Secure Routing Protocol In Wireless Sensor Networks: A Survey

T.G. Ganga[1], R. Roseline[2]
[1]Dept of Computer Science
[2]Associate Professor and Head, Dept of Computer Science
[1, 2] Government Arts College, Coimbatore

Abstract*- Due to its wide application, the use of wireless sensor networks (WSNs) is now increasing for a day. The WSNs are capable of reconfiguration, unlike standard networks, whenever there is a defect in the network. However, because of its lack of security, data loss occurs during routing in these networks. With the help of routing protocols, network communication is initialized and achieved. A routing protocol is a collection of rules that govern the phenomenon of routing. Because of their excessive scope of improvement, WSN protocols for routing have been the researchers' omnipresent choice in recent years. A routing protocol aims to search for an appropriate route between sender and recipient to achieve successful transmission at the destination. One of the main points of research gaps has always been the dissipation of energy and the lengthening network duration. Because a battery operates the nodes in WSNs, they can only use limited energy to continue communication and transmission. Several researchers have come up with developments in energy efficiency and WSN routing protocols to cope with this. In this paper, a reify summary of some protocols for routing purposes has been manifested.*

Keywords- Routing Protocols, WSN, Sensor node

I. INTRODUCTION

WSN is widely used in various applications, such as monitoring of habitats and structural health. In particular, it is possible to classify routing protocols for ad hoc networks into three Types, based on the mechanism for updating the routing information. The reactive protocol, proactive, and hybrid protocol[1] are the three types. Despite all these outcomes, WSNs are highly susceptible to ultimatum security, energy constraints, and malicious node impingement. In sensor networks, camouflaged malicious nodes can seriously distort the normal functioning of wireless sensors' networks. Once the malicious nodes initiate the attack, it is difficult to identify the incursions. Sensory nodes are battery-powered nodes protected by a restricted-energy resource[2] and are demanding requirements when considering network design. There are a large number of security vulnerabilities in WSNs that are responsible for many types of attacks. These attacks are primarily focused on the routing layer, which can sometimes lead to paralysis. To protect routing and WSNs[3], it is essential to design effective security routing protocols. In an open, collaborative, and too random environment, the wireless sensor network operates.

Consequently, it has features such as self-organization, dynamic topology, random movement, limited resources, etc. There are many security loopholes in the network itself, which lead to a variety of attack types. Most attacks are focused on the routing layer, leading to paralysis of the entire network in severe cases. Therefore, the security of wireless sensor network security routing is an essential guide for research [6].

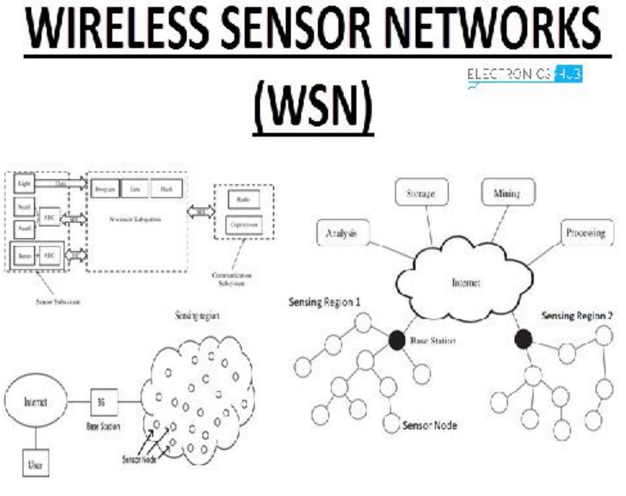


Figure 1: WSN Architecture Diagram

Due to the severe energy constraints of large numbers of densely deployed sensor nodes, the implementation of different network control and management functions such as synchronization, node localization, and network security requires a network protocol suite. There are several shortcomings in the traditional routing protocols when applied to WSNs, mainly due to such networks' energy-restricted nature [4]. For example, flooding is a technique in which a given node transmits the data and control packets it has received to the rest of the network nodes.

This process is repeated until it reaches the destination node. Note that the energy constraints imposed by WSNs are not taken into account in this technique. Consequently, it leads to implosion and overlap [2] when used for data routing in WSNs. Because flooding is a blind technique, duplicated packets can keep the network in circulation, and sensors will receive those duplicated packets, causing a problem with the implosion. When two sensors sense the same region and simultaneously transmit their sensed data, their neighbors will receive duplicated packets. Another technique known as gossiping can be applied to overcome the shortcomings of flooding [8]. A sensor would randomly select one of its neighbors when gossiping, receiving a packet, and sending it. The same process is repeated until all the sensors receive this packet. Using gossip, only one copy of the packet being sent would be received by a given sensor. There is a significant delay for a packet to reach all sensors in a network, while gossiping addresses the problem of implosion.

II. BACKGROUND STUDY

Bhat, P. et al.[2] The detection of malicious nodes in wireless sensor networks and energy was performed through secure load balance clustering and reliable multipath node-disjoint routing technique. The basic idea is to balance the node's remaining energy and confidence value to select secured primary and secondary backup cluster head nodes to balance the load between clusters that increase the network's lifetime. Security is also integrated by analyzing the behavior of nodes within a cluster. Suppose all information has been dropped by a node, which implies that a node has been compromised or is malicious. Energy utilization is distributed between the cluster heads in the proposed algorithm, making it work longer than the single-cluster head cluster. The secondary cluster head also continues to operate in the event of primary cluster head failure due to energy depletion without affecting the sensor network's topology, thus maximizing the network's life.

Karthick, S. et al. [4] Security of information is the most concentrated problem in every network system, a challenging task in the case of WSNs. The security of the WSN can be achieved through proper routing, so a novel routing protocol is proposed in this paper. Topology management is initially carried out in the proposed protocol using an enhanced k-means algorithm. Then, each node's fitness is calculated by sending and receiving a set of sample packets (or hello packets). The ratio of receiving to transmitting is denoted as the ability to trust or the fitness of a node. A grade for each node is defined based on this fitness, which is similar to the ranking of nodes in the range of five. Finally, depending on the grade of the node, the most appropriate path for transmission is selected.

Nandhini, M. et al. [5], users can easily monitor the environmental factors in many application fields. Here, we can recover the network from the loss of connections quickly. Thus, users can improve the network's lifetime, and the drop in packets should be minimized. The firefly algorithm in this paper helps to find optimal routes for secure data transmission. It satisfies the tradeoff between the lifetime of energy and the network. The selection of the cluster head results in power consumption and time delays in the wireless environment.

Shi, Q. et al. [6] In this protocol, malicious nodes are added through the tabu table's authentication mechanism. Creditworthiness is determined by the packet loss rate, energy, and time delay of connection as an ant colony optimization control factor in the improved QoS algorithm based on Aco.

Shinde, M. et al. [7] Security is the most challenging problem for WSN. This paper examined different types of attacks during routing in most security problems, secure routing, and also some recent solutions to provide secure routing. This paper concentrates on the attack on the black hole and selective forwarding. The system uses the updated active trust system and data routing system to detect and prevent such attacks, along with data type checking during routing to detect and prevent such attacks. The system also improves data privacy by encrypting it using the ECC algorithm before the actual routing starts. Experimental results show that the proposed system is better than the existing one in security, reliable routing, and network lifetime and energy consumption.

Wei, L. et al. [8] We put forward a trust-based secure routing algorithm for the weak resistance of general secure routing protocols for internal malicious nodes by improving the evidence theory to decrease the computational complexity of the degree of trust. For the routing selection, the confidence degree is then used. This algorithm can efficiently resolve the problems caused by internal malicious nodes from simulation results, providing reliable data transmission. However, energy consumption upgrades are due to the implementation of the trust management mechanism. Therefore, the next step for us is to improve the routing protocol based on trust and develop an effective routing algorithm suitable for WSNs.

III. SECURE ROUTING PROTOCOLS

Energy-Aware QoS Routing Protocol: Real-time traffic is generated through imaging sensors in this QoS conscious protocol for sensor networks. The proposed protocol extends the routing approach and finds a path that meets unavoidable end-to-end delays during the less expensive and energy-efficient connection. The link's cost is a function that captures the nodes' energy reserve, transmission energy, error rate, and other parameters of communication. A class-based queuing model is used to support both the best effort and real-time traffic at the same time.

Sequential Assignment Routing (SAR): SAR is one of the first routing protocols for WSNs to introduce the concept of QoS in routing decisions. It is a multipath table-driven approach that strives to achieve energy efficiency and tolerance for fault. Three factors depend on the routing decision for SAR: energy resources, QoS on each path, and the priority level of each packet. By taking into account the QoS metric, the energy resource on each path, and each packet's priority level, the SAR protocol generates trees rooted in one-hop neighbors of the sink. Several paths from the sink to sensors are formed through the use of created trees. Following the energy resources and QoS on the path, one of these paths is selected.

Sensor Protocols for Information via Negotiation (SPIN): The SPIN protocol was designed to enhance conventional flooding protocols and to overcome, for example, implosion and overlap issues. The SPIN protocols are conscious of resources and adaptive to resources. The sensors that operate the SPIN protocols can calculate the energy consumption required for the network to compute, send, and receive data. They can, therefore, make informed choices to make efficient use of their resources.

Directed Diffusion: A data-centered routing protocol for the dissemination and processing of sensor queries is directed diffusion. It meets the main requirements of WSNs, such as energy efficiency, robustness, and scalability. There are several key dissemination elements: data naming, interests and gradients, data propagation, and strengthening.

Energy-Aware Data-Centric Routing (EAD): EAD is a new distributed routing protocol that creates a virtual backbone of active sensors responsible for processing in-network data and traffic transmission. A network is represented in this protocol by a broadcast tree spanning all the sensors in the network and rooted at the gateway in which the radios of all leaf nodes are switched off. In contrast, all other nodes correspond to the active sensors forming the backbone and are therefore switched on by their radios. There are different protocols for routing

1) Proactive Protocols:

Each node has final data concerning the entire topology of the system in this convention. If any progression occurs in the system's topology, then the guiding tables are naturally upgraded, and these overhauled parcels must be transmitted throughout the system.

2) Reactive Protocols as follows:

In this kind of routing protocol, every node in a system finds or keeps up a course in the light of interest. While finding a study, it surges a control message by globally communicating, and when course is found, then transfer speed is used for the transmission of information.

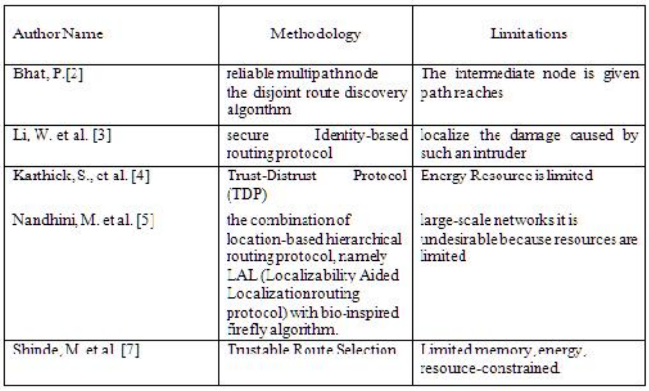
3) Hybrid Protocols, as follows:

This convention is a blend of conventions that are proactive and reactive. These conventions are intended for a system of substance. It maintains the movement stack over the system, and every node must have a predefined zone known as a group.

IV. COMPARATIVE ANALYSIS OF SURVEY

Normally the proposed sort is made by considering the various drawbacks of the present framework's organization correspondence.

Table 1: Evaluation of various authors' views.



Author Name	Methodology	Limitations
Bhat, P.[2]	reliable multipathnode the disjoint route discovery algorithm	The intermediate node is given pathreaches
Li, W. et al. [3]	secure Identity-based routing protocol	localize the damage caused by such an intruder
Karthick, S., et al. [4] Nandhini, M. et al. [5]	Trust-Distrust Protocol (TDP) the combination of location-based hierarchical routing protocol, namely LAL (Localizability Aided Localizationrouting protocol) with bio-inspired firefly algorithm.	Energy Resource is limited large-scale networks it is undesirable because resources are limited
Shinde, M. et al. [7]	Trustable Route Selection	Limited memory, energy, resource-constrained

IV. DISCUSSION

Limited energy capacity: Since batteries power sensor nodes, they have limited energy capacity. For example, in hostile environments, a battlefield where it is impossible to access the sensors and recharge their batteries, energy poses a big challenge for network designers. Besides, the sensor will become defective when a sensor's energy reaches a certain threshold and will not function properly, which will significantly impact the network's performance. Routing protocols designed for sensors should be as energy-efficient as possible to extend their lifetime and thus prolong the network's lifetime while guaranteeing overall good performance.

Sensor locations: Managing the locations of the sensors is another challenge facing the construction of routing protocols. Most of the proposed protocols assume that the sensors are either equipped with global positioning system (GPS) receivers or can learn about their locations using some localization technique.

Limited hardware resources: Sensor nodes also have limited processing and storage capabilities and limited energy capacity and can only perform limited computational functionalities. In software development and network protocol design for sensor networks, these hardware constraints present many challenges that must consider the energy constraints of sensor nodes and the processing and storage capabilities of sensor nodes.

Massive and random node deployment: The deployment of sensor nodes in WSNs is dependent on the application and can be either manual or random, which ultimately affects the routing protocol performance. Sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region in most applications. If the resulting distribution of nodes is not uniform, optimal clustering is necessary to enable connectivity and enable the network's energy efficiency.

Network characteristics and unreliable environment: In a dynamic and unpredictable environment, a sensor network typically operates. The network topology, which is defined by the sensors due to sensor addition, deletion, node failure, damage, or energy depletion, frequently changes the sensors' communication links. The sensor nodes are also linked by a wireless medium, noisy, prone to errors, and various time. Therefore, because of limited energy and sensor mobility, routing paths should consider network topology dynamics and increase the network's size to maintain specific application requirements in terms of coverage and connectivity.

Aggregation of data: Since sensor nodes can generate significant, redundant data, it is possible to aggregate similar packets from multiple nodes to reduce transmissions. Data aggregation technique has been used in several routing protocols to achieve energy efficiency and data transfer optimization.

V. CONCLUSION

Security in the WSN is currently an active research area that has attracted a great deal of attention due to the rapid growth of WSN applications. The ultimate goal behind the routing protocol's design is to keep the sensors operating for as long as possible, thus extending the network's lifetime. The transmission and reception of data dominate the energy consumption of the sensors. Routing protocols designed for WSNs should be as energy-efficient as possible to prolong the individual sensors' lifetime, thus the lifetime of the network. This paper considers several classification criteria, including location information, network layering, and in-network processing, data centricity, path redundancy, network dynamics, QoS requirements, and heterogeneity of the network; we surveyed a sample of routing protocols. We have discussed a couple of example protocols for each of these categories.

REFERENCES

[1] AlMansour, N., &Alahmadi, S. (2018). Secure Ad Hoc On-Demand Distance Vector Routing Protocol in WSN. 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). doi:10.1109/cais.2018.8441991.

[2] Bhat, P., & Reddy, K. S. (2015). Energy efficient detection of malicious nodes using secure clustering with load balance and reliable node disjoint multipath routing in Wireless Sensor Networks.2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI). doi:10.1109/icacci.2015.7275734

[3] Li, W., Li, H., Xie, M., & Bu, S. (2011). An Identity-based Secure Routing Protocol in WSNs. 2011 Seventh International Conference on Computational Intelligence and Security. doi:10.1109/cis.2011.160

[4] Karthick, S., Devi, E. S., &Nagarajan, R. V. (2017). Trust-distrust protocol for the secure routing in wireless sensor networks.2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET). doi:10.1109/icammaet.2017.8186688

[5] Nandhini, M., &Priya, P. (2017). A hybrid routing algorithm for secure environmental monitoring system in WSN.2017 International Conference on Communication and Signal Processing (ICCSP). doi:10.1109/iccsp.2017.8286537

[6] Shi, Q., & Li, Z. (2013). A Secure QoS Routing Algorithm Based on ACO for Wireless Sensor Network. 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013

IEEE International Conference on Embedded and Ubiquitous
Computing. doi:10.1109/hpcc.and.euc.2013.176

[7] Shinde, M., &Mehetre, D. C. (2017). Black Hole and Selective Forwarding Attack Detection and Prevention in WSN.2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). doi:10.1109/iccubea.2017.8463929

[8] Wei, L., Qing, Y., & Nan, Y. (2015). A trust-based secure routing algorithm for wireless sensor networks.2015 34th Chinese Control Conference (CCC). doi:10.1109/chicc.2015.7260866