Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777513

DESIGN OF RELIABLE ENERGY-EFFICIENT WIRELESS SENSOR NETWORK ROUTING PROTOCOL

PavanKumar Kolluru[1], Dr Y Padma[2], Anusha Marouthu[3], Dr. Shaik.Nagul[4], Deevi Radha Rani[1]

[1]Department of CSE, VFSTR Deemed to be University, Guntur, India
[2]Department of InformationTechnology,P V P Siddhartha Institute of Technology,Vijayawada, India,
[3]Department of CSE, Koneru lakshmaiah Education Foundation, Vaddeswaram, Guntur, India,
[4]Department of CSE, Lendi Institute of Engineering and Technology, Vizianagaram, India

Abstract

WSNs have been the focus of intensive studies and have seen explosive development in recent years. They have been used in a variety of critical applications, including tracking, decision-making, and time-critical processes, and are capable of integrating sensitive data. For better performance, WSNs employ collaborative steps such as data collection, compilation, analysis, and management of sensing operations. Low-power nodes will have to go through several hops to connect with the sink node. This necessitates the use of neighbors' nodes as relays. Packets relayed via malicious users, on the other hand, will impede communication and thereby deplete Wireless Sensor Network resources. This paper discusses the architecture, security services, design issues, security challenges, attacks, and routing protocols of wireless sensor networks. This paper also proposes protocols which is more efficient and designed to overcome the issues in the existing routing protocols and the performance is evaluated based on parameters like energy consumption, throughput, delay, packet delivery ratio, packet loss and reliability.

Keywords: Wireless Sensor Network, routing protocols, cooja simulator, network throughput

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have quickly established themselves as a leading network of intelligent and smallcomputenodes for building a stable, flexible, and robust network. WSNs are a form of multi-hop wireless network that has a high usage rate but limited resources. They have been used in a variety of critical applications, including tracking, decision-making, and time-critical processes, and are capable of integrating sensitive data. Power, network throughput, range of communication, and capacity are all constrained of WSN sensor nodes.

Wireless sensor network application spaces are diverse due to the openness of miniaturized scale sensors and minimal control remote communication. After the sensor centre points have been moved on, they are in charge of working with a reasonable system configuration in a coherent manner by allowing multi-bounce correspondence [8]. Figure 1 shows the model of Wireless Sensor Network.

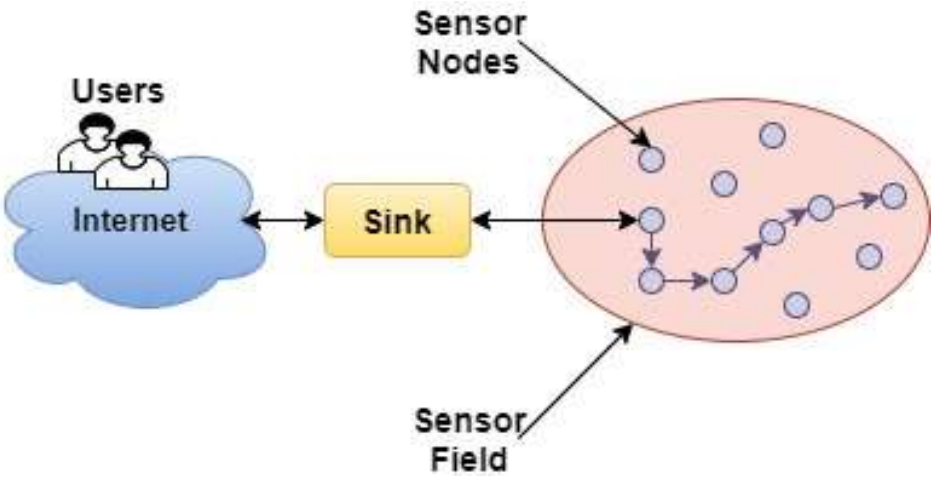

Figure 1 Wireless Sensor Network Model

To examine and achieve real-time information, hundreds of nodes are distributed for a definite category of applications. In several sensitive wireless-based applications, establishing effective multipath connectivity between sensor nodes is critical for securely transmitting data. Big WSNs, on the other hand, can be difficult to plan, deploy, and maintain due to resource constraints.

For better performance, WSNs employ collaborative steps such as data collection, compilation, analysis, and management of sensing operations. Low-power nodes will have to go through several hops to connect with the sink node. This necessitates the use of neighbors' nodes as relays. Packets relayed via malicious users, on the other hand, will impede communication and thereby deplete Wireless Sensor Network resources. It is enviable to maintain source-to-sink anonymity and to extend network's lifespan by seeking energy-efficient safe routes. Processing needed for safe routing and connectivity is spread through several nodes, necessitating careful monitoring. Providing defense in such networks is both crucial and complex. Energy-aware secure routing is an important reflection in this view, as it is critical to the smooth operation of WSNs.

The outline of the paper is planned as follows: Section II confers the related work on Wireless Sensor Networks i.e. architecture, security services, design issues, security challenges, attacks, and routing protocols. Section III presents the proposed routing protocols which is more reliable and designed to overcome the issues in the existing routing protocols. Section IV evaluates the performance of proposed routing protocol and Section V gives the conclusion of the paper.

II. RELATED WORK

A. Architecture of Wireless Sensor Networks

The components in the architecture of WSN are: "Network manager, Security manager, Gateway, Field devices" shown in Figure 2.A network manager is responsible for the system's structure, the steering table, planning gadget communications, and testing and announcing the system's soundness where as security manager is responsible for key management. Sensor nodes are also known as field devices.

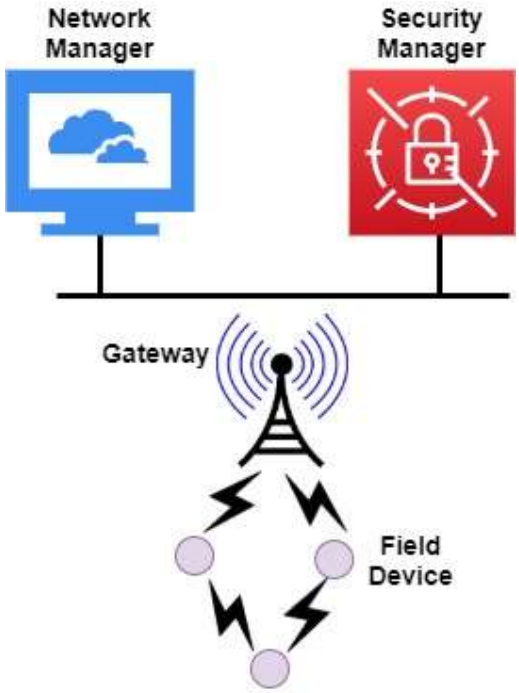

Figure 2 Architecture of Wireless Sensor Networks

For the advantages of various applications, sensor nodes or *"field devices"* have to be appropriate for routing packets. A *"router"* is unique type of field device that do not need to route sensor or control data. A *"gateway"* establishes the connection between sensor nodes and the actual users.

B. Security Services of Wireless Sensor Networks

Secure Wireless Sensor Networks should offer secure services described below [1]:

Confidentiality: Sensor nodes share sensitive information and must communicate safely and securely over wireless transmission networks to avoid eavesdropping attacks. Information, cryptographic keys, and other sensitive information must be transmitted in encoded format only to the specified recipient.

Integrity: Integrity guarantees the data sent by sensor nodes is not tampered with or manipulated during transmission.

Authentication:Sensor nodes in a WSN must validate the identity of all key stakeholders prior granting access to services or other resources. Nodes must therefore be certain that the information is being sanded and routed by the specified sources.

Figure 3 Security Services of Wireless Sensor Networks

Availability: Nodes have a small power supply and are highly reliant on their battery life. Due to computing and connectivity, nodes can become inaccessible. Furthermore, unreliable routing protocols can cause them to rapidly lose their energy demands.

Self-Organization: To help fault tolerance in the network, distributed Wireless Sensor Networks must self-organize. For flexible nodes, the network also should allow multipath routing. In Wireless Sensor Networks, stable self-organization is difficult to enforce.

Access Control: To access the available resources and data, sensors connected to the Wireless Sensor Network should be authenticated.

Secure Localization: The ability of a Wireless Sensor Networks to precisely and quickly trace each sensor in the network determines its effectiveness. An attacker, on the other hand, might claim a replayed signal or incorrect transmitted strength, and easily exploit a non-secured position.

C. Design Issues of Wireless Sensor Networks

The following critical wireless sensor network design concerns must be considered in order to satisfy the directional trend toward sustainability [2].

Reliability: Owing to the intermittent character of sensor nodes & the complex structure of the network, reliable data transfer is challenging.

Fault-Tolerance: The capability of a device to continue running without disruption due to sensor node faults is referred to as fault tolerance. When a sensor node is unable to forward its data packets to the sink, it may take advantage of the accessibility of alternate paths to save its packets from node or network failures. Data forwarding can be resumed without delay even if a route fails according to this method, as long as an alternate path is available. Many routes can also be used at the same time to improve data transfer efficiency.

Scalability: It is quick to arrange a few nodes in a Wireless Sensor Networks. As the nodes multiply, the difficulty of handling time-varying features of a vast number of nodes grows, eventually creating more coordination device disruption.

Quality of Service: It's acollection of tools for efficiently handling the WSN. It allows for the calculation of sensor node energy usage, lifespan, latency, identification of varying network performance (such as overcrowding or bandwidth accessibility), efficiency, location-awareness, mutual processing, and traffic prioritization or throttling.

Latency and Overhead: A WSN's latency is an indicator of the amount of time it takes for data to arrive. This network delay can be triggered by multi-hop data relays and aggregation. Furthermore, some routing protocols create excessive overheads in order to execute their algorithms, making them unsuitable for severe energy-conserving networks. These considerations can have a substantial effect on the routing protocol's design [7].

Figure 4 Design Issues of Wireless Sensor Networks

Network Dynamics: In most WSN architectures, network elements including sensor and sink nodes, and event tracking are considered to be stationary. But, it is critical that WSN maintain sink mobility, cluster-head (gateway) mobility, sensor node mobility, event management. Routing and sensitive datafrom one moving node to another is further complex because of path steadiness, power usage, and network capacity will be significant considerations.

D. Security Challenges in Wireless Sensor Networks

Since wireless sensor networks are ad hoc, no static structure can be established. Since nodes may be distributed by airdrop, the topology is unknown prior to deployment. The network must accept self-configuration because nodes will malfunction or be restored. Security systems must be able to respond to this changing climate [3].

Because of its broadcast existence, the wireless medium is necessarily less safe. Eavesdropping is simple. An adversary can quickly capture, change, or replay any transmission. An attacker can quickly capture legitimate packets and insert malicious ones using the wireless medium. Existing methods must be optimized to run effectively on sensor networks, despite the fact that this challenge is not special to sensor networks [4].

The aggressive atmosphere in which sensor nodes operate is the next difficult aspect. Motes are at risk of being destroyed or captured by attackers. For security analysts, the hostile climate poses a significant threat.

Protection protocols would face a major challenge due to the proposed size of sensor networks. Networking tens of thousands to hundreds of thousands of nodes has proved to be a difficult challenge [8].

E. Attacks on Secure Routing Protocols in Wireless Sensor Networks

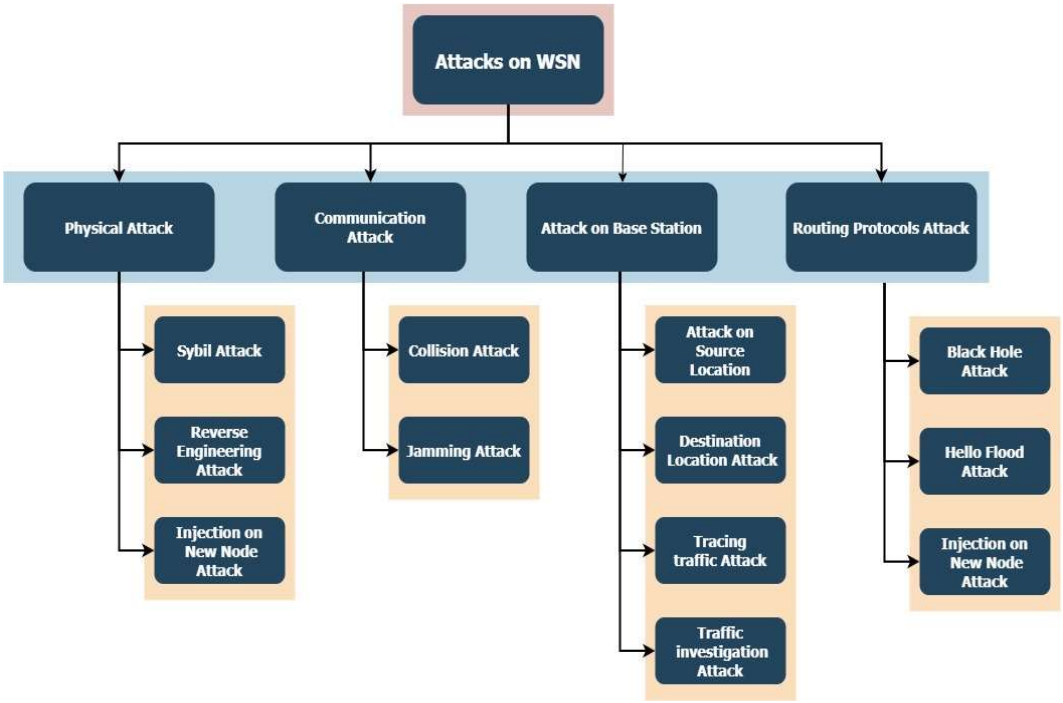

Figure 5 Attacks on Secure Routing Protocols in Wireless Sensor Networks

Physical Attack

The purpose of a this attack is to physically revoke the sensor or delete the sensor from the designated region [9]. The attacker may think of and deconstruct the system; the attacker can isolate secrecy keys used in cryptographic techniques; the attacker may convert the one and then insert duplicated nodes into the framework.

Sybil Attack: Device availability and maintainability are enhanced by redundancy. An intruder may build a node with a variety of characteristics that performs this role. In a Sybil attack, one node will imitate the characteristics of a huge number of other nodes. It was very hard and confusing to distinguish between the false and original nodes in this case.This type of attack has a negative impact on data privacy, data protection, and resource use [10].

Reverse Engineering Attack: To grasp the process's inner functionality order, which is approximated in the actual order; Reverse engineering is the practise of learning about working principles and doing device analysis in order to re-produce or copy something. The intruder takes the same useful details.

Injection on New Node Attack: The malicious user introduces a new node called malicious node into the network to steal valuable data. The malicious node will appear as a valid node, allowing it to compromise the system's security.

Communication Attack

Jamming Attack: Jamming attacks on the physical layer arise in the WSN protocol architecture. The perpetrator has disrupted a communication signal by using frequency jammers. The communication signals would be blocked, resulting in unavailability.

Collision Attack: In this kind of attack, the intruder constantly deliver packets in both directions, causing legitimate packets to be corrupted and other packets to be retransmitted.Service cannot be delivered to fair nodes due to node energy and retransmission delay.

Attack on Base Station

Datahave to be collected from nearby nodes and chat will be broadcast to the outside, where the base station will be using the internet. Traffic tracing and traffic control are two types of attacks on base stations.

Attack on Source Location: The invaderobserve the information by looking for a signal formed by a node. Using the packet tracing method, an attacker identifies one packet when transmitting it, and the packet address can be traced; this method would be repeated before the packet enters the source node using packet tracing in return.

Destination Location Attack: The invader looks for the receiver node in this attack. He's looking for a base station or another aggregator node. In a destination location attack, traffic mapping or traffic tracing methods are used.The attacker analyses the node's traffic density in comparison to all nearby nodes, and wherever the attacker notices a broad traffic flow, he deduces the location of the receiver node.

Tracing traffic Attack: By being familiar with the source and receiver fields, the attacker targets packets and uses the information to effectively trace a single node. He knows how to use forged packages and land unreachability to strike the wounded party. This form of attack impacts both the source and the destination [11].

Traffic investigation Attack: The area of a base station is deducted by an attacker who is not monitoring the content of information [12]. The attacker is uninterested in understanding what protocol was used or what cryptographic technique was used. Attackers track traffic density across the whole system; he essentially identifies the base station using techniques for crushing traffic and transmits the attack to damage the operation of base station.

Routing Protocols Attack

Any one of its operations is covered by a versatile operating system. An attacker can quickly manipulate the operating system's flaws [13].

Black Hole Attack: An attacker examines all traffic sent from different nodes, which is then suffocated and dropped. This attack takes advantage of a weakness in the generating calculation/convention: the zero cost & the dark opening nodes tend to the nearest to each other. The nearest valid node is taken into account by encompassing nodes with all traffic density it encounters, but it will do little. The infused node functions as a legitimate node, and actual genuine nodes trust it.

Hello Flood Attack: The attacker's use of high-power radio communication triggered a double-cross legitimate node. The high transmitting nodes assault the small number of nodes. In this physical attack, the authentic hub pursuesattacker hub, causing traffic congestion and

package delivery delays. Any subsequent communication is submitted to attacker hub, who screens and examines all machine traffic in order to carry out nefarious actions/tasks.

F. Secure Routing Protocols in Wireless Sensor Networks

Routing protocols describe how nodes interact with one another and how data is distributed across the network. Many researchers came out with many routing protocols that work with the characteristics of wireless sensor networks [14-21]. We categorize the vast list of protocols based on network organization, route discovery [9] and operation. Figure 6 shows the categories and list of protocols proposed by various researchers. As the technology advances, authors came up with energy efficient, clustering based and intelligent routing protocols for wireless sensor networks.

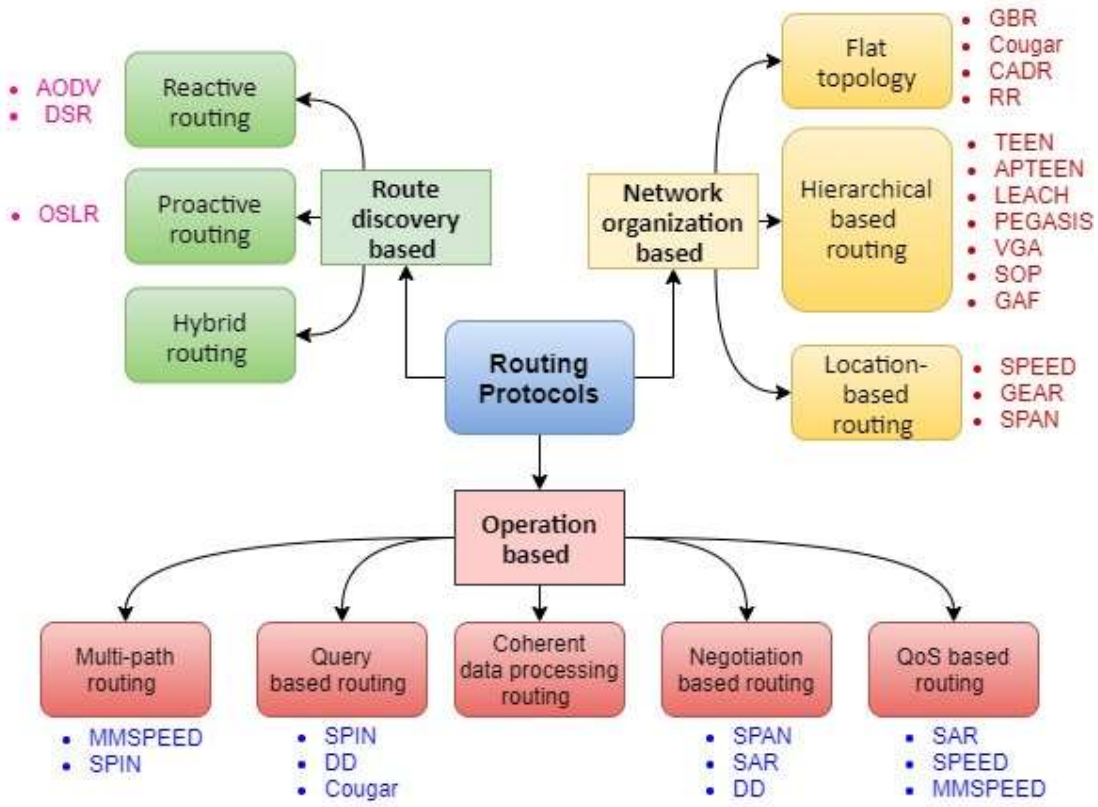

Figure 6 Secure Routing Protocols in Wireless Sensor Networks

Reactive routing protocols will not maintain the routes to all the nodes; instead, they find routes only when a node has to transfer data to another node. As a result, when requests are launched, the routes are built on request. Ex: AOODV, DSR. Proactive routing protocols are table-driven routing protocols, even though there is no data for transmission they maintain the routing table and update continuously by exchanging the packets and calculates the cost or distance to reach every node in the network. This happens even though there is a data to transfer or not. Ex: OSLR. Hybrid Routing Protocols combines the features of both the above protocols and avoids the demerits.

In a flat topology all the nodes have same priority and processes similarly. Flat topology is most commonlyset up in homogeneous networks in which all nodes havesame characteristics and functions. Ex: GBR, Cougar, CADR, RR. However, most heterogeneous networks utilize

hierarchical routing protocols, in which some nodes are more sophisticated and efficient than others. However, this is not necessarily the case; in hierarchical (clustering) protocols, nodes are clustered to form a cluster, and a cluster head is allocated to each cluster, which interacts with the base node. Ex: TEEN, APTEEN, LEACH, PEGASIS, VGA, SOP. In location-based routing, nodes may use different localization protocols to determine their current location. Location data aids in the optimization of routing procedures and allows sensor networks to offer additional services. Ex: SPEED, GEAR, SPAN.

Multi-path routing protocols distribute data through different routes, resulting in route optimization, reduced latency, and increased network performance. In the event that one of the routes fails, the multiple routing protocol offers an alternative route. Multiple route networks are particularly appealing to dense networks. Multiple route routing is not energy efficient since intermittent signals must be sent at specific times to keep the routes intact. Ex: MMSPEED, SPIN. Query based routing protocols are started by the receiver nodes. The sensor nodescan submit data in reply to the receiver. The goal node senses the information and sends it to the node that requested the message, and the receiver node sends a question of interest for obtaining any information across the network. Ex: SPIN, DD, Cougar. Negotiation-based routing protocols hold redundant data transmission to a bare minimum; sensor nodes negotiate with other nodes and exchange information about available resources with adjacent nodes, and data transmission decisions are taken during the negotiation process. Ex: SPAN, SAR, DD. These protocols are used to guarantee consistent service efficiency. QoS aware protocols attempt to find a route from source to sink that meets the degree of metrics associated with successful QoS, such as throughput, data transmission, energy consumption, and latency, while still allowing the best use of network resources. Ex: SAR, SPEED, MMSPEED. Until sending data to other sensor nodes or aggregators, nodes in the coherent data processing routing protocol perform limited processing (time stamping, data compression, etc.). The aggregator gathers data from multiple nodes and then transfers it to the sink node.

By studying all the existing routing protocols that fit with wireless sensor networks, hierarchical routing protocols are energy efficient but are not trusted. So, in this paper we propose a trusted and energy efficient routing protocol for Wireless sensor networks.

III. PROPOSED ENERGY EFFICIENT SECURE ROUTING PROTOCOL

This section presents our proposed routing algorithm with is more efficient and reliable compared to exiting routing protocols in wireless sensor networks. The proposed routing protocol belongs to the category of hierarchy clustering routing protocol. The architecture of such network consists of base stations, cluster head sensors and sensing and forwarding sensors. The entire network is divided into small clusters with cluster head. The sensing and forwarding sensors senses the data and forwards to the cluster head sensor. Cluster head can transmit for a longer distance with more energy. Our proposed routing protocol has 3 basic principles:

1. Using suitable authorization and flooding methods, the proposed protocol limits malicious nodes in its proximity.
2. To reduce the WSN's "*computation, storage, and bandwidth*" requirements, the protocol performs resource-intensive computations at the sink nodes and base station, such as constructing routing tables, stability, and intrusion resistance concerns.

3. The protocol exploit redundancy and accept intrusions in an area, and they function properly even when there are malicious user

Our proposed protocol consists of following phases:

1. Phase of discovering the neighboring node
2. Phase of forming the cluster
3. Phase of forwarding the data

In phase 1, all nodes transmit a message to all the nodes in its proximity range. The transmitted message consists of a sequence number (*Ss*), node identification (*IDs*), MAC for authentication. MAC is generated using key (*Ks*) and Nonce (Ns).

$$\text{Transmitted message} = Ss \mid IDs \mid Mac(Ks,\ IDs|Ns)$$

When a node transmits a message to neighboring node, the message is verified using hash function [23]. The (Pr) is power of node receiving the message; it is calculated using the equation

$$\Pr = \frac{Ps * Gs * Gr * \lambda^2}{(4\pi r)^2}$$

Where *Ps* is power of node sending the message, *Gs* is gain of sender antenna, *Gr* is gain of receiver antenna. In our protocol, after calculating the power of receiving node, it is compared with the threshold (T). If Pr is less than T, the node is send to be far node or malicious.

The node receiving the message sends a reply, which consist of sequence number (Sr) identification (*IDr*), MAC for authentication. MAC is generated using same key used by sender (*Ks*) and Nonce (Nr).

$$\text{Reply message} = Sr \mid IDs \mid IDr \mid Mac(Ks,\ IDs|IDr|Nr)$$

The reply message is verified by the sender, if it is correct, the node is considered as a neighboring node. Likewise, all the nodes collect the neighboring information and stores at the node. The same information is also sent to the cluster head in the form of a message. Now cluster head can find the multiple paths to each node in the network and constructs the reachability matrix and also generates the secret key for each pair of neighboring nodes to forward the data. The cluster node sends the reachability information and secret key for each pair to all the nodes in the network. The following message is sent to each node from cluster node:

$$secret\ key|Sc|IDc|IDs|IDr|MAC(Kc, secret\ key|Sc|IDc|IDs|IDr|Nc)$$

Where *Sc* is sequence number of cluster node messages, *IDc* is identity of cluster node, *Nc* is nonce of cluster node, *secret key* is key generated between pair of nodes identified by *IDs* and *IDr.*

In phase 2, cluster heads exchange the neighboring information of each cluster to the other clusters. As shown in the phase 1, the nodes in the cluster send the neighboring information to the cluster head, similarly, the cluster heads share the neighboring information between them. This helps the nodes in one cluster to communicate or send data to the node belonging to other clusters. The cluster head transmits this information to cluster nodes in its proximity range.

$$Sch1|IDcn1|MAC(Ks, IDcn1|Ncn1)$$

Where *Scn1* is sequence number of the message from cluster node1, *IDcn1* is identification of cluster node1, *Ks* is secret key and *Ncn1* is nonce of cluster node1.

After receiving the message from the cluster nodes, the other cluster nodes reply using the message:

$$Sch2|IDcn1|IDcn2|MAC(Ks, IDcn1|IDcn2|Ncn2)$$

Where *Scn2* is sequence number of the message from cluster node2, *IDcn2* is identification of cluster node2, *Ks* is secret key and *Ncn2* is nonce of cluster node2.

However the nodes in cluster collects the neighboring information and sends it to the cluster head, similarly, cluster heads collects the reachability information and sends it to the base station. Base station generates the secret key for the communication between pair of cluster heads and transmit the same to the cluster heads.

In phase 3, the source nodes forwards the data to the destination node i.e. sink node through neighboring nodes.

$$data|secret\ key|IDs|MAC(Ks, E(secret\ key, data)|NS)$$

IV. PERFORMANCE OF PROPOSED ROUTING PROTOCOL

In our experiment testbed we used Cooja Simulator on Contiki Operating System. We constructed the wireless sensor network model with 100 nodes and evaluated the performance of our proposed protocol with respect to energy consumption, throughput, delay, packet delivery ratio, packet loss and reliability. Our proposed routing algorithm is compared with clustering and hierarchical routing protocols like"*Threshold sensitive energy efficient sensor network*" (TEEN) and "*Low energy adaptive clustering hierarchy*" (LEACH). The simulation results is revealed in the Figure 7(a), 7(b), 7(c), 7(d), 7(e), 7(f) for energy consumption, throughput, delay, packet delivery ratio, packet loss and reliability respectively.

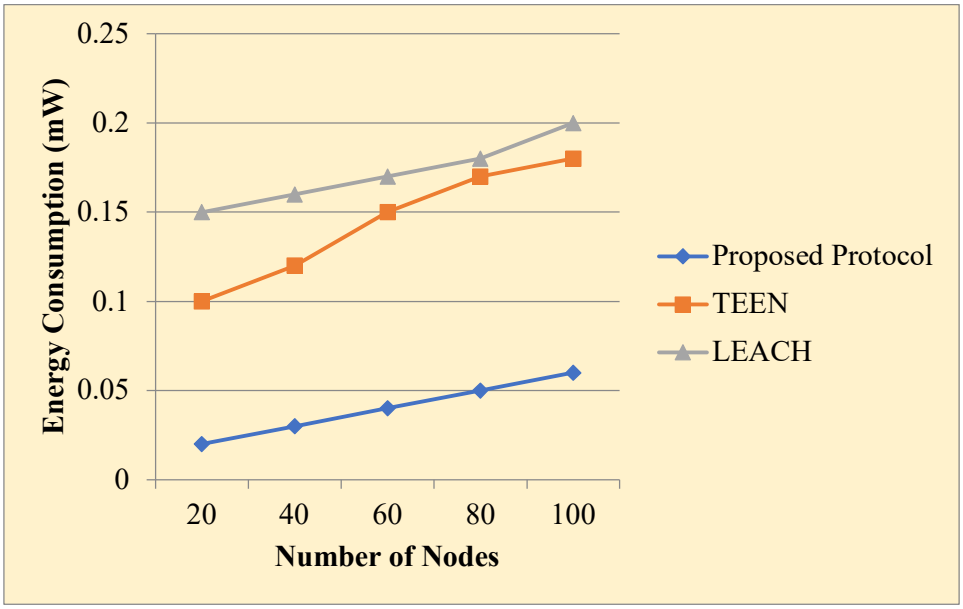

Figure 7(a) Energy consumption comparison analysis

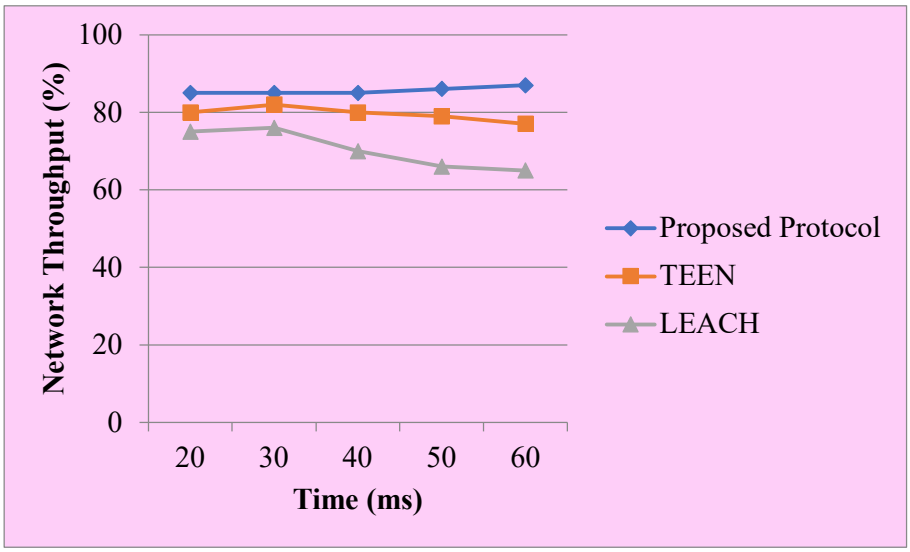

Figure 7(b) Network throughput comparison analysis

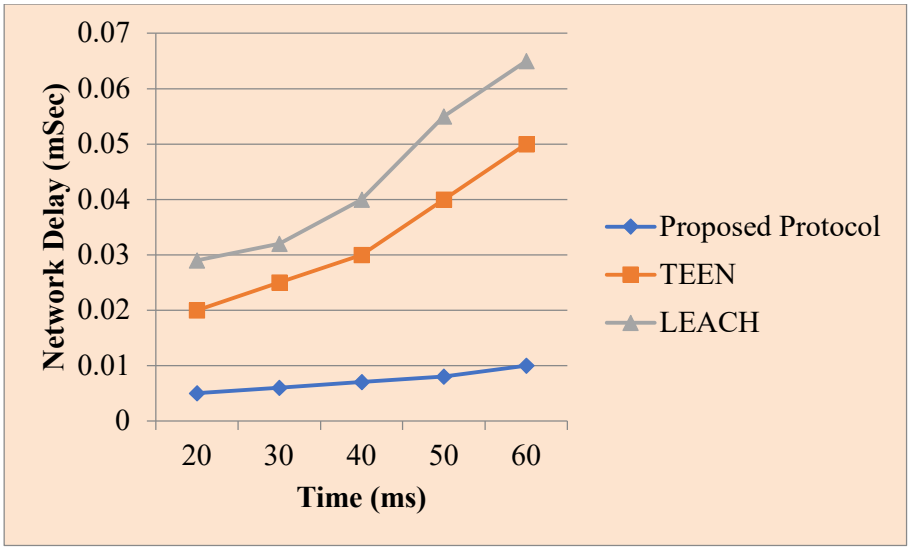

Figure 7(c) Network delay comparison analysis

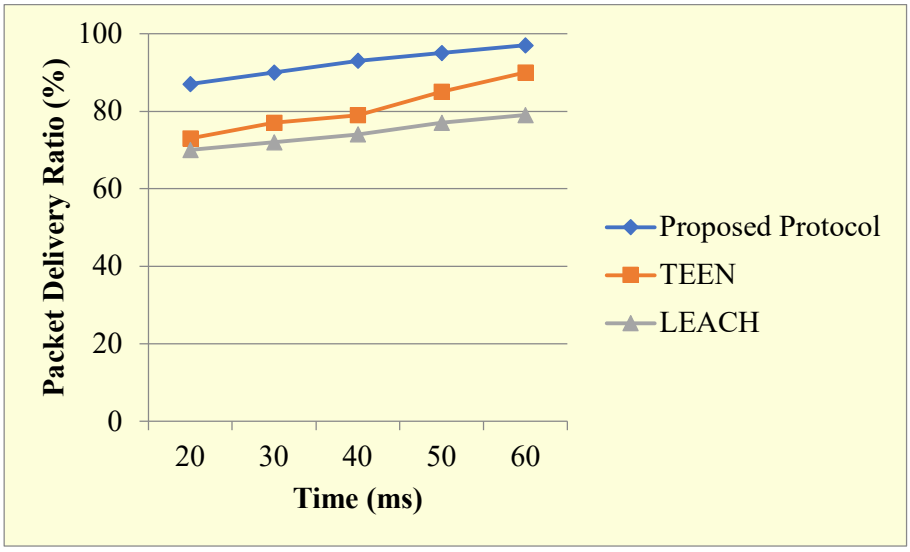

Figure 7(d) Packet delivery ratio comparison analysis

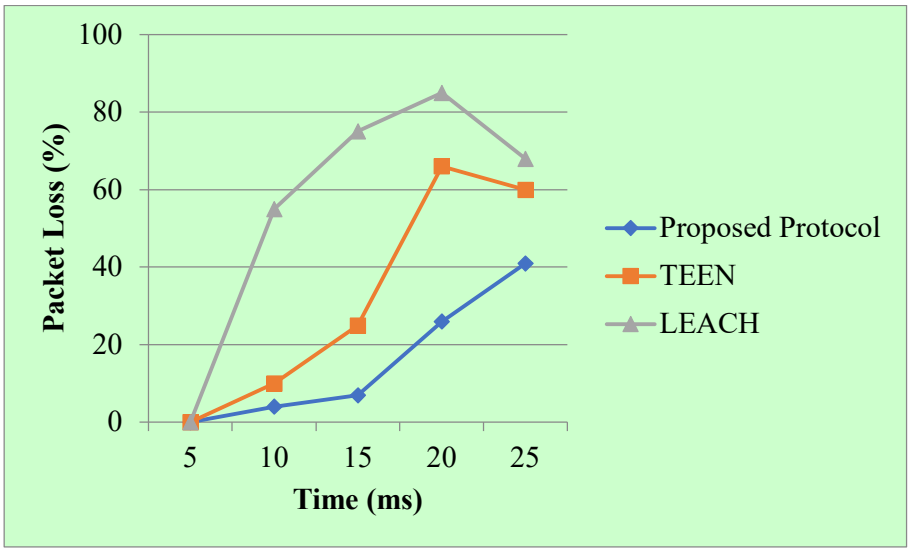

Figure 7(e) Packet loss comparison analysis

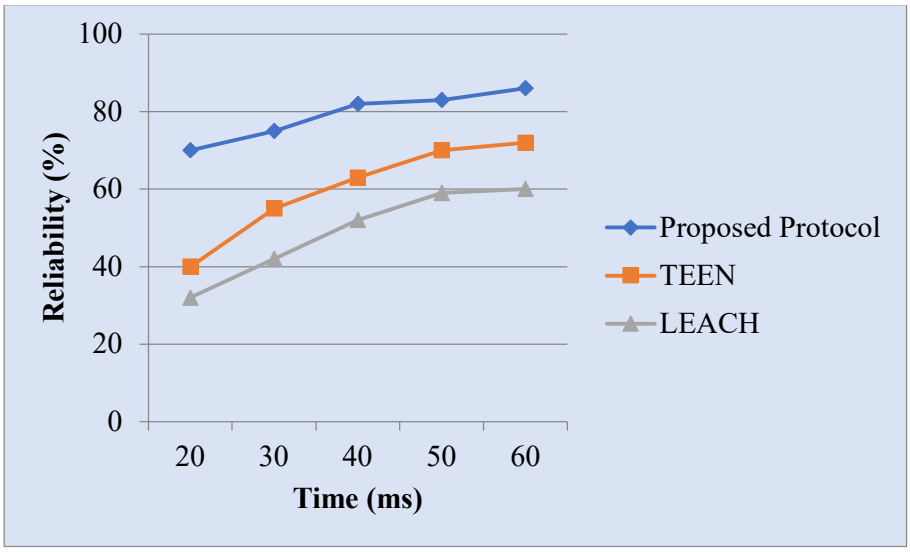

Figure 7(f) Reliability comparison analysis

After simulating and evaluating, we observed that the proposed protocol has less energy consumption, more throughput, less network delay, good packet delivery with minimal packet loss and more reliable compared to TEEN and LEACH hierarchical routing protocols.

V. CONCLUSION

Wireless Sensor Networks (WSNs) have quickly established themselves as a leading network of intelligent and small computenodes for building a stable, flexible, and robust network. Providing defense in such networks is both crucial and complex. In this paper, We discussed the architecture, security services, design issues, security challenges, attacks, and routing protocols of wireless sensor networks. Also designed a reliable and energy-efficient protocol for routing in wireless sensor network environment. Our proposed protocol is efficient and reliable compared to other hierarchical routing algorithms like TEEN and LEACH.

References

1. Salehi, S. Ahmad, et al. "Security in wireless sensor networks: Issues and challanges." *2013 IEEE International Conference on Space Science and Communication (IconSpace)*. IEEE, 2013.
2. Riad, A. M., Hamdy K. El-Minir, and Mohamed El-hoseny. "Secure routing in wireless sensor networks: a state of the art." *International Journal of Computer Applications* 67.7 (2013).
3. Dinker, Aarti Gautam, and Vidushi Sharma. "Attacks and challenges in wireless sensor networks." *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2016.
4. Hassan, Abdalraouf, and Christian Bach. "Improving security connection in wireless sensor networks." *International Journal of Innovation and Scientific Research* 2.2 (2014): 301-307.
5. Ishmanov, Farruh, and Yousaf Bin Zikria. "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues." *Journal of Sensors* 2017 (2017).
6. Yang, Tao, et al. "A secure routing of wireless sensor networks based on trust evaluation model." *Procedia computer science* 131 (2018): 1156-1163.
7. Kumar, Vikash, Anshu Jain, and P. N. Barwal. "Wireless sensor networks: security issues, challenges and solutions." *International Journal of Information and Computation Technology (IJICT)* 4.8 (2014): 859-868.
8. Rajput, Monali, and Usama Ghawte. "Security challenges in wireless sensor networks." *Int. J. Comput. Appl* 168 (2017): 24-29.
9. Tripathi, Khushboo, Manjusha Pandey, and Shekhar Verma. "Comparison of reactive and proactive routing protocols for different mobility conditions in WSN." *Proceedings of the 2011 International Conference on communication, computing & security*. 2011.
10. Udhayamoorthi, M., et al. "An analysis of various attacks in manet." *International Journal of Computer Science and Mobile Computing* 7 (2014): 883-887.
11. Kamat, Pandurang, et al. "Enhancing source-location privacy in sensor network routing." *25th IEEE international conference on distributed computing systems (ICDCS'05)*. IEEE, 2005.
12. Mottola, Luca, and Gian Pietro Picco. "Programming wireless sensor networks: Fundamental concepts and state of the art." *ACM Computing Surveys (CSUR)* 43.3 (2011): 1-51.
13. Elsts, Atis, and Leo Selavo. "A user-centric approach to wireless sensor network programming languages." *2012 Third International Workshop on Software Engineering for Sensor Network Applications (SESENA)*. IEEE, 2012.
14. Sarkar, Amit, and T. Senthil Murugan. "Routing protocols for wireless sensor networks: What the literature says?." *Alexandria Engineering Journal* 55.4 (2016): 3173-3183.
15. Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." *Ad hoc networks* 3.3 (2005): 325-349.
16. Singh, Shio Kumar, M. P. Singh, and Dharmendra K. Singh. "Routing protocols in wireless sensor networks–A survey." *International Journal of Computer Science & Engineering Survey (IJCSES)* 1.2 (2010): 63-83.

17. García Villalba, Luis Javier, et al. "Routing protocols in wireless sensor networks." *Sensors* 9.11 (2009): 8399-8421.
18. Goyal, Deepak, and Malay Ranjan Tripathy. "Routing protocols in wireless sensor networks: A survey." *2012 Second International Conference on Advanced Computing & Communication Technologies*. IEEE, 2012.
19. Pantazis, Nikolaos A., Stefanos A. Nikolidakis, and Dimitrios D. Vergados. "Energy-efficient routing protocols in wireless sensor networks: A survey." *IEEE Communications surveys & tutorials* 15.2 (2012): 551-591.
20. Biradar, Rajashree V., et al. "Classification and comparison of routing protocols in wireless sensor networks." *Special Issue on Ubiquitous Computing Security Systems* 4.2 (2009): 704-711.
21. Singh, Santar Pal, and S. C. Sharma. "A survey on cluster based routing protocols in wireless sensor networks." *Procedia computer science* 45 (2015): 687-695.
22. Shabbir, Noman, et al. "Routing protocols for small scale WLAN based Wireless Sensor Networks (WSNs)." *2015 9th International Conference on Sensing Technology (ICST)*. IEEE, 2015.
23. Rani, D. R., Kumar, B. S., Rao, L. T. R., Jagadish, V. S., & Pradeep, M. (2012). Web security by preventing sql injection using encryption in stored procedures.