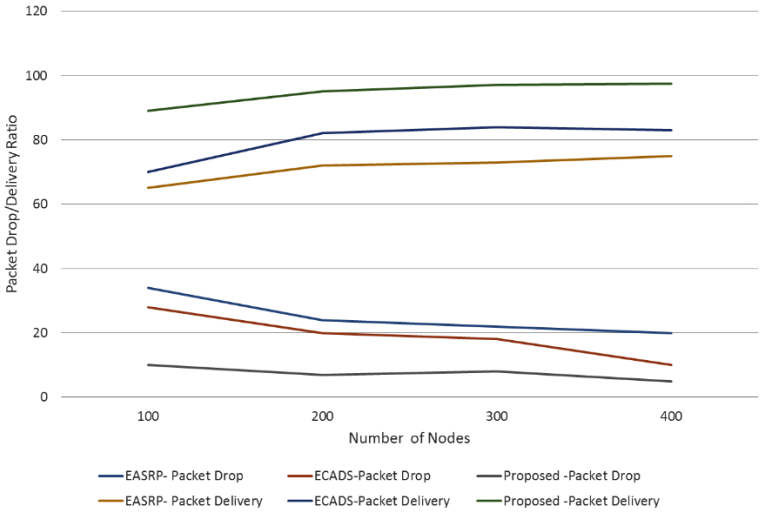

Figure.6 Packet Drop and Delivery Ratio

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

Both the packet delivery and the drop or estimated by enumerating the number of packets delivered successfully for the number of packets transmitted. The evaluation results of the same is depicted in figure .6 the comparison with the EASRP and the ECADS shows the proposed has a lesser drop ratio and higher delivery ratio than the ESARP and the ECADS.

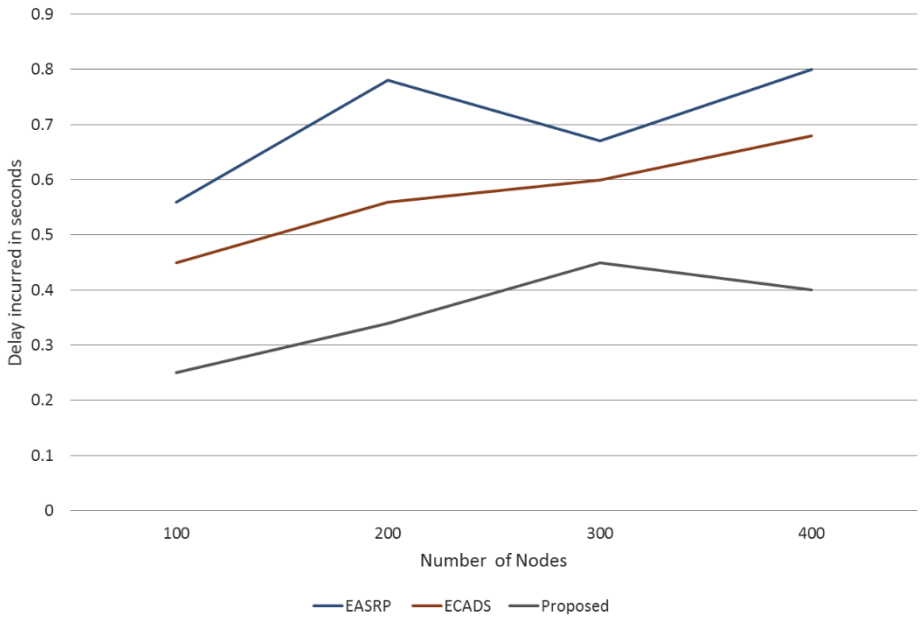

Figure.7 Delay Incurred

The difference obtained in the time of transmission and the time of reception is termed as the delay, the process includes, the time in network formation, in devising the route, in encrypting etc. in the transmitter side and the time taken to reach the destination, and decrypt in the receiver side. The delay in the data transmission is reduced to a certain limit as shown in figure.7 as the least distance, devices and the routers are sorted out to send the information to the gateway.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

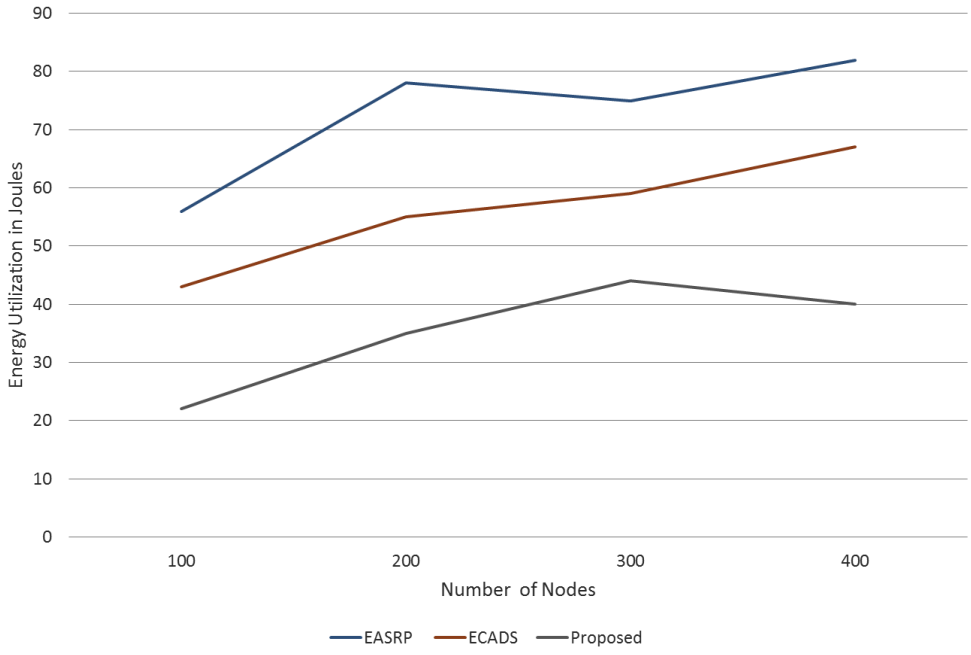

Figure.8 Energy Efficiency

The energy utilization of the complete network while transmitting is evaluated, and depicted as shown in figure.8 as the energy depends on the distance and the efficiency of the link the energy utilization of the proposed work is moderate compared to the prevailing method EASRP and the ECADS. Each device in the mesh is assigned with the initial energy of 2 Joules.

5. Conclusion

To establish a reliable data transmission in the mobile networks organized in the mesh topology, the paper utilizes the Paillier cryptosystem that uses both the public and the private key for the encryption and the decryption respectively. The path between the devices, router and the gateway are established in a proactive way enumerating the link efficiency and the distance between the nodes. The method is simulated using the NS-2 with respect to the throughput, energy efficiency, packet drop and delivery rate and the delay incurred. The simulation results proved the proficiency of the proposed more over the other state of art methods such as the EASRP and the ECADS.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

References

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

[2] 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.

[3] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." Wireless Personal Communications 104, no. 1 (2019): 1-20.

[4] Kumar, R. Praveen, and S. Smys. "A novel report on architecture, protocols and applications in Internet of Things (IoT)." In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 1156-1161. IEEE, 2018.

[5] Anand, J. V. "Design and Development of Secure and Sustainable Software Defined Networks." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 1, no. 02 (2019): 110-120.

[6] Mugunthan, S. R. "Security and Privacy Preserving Of Sensor Data Localization Based On Internet of Things." Journal of ISMAC 1, no. 02 (2019): 81-91.

[7] Neelaveni, R. "Performance Enhancement and Security Assistance for VANET Using Cloud Computing." Journal of trends in Computer Science and Smart technology (TCSST) 1, no. 01 (2019): 39-50.

[8] Sridhar, S., and S. Smys. "Intelligent security framework for iot devices cryptography based end-to-end security architecture." In 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1-5. IEEE, 2017.

[9] Bhalaji, N. "Efficient and Secure Data Utilization in Mobile Edge Computing by Data Replication." Journal of ISMAC 2, no. 01 (2020): 1-12.

[10] Rahimunnisa, K. "Hybridized Genetic-Simulated Annealing Algorithm for Performance Optimization in Wireless Adhoc Network." Journal of Soft Computing Paradigm (JSCP) 1, no. 01 (2019): 1-13.

[11] Shakya, Subarna, and Lalitpur Nepal Pulchowk. "Intelligent and Adaptive Multi-Objective Optimization in WANET Using Bio Inspired Algorithms." *Journal of Soft Computing Paradigm (JSCP)* 2, no. 01 (2020): 13-23.

[12] O'Keeffe, Michael. "The Paillier cryptosystem." A Look into the Cryptosystem and Its Potential Application, college of New Jersey (2008).

[13] Das, Angsuman, and Avishek Adhikari. "An efficient IND-CCA2 secure Paillier-based cryptosystem." Information Processing Letters 112, no. 22 (2012): 885-888.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 106-117
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.004

Biography: Dr. N. Bhalaji,has more than 15 years of teaching experience. He received his B.E. & M.E. degree both in the discipline of Computer Science and Engineering and Ph.D. specializing in Trust Based Routing approach for MANETs from Anna University, Chennai. His current research interests include Application of Trust over information and communication domains namely Internet of Things and Blockchain Technologies. He is also a recognised supervisor of Anna University. He is also serving as a Doctoral Committee member for VIT, SRM and Satyabhama University and as a member of the board of studies in SRM Valliammai Engineering College and Vels University, Chennai**.**

ISSN: 2582-1369 (online)