iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: VII Month of publication: July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45959

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs

Kavana E

Abstract:** Modern advancements in insolent sensors, RFID, Web - based machineries, and technical requirements are made possible by the Internet of Things (IoT). Sensor nodes are often employed to collect and transmit sensed data and are thought of as intelligent devices. In addition to these inherent limitations, sensor nodes are also open to a number of security risks. In order to improve the quality of renewable energy with multi-hop information security versus malicious acts, this work provides (ESMR) protocol. There are three primary components to the suggested procedure. The network field is first divided into inlet and outlet zones depending on the placement of the nodes. Additionally, a large number of clusters are created in each zone based on the proximity of the node neighbourhood. Second, the suggested effective secret sharing mechanism is used to protect the data transfer from cluster members in each zone to the bowl node. In order to reduce routing disruption, the suggested approach examines the mathematical analysis of data connections. The work described offers a multi-hop, compact, secure data analyst solution for limited wireless communications based on the Internet of Things (WSNs). In terms of bandwidth by 38 percent, network available bandwidth by 34 percent, electricity intake by 34 percent, median end-to-end postponement by 28 percent, and high latency by 36 percent when compared to the conventional work, the experimental results of the part of the application and secure number of co routing protocol.

I. INTRODUCTION

WSN comprises of transitory, ad-hoc iot devices that transfer data to a base station (BS) or sink node. Sensor nodes [3]–[6] have cognitive, resource, bandwidth, and storage restrictions [1], [2]. WSNs join autonomous sensor nodes wirelessly. Routers enhance latency and average throughput in network management. Standard approaches aren't ideal for IoT due to its complexity and instability in a wireless setting [7, 8]. Information and network hazards slow IoT's development [9, 10]. Two types of data aggregating and forwarding exist. First, structure-free method combines imperfect sensor data. Framework network clustering. Each area has a local information [15]–[18] node. After accumulating information, it delivers it to sink node. Most WSNs operate sensor nodes independently, creating security risks. Wireless sensor networks include secure routing approaches [19]–[22], but they need standard cryptographic primitives, which increases processing capabilities and routing costs [23], [24]. This doesn't prevent multipoint communications from malware. Most modern systems employ multi-hop data forwarding. Resource constraints force sensor nodes to multihop. Unauthorized forwarding nodes may disrupt network operations

This study provides (ESMR) using XOR-based visual cryptography for renewable energy and reliable forwarding across safe intermediate nodes against data assaults. ESMR makes the following contributions. Distance determines how ESMR divides network nodes. Each zone is split by its neighbour. Node partitioning increases network performance and latency. ESMR provides a nice XOR-based secret sharing approach for sensor nodes. XOR logical procedures secure data from unfriendly nodes between collection heads and BS, resulting in a reliable end-to-end communication. Using XOR simplifies numerical computation. XOR encryption requires less CPU resources in sensor nodes. Reactive routing minimises routing disruptions via quantitative network node analysis.

ESMR affects wireless and unstable monitoring zones. Safe multi-hop data routing enhances network robustness under malevolent assaults. Continued: 2 mentions primary sources. Section 3 motivates problem-solving. Section 4 describes ESMR's techniques and framework. Section 5 outlines network parameters and model. Section 6 compares the proposed solution to previous work. Recommended end Section 7.

II. RELATED WORK

Wireless technology has lately made it feasible to build and control the coverage area because of the low cost of intelligent houses. Sensor nodes are connected phones that have a wide range of capabilities but also certain restrictions. Data may be gathered, analysed, and delivered back to the BS or sink node through wireless connections between iot devices in networks. Nowadays, radar nodes are being researched intensively in a broad variety of applications, including home automation, intelligent buildings and farming, as well as in the military and in the healthcare industry.

Researchers have come up with a slew of ideas on how WSNs might benefit society in a variety of ways. However, the battery life of sensor nodes limits the usefulness of many of the proposed solutions. Since this is the case, many scholars have turned their attention to finding methods to increase energy efficiency while increasing data transfer speed. Furthermore, hostile nodes may intercept data transfers and steal information from sensor nodes since they utilise open media to communicate. The bulk of suggested methods for securing wireless sensor transmission include network and computation overheads, despite the fact that there are numerous. In addition, the approaches disclosed allow end-to-end secure transport network without analysing the security of intermediary nodes. Considering that processing elements are considered forwarders, they might be at risk. In this case, the logistics providers may provide access to private information to stripy nodes. Passive or proactive security threats are also possible. An active attack occurs when a hostile node intercepts data, alters it, and then sends it on to other nodes nearby. By using passive means, the rogue node only has access to the victim's private information. Distributed security enforcement with several hops and lightweight solutions is another significant problem.

For reducing communication costs, extending the life of networks, and enabling them to grow in size, researchers have lately developed cluster-based approaches. Open media, on the other hand, is fraught with network dangers and criminal activities, therefore the suggested remedies are seldom implemented. With so many extra responsibilities beyond just gathering local data, choosing an appropriate leader for the cluster becomes critically vital throughout the setup phase.

Cluster heads [25, 26] are vulnerable to being overloaded with data and experiencing fast energy depletion because of their role as the hub for all cluster activities. There is also the possibility that transceiver cluster heads may be abused and vulnerable to network attacks. As a result, the difficult task is to discover a route that is both safe and energy-efficient from beginning to conclusion [27], [28]. Reducing sentral and delays is made possible by the removal of rogue nodes.

The first active routing system was the low energy adaptive clustering hierarchy (LEACH) [29], which comprises of numerous transmitting data cycles. In LEACH, clusters are formed through a random process. The cluster head position is rotated at a predefined time interval. When compared to more traditional algorithms, the suggested approach is more energy efficient and requires less network upkeep. However, the demand for the network is not evenly distributed throughout the clusters. Later, a modified variant of LEACH called PEGASIS [30] was published, which uses a greedy technique to organise all nodes into a chain-like structure. Since all nodes may send and receive data across their next-hops, they are said to have comprehensive sensor professional skills. The routing chain is rebuilt when a node loses energy below a certain threshold. The routing chain is built from a node that is a significant distance away from the BS. For high-density networks, this optimizer delay ratio is a major problem since it doesn't perform well. Energy and data dependability are considered in the selection of the group head in the proposed LEACH-ER (LEACH-ER) method [31]. It is proposed that a cluster border be created between cluster heads and member nodes in order to reduce the packet receipt rate, which might lead to a longer network lifetime and more uniform distribution energy usage. Substandard routes have been developed, which have resulted in additional expenses and delays in the delivery of goods and services.

An energy and trust-aware routing system was presented in the ambient trust sensor routing (ATSR) [32]. Methods like decentralized safe routing protocols and trust metrics are proposed in this approach in an effort to thwart malevolent nodes. The ATSR protocol is usually significant since the decision is derived from data from the network's partners. However, this program's deluge of route request and response packets raises network traffic and amplifies energy consumption to dangerously high levels.

An AODV (Fr-AODV) protocol is suggested to fight network hazards and malicious nodes on the routing path. Node identity and reputation are used to calculate a trust value. An attribute number is assigned to each feature, and this number is delivered along with the data itself. An attribute number must match before data may be delivered to its next-door neighbour. The Fr-AODV protocol encounters route re-discoveries and re-transmissions while adopting a comparable manner of route management.

Rogues' undesirable behaviour may be dealt with with TSRF [34]'s trust-aware, secure routing infrastructure. TSRF considers both straight and secondary trust for determining the dependability of nodes. An inconsistencies check mechanism is part of the TSRF security infrastructure, which guards against threats posed by rogue nodes. Only hostile nodes may be categorised in a multi-hop manner by the TSRF, but the WSN's limited resources are ignored, resulting in a shortened network lifetime.

Using the WSN's resource limits, another research presents the SEER protocol [35]. Due to the utilisation of several paths for data routing, the proposed method may have a short lifetime. The sink node receives the gathered data via the use of steering tables continued by the nodes themselves. Remaining energy is also affected by the number of data packets delivered and received in a routing path. Multi-path design adds additional expenditures even while SEER proto-col improves network consistency in terms of network longevity and data delivery speed. SEER is also unable to alter network measurements, resulting in muddled or broken routes.

III. MOTIVATIONS AND PROBLEM FORMULATION

Exploring the literature study reveals that the majority of the solutions offered do not provide acceptable security measures for reliable and secure data transmission performance. Additionally, since these approaches are designed for conventional wire-free networks, the applied cryptographic algorithms are inappropriate for sensor networks with limited resources. The suggested systems also incur significant transmission cost with connection overheads by exchanging multiple route discovery process and route reply updates in order to accomplish reliable data routing. Additionally, a lot of these methods do not take into account how dynamic sensor nodes are, which might cause congestion problems and periodic route learning point of view. The majority of the secure algorithms that have been presented test their effectiveness using LEACH, DSR, and AODV, three common routing protocols [36, [37]]. Because the discoveries of network threats and hostile nodes are beyond the purview of conventional data routing algorithms, we contend that such a comparison is not acceptable. Therefore, the primary benefit of the suggested method is the development of a simple, secure, and electricity protocol for WSNs operating in multi-hop environments. The suggested solution does not need a specific set of resources or place an excessive amount of computational burden on constraint nodes. Additionally, the suggested system monitors network parameters on demand and dynamically detects network hazards, which might result in increased network throughput and energy efficiency.

IV. PROPOSED ENERGY-AWARE AND MULTI-HOP SECURE ROUTING PROTOCOL

This section presents the proposed energy-aware and secure multi-hop routing (ESMR) protocol for constrained WSNs, which is based on a secret sharing method. The next subsections will go into depth on each of its parts. Euclidean distance factor in the first element, the network nodes are divided into inner and outer zones.

Further, the nodes inside every zone are grouped into different clusters using the k-nearest neighbours (k-NN) technique. To facilitate further data routing, each cluster is set up in a hierarchical fashion. The second part consists of,

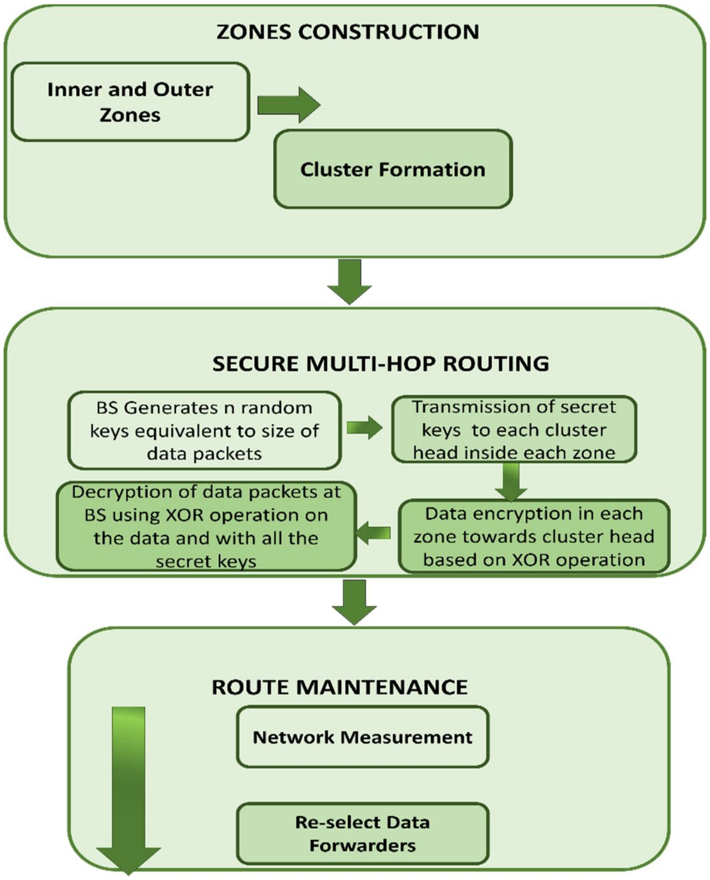

ZONES CONSTRUCTION
Inner and Outer Zones
Cluster Formation
SECURE MULTI-HOP ROUTING
BS Generates n random keys equivalent to size of data packets
Transmission of secret keys to each cluster head inside each zone
Data encryption in each zone towards cluster head based on XOR operation
Decryption of data packets at BS using XOR operation on the data and with all the secret keys
ROUTE MAINTENANCE
Network Measurement
Re-select Data Forwarders

Figure 1. ESMR Protocol Block Diagram.

The major goal is to strike a balance between energy use and dependable packet forwarding, and to suggest a safe multi-hop routing strategy that is resource and resistant to malicious assaults. Based on the XOR secret sharing mechanism in restricted sensor nodes, it offers a simple solution. Additionally, it does not contribute to the network's computing overheads. The third category is performing route maintenance to find problematic connections in the created routing routes and lessen the likelihood of route malfunctions and packet drop. In this situation, the suggested protocol re-adjusts the logistics services based on the measurable data and might result in an extended network lifespan with increased route dependability. The experimental findings are superior to the strategies currently in use. The block diagram of the ESMR protocol is shown in Fig.1.

A. Region Based Zones Construction

In order to monitor a square-sized region, the n nodes are randomly distributed over the network.Upon completion of the installation, each node will have an own identity. All of the nodes have similar qualities, but the sink node has all of the most powerful capabilities with no limits on the amount of resources available. A multi-hop method is first used by the BS to transmit its identification and location data in the sensor field. Every node has got the BS information and transmit it in their forwarding table through their next-hop.

$$(\beta - 1)\alpha < Z_\beta < \alpha\beta \qquad (1)$$

When a node's neighbours change, its routing tables are automatically updated. After that, the dynamic limits from the BS is used to establish each zone's border, as illustrated in equation 1.

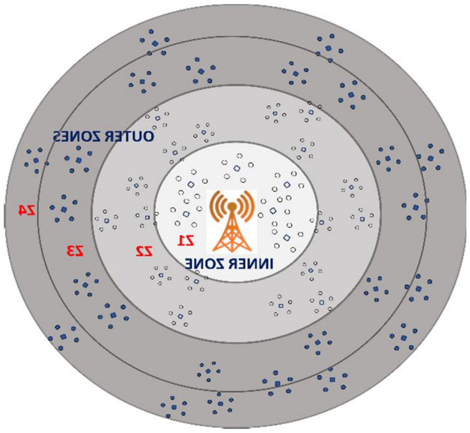


Figure2. Generations of inner outer zones and clusters formulation.

where β represents the zones $\beta^{\in}(1, 2, . . . n)$ and α is the preset distance. Suppose, for second zone, i.e., zone-2, $\beta 2\ \alpha < Z_2 < 2\alpha$. Zones 1, 2, 3,..., n may be represented by the symbol () and their distance from one another can be represented by the symbol (). Suppose that for the second zone, i.e., zone-2, 2 Z2 2. As a result, a series of circular zones will be built around the BS. Sending data straight to the BS from the inner zone uses less transmission power. The outer zones, on the other hand, utilise their higher zones as intermediaries for the effective transfer of sensory information. As shown in Figure 2, the newly created zones are then further divided into several clusters using the lightweight and simple k-nearest neighbours (k-NN) technique.

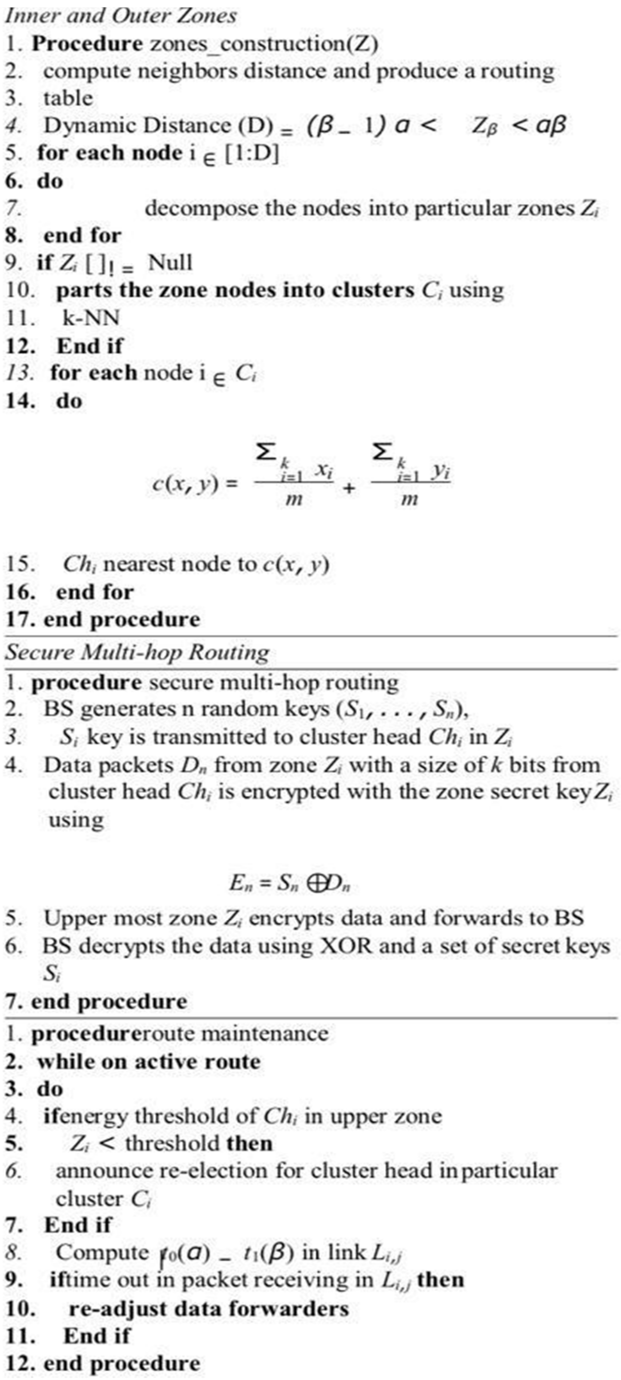
The suggested approach makes use of the distance function and the K-NN algorithm to combine the closest neighbours into a single cluster. In order to calculate K, the number of nodes in a given zone is divided by the square root of that number. To distinguish each cluster from other clusters, each zone is broken down into a number of smaller clusters. In addition, the initial cluster head in each cluster is designated to a node that is closer to the centroid in order to reduce net work costs. It's a virtual node that sits in the middle of the cluster, essentially. This is the set of all nodes in the cluster (ci, n1, n2, n3,..., nk). The cluster's centroid c(x, y) is determined by investigating the nodes' spatial coordinates

$$c(x, y) = \frac{\sum_{i=1}^{k} x_i}{m} + \frac{\sum_{i=1}^{k} y_i}{m} \qquad (2)$$

Following are the procedures that reveal the multi-hop routing secret sharing scheme:

1) Secret keys (S1, S2, S3, and so on) are generated by the BSS and each has the same size as the data packet ('k' bits). Transmission of these keys is made to each zone's respective cluster head (Z).a
2) The XOR operation specified in equation 3 is used to encrypt the data Dn from zone 'Zn' with a size of k bits from the cluster head. If En is equal to Sn Dn, then (3) To the designated cluster head in the higher zone Zn 1, the encrypted data bits En of a specific cluster in zone n, 'Zn,' are sent. iii.
3) The zone secret key Sn 1 is used to encrypt the data once it reaches the cluster head in zone Zn 1 by executing the XOR operation as shown in equation.

Algorithm 1 Secret Sharing Based Energy-Aware and Secure
Multi-Hop Routing Protocol



```
Inner and Outer Zones
Procedure zones_construction(Z)
  compute neighbors distance and produce a routing
  table
  Dynamic Distance (D) = $(\beta - 1)\alpha < Z_\beta < \alpha\beta$
 for each node i $\in$ [1:D]
 do
            decompose the nodes into particular zones $Z_i$
  end for
 if $Z_i$ [ ]! = Null
   parts the zone nodes into clusters $C_i$ using
    k-NN
   End if
  for each node i $\in$ $C_i$
   do

        $c(x, y) = \frac{\sum_{i=1}^{k} x_i}{m} + \frac{\sum_{i=1}^{k} y_i}{m}$

    $Ch_i$ nearest node to $c(x, y)$
   end for
end procedure
Secure Multi-hop Routing
procedure secure multi-hop routing
  BS generates n random keys ($S_1, . . . , S_n$),
    $S_i$ key is transmitted to cluster head $Ch_i$ in $Z_i$
  Data packets $D_n$ from zone $Z_i$ with a size of $k$ bits from
   cluster head $Ch_i$ is encrypted with the zone secret key $Z_i$
   using

        $E_n = S_n \oplus D_n$

  Upper most zone $Z_i$ encrypts data and forwards to BS
  BS decrypts the data using XOR and a set of secret keys
   $S_i$
end procedure
procedureroute maintenance
 while on active route
 do
  ifenergy threshold of $Ch_i$ in upper zone
     $Z_i$ < threshold then
    announce re-election for cluster head inparticular
    cluster $C_i$
  End if
    Compute $t_0(\alpha) - t_1(\beta)$ in link $L_{i,j}$
   iftime out in packet receiving in $L_{i,j}$ then
     re-adjust data forwarders
    End if
end procedure
```

4) This method of encryption utilising Bitwise con- tinues from cluster members in the bottom zones Zn to the highest most zone Z1 from around BS.

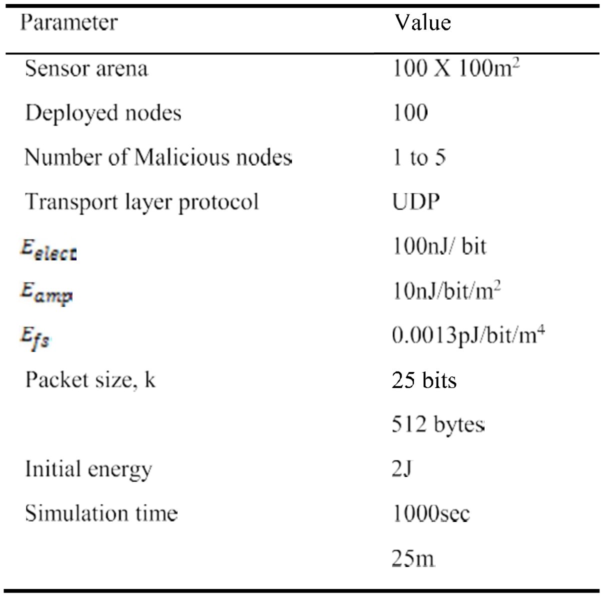
using equation 5.
$PDV = |t_0(\alpha) - t_1(\beta)|(5)$
All of the secret keys Si may be decrypted by conducting XOR procedures on the encrypted files, as shown in equation 4, at the uppermost zone, Z1.
$Di = S1 \oplus S2 \oplus S3, \ldots \oplus En \qquad (4)$
There is no risk of data loss or changes the amount with the suggested secret sharing technique since it may be implemented from any zone.

B. Route Maintenance

To reduce the likelihood of route damages and re-forwarding, the element of dynamic routing is carried out. The ESMR starts the search for an alternative routing route if it determines that a cluster head in the higher zone is unsuitable for further data forwarding. In the following situations, the path discovery process is often called.

1) Firstly, whenever in the upper zone the energy As soon as a cluster head's resources falls below a certain level, the packet transmission process is halted, and the election process is announced again within a predetermined boundary. Nodes that are closer to the centre of the cluster are voted as new heads, and their status is updated.
2) Second, based on the packet delay variation (PDV) variable, the effectiveness of the connection between the cluster - head Li,j is also assessed. The absolute amount provided by the PDV is the variation successive packets of the same transmission. link. Let's figure shows an example: the PDV may be calculated if packet is sent and it takes t0 time to traverse the system and packet takes t1 time to do so.

Table 1. Default Simulation Parameters.



Parameter	Value
Sensor arena	100 X 100m^2
Deployed nodes	100
Number of Malicious nodes	1 to 5
Transport layer protocol	UDP
E_{elect}	100nJ/ bit
E_{amp}	10nJ/bit/m^2
E_{fs}	0.0013pJ/bit/m^4
Packet size, k	25 bits
	512 bytes
Initial energy	2J
Simulation time	1000sec
	25m

V. NETWORK ASSUMPTIONS AND MODEL

This part use NS2 as a simulation environment to test the efficiency of the ESMR protocols against Fr-AODV and the TSRF solution. We set up a network field with 100 sensor nodes, each with a different number of malicious nodes, ranging from 1 to 5. False route solutions are broadcasted by botnets, and as a result, they are picked as data freight forwarder. In actuality, they just discard the datagrams that they receive. In the beginning, all nodes have a 2J energy level with a 25m transmission capacity. An energetic model is used to estimate the sensor's energy consumption. ESMR's findings in terms of network longevity, throughput, latency from end to end, and communication cost are compared to prior studies. Table 1 summarises the default settings for numerous simulation studies.

VI. RESULTS AND DISCUSSION

A. Network Lifetime

Fig.3 shows how the proposed ESMR protocol stacks up against Fr-AODV and TSRF in terms of network life expectancy. Experiment findings show that the ESMR protocol improves bandwidth efficiency by an average of 38% over other systems. As a result, the network nodes are prioritised for both efficiency and dependability. Due to their lack of consideration for network circumstances, both the FR-AODV and the TSRF procedures pick forwarders prematurely, which might result in a shorter lifespan for the forwarder. For active routing pathways, ESMR finds the most efficient and trustworthy forwarders..

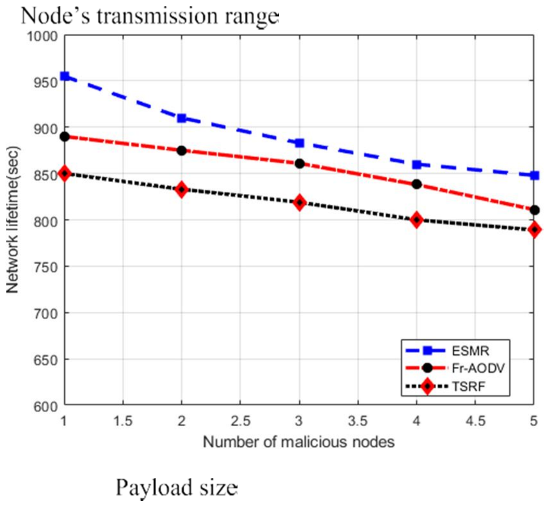


Figure 3. Network lifetime in varying malicious nodes.

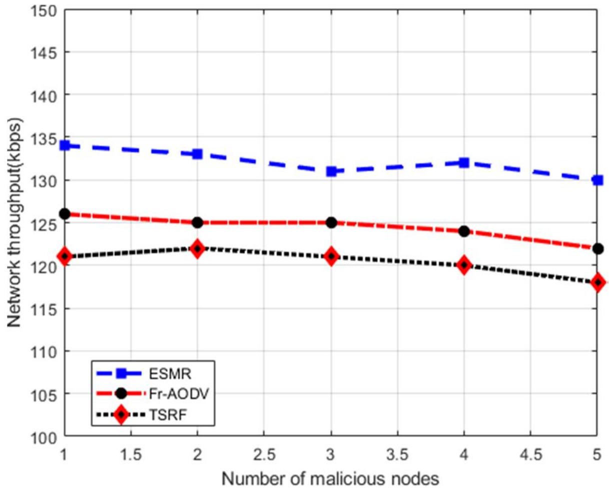


Figure 4. Network throughput in varying malicious nodes.

B. Network Throughput

Figure 4 compares the ESMR protocol's network performance with that of other alternatives under a variety of anomaly based counts. After conducting experiments, it can be observed that the performance of routing protocols may be affected by bandwidth utilization. When comparing ESMR to other solutions, it can be shown that data transmission improved by an average of 34%. This is owing to the fact that ESMR has an energy-efficient and strong cluster management, as well as multi-hop security, which makes it more secure. There is a lack of detection and forwarding of packets of data on electricity and reliable routing pathways in the caused by malicious threats in the AODV/TSRF protocols that reduces network performance.

C. Energy Consumption

Figure 5 shows the comparison of the ESMR protocol's energy usage with that of the alternatives. ESMR has been shown to have a positive impact on energy usage.

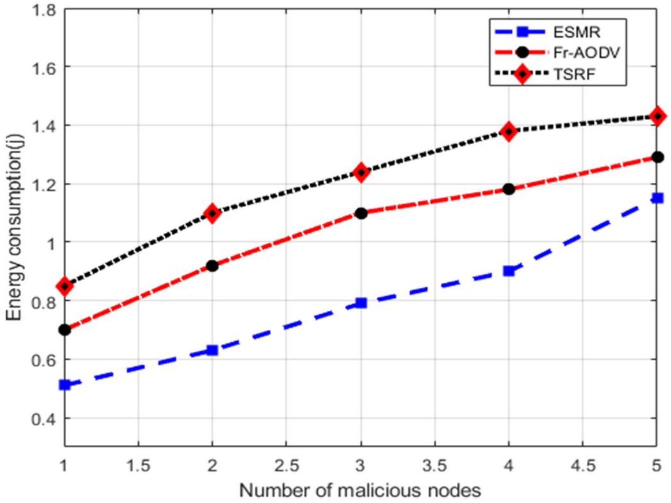


FIGURE 5. Energy consumption in varying malicious nodes.

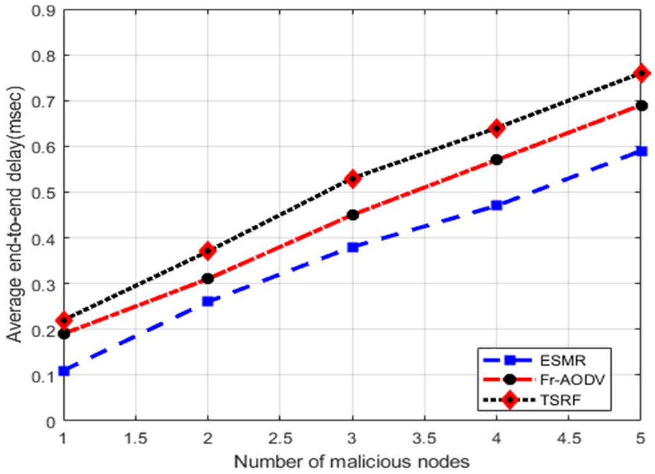


Figure 6. A measure of the average end-to-end latency for malicious nodes.

The formation of clusters based on the proximity of the adjacent neighbourhood has resulted in a 34% decrease in the number of existing works. Route fractures are more common with Fr-AODV and TSRF procedures, which might contribute to increased energy usage. Efficient and energy-sufficient nodes are used in the construction of routing pathways, lowering the need for re-transmissions and increasing energy usage in ESMR, even in the presence of malevolent nodes.

D. Average End-To-End Delay

ESMR is compared to previous methods in terms of end-to-end latency under varied numbers of malicious nodes. In the presence of malicious nodes, as shown in Fig. 6, the ESMR protocol improved end-to-end latency by an average of 28%. The selection of optimum forwarders with the quickest routing pathways allows ESMR to surpass Fr-AODV and TSRF. Because of their longer routing pathways, Fr-AODV and TSRF protocols use up forwarders' energy more quickly. Data transfers are more often and the end-to-end latency is greater in long-distance routing pathways. In addition, the current solutions do not include the To limit the availability of communication networks for data packets, quantifiable measurements are used to detect crowded and defective connections.

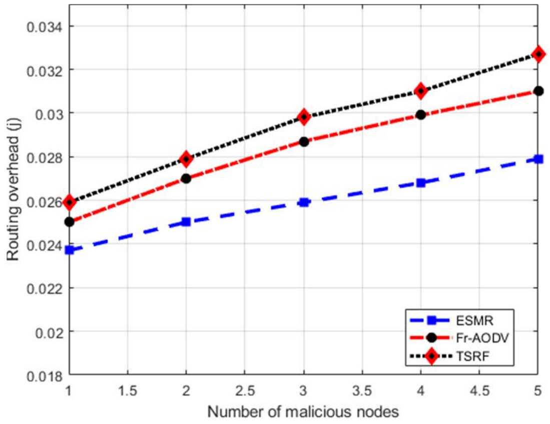


Figure 7. Routing overhead in varying malicious nodes.

E. Routing Overhead

For every data relaying protocol, exists has an important impact on the assessment since increasing routing delay may have a negative impact on energy efficiency and delivery results. In addition, hostile threats, calls for alternative route development, and re-transmissions have escalated in recent years. The ESMR increases routing inefficiency performance by an average of 36%, since data forwarding pathways are created based on dependability and energy economy considerations (see Fig.7). The ESMR encryption also recommends the use of a lightweight XOR algorithm to protect forwarders in networks with limited resources against attack. The higher energy usage of network nodes in protocols like Fr-AODV and TSRF results in an excessive number of requests for route re-adjustment. In addition, the Fr-AODV and TSRF protocols have a large number of route restorations, which results in a high routing overhead that has a detrimental effect on the network's lifespan.

VII. CONCLUSION

This work describes the ESMR procedure for IoT-based WSNs, which seeks to provide efficient and power routing against the malicious behaviour of advancing the packets of nodes. Based on node placements, the ESMR protocol produces inner and outer zones. Furthermore, nodes in the network are grouped into several clusters using the closest neighbourhood approach. A lightweight XOR encryption is also provided by the suggested technique in order to secure multi-hop data forwarding in resource-constrained networks. For data transmission, the ESMR protocol instructs forwarders to choose the shortest path possible, which includes reliable and electricity nodes. It is also possible to reduce routing disruption and re - transmission by using the suggested protocol's statistical analysis to detect congestion on specific links. Research in simulation show that the ESMR protocol is superior than all other currently used protocols. Mobile sensors with diverse network topologies need to be used to verify the efficiency of ESMR in thefuture

REFERENCES

[1] T. Meng, F. Wu, Z. Yang, G. Chen, and A. V. Vasilakos, ‘‘Spatial reusability-aware routing in multi-hop wireless networks,’’ *IEEE Trans. Comput.*, vol. 65, no. 1, pp. 244–255, Jan. 2016.

[2] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Athanasios, ‘‘Software- defined and virtualized future mobile and wireless networks: A survey,’’ *Mobile Netw. Appl.*, vol. 20, no. 1, pp. 4–18, Feb. 2014.

[3] S. Rani, R. Talwar, J. Malhotra, S. H. Ahmed, M. Sarkar, and H. Song, “A novel scheme for an energy efficient Internet of Things based on wireless sensor networks,’’ *Sensors*, vol. 15, no. 11, pp. 28603–28626, 2015.

[4] B. Rashid and M. H. Rehmani, ‘‘Applications of wireless sensor networks for urban areas: A survey,’’ *J. Netw. Comput. Appl.*, vol. 60, pp. 192–219, Jan. 2016.

[5] R. A. Roseline and P. Sumathi, ‘‘Local clustering and threshold sen- sitive routing algorithm for wireless sensor networks,’’ in *Proc. Int. Conf. Devices, Circuits Syst. (ICDCS)*, Coimbatore, India, Mar. 2012, pp. 365–369.

[6] F. Ruan, C. Yin, J. Chen, J. Wang, and S. Xue, ‘‘A distance clustering routing algorithm considering energy for wireless sensor networks,’’ *Int. J. Future Gener. Commun. Netw.*, vol. 6, no. 5, pp. 73–80, 2013.

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ‘‘Internet of Things (IoT): A vision, architectural elements, and future directions,’’ *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[8] M. T. Lazarescu, ‘‘Design of a WSN platform for long-term environmental monitoring for IoT applications,’’ *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 45–54, Mar. 2013.

[9] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, ‘‘TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things,’’ *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.

[10] K. T. Nguyen, M. Laurent, and N. Oualha, ‘‘Survey on secure communica- tion protocols for the Internet of Things,’’ *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.

[11] M. Ding, X. Cheng, and G. Xue, ‘‘Aggregation tree construction in sensor networks,’’ in *Proc. IEEE 58th Veh. Technol. Conf. (VTC-Fall)*, Oct. 2003, pp. 2168–2172.

[12] A. M. Krishnan and P. G. Kumar, ‘‘An effective clustering approach with data aggregation using multiple mobile sinks for heterogeneous WSN,’’ *Wireless Pers. Commun.*, vol. 90, no. 2, pp. 423–434, 2016.

[13] J. Yuea, W. Zhang, W. Xiao, D. Tang, and J. Tang, ‘‘Energy efficient and balanced cluster-based data aggregation algorithm for wireless sensor networks,’’ *Procedia Eng.*, vol. 29, pp. 2009–2015, Feb. 2012.

[14] Z. Zhou, J. Tang, L.-J. Zhang, K. Ning, and Q. Wang, ‘‘EGF-tree: An energy-efficient index tree for facilitating multi-region query aggre- gation in the Internet of Things,’’ *Pers. Ubiquitous Comput.*, vol. 18, no. 4, pp. 951–966, 2014.

[15] M. Alagirisamy and C.-O. Chow, ‘‘An energy based cluster head selection unequal clustering algorithm with dual sink (ECH-DUAL) for continuous monitoring applications in wireless sensor networks,’’ *Cluster Comput.*, vol. 21, no. 1, pp. 91–103, 2018.

[16] P. K. Batra and K. Kant, ‘‘LEACH-MAC: A new cluster head selection algorithm for wireless sensor networks,’’ *Wireless Netw.*, vol. 22, no. 1, pp. 49–60, 2016.

[17] U. Venkanna and R. L. Velusamy, ‘‘TEA-CBRP: Distributed cluster head election in MANET by using AHP,’’ *Peer-Peer Netw. Appl.*, vol. 9, no. 1, pp. 159–170, 2016.

[18] K. A. Darabkh, W. S. Al-Rawashdeh, M. Hawa, and R. Saifan, ‘‘MT-CHR: A modified threshold-based cluster head replacement protocol for wireless sensor networks,’’ *Comput. Elect. Eng.*, vol. 72, pp. 926–938, Nov. 2018.

[19] M. B. Krishna and M. N. Doja, ‘‘Multi-objective meta-heuristic approach for energy-efficient secure data aggregation in wireless sensor networks,’’ *Wireless Pers. Commun.*, vol. 81, no. 1, pp. 1–16, 2015.

[20] K. A. Kumar, A. V. N. Krishna, and K. S. Chatrapati, ‘‘New secure rout- ing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks,’’ *J. Inf. Optim. Sci.*, vol. 38, no. 3, pp. 341–365, 2017.

[21] S. Ozdemir, ‘‘Secure and reliable data aggregation for wireless sensor networks,’’ in *Proc. Int. Symp. Ubiquitious Comput. Syst.* Berlin, Germany: Springer, 2007.

[22] Z. Yu-Quan and W. Lei, ‘‘A new routing protocol for efficient and secure wireless sensor networks,’’ *TELKOMNIKA Indonesian J. Elect. Eng.*, vol. 11, no. 11, pp. 6794–6801, 2013.

[23]]S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and V. Gupta, ‘‘Design of a secure anonymity-preserving authentication scheme for session initia- tion protocol using elliptic curve cryptography,’’ *J. Ambient Intell. Human- ized Comput.*, vol. 9, no. 3, pp. 643–653, 2018.

[24] S. Adamovic, M. Sarac, D. Stamenkovic, and D. Radovanovic, ‘‘The importance of the using software tools for learning modern cryptography,’’ *Int. J. Eng. Educ.*, vol. 34, no. 1, pp. 256–262, 2018.

[25] S. Din, A. Paul, A. Ahmad, and J. H. Kim, ‘‘Energy efficient topol- ogy management scheme based on clustering technique for software defined wireless sensor network,’’ *Peer-to-Peer Netw. Appl.*, vol. 12, no. 2, pp. 348–356, 2019.

[26] K. Babber and R. Randhawa, ‘‘Energy efficient clustering with secured data transmission technique for wireless sensor networks,’’ in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 3023–3025.

[27] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, ‘‘A secure data rout- ing schema for WSN using elliptic curve cryptography and homomor- phic encryption,’’ *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 28, no. 3, pp. 262–275, 2016.

[28] D. He, S. Chan, and M. Guizani, ‘‘Cyber security analysis and protection of wireless sensor networks for smart grid monitoring,’’ *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 98–103, Dec. 2017.

[29] W. R. Heinzelman and A. Chandrakasan, and H. Balakrishnan, ‘‘Energy- efficient communication protocol for wireless microsensor networks,’’ in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Maui, HI, USA, Jan. 2000, p. 10.

[30] S. Lindsey and C. S. Raghavendra, ‘‘PEGASIS: Power-efficient gathering in sensor information systems,’’ in *Proc. Aerosp. Conf.*, Mar. 2002, p. 3. [31]Y. Guo, Y. Liu, Z. Zhang, and F. Ding, ‘‘Study on the energy efficiency based on improved LEACH in wireless sensor networks,’’ in *Proc. 2nd Int. Asia Conf. Inform. Control, Automat. Robot. (CAR)*, Mar. 2010, pp. 388–390.

[31] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, ‘‘A novel trust-aware geographical routing scheme for wireless sensor networks,’’ *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 805–826, 2013.

[32] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, ‘‘Trust-based routing mechanism in MANET: Design and implementation,’’ *Mobile Netw. Appl.*, vol. 18, no. 5, pp. 666–677, 2013.

[33] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, ‘‘TSRF: A trust-aware secure routing framework in wireless sensor networks,’’ *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 1, 2014, Art. no. 209436.

[34] N. Nasser and Y. Chen, ‘‘Secure multipath routing protocol for wireless sensor networks,’’ in *Proc. 27th Int. Conf. Distrib. Comput. Syst. Work- shops (ICDCSW)*, Jun. 2007, p. 12.

[35] R. Bai and M. Singhal, ‘‘DOA: DSR over AODV routing for mobile ad hoc networks,’’ *IEEE Trans. Mobile Comput.*, vol. 5, no. 10, pp. 1403–1416, Oct. 2006.

[36] M. Barati, K. Atefi, F. Khosravi, and Y. A. Daftari, ‘‘Performance eval- uation of energy consumption for AODV and DSR routing protocols in MANET,’’ in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Jun. 2012, pp. 636–642.

KHALID HASEEB received the M.Sc. degree in information technology from the Institute of Man- agement Sciences, Pakistan, and the Ph.D. degree in computer science from the Faculty of Com- puting, Universiti Teknologi Malaysia, in 2016. During his Ph.D., he was a member of the Per- vasive Computing Research Group. Since 2008, he has been with the Computer Science Depart- ment, Islamia College Peshawar, Pakistan. His research interests include sensors and ad-hoc networks, network security, cloud computing, and mobile communication. He is a Reviewer for many reputed international journals and conferences.

NAVEED ISLAM received the Ph.D. degree in computer science from the University of Montpel- lier II, France, in 2011. He is currently an Assis- tant Professor with the Department of Computer Science, Islamia College University, Peshawar, Pakistan. He has authored numerous international journal and conference articles. His research inter- ests include computer vision, machine learning, artificial intelligence, and data security. He is a Regular Reviewer of IEEE, Elsevier, and Springer Journals.

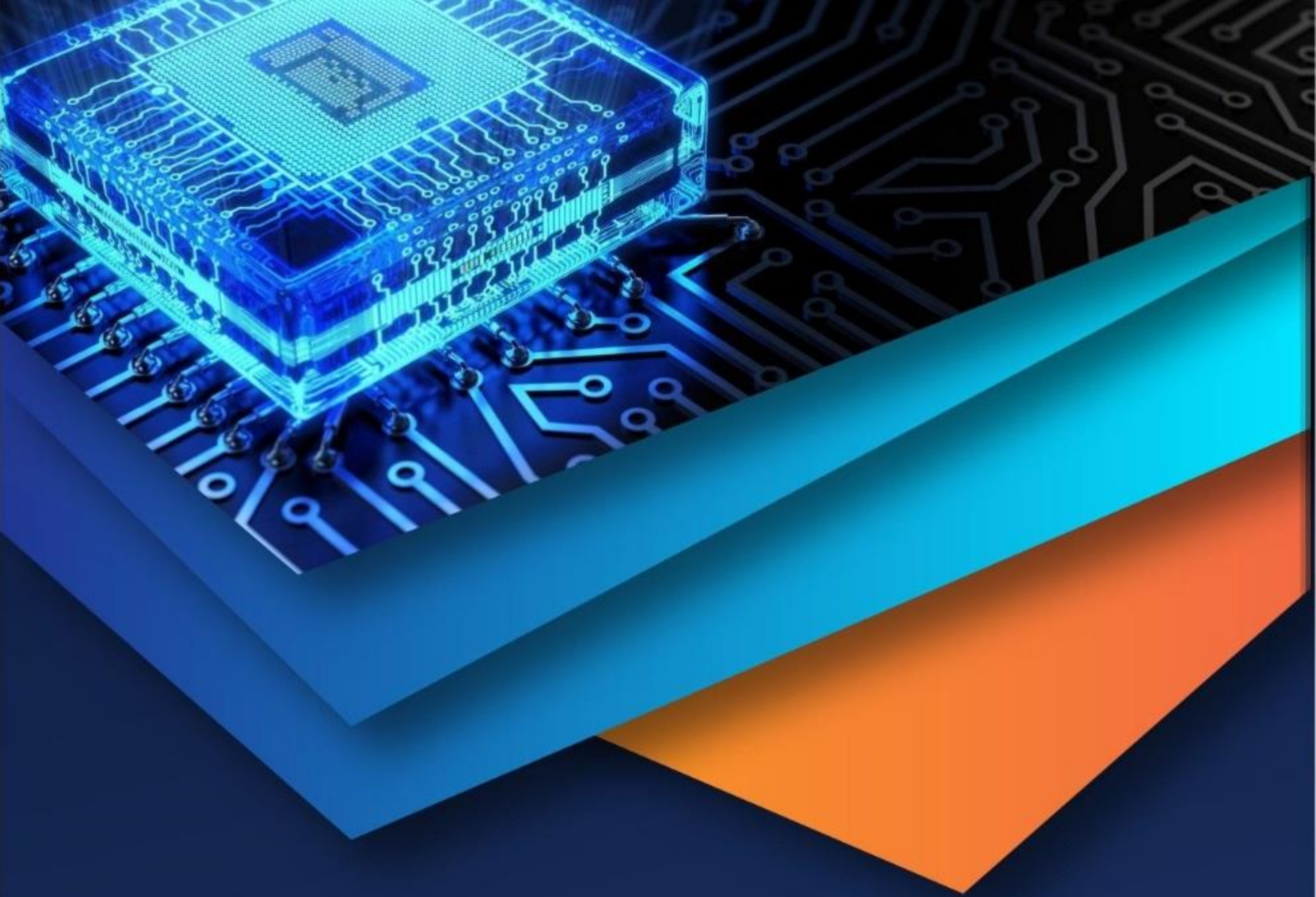
AHMAD ALMOGREN received the Ph.D. degree in computer science from Southern Methodist Uni- versity, Dallas, TX, USA, in 2002. He was an Assistant Professor of computer science and a member of the Scientific Council, Riyadh Col- lege of Technology. He also served as the Dean of the College of Computer and Information Sci- ences and the Head for the Council of Academic, Al Yamamah University. He is currently a Profes- sor and the Vice Dean of development and quality with the College of Computer and Information Sciences, King Saud Univer- sity. His research interests include mobile and pervasive computing, cyber security, and computer networks. He has served as a Guest Editor at several computer journals.

HISHAM N. ALMAJED received the bachelor’s degree in information systems from the College of Computer and Information Sciences, King Saud University, in 2004, and the M.Sc. degree in computer applications and systems administration from the Computer Section, Arabeast Colleges, in 2015. He is currently pursuing the Ph.D. degree in computer science with the College of Computer and Information Sciences, King Saud University. He is also with Saline Water Conversion Corporation Head Quarter, Riyadh, Saudi Arabia, as an Information Technology Governance Team Member. His research interests include computer security and wireless sensor network security. He received several professional cer- tifications, including PMP, CISA, ISO27001 Lead Auditor, ISO27001 Leas Implementer, TOGA9, and ITIL Expert.

IKRAM UD DIN (S’15–SM’18) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, and the Ph.D. degree in com- puter science from the School of Computing, Universiti Utara Malaysia (UUM). He also served as the IEEE UUM Student Branch Professional Chair. He has ten years of teaching and research experience in different universities/organizations.

His current research interests include resource management and traffic control in wired and wireless networks, vehicular communications, mobility and cache management in information-centric networking, and the Internet of Things.

NADRA GUIZANI is currently pursuing the Ph.D. degree with Purdue University, where she is also a Graduate Lecturer and completing a thesis in pre- diction and access control of disease spread data on dynamic network topologies. Her research inter- ests include machine learning, mobile networking, large data analysis, and prediction techniques. She is an Active Member in the Women in Engineering Program and the Computing Research Association for Women.



doi crossref
10.22214/IJRASET

INDEX COPERNICUS
45.98

ISRA JIF
IMPACT FACTOR:
7.129

SJIFactor
TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)