International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 6, Nov-Dec-2021, ISSN (Online): 2395-566X

Survey Paper on Security against Dynamic Routing in Wireless Sensor Networks and Internet

M. Tech. Scholar Md Abid Hussain, Assistant Professor Mr. Manish Sahu
Department of Electronics and Communication,
SORT, People's University,
Bhopal, India

Abstract- Wireless sensor networks (WSNs) have been identified as one of the most innovative application of technologies in the 21stcentury. The small sized, low cost and low power sensors nodes are designed to communicate within a short range and work together to form a sensor network to gather data from a field.Cluster-based routing protocol is well known for enhancing the lifetime in WSN. Low Energy Adaptive Cluster Hierarchy (LEACH) protocol is one of the foremost and prominent protocols in the category of hierarchical protocols that enhanced the network lifetime by reducing and distributing the energy consumption among the nodes in a network. In this paper is studied of wireless sensor network based on fuzzy system. To improvement is lifetime of network with the help of fuzzy system.

Keywords- Wireless Sensor Network, Cluster Head, Fuzzy System.

I. INTRODUCTION

The recent advancements in the technology and manufacturing of small and low-cost sensors have made application of these sensors technically and economically feasible. These sensor nodes are designed to possess certain sensing, computing and wireless communication capabilities. These sensors measure ambient conditions in the environment surrounding them and then convert these measurements into signals that can be processed to reveal some information about phenomena located in the area around these sensors.

A large number of these sensors can be networked in many applications that require unattended operations, hence creating a wireless sensor network (WSN). One of the advantages of wireless sensors networks(WSNs) is their ability to operate unattended in harsh environments in which present-day human monitoring schemes are risky, inefficient and sometimes in feasible.

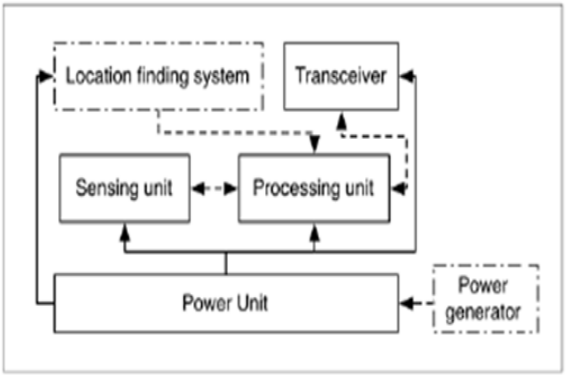

Fig 1. Functional blocks in a Sensor Node.

Typically, WSNs contain hundreds or thousands of these sensor nodes, and these sensors have the ability to communicate either among each other or directly to an external base station (BS). A greater number of sensors allow sensing over larger geographical regions with greater accuracy. Figure 1 shows a schematic diagram of sensor node components [1].

Basically, each sensor node comprises of sensing, processing, transmission, power units and optional units like location finding system. Sensor nodes are usually scattered in a sensor field in an area where the monitoring is required. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources [2].

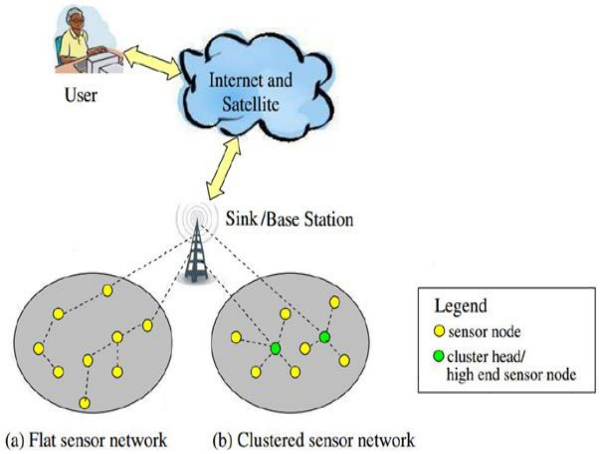

Fig 2. Architecture and operation of WSN.

Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external BS(s). A BS may be a fixed or mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data. Figure 2 shows the architecture of WSN with flat & hierarchical topology.

II. DESIGN ISSUE OF WIRELESS SENSOR NETWORK

Despite the numerous applications of WSNs, these networks have several constraints, such as limited energy supply, limited computing power, and limited bandwidth in the wireless linkage between the connecting sensor nodes. One of the main design goals of WSNs is to carry out data communication from sensing field to base station, while trying to prolong the lifetime of the network and prevent connectivity degradation by employing severe energy management techniques.

The design of routing protocols in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs. Some of the routing challenges and design issues that affect routing process in WSNs are:

1. Deployment of Nodes:
Node deployment in WSNs is application dependent and it affects the performance of the routing protocol. The deployment can be either predetermined or random in nature. In pre-determined deployment, the sensors are placed manually and data is routed through pre-determined paths. However, in random deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad-hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation with routing through multi-hop communication [6].

2. Energy Consumption:
Sensor nodes use up their limited supply of energy performing computations and transmitting information in a wireless environment. Sensor node lifetime is strongly dependent on the battery capacity. In a multi-hop WSN, each node plays a dual role as data sender and data router. The depletion of energy of a specific node may lead to malfunctioning and can further cause significant topological changes and sometimes, require rerouting of packets and reorganization of the network.

3. Data Reporting:
Data sensing and reporting in WSNs is the main purpose of its application. Data reporting varies with the application and its time criticality. Data reporting can be categorized as time-driven(continuous), event-driven (upon occurrence of an event), query-driven (query from the user), and hybrid. The design of the routing protocol is highly influenced by the data reporting model [7].

4. Fault Tolerance:
Some sensor nodes may fail due to depletion of energy, physical damage, or environmental interference. The failure of such sensor nodes may lead to overall malfunction of the sensor network. In the event of node failures, routing protocols must configure to re-establish new links and routes to send the data to base stations without any disruption. This may require active adjustment of transmission power and data rates on the existing links to reduce energy consumption, or reroute packets through regions of the network where more energy is available.

5. Node Heterogeneity:
In several studies, it is assumed that all sensor nodes are homogeneous, i.e., having equal capacity in terms of computation, communication, and power. However, depending on the application, sensor nodes can have different role or capability. The existence of heterogeneous set of sensors can mitigate the burden of transmission of data to the BS. For example, hierarchical protocols designate a cluster-head node different from the normal sensors. These cluster heads can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth, and memory [8].

6. Scalability:
The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Thus, routing scheme must be able to work with any number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to dynamic changes in the environment.

7. Network Dynamics:
In most of the applications, the sensor nodes in a network are assumed to be stationary. However, some applications demand mobility of either BS‟s or sensor nodes (Ye et al 2002). Routing messages from or to moving nodes is more challenging since maintenance of route stability and network topology becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., detection of moving target or forest monitoring for early fire prevention. Monitoring of static events generates traffic only when reporting and dynamic events require periodic reporting, and generate significant traffic in the network [9].

8. Quality of Service:
In some applications, quality of the data delivered might be more important. In such cases, the delivery of data within the stipulated time is very essential or otherwise the data will be deemed useless. In time constrained

applications, confined latency for data delivery is another condition. In general, many applications of WSN demand conservation of energy rather than the quality of data sent, in order to extend the network lifetime. As the energy gets depleted in sensor nodes, the quality of the data is compromised to obtain the reduction in energy dissipation in the nodes [10].

III. LITERATURE REVIEW

Na Wang et al. [1], in wireless sensor networks, it is common that adversaries capture some nodes to intercept, tamper, or drop valuable packages. We can employ reputation systems to identify the compromised nodes (CNs). In this paper, the areas that cover a set of dense CNs are called compromised regions (CRs) and apparently, they are a greater threat to the networks than single CNs. To defend against the attack of CRs, we design a secure shortest path routing algorithm (SPRA) to deliver packages properly around, rather than through, the CRs.

Specifically, a source node first computes the shortest geometric path to the sink node without crossing any CRs and then decides agent nodes along with the path by a set of virtual locations in an indirect way. At last, a sophisticated mechanism is designed based on geographic information to guarantee that the packages can be delivered in a relay manner between the agent nodes until they are transmitted to the sink node successfully.

M. Bheemalingaiah et al. [2], is used power-aware Node-disjoint Multipath Source Routing (PNDMSR) to execute and break down its execution with particular to Multipath Dynamic Source Routing (MDSR) by utilizing different quantitative execution measurements like, directing control overhead, throughput, packet delivery ratio, packet loss and energy efficiency by shifting different parameters like system's size, versatility of hub, delay time, information rate and load .The fundamental target of the PNDMSR is selecting energy aware node disjoint multipath from source to destination by enhancing the overhead utilizing node's cost and it increase the system of lifetime.

DoganYildiz et al. [3], in this paper, statisticulated social network routing (SSNR) and Obfuscated social network routing (OSNR) were used. In SSNR the friends list is modified by adding or removing nodes for each message transmission. Hence it is not easy for a node to identify the original friends list of a sender by just interpreting a single message. In OSNR the friends list of source node is embedded in a bloom filter.

Alexandros Ladas et al. [4], is used self-reported social networks (SRSNs) are used to collect social network data. These SRSNs are utilised to provide reputation for every member node. As the network initialises, the nodes are assigned higher trust values by SRSN. By tracking the history of encounters, selfishness is analysed. This might also include special scenarios where a node might have become power deficient which had resulted in such non-cooperative behaviour. Once a node is detected as selfish the detecting node decrements the value of selfish node by a behaviour constant.

Pengwu Wan et al. [5], in this paper**,** the efficiency of caching protocols lies truly in the selection of sensor nodes which will take special roles in running the caching and request forwarding decisions. For efficient caching, cache discovery, cache admission control, cache consistency and cache data replacement are essential.

Mohammadi K et al. [6], is used global cluster cooperation scheme (GCCS) for caching in wireless sensor networks. WSNs have a finite limited amount of cache and therefore a new replacement policy, called Frequency-Based-First In First Out (FB-FIFO) which outperforms both Least Recently Used (LRU) and First In First Out (FIFO). The fundamental challenge lies in maintaining the cache freshness. The reason is mainly due to the disrupting network connectivity followed by lack of information about cached data.

Miriam Carlos-Mancilla et al. [7], in this paper**,** mainly focuses on how the underlying heterogeneity structure of mobile nodes' contact dynamics impacts the performance of epidemic routing algorithm. The mobility models exploit the heterogeneity in contact rate between the nodes. The two mobility models are Individually Heterogeneous Network Model and Spatially Heterogeneous Network Model (SHNM).

In the Individually Heterogeneous Network Model (IHNM) the heterogeneity is characterized by allowing different contact rates for different node pairs in different groups. In the spatially heterogeneous network model the heterogeneity arises on each spatial cluster (site) in which mobile nodes reside, while they can move to other spatial clusters.

Park S. Y. et al. [8], proposed that Minimum Cost Forwarding Algorithm (MCFA) is another routing protocol for Wireless Sensor Network that exploits the fact that the direction of routing is always known and it is towards the fixed external Base Station. The sensor nodes need not have a unique ID or they do not need to maintain routing tables. Each sensor node maintains the least cost estimate from itself in order to reach the Base Station.

Whenever a sensor node has packets to forward to the Base Station, it broadcasts to its neighbours. After a node receives the packet, it checks if it is on the least cost route between the source sensor node and the Base Station. If it is so, the receiving node rebroadcasts the packet to its neighbours.

IV. METHODOLOGY

The Dynamic cluster head selection algorithm (D-LEACH) is a modified version of the LEACH protocol and it considers the residual energy available in the nodes before cluster head selection process is initiated in LEACH. The cluster heads are selected from the set of given nodes N based on probability in the first round and at the end of first round, the residual energy available in the cluster heads are compared with a threshold value.

If cluster heads are found to have energy above the threshold, the cluster head selection process is ignored and the existing cluster heads are allowed to continue as cluster head with the same member nodes in the next round. The whole process is repeated until the end of all rounds.

This D-LEACH algorithm reduces the number of cluster heads selected and thereby reduced overhead in selection process and minimized energy dissipation in all nodes. The Dynamic cluster head selection algorithm is shown in Figure 3.

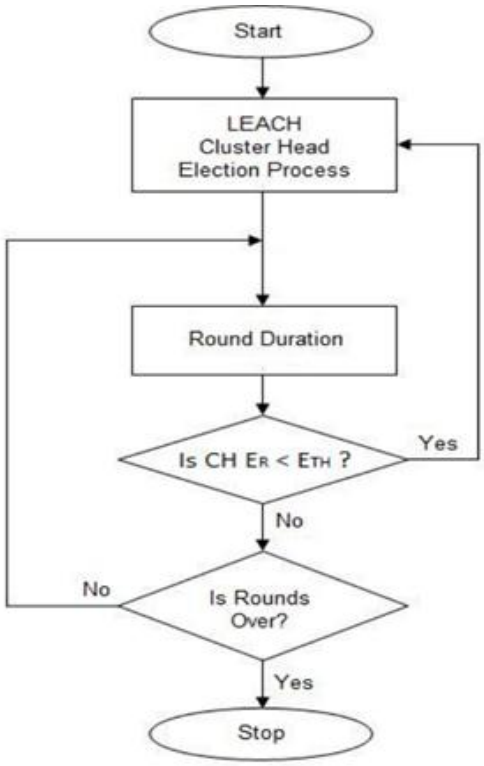

Fig 3. Dynamic Cluster Head Election Algorithm

1. Fuzzy System:
The Fuzzy Logic Algorithm is illuminated by the powerful capability of fuzzy logic system to handle uncertainty and ambiguity. Fuzzy logic system is well known as model free. Their membership functions are not based on statistical distributions. In this paper, we apply fuzzy logic system to optimize the routing process by some criterion. The main goal is designing the algorithm to use Fuzzy Logic Systems to lengthen the lifetime of the sensor networks.

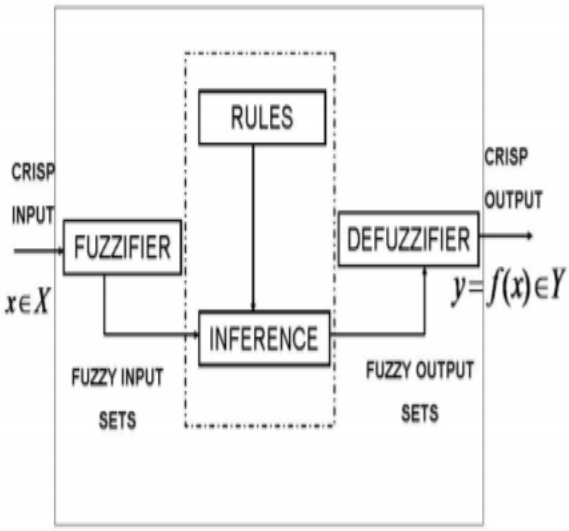

Fig 4. The structure of a fuzzy logic system.

The process of finding the optimal path, and broadcasting it in the network and sending data from all nodes to the base station by following this routing schedule is repeated in every round. Computation of routing schedule is done dynamically with the consideration of current level of some criteria of each node.

For this, normally it may require the nodes to report their criteria periodically to the base station. The base station can then determine the routing schedule based on this updated information.

The proposed method assumes that:

- All sensor nodes are randomly distributed in the area and every sensor node is assumed to know its own position as well as that of its neighbors and the sink;
- All sensor nodes have the same maximum transmission range and the same amount of initial energy.

2. Fuzzy Set Operations:
In crisp set theory we have the concepts of union and intersection of two sets. This concept should be extended to fuzzy sets. Also the concept of complement of a set in crisp set theory should be extended to fuzzy sets.

Definition: Let A and B be two fuzzy sets on a nonempty set X. The union of A and B denoted as AUB is defined as

$$\mu_{AUB}(x) = \max$$

Where μ_{AUB} is the membership function of AUB is map from X to [0, 1]. Hence AUB is a fuzzy set on X. This is called the standard union of two fuzzy sets.

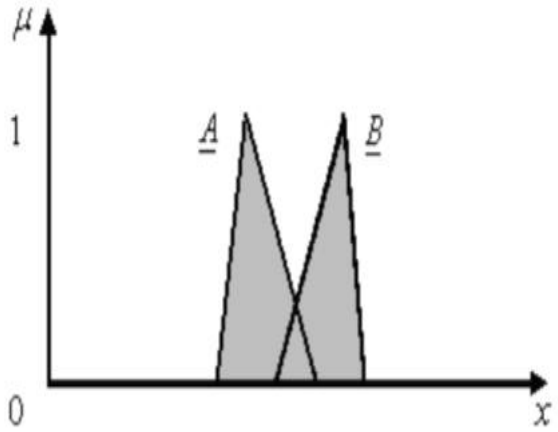

Fig 5. Union of Fuzzy Sets A and B.

Definition: Let A and B be two fuzzy sets on a nonempty set X. The intersection of A and B denoted as A ∩B is defined by

$$\mu_{A\cap B}(x) = \min$$

Where $\mu_{A\cap B}$ is the membership function of A ∩ B is fuzzy set on X. This is called the standard intersection of two fuzzy sets.

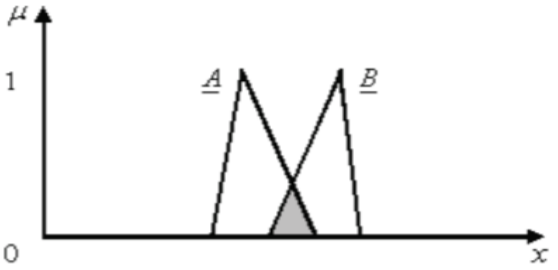

Fig 6. Intersection of Fuzzy sets A and B.

V. CONCLUSION

In this paper, the study of an energy efficient multipath routing protocol for WSN. This protocol is designed to decrease the routing overhead, improve the latency and packet delivery ratio and through discovering multiple paths from the source to the destination. It has a sink initiated Route Discovery process with the location information of the source known to the sink.

There are two types of nodes which are used here one is primary and the other is alternate. At the end of the route formation one primary path and multiple alternate paths are built and all nodes except the primary paths nodes are put to sleep mode which helps us to save energy and generate a collision free environment, the primary path is used to transmit the data from source to the sink and if the route disrupts, the next best alternate routeis used for the purpose and if no path exists between the source and destination thenthe route discovery algorithm calls.

REFERENCE

[1] Na Wang and Jian Li, “Shortest Path Routing With Risk Control for Compromised Wireless Sensor Networks”, Received January 12, 2019, accepted January 31, 2019, date of publication February 7, 2019, date of current version February 22, 2019.

[2] M. Bheemalingaiah and M. M. Naidu, “Performance Analysis of Power -aware Node-disjoint Multipath Source Routing in Mobile Ad Hoc Networks”, IEEE 7th International Advance Computing Conference, PP. No. 361-371, IEEE 2017.

[3] DoganYildiz, SerapKaragol and OkanOzgonenel, “A Hyperbolic Location Algorithm for Various Distributions of a Wireless Sensor Networks, Smart Grid and Cities Congress and Fair (ICSG), 5th International Istanbul, PP. No. 451-459, IEEE 2016.

[4] Alexandros Ladas, Nikolaos Pavlatos, NuwanWeerasinghe and Christos Politis, “Multipath Routing Approach to Enhance Resiliency and Scalability in Ad-hoc Networks, Ad-hoc and Sensor Networking Symposium, PP. No. 01-06, IEEE 2016.

[5] Pengwu Wan, Benjian Hao, Zan Li, Licun Zhou, Mian Zhang, "Time differences of arrival estimation of mixed interference signals using blind source separation based on wireless sensor networks", IET Signal Processing, vol.10, issue 8, pp.924-929, 2016.

[6] Mohammadi K., Alavi O., Mostafaeipour A., Goudarzi N. And Jalilv and M., "Assessing different parameters estimation methods ofWeibull distribution to compute wind power density", ELSE VIER Energy Conversion and Management Journal, Vol.108, pp. 322-335, 2016.

[7] Miriam Carlos-Mancilla, Ernesto López-Mellado, and Mario Siller,“Wireless Sensor Networks Formation: Approaches and Techniques,” Journal of Sensors, vol. 2016, Article ID 2081902, 18pages, 2016.

[8] Park S. Y. and Lee J. J., "Stochastic Opposition-Based Learning Usinga Beta Distribution in Differential Evolution", IEEE Transactions On Cybernetics, vol. 46, Number 10, pp.2184-2194, October 2016.

[9] Osama Ennasr, Guoliang Xing and Xiaobo Tan, " Distributed Time-Difference-of-Arrival (TDOA)-based Localization of a Moving Target", in Proc. IEEE 55th Conference on Decision andControl (CDC), pp. 2652-2658, IEEE 2016.

[10] Santar Pal Singh, S.C. Sharma, "Range-Free Localization Techniquesin Wireless Sensor Networks: A Review", in Proc. 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), vol.57, pp. 7 – 16, 2015.

[11] Yildiz D., Karagol S., Ozgonenel O., Tadiparthi S., Bikdash M."ANovel Self Localization Approach for Sensors", Sensor Signal Processing for Defense (SSPD), Edinburgh, Scotland, 2015.
[12] P. Fazio, M. Tropea, S. Marano, "A distributed hand-over management and pattern prediction algorithm for wireless networks with mobile hosts," 9th International Wireless Communications and Mobile Computing Conference, IWCMC, pp. 294-298, IEEE 2013.