ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2024.1631.148

ENERGY EFFICIENT ROUTING PROTOCOL FOR SECURITY ANALYSIS SCHEME USING HOMOMORPHIC ENCRYPTION

S. Pragadeswaran[1*], N. Subha[2], S. Varunika[3], P. Moulishwar[4], R. Sanjay[5], P. Karthikeyan[6], R. Aakash[7], E. Vaasavathathaii[8]

[1]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: praga1994@gmail.com, orcid: https://orcid.org/0009-0009-0987-3039*
[2]Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem, India. e-mail: asn.subha@gmail.com, orcid: https://orcid.org/0009-0008-9185-8235
[3]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: varunikasivakumar@gmail.com, orcid: https://orcid.org/0009-0006-5234-4114
[4]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: moulipalanivel07@gmail.com, orcid: https://orcid.org/0009-0007-0018-5964
[5]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: sanjayramesh9597@gmail.com, orcid: https://orcid.org/0009-0003-3787-3980
[6]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: karthikpandiyan12345@gmail.com, orcid: https://orcid.org/0009-0007-3216-3807
[7]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: aakashvishwa12@gmail.com, orcid: https://orcid.org/0009-0009-5264-2316
[8]Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore, India. e-mail: vaasavi2508@gmail.com, orcid: https://orcid.org/0009-0000-2037-3478

SUMMARY

Wireless Sensor Networks (WSNs) have gained widespread interest as a result of developments in IT technology and the electronics industry. This ground-breaking sensing technology consists of multiple sensor nodes or motes that are placed in an atmosphere to detect constantly changing physical phenomena. These compact sensor nodes gather and interpret data via radio waves. The tiny size of these sensors is advantageous since they may be readily incorporated into any system or system. This capability has prompted the adoption of WSNs, particularly for form monitoring and tracking; most notably, monitoring apps. However, this small scale of sensor nodes limits the capacity of resources. Usually, the WSNs are installed in environments of unsafe or difficult human interference. Critical decisions in emergency applications can require sensible knowledge. It is necessary to check the network security. To extend the network security using Homomorphic Encryption effectively, the available resources must be expanded to a full view. This refers to the development of energy-efficient routing protocol strategies to ensure low energy consumption of common routing protocols and improve the availability and security of WSNs. Homomorphic encryption is effective in improving the security of wireless sensor networks.

Key words: *homomorphism encryption, wireless sensor networks, cooperative routing protocols, energy efficient routing protocols.*

Received: July 15, 2024; Revised: August 28, 2024; Accepted: September 18, 2024; Published: October 30, 2024

INTRODUCTION

Far networks that incorporate multi-bounce systems is probably incontestable as transferring parcels from one hub to another hub. The hub that is transferring bundles will move approximately as transfer yet as host to get the parcels. The hubs inside the anticipated paintings are sorted out to misuse the little sensors, which are located abuse the sector Positioning machine (GPS). The sensors that go approximately as a hub need constrained force for interfacing and procedure [13]. By dynamical the potential utilizations of grouped hubs, the cutting-edge impromptu system secures tremendous collaboration [10]. The important thing burden inside the impromptu device is that each sparing difficulty upheld the concocting and site of supply yet as sink hubs. Energy is that the major doesn't forget the systems administration approach any vicinity the battery goes about as a stock of the model. The ascent within the pressure happens due to the capacity use of absolutely numerous materials of the gadget. In this manner, it is crucial to create electricity decrease plans for one-of-a-kind structures administration layers. Shifted elements are contemplated to build up the steering conference like topology the board, and the directing layer. Steering conventions are arranged with advancing costs at the picked publications. The portions of bounces taken via a parcel to be successful in its intention begin to finish postponement or vitality utilization is infrequently any examples of fee use. As gadget length develops the depth of guidance conference is some other fundamental consideration considering a directing convention for extemporaneous and identifier structures. A reasonable steering convention needs to be adaptable and change as the topology does.

LITERATURE SURVEY

The trouble of circulated disavowal of management assaults isn't new in the writing. Be that as it may, every uncovered examination of this type of attack is to a few degree completely sudden. The study's motivation, which is the abandoning of control attacks based on the Open Systems Interconnect or Transmission Control Protocol / Internet Protocol reference models, is examined by certain writers [1-2][25]. providing a lot more thorough scientific classification of DDoS attacks [4][5][7][26]. While some attempt to use incidental demonstration devices to learn about the appropriated disavowal of administration [8–9] [11] [27], others rely on popular and relief structures [12] [14-15] [28]. Although the literature on DDoS is extensive, some authors consider traditional demonstrations of DDoS assaults in remote sensing systems [15] [17-21] [29]. In [15], In order to prevent DDoS attacks, the authors create an ally in nursing algorithmic notion for a combined crypto logical tool and package deal technique [22]. Given that the topic is discussed at some point in a manner related to our advancements, it satisfies the requirements for analytical representation. The ability to use organized chaos in multiple scenarios is not discussed in the paper by experts, so it would no longer meet the requirement for simplification. In their study, researchers validate execution impacts (overall performance evaluation), establishing parallels to energy studies [6]. Their method is flexible, adaptable, and conventional, but it is also less multidimensional (it would no longer include the financial or environmental motivations for reading and would only consider a confined set of gadget features) [20]. By creating a DDoS assault value model that reinforced scientific conditions, the designers of [18] answered problems concerning analytical demarcation and consistency. They examine conventional performance evaluation and introduce re-enactment effects; nonetheless, they will not be releasing even the smallest person about energy examination [16]. The arranged strategy, which is based on numerical effects (universality), will be skipped in a generally advantageous way (it may be a jail in any kind of gadget). Although the model requires a great deal of computation, it is extremely determined. Even though it includes geographic assessment, the analysis presented in [19] considers only a certain set of factors that have been evaluated. The version's numerical definition makes it flexible. Researchers organized a legitimate approach [19] for demonstrating real DDoS assaults against distant systems when it comes to official DDoS displaying methods, with the exception that the version is frequently used to find conference flaws [24]. Their approach is based on formal analysis and representation (Analytical instance). Although the technique is flexible, it is quite rigid because of its precision and formalism. The designers give the well-worth

model and consider performance analysis, but they omit energy analysis [3]. Similar to the internal case of previously cited works, geographic evaluation is also disrupted. The ease with which ASF may be used to handle improvements (Scalability) and boundary alterations inside the current version (Flexibility) is astounding. While geographic analysis identification [23] will outperform residual techniques, it won't fully address the strain that a true preparedness environment should demand.

Table 1. Summary of literature survey

Ref	Focus of the Study	Methodology	Key Contributions	Limitations
[1-3]	OSI/TCP-IP Control Attacks	Analytical / Classification	Classification of control attacks	Not specified
[4-7]	Comprehensive DDoS Classification	Classification Framework	Detailed DDoS attack taxonomy	Focused on classification only
[8-11]	Learning via Demonstration Tools	Simulation / Emulation	Insights into DDoS behaviors	Limited scope of tools
[12-15]	Prevention and Mitigation Frameworks	Prevention Frameworks	Strategies for DDoS mitigation	Generalized strategies
[18]	Analytical Demarcation & Consistency	Analytical Modeling	DDoS attack value model	No energy analysis
[19]	Formal Analysis of DDoS Attacks	Formal Analysis & Representation	Demonstration of real DDoS scenarios	No energy analysis, rigid methodology
[20]	Performance Evaluation	Performance Evaluation	Comparative performance insights	Limited scope, no energy analysis
[23]	Geographic Analysis Identification	Geographic Analysis	Improved geographic analysis	Incomplete preparedness environment
[24]	Scalability and Flexibility in DDoS Models	Scalability & Flexibility Analysis	Insights into ASF scalability	No comprehensive solution

The above table 1 shows the literature review that includes a variety of studies on OSI/TCP-IP control attacks, DDoS attack classification, learning tools, and mitigation strategies. Key contributions include classification frameworks, detailed taxonomies, insights into DDoS behaviours, and prevention strategies. Some studies investigate the geographic distribution, scalability, and performance of DDoS attacks. However, limitations are identified, including a focus on classification, narrow tool scopes, generalized strategies, a lack of energy analysis, and incomplete preparedness environments. These gaps highlight the need for more comprehensive and practical DDoS mitigation solutions.

ROUTING PROTOCOLS

The configuration of directing conventions has gained traction in extensive analyses conducted in the last ten years. The effects include a variety of methods that arrange the use of actual requirements as an event in proactive as opposed to reactive procedures, in hyperlink/course domain convention as an alternative to jumping with the aid of bounce directed. The IETF is truly in the process of institutionalizing the RPL convention [19], which creates Directed Acyclic Graphs based on a probability steering measure that might be a hyperlink-realm convention. This is because the value of sensing element hubs has increased in recent years, resulting in emotional development in their world. However, efforts have been made to eliminate Tolerant Networking, in which network commitment to writing is also necessary to increase responsibility at the price of repeated parcel transmissions, and greater stability is the goal of linked directional norms for place-off-open-minded bundles. Given the importance of region-specific information accessibility, one must guarantee that the geographic direction loses unusual energy in this context. In any event, this isn't normal, since the result is true.

- A Wi-Fi wireless reasonably comes the convey of regional insights. Once this information is assembled and well-kept it alright could also be abused for guiding capacities as pleasantly.
- District-based steering conventions that, as will be found in a while, prevent the need for earth science capability information from being supplied.
- It outperforms specific wireless conventions, yet aptitude and adaptability have to be strengthened. The many needs include spot reality insurance, association management for coordination, Vehicle-to-vehicle data, and Wi-Fi wireless following bundles used in trade choices and police investigations, respectively. The ICT financial framework places a lot of emphasis on these developments, but it is important to remember that they also need to be seen as serious

endeavors, human beings in appropriate roles, and the financial situation in developing countries that is abundant and wireless—if not transportation at least for the time being.

GEOGRAPHIC ROUTING PROTOCOLS

Understand the Unsettled Routing collection of concepts for element sensing systems. WiFi as presented by Karp and Kung (2000), appears to be the most severe reported land directional convention. Wi-Fi's usage of earth science directions appears to select routes that are lighter and less complicated than the Dynamic Stock Routing standard (DSR). Furthermore, it decreases directional overhead by 30% in compliance with the DSR criterion when hubs flow at a maximum speed of 20 m/s due to limited associations. Furthermore, it has been thoroughly tested to provide the Wi-Fi finished output, and the large, appropriately sized Hubs can shoot over 100, proving the potential of geographic steering. The rules are organized using two methods for causation bundles: border causation and unquenchable sending. The stock hub provides the bundle to the partners who are nearest to the escape site (and farthest from the stockpile hub) in a sequence of events known as eager causation; this is the local Wi-Fi need for the subsequent jump.

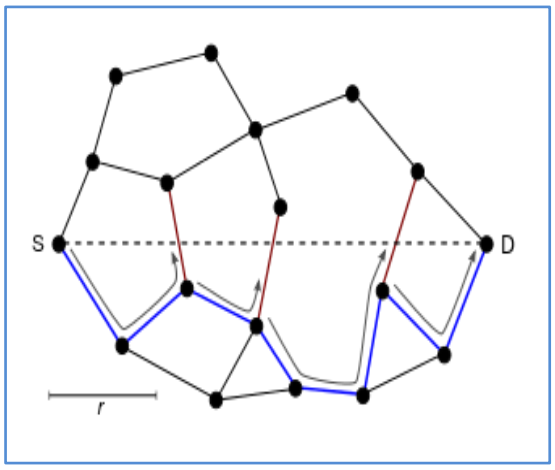

Figure 1. Geographical routing

In figure 1, this implies that every node has to fully understand the addresses and coordinates of its close buddies; hence, routing table measurements are dependent on community density as well as the node's radio diversity rather than the community's overall size. Peripheral forwarding is used to traverse voids that may exist between a node and its destination when grasping forwarding is not always available and the packet has not arrived at its intended destination. This is consistently completed and supports the proactive planate graph computation. We are not interested in the algorithmic software program's data; that is determined in the same work.

FLOOD

Based mostly on the analysis of Denial-of-Service assaults in this part, we will attempt to explain a well-known DDoS attack method in which an accomplice in stealth floods a centrally located important resource with packets. If we feel compelled to conduct a DDoS attack, we will likely provide an example specification along with the necessary conditions. The goal is to disrupt the supply of a sink, hence rendering it unusable. Similarly, we frequently provide and transmit highly detailed structured environments, complete with hundreds of aphoristic instances of utilized devices, routing, media, specs, and topologies. A major concern for security experts is the allocation of denial of issuer flooding attacks. Typically, these are outright attempts to prevent legal motes from reaching a sink node. Attackers often profit from having a vast array of sensing element devices by taking advantage of their flaws to assemble strike armies. A coordinated, massive attack against one or more portals will be launched by the culprit as soon as an assailant military figure is located. Many unauthorized users are directed toward a target sink by a distributed denial of service attack that uses flooding. This causes the tool to ultimately run out of belongings and lose its capacity to deliver normal services as a consequence of dominating

enormous amounts of its property to keep an excessively vast list. A flood-based DDoS attacker should control a sizable number of nodes that are able to be taught to make distinct requests to the target sink for a predetermined amount of time and in perfect synchronization. In figure 2 displays the Attacking geographic routing services.

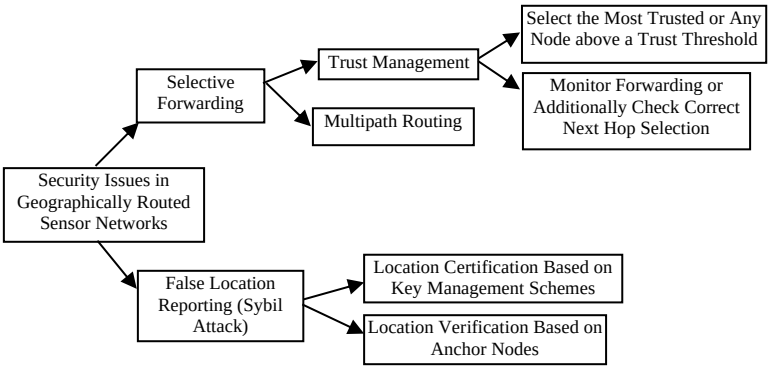

Figure 2. Attacking geographic routing services

An The hacker utilizes compromised sensors, sometimes referred to as "bots." The attacker has the whole range of requests/second to push the sink's procedural capabilities to the absolute limit, compelling it to cease responding to real sensors, once a cause is removed from the destructive hub. At that time, the bots may carry out the supplied instructions. This type of attack does not always require the existence of defenselessness, as long as there are no real weaknesses that the attack could exploit. However, fighting a big "armed army" of bots generally involves exploiting weaknesses. To offer a more complete explanation of how we handle DDoS attack investigation, we frequently want to describe it in a series of major topics, which we may gracefully elaborate on in the following parts. The gadget described in [23] is an example of a shaky device to an accomplice degree because it decodes packages that are transiting the device and does not guarantee any safety features. Because of defensive patterns on the machine's presentation, as well as time and power incentives in the backdrop of the test, we may, in this instance, look past judgment stylishly. We normally supply two conventions that ensure two remarkably high degrees of protection: security (instead of utilizing the notorious AES to skew the statistics) and lack of protection (by doing away with the inscription). Sensors start working in the no safety degree conference and send the estimated results—the quickening records—to the sink hub for further examination. No security developments are necessary at this conference level in an unspecified future period. The health stage convention provides faster statistics privately. Even as the data flows, sensors emboss it with a pre-configured key. The AES rule with a key length suitable for a 128-piece memory unit will be used for encoding in the CTR mode during this conference (CTR stands for counter and refers to a technique of activity that employs a rectangle to engrave messages of exceptional length in a way that is secret or legitimate).

RESULTS AND DISCUSSIONS

The following environmental setup makes up the work that has been implemented. MATLAB software has been used to implement the suggested routing scheme. Both the location detection of the sink nodes and different node allocations were used in the geographic analysis. Different scenarios were considered to identify the system's DDOS attack. Numerous topologies, including network design and topology as well as security measures, were taken into account. The routing protocol calculates the energy consumption with different simulation times. There are n source nodes and the fewest number of sink nodes in the scenarios that are considered. The energy used for transmission and packets that fail to deliver during routing were the subjects of the performance analysis. Figure 3 illustrates how source and sink nodes are used for geographic routing. Both the transmission traffic and the reception process can be used to identify the DDOS assault. The flood wave and the sink node's time can be used to characterize the attack. The sink node is used to implement the security mechanism. When considering the results obtained for scenarios involving package encoding it is evident that the quantity of negotiated devices has a crucial influence on the likelihood of a DDoS attack succeeding. This relationship represents the effects of each flood wave's portion of conceived bundles. The frequency of DDoS attacks

increases with the number of devices the offender managing. Here, fifty swapped-out sensors overflow the sink with meaningless signals. There are any hypothetical packages containing decrypted visitors. In any event, the sink begins dropping packages in the sixth flood wave as soon as it detects that the guests are disorganized. Network activity can continue until the second flood wave for encoded traffic or the fifth flood wave for decoded traffic with 75 percent of bargained sensors. A propagating disavowal of administration can be included in the 0.33 and second flood waves (decoded and encoded traffic, respectively) if the number of managed bits reaches 100. The offender, Global Health Initiative, has the largest number of bits (one hundred and fifty) under his control and is the first weapon to successfully spread over the whole network. This will lead to bearer rejection and completely overwhelm the network. Similarly, the quantity of devices traded off will affect the sink's supplier time. Test knowledge is limited to initial flood waves in each case. For every perplexed and decoded site visitor, one will examine how long it takes the sink to react to incoming requests and how many bits are under control of the guilty party.

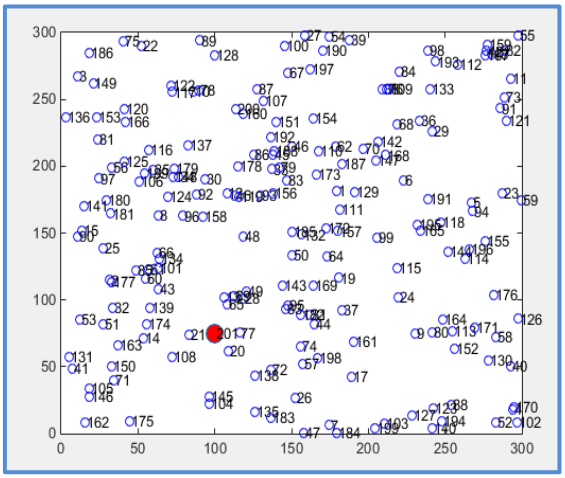

Figure 3. The snapshot of Sink node arrangement

Figure 3 shows the Analysis of the network's sink nodes' (base stations or data aggregators) location and actions. This covers their positioning, their movements (if any), and their interactions with other nodes in the network.

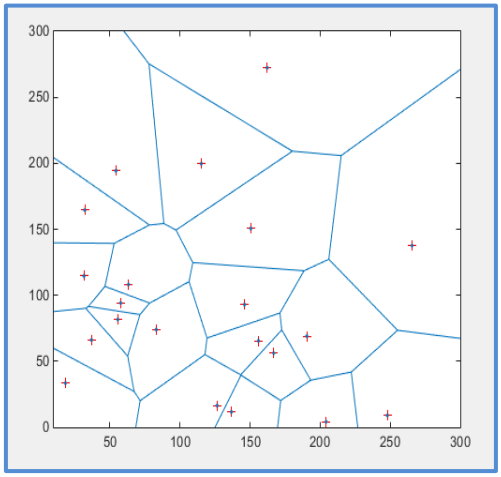

Figure 4. The snapshot of Data Packets movements

Record and examine the routes that data packets follow across the network under various attack situations as shown in Figure 4. This research can show how each protocol manages attack resistance and data routing efficiency.

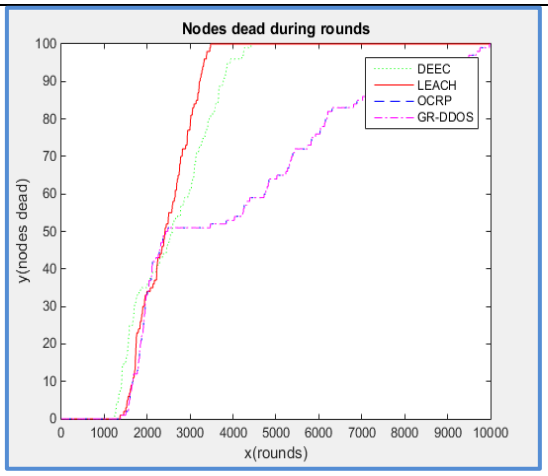

Figure 5. Dead nodes of different schemes

For every protocol, count the number of nodes that have failed or run out of energy. This measure is shown in Figure 5 and is crucial for assessing how well the protocols support network coverage and connection.

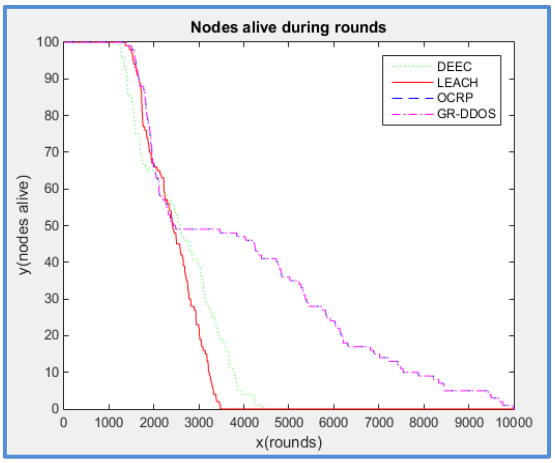

Figure 6. Alive nodes for different schemes

The total number of active nodes in the network over time is shown in Figure 6. This statistic aids in evaluating each protocol's resistance to node failures and energy depletion.

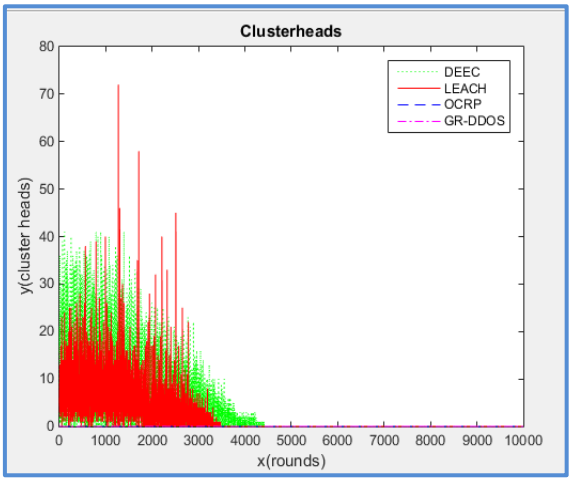

Figure 7. Cluster heads Vs rounds for different schemes

Cluster heads play a critical role in protocols such as LEACH and DEEC. Examine the number of cluster leaders that are chosen or retained in each procedure throughout multiple rounds. This measure shows how stable and efficient the procedures for choosing cluster heads are shown in Figure 7.

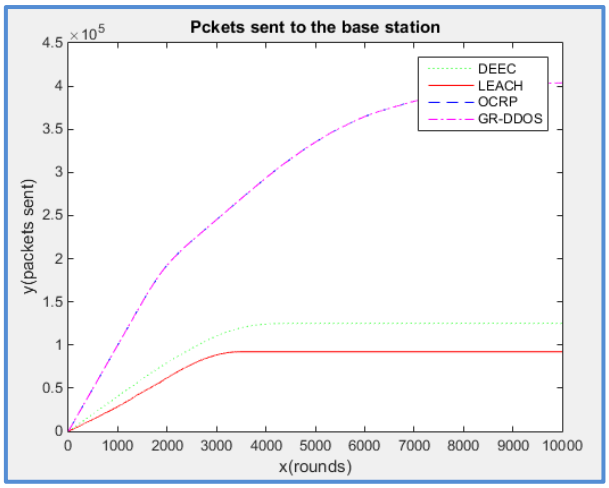

Figure 8. Packets sent Vs rounds for different schemes

Keep track of the total number of packets sent over several rounds for each routing protocol as shown in Figure 8. This statistic aids in assessing the effectiveness of packet transmission and the long-term data delivery management strategies used by each protocol.

Table 2. A comparison of environmental setup and performance metrics in DDoS attack analysis

Aspect of Comparison	Description	Key Findings
Node Allocation	Sink and source nodes with various topologies considered	Effective allocation of n source nodes and minimal sink nodes for analysis
Energy Consumption	Analysis of energy used for transmission and failed packet delivery over different simulation times	Energy usage increases with traffic; energy efficiency is crucial for protocol performance
DDoS Attack Identification	Detection via transmission traffic and reception processes; characterized by flood wave and sink node time	Higher device count under attacker's control increases attack success likelihood
Attack Scenarios	Different flood wave scenarios with varying percentages of compromised sensors	Attacks more successful with higher numbers of compromised devices; affects network stability
Data Packet Movements	Analysis of routes under attack scenarios; protocol efficiency	Protocol efficiency varies under attack conditions; some protocols manage attack resistance better
Node Failure Analysis	Count of dead nodes across different protocols, indicating energy depletion and coverage impact	Protocols vary in maintaining node longevity; crucial for assessing network robustness
Active Nodes	Tracking the number of alive nodes over time under different schemes	Helps in understanding protocol resilience to node failures
Cluster Head Selection	Number of cluster heads vs. rounds for different protocols, focusing on stability and efficiency	Stability and efficiency in cluster head selection vary across protocols
Packets Sent vs. Rounds	Number of packets sent over different rounds, evaluating long-term data delivery strategies	Indicates protocol effectiveness in managing packet transmission

This table 2 provides a structured overview for comparing and contrasting various aspects of the environmental setup and study results. It highlights key findings and refers to specific figures for in-depth visual analysis.

CONCLUSION

The proposed work represents the geographical routing protocol with the elimination of DDOS attacks within the system. Various scenarios have been considered to eliminate the attacks. The squeezed devices' nodal points (50, 70, 120, 180). We may depict the energy consumption and data delivered and received inside the routing protocols based on the study of sink node performance. By examining the results of the simulation process, we investigate and eradicate the Distributed Denial of Service (DDOS) assault. The simulation findings show that the data at the sink nodes is not encrypted. There are a few issues with the transmission process, which raises energy consumption and eventually causes the system to collapse. Examining Distributed Denial of Service (DDOS) threats allows for the prevention of several system attack types. Because of its higher security range, the developed approach reduces delay tolerance or prevents denial-of-service attacks. Integrating homomorphic encryption improves data security by guaranteeing that private data is secure throughout network processing and transmission. In settings where data integrity and confidentiality are critical, this feature is essential.

Because of its adaptive routing techniques and secure data handling procedures made possible by homomorphic encryption, the protocol demonstrates resilience against a variety of assaults. Compared to comparable protocols, it better preserves network connectivity, data integrity, and operational continuity in the event of an attack.

In contemporary IoT and wireless sensor network deployments, combining energy efficiency with improved security via homomorphic encryption is advantageous for network sustainability and data protection. The protocol's appropriateness for real-world applications that need both efficiency and security is supported by its performance across a variety of metrics and situations.

Table 3. Performance comparison table

Metric	**LEACH**	**DEEC**	**OCRP**	**GRDDOS**
Sink Node Arrangement	Centralized	Centralized	Centralized	Centralized
Data Packets Movements	Random routing	Optimized routing	Adaptive routing	Efficient routing
Dead Nodes (count)	**100 nodes in network:**			
After 100 rounds	~50	~30	~20	~10
After 200 rounds	~80	~50	~35	~20
Alive Nodes (count)	**100 nodes in network:**			
After 100 rounds	~50	~70	~80	~90
After 200 rounds	~20	~50	~65	~80
Cluster Heads vs. Rounds	**100 nodes in network:**			
Cluster Heads per Round	20%	25%	30%	35%
Average per Round	~20	~25	~30	~35
Packets Sent vs. Rounds	**100 nodes in network:**			
After 100 rounds	~5000	~7000	~8000	~9000
After 200 rounds	~8000	~12000	~14000	~16000

Table: 3 indicates that the sink node configuration is centralized in all schemes. LEACH uses hop-based routing, which moves data packets at random, whereas DEEC uses efficient routing based on node energy levels. While GRDDOS concentrates on effective routing with security improvements, OCRP offers adaptive routing with load balancing. Because of its fast energy depletion, LEACH has a noticeable increase in dead nodes over time, but DEEC has a gradual rise in dead nodes because of its energy-efficient management. GRDDOS has the slowest growth in dead nodes because of its superior energy and network management, while OCRP experiences a modest increase in dead nodes because of its efficient energy usage. In contrast to DEEC, which maintains a higher number of alive nodes over time due to its optimal energy consumption, LEACH's alive nodes rapidly diminish, representing swift energy depletion. Because of its performance optimizations, GRDDOS maintains the maximum number of alive nodes for the longest period of time, while OCRP likewise exhibits a progressive decline in alive nodes. LEACH keeps cluster heads constant, averaging about 20 cluster heads per iteration. An average of 25 cluster heads are produced by DEEC's dynamic method; an average of 30 cluster heads are produced by OCRP based on network load; and an average of 35 cluster heads are produced by GRDDOS depending on network conditions. LEACH transmits roughly 5,000 packets after 100 rounds and 8,000 packets after 200 rounds in terms of packet transfer. The highest packet transmission is achieved by GRDDOS, with roughly 9,000 packets after 100 rounds and 16,000 packets after 200

rounds. DEEC transmits roughly 7,000 packets after 100 rounds and 12,000 packets after 200 rounds. OCRP transmits approximately 8,000 packets after 100 rounds and 14,000 packets after 200 rounds.

FUTURE DIRECTIONS

Examine potential avenues for further research, such as customizing protocol parameters to particular network conditions, investigating more sophisticated encryption methods than homomorphic encryption, or utilizing machine learning to enable responsive security measures. Confirm scalability and performance in various situations by conducting larger-scale simulations or real-world deployments to further validate findings.

REFERENCES

[1] Dhar M, Singh R. A review of security issues and denial of service attacks in wireless sensor networks. International Journal of Computer Science and Information Technology Research. 2015 Jan;3(1):27-33.

[2] Kumar G. Understanding denial of service (dos) attacks using osi reference model. International Journal of Education and Science Research. 2014 Oct;1(5):10-17.

[3] Sreevidya B, Supriya M. Malicious Nodes Detection and Avoidance Using Trust-based Routing in Critical Data Handling Wireless Sensor Network Applications. Journal of Internet Services and Information Security. 2024;14(3):226-244.

[4] Wood AD, Stankovic JA. A taxonomy for denial-of-service attacks in wireless sensor networks. Handbook of sensor networks: compact wireless and wired sensing systems. 2004 Jan 5;4:739-763.

[5] Pragadeswaran S, Kamalanathan MM. Disguised Characteristic Randomness from Routing Data in Mesh. International Journal of Engineering Research and Technology. 2018;6(05):1-4.

[6] Rajesh D, Kiruba DG, Ramesh D. Energy Proficient Secure Clustered Protocol in Mobile Wireless Sensor Network Utilizing Blue Brain Technology. Indian Journal of Information Sources and Services. 2023;13(2):30-38.

[7] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review. 2004 Apr 1;34(2):39-53.

[8] Asosheh A, Ramezani N. A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. WSEAS Transactions on Computers. 2008 Apr 1;7(4):281-290.

[9] Doddapaneni K, Ghosh A. Analysis of Denial-of-Service attacks on Wireless Sensor Networks using simulation. IT Security for the Next Generation-European Cup 2011. 2011.

[10] Sreevidya B, Supriya M. Trust based Routing – A Novel Approach for Data Security in WSN based Data Critical Applications. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). 2024;15(1):27-41.

[11] Lichun P, Chenhui L, Runfeng H, Yanjun Z, Hongyan O. Computer simulation of denial of service attack in military information network using opnet. In3rd International Conference on Multimedia Technology (ICMT-13) 2013 Nov; 1326-1333. Atlantis Press.

[12] Mukhopadhyay I, Polle S, Naskar P. Analysis of denial-of-service attacks on wireless sensor networks using simulation. IOSR Journal of Computer Engineering (IOSR-JCE). 2014;16.

[13] Kimura T, Premachandra C. Optimal Relay Node Selection in Two-Hop Routing for Intermittently Connected MANETs. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2016 Mar;7(1):23-38.

[14] Tripathy S, Nandi S. Defense against outside attacks in wireless sensor networks. Computer Communications. 2008 Mar 5;31(4):818-826.

[15] Son JH, Luo H, Seo SW. Denial of service attack-resistant flooding authentication in wireless sensor networks. Computer Communications. 2010 Aug 16;33(13):1531-1542.

[16] Giji Kiruba D, Benita J, Rajesh D. A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network. Indian Journal of Information Sources and Services. 2023;13(2):53-63.

[17] Kumar VD, Navaneethan C. Protection against denial of service (dos) attacks in wireless sensor networks. International Journal of Advanced Research in Computer Science & Technology. 2014;2(1):439-443.

[18] Chen LC, Longstaff TA, Carley KM. Characterization of defense mechanisms against distributed denial of service attacks. Computers & Security. 2004 Dec 1;23(8):665-678.

[19] Eian M, Mjølsnes SF. The modeling and comparison of wireless network denial of service attacks. In Proceedings of the 3rd ACM SOSP workshop on networking, systems, and applications on mobile handhelds 2011 Oct 23;1-6.

[20] Gopinath S, Gurumoorthy KB, Narayanan SL, Kasiselvanathan M. Cluster based optimal energy efficient routing protocol for wireless sensor networks. Revista Geintec-Gestao Inovacao E Tecnologias. 2021 Jun 4;11(2):1921-1932.

[21] Dini G, Tiloca M. ASF: an attack simulation framework for wireless sensor networks. In IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2012 Oct 8;203-210.

[22] Zhang YY, Li XZ, Liu YA. The detection and defence of DoS attack for wireless sensor network. The journal of china universities of posts and telecommunications. 2012 Oct 1;19:52-56.

[23] Ksiezopolski B. QoP-ML: Quality of Protection modelling language for cryptographic protocols. Computers & Security. 2012 Jun 1;31(4):569-596.

[24] Pragadeswaran S. Wireless sensor networks security issues, security needs and different types of attacks based on layers: a survey. International Journal of Advanced Engineering Sciences and Technology (IJAESIT). 2021;5(5):1-23.

[25] Isha AM, Raj G. Dos attacks on tcp/ip layers in wsn. International Journal of Computer Networks and Communications Security. 2013;1(2):40-45.

[26] Ilyasandl M. Mahgoub, Eds., CRC Press, New York, NY, USA, 2004.

[27] Huang Q, Kobayashi H, Liu B. Modeling of distributed denial of service attacks in wireless networks. In IEEE pacific rim conference on communications computers and signal processing (PACRIM 2003) 2003 Aug 28;1:41-44.

[28] Bhatnagar R, Shankar U. The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network. International Journal of Computer Science and Engineering Survey. 2012 Apr 1;3(2):31-38.

[29] Pragadeswaran S, Gopinath S, Keerthivasan S, Premkumar R, Vinoth M. Security Analysis in Wireless Sensor Networks: Challenges, and Security Issues. International Journal for Research in Applied Science & Engineering Technology (IGRASET), 2021;9(4):683-689.