International Journal of Recent Trends in Engineering & Research (IJRTER)
Conference on Electronics, Information and Communication Systems (CELICS'17)
Special Issue; March - 2017 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

CLUSTER BASED SECURE ROUTING FOR MOBILE SINK IN WIRELESS SENSOR NETWORKS

Mr. S. Gladwin Moses[1], Priyanka. T[2], Rubavathy Rachel. R[3], Vinumala. K[4]
[1]Professor, [2,3,4,5]Student Members
Department of Electronics and Communication Engineering,
Akshaya College of Engineering and Technology

ABSTRACT

In wireless sensor networks (WSNs), the mobile sink is used in order to prolong the network lifetime. In physical environments, all kinds of obstacles could exit in the sensing field. Mobile sink starts the data-gathering route periodically from the starting site, then directly collects data from these cluster heads in a single-hop range, and finally returns to the starting site. However, due to the complexity of the scheduling problem in WSNs with obstacles, the conventional algorithms are difficult to resolve. In this paper, we propose a cluster based secure dynamic keying technique to authenticate the nodes during mobility. The nodes with high configuration are chosen as cluster heads based on the weight value which is estimated using

parameters such as the node degree, average distance, node's average speed, and virtual battery power. The keys are dynamically generated and used for providing security. Even the keys are compromised by the attackers, they are not able to use the previous keys to cheat or disuse the authenticated nodes. In addition, a bidirectional malicious node detection technique is employed which eliminates the malicious node from the network. By simulation, it is proved that the proposed technique provides efficient security with reduced energy consumption during node mobility.

KEYWORDS

Mobile sink, wireless sensor network, obstacles, dynamic key, cluster.

1. INTRODUCTION

1.1 Wireless Sensor Network

Sensors integrated into structures, machinery, and the environment, coupled with the efficient delivery of sensed information, could provide tremendous benefits to society. Potential benefits include: fewer catastrophic failures, conservation of natural resources, improved manufacturing productivity, improved emergency response, and enhanced homeland security. However, barriers to the widespread use of sensors in structures and machines remain. Bundles of lead wires and fiber optic "tails" are subject to breakage and connector failures. Long wire bundles represent a significant installation and long term maintenance cost, limiting the number of sensors that may be deployed, and therefore reducing the overall quality of the data reported. Wireless sensing networks can eliminate these costs, easing installation and eliminating connectors.

The ideal wireless sensor is networked and scalable, consumes very little power, is smart and software programmable, capable of fast data acquisition, reliable and accurate over the

Special Issue; March - 2017 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

long term, costs little to purchase and install, and requires no real maintenance.

Selecting the optimum sensors and wireless communications link requires knowledge of the application and problem definition. Battery life, sensor update rates, and size are all major design considerations. Examples of low data rate sensors include temperature, humidity, and peak strain captured passively. Examples of high data rate sensors include strain, acceleration, and vibration. Recent advances have resulted in the ability to integrate sensors, radio communications, and digital electronics into a single integrated circuit (IC) package.

A wireless sensor network (WSN) generally consists of a base station (or "gateway") that can communicate with a number of wireless sensors via a radio link. Data is collected at the wireless sensor node, compressed, and transmitted to the gateway directly or, if required, uses other wireless sensor nodes to forward data to the gateway. The transmitted data is then presented to the system by the gateway connection. The purpose of this chapter is to provide a brief technical introduction to wireless sensor networks and present a few applications in which wireless sensor networks are enabling.

1.2 Sensor Node Architecture

A Wireless Sensor Network (WSN) contains hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy. Figure 1.1 shows the schematic diagram of sensor node components. Basically, each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units (some of these components are optional like the mobilizer). The same figure shows the communication architecture of a WSN. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. 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. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external base station(s). A base-station may be a fixed node or a 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.

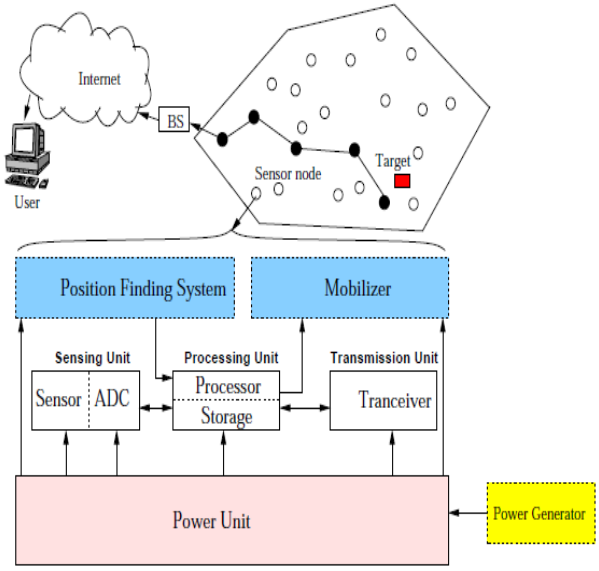

Fig 1.1 Wireless sensor node functional block diagram

Networking unattended sensor nodes may have profound effect on the efficiency of many military and civil applications such as target field imaging, intrusion detection, weather monitoring,

Special Issue; March - 2017 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management. Deployment of a sensor network in these applications can be in random fashion (e.g., dropped from an airplane) or can be planted manually (e.g., fire alarm sensors in a facility). For example, in a disaster management application, a large number of sensors can be dropped from a helicopter. Networking these sensors can assist rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in the disaster area. In the past few years, an intensive research that addresses the potential of collaboration among sensors in data gathering and processing and in the coordination and management of the sensing activity were conducted. Thus, innovative techniques that eliminate energy inefficiencies that would shorten the lifetime of the network are highly required. Such constraints combined with a typical deployment of large number of sensor nodes pose many challenges to the design and management of WSNs and necessity of energy-awareness at all layers of the networking protocol stack. For example, at the network layer, it is highly desirable to find methods for energy-efficient route discovery and relaying of data from the sensor nodes to the BS so that the lifetime of the network is maximized.

1.3 Applications of Wireless Sensor Networks

Sensor networks offer economically viable solutions for a variety of applications. For example, current implementations monitor factory instrumentation, pollution levels, freeway traffic, and the structural integrity of buildings. Other applications include climate sensing and control in office buildings and home environmental sensing systems for temperature, light, moisture, and motion.

1.3.1 Structural Health Monitoring – Smart Structures

Sensors embedded into machines and structures enable condition-based maintenance of these assets. Typically, structures or machines are inspected at regular time intervals, and components may be repaired or replaced based on their hours in service, rather than on their working conditions. This method is expensive if the components are in good working order, and in some cases, scheduled maintenance will not protect the asset if it was damaged in between the inspection intervals. Wireless sensing will allow assets to be inspected when the sensors indicate that there may be a problem, reducing the cost of maintenance and preventing catastrophic failure in the event that damage is detected. Additionally, the use of wireless reduces the initial deployment costs, as the cost of installing long cable runs is often prohibitive. In some cases, wireless sensing applications demand the elimination of not only lead wires, but the elimination of batteries as well, due to the inherent nature of the machine, structure, or materials under test. These applications include sensors mounted on continuously rotating parts, within concrete and composite materials, and within medical implants.

1.3.2 Industrial Automation

In addition to being expensive, lead wires can be constraining, especially when

DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

moving parts are involved. The use of wireless sensors allows for rapid installation of sensing equipment and allows access to locations that would not be practical if cables were attached.

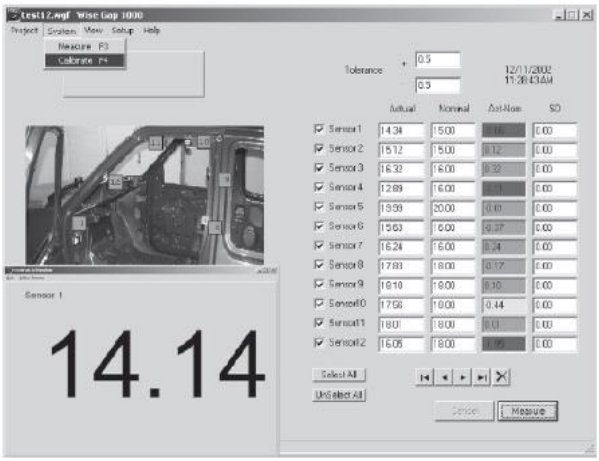

Fig 1.2 Industrial application of wireless sensor

An example of such an application on a production line is shown in Figure 1.5. In this application, typically ten or more sensors are used to measure gaps where rubber seals are to be placed. Previously, the use of wired sensors was too cumbersome to be implemented in a production line environment. The use of wireless sensors in this application is enabling, allowing a measurement to be made that was not previously practical. Other applications include energy control systems, security, wind turbine health monitoring, environmental monitoring, location-based services for logistics, and health care.

1.3.3 Civil Structure Monitoring

One of the most recent applications of today's smarter, energy-aware sensor networks is structural health monitoring of large civil structures, such as the Ben Franklin Bridge , which spans the Delaware River, linking Philadelphia and Camden, N.J . The bridge carries automobile, train and pedestrian traffic. Bridge officials wanted to monitor the strains on the structure as high-speed commuter trains crossed over the bridge.

A star network of ten strain sensors were deployed on the tracks of the commuter rail train. The wireless sensing nodes were packaged in environmentally sealed NEMA rated enclosures. The strain gauges were also suitably sealed from the environment and were spot welded to the surface of the bridge steel support structure. Transmission range of the sensors on this star network was approximately 100 meters.

The sensors operate in a low-power sampling mode where they check for presence of a train by sampling the strain sensors at a low sampling rate of approximately 6 Hz. When a train is present the strain increases on the rail, which is detected by the sensors. Once detected, the system starts sampling at a much higher sample rate. The strain waveform is logged into local Flash memory on the wireless sensor nodes. Periodically, the waveforms are downloaded from the wireless sensors to the base station. The base station has a cell phone attached to it which allows for the collected data to be transferred via the cell network to the engineers' office for data analysis. This low-power event-driven data collection method reduces the power required for continuous operation from 30 mA if these sensors were on all the time to less than 1 mA continuous. This enables a lithium battery to provide more than a year of continuous operation.

1.4 Problem Definition:

1. Symmetric-key based approach requires complex key management, lacks of scalability, and is not resilient to large

Special Issue; March - 2017 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

numbers of node compromise attacks since the message sender and the receiver have to share a secret key.

2. The scalability problem, a secret polynomial based message authentication scheme is similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial.
3. Computational complexity, memory usage, and security resilience

2.PROPOSED METHOD

A cluster based secure dynamic keying technique authenticate the nodes during mobility. The nodes with high configuration are chosen as cluster heads based on the weight value which is estimated using parameters such as the node degree, average distance, node's average speed, and virtual battery power.

The keys are dynamically generated and used for providing security. Even the keys are compromised by the attackers, they are not able to use the previous keys to cheat or disuse the authenticated nodes. In addition, a bidirectional malicious node detection technique is employed which eliminates the malicious node from the network.

The sensor layer is the bottom and basic layer. For generality, we do not make any assumptions on sensor distribution or node capability, such as location-awareness. Each sensor is assumed to be able to communicate only with its neighbors, i.e., the nodes within its transmission range. In an

Authentication technique the attackers try to compromise the keys that are used by the sensor nodes for authentication. If the attackers compromise the keys, they may disuse the authenticated nodes from the network.

To prevent the attackers from cheating the authenticated nodes, the keys are dynamically changed and the same keys are used for generating HMAC code. By this the attackers are not able to use the previous keys for cheating the authenticated nodes. A bidirectional malicious node detection technique is employed and it eliminates the malicious nodes and the malicious CH from the network. When the cluster member tends to leave or join the network, the CH employs the authenticated key management mechanisms to ensure the security. When the CH tends to leave the network, the CH re-election is performed by the cluster member nodes. The proposed scheme prevents both insider and outsider attacks. By increasing the number of nodes, number of attackers and number of rounds, it is proved that the proposed scheme provides efficient security with reduced energy consumption, control overhead and packet loss

2.1 SYNCHRONIZATION AMONG CLUSTER HEADS

To perform data collection by TDMA techniques, intra cluster time synchronization among established cluster heads should be considered. The fourth phase is to synchronize local clocks among cluster heads in a CHG by beacon messages. First, each cluster head will send out a beacon message with its initial priority and local clock information to other nodes in the CHG. Then it examines the received beacon messages to see if the priority of a beacon message is higher. If yes, it adjusts its local clock according to the timestamp of the beacon message.

In our framework, such synchronization among cluster heads is only performed while Senosor Car is collecting data. Because data collection is

DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

not very frequent in most mobile data gathering applications, message overhead is certainly manageable within a cluster.

2.2 CLUSTER HEAD LAYER: CONNECTIVITY AMONG CHGS

The cluster head layer as a fore mentioned the multiple cluster heads in a CHG coordinate among cluster members and collaborate to communicate with other CHGs. Hence, the inter-cluster communication in LBC-DDU is essentially the communication among CHGs. By employing the mobile collector, cluster heads in a CHG need not to forward data packets from other clusters. Instead, the inter-cluster transmissions are only used to forward the information of each CHG to Sensor Car. The CHG information will be used to optimize the moving trajectory of Sensor Car, which will be discussed in the next section. For CHG information forwarding, the main issue at the cluster head layer is the inter-cluster organization to ensure the connectivity among CHGs.

2.3 PROPERTIES OF POLLING POINTS

The Sensor Car is equipped with two antennas, as it is not difficult to mount two antennas on Sensor Car, while it likely becomes difficult and even infeasible to mount more antennas due to the constraint on the distances between antennas to ensure independent fading.

Note that each cluster head has only one antenna. The multiple antennas of Sensor Car, which act as the receiving antennas in data uploading, make it possible for multiple cluster heads in a CHG to transmit distinct data simultaneously. To guarantee successful decoding when Sensor Car receives the mixed streams, to limit the number of simultaneous data streams to no more than the number of receiving antennas. In other words, since Sensor Car is equipped with two receiving antennas, at most two cluster heads in a CHG can simultaneously send data to Sensor Car in a time slot an equivalent 2 * 2 MIMO system for an uplink transmission is formed, which achieves spatial multiplexing gain for higher data rate. With such concurrent transmissions, data uploading time can be greatly reduced. If there are always two cluster heads that simultaneously upload their data to Sensor Car in each time slot, data uploading time can be cut into half in the ideal case.

In fact, when the size of a CHG is larger than 2, we have multiple choices to schedule cluster head pairs to communicate with Sensor Car. Each such a pair is called a scheduling pair.

Use P to denote all the possible scheduling options in a CHG. Without loss of generality, we assume that M is an even number. For a given schedule P 2 P, there are M 2 scheduling pairs. The Sensor Car will choose a selected polling point for each of them. When Sensor Car arrives at a cluster, it will visit each selected polling point, where it stops to simultaneously collect data from the two cluster heads in a scheduling pair. To collect data as fast as possible in a cluster, the following two requirements should be satisfied.

The two cluster heads in a scheduling pair both should be covered by Sensor Car with the same transmission range as a sensor, i.e. Rs , when Sensor Car is at the selected polling point specific for this scheduling pair. By visiting the selected polling points in a cluster, Sensor Car should achieve maximum sum of the uplink MIMO capacities in the cluster. For each polling point, we assume that Sensor

DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

Car has the knowledge of the IDs of sensors in the proximity within range Rs and the channel vectors between the sensors and Sensor Car located at the polling point.

The information can be collected prior to each data collection tour. Upon receiving the CHG information which contains the IDs of the cluster heads in a CHG, for each possible schedule p, Sensor Car can choose a set of candidate polling points for each scheduling pair in p, each of which can cover the two cluster heads in a scheduling pair at the same time.

The distribution condition of the polling points to guarantee that there are always candidate polling points for choosing, and then present the criteria for selecting the For each polling point, we assume that Sensor Car has the knowledge of the IDs of sensors in the proximity within range Rs and the channel vectors between the sensors and Sensor Car located at the polling point. The information can be collected prior to each data collection tour. Upon receiving the CHG information which contains the IDs of the cluster heads in a CHG, for each possible schedule p, Sensor Car can choose a set of candidate polling points for each scheduling pair in p, each of which can cover the two cluster heads in a scheduling pair at the same time.

3. SIMULATION RESULTS

3.1 END-TO-END DELAY

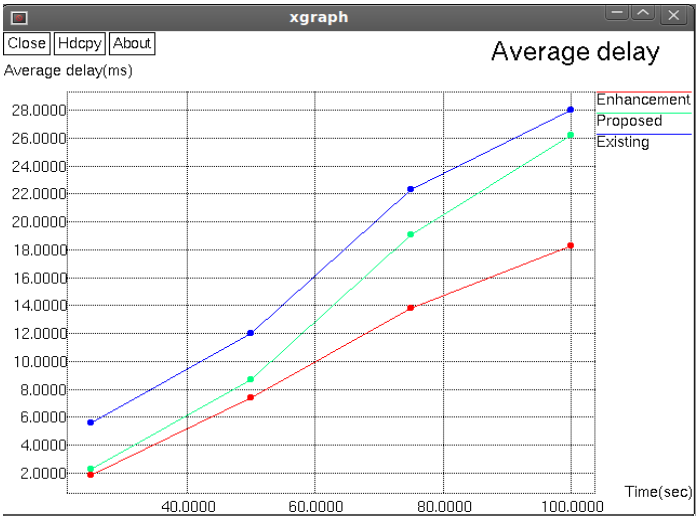

Figure 3.1 Time VS End-to-end delay

3.2 PACKET DELIVERY RATIO

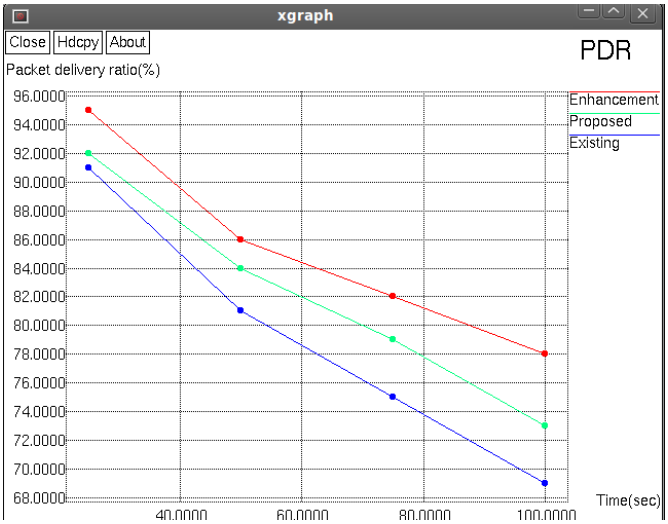

Figure 3.2 Time VS PDR

3.3 OVERHEAD

DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

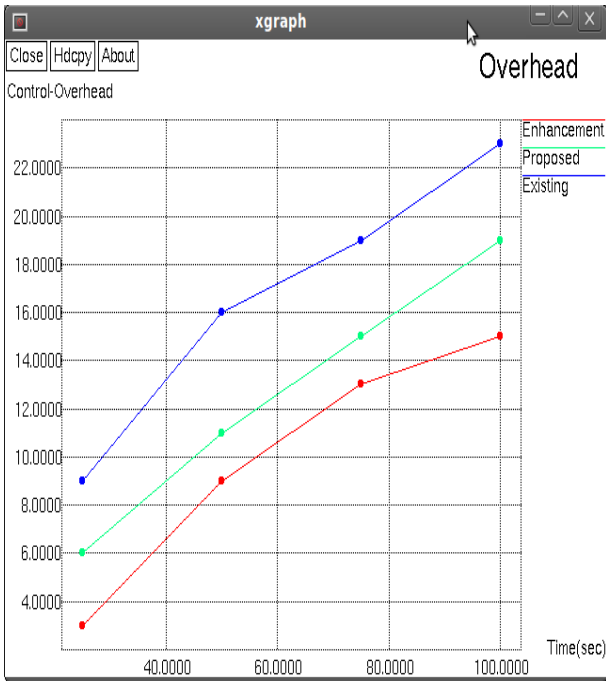

Figure 3.3 Time VS Overhead

3.4 THROUGHPUT

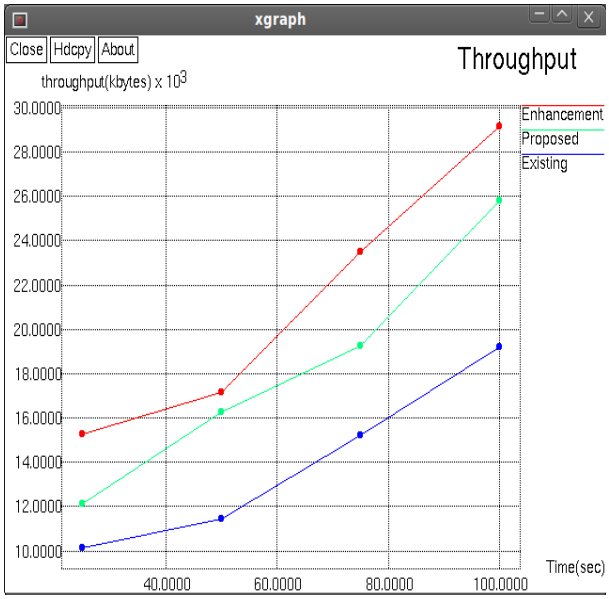

Figure 3.4 Time Vs Throughput

3.5 PACKET LOSS

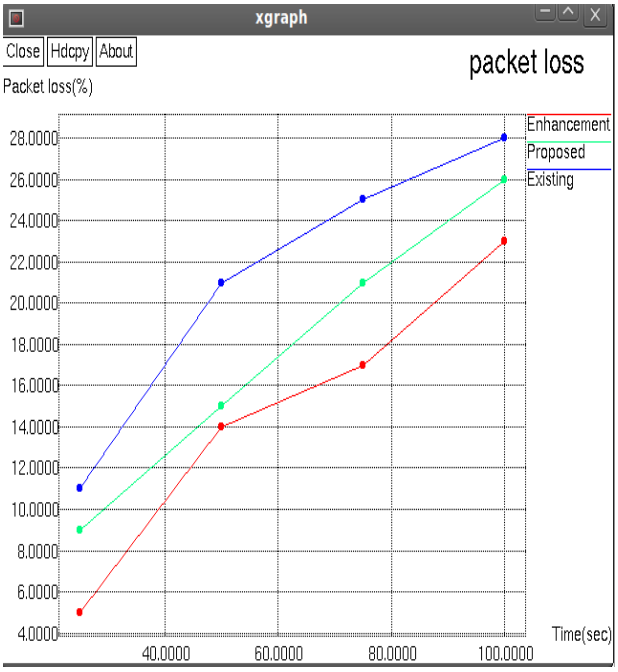

Figure 3.5 Time Vs Packet loss

4.CONCLUSION

Mobile Data Collection Employs Distributed Load Balanced Clustering for Sensor Self-Organization, Adopts Collaborative Inter-Cluster Communication For Energy-Efficient Transmissions Among Changes, Uses Dual Data Uploading For Fast Data Collection, and Optimizes Sensor car's Mobility To Fully Enjoy The Benefits Of Mu-Mimo. The Sensor Nodes Are Energy Constrained And Have Limited Lifetime, Energy Consumption Of Sensor Nodes Research Framework Is To Provide a Better Approach To Reduce The Energy Consumption In Wsn's And To Prolong the Network Lifetime. It Is Achieved By Two Main Approaches: 1) Clustering-Based: Sensor Nodes Form Clusters And Elect The Cluster Heads In Such a Way To Improve Energy Efficiency, And 2) Prediction Based: Energy-Aware Prediction Is Used To Find The Subtle Trade-Off Between Communication And Prediction Cost.

Special Issue; March - 2017 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.20170331.032.IHXAI

5.FUTURE SCOPE

The protocol divides the nodes of the ad hoc network into a number of overlapping or disjoint 2-hop- diameter clusters in a distributed manner. A cluster head is elected for each cluster to maintain cluster membership information. Inter-cluster routes are discovered dynamically using the cluster membership information kept at each cluster head. By clustering nodes into groups, the protocol efficiently minimizes the flooding traffic during route discovery and speeds up this process as well Cluster Formation

The goal of Cluster Formation is to impose some kind of structure or hierarchy in the otherwise completely disorganized ad hoc network. The algorithm is a variation of the simple "lowest ID" clustering algorithm in which the node with a lowest ID among its neighbors is elected as the Cluster Head.

REFERENCES

[1] **Radhakrishnan.S, Thiruppathy Kesavan. V, "Cluster Based Secure Dynamic Keying Technique for Heterogeneous Mobile Wireless Sensor Networks"**, China Communications, June 2016.

[2] **Feng Pan and Guangqian Xie, "Cluster-Based Routing for the Mobile Sink in Wireless Sensor Networks With Obstacles",** IEEE ACCESS, Volume 4, May 2016.

[3] **W. Nicholls, N. Shenoy and H. Zhou,** "**Efficient minimum spanning tree construction without Delaunay triangulation",** INF.Process.Lett, 2002.

[4] **A. Bestavros, Matta, and G. Smaragdakis, SEP: "A stable election protocol for clustered heterogeneous wireless sensor network",** Proc.SANPA, 2004.

[5] **Ossama Younis and Sonia Fahmy, HEED: "A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks",** IEEE Transaction, 2004.

[6] **Patrick Traynoretal, "Efficient hybrid security mechanisms for heterogeneous sensor networks",** IEEE Transaction, 2007.

[7] **Bin Xie, Demin Wang, Dharma P Agrawal, , Xiaodong Wang and Yun Wang, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks",** IEEE Transaction, 2007.

[8] **Kahina Chelli, "Security issues in wireless sensor networks",** International Journal of Communications Letters, 2008.

[9] **Dilip Kumar, R.B. Patel and Trilok C. Aseri, EEHC: "Energy efficient heterogeneous clustered scheme for wireless sensor network",** Computer Communications, 2009.

[10] **Chellappan Sriram, Dutta Neelanjana, Wenjun Gu and Xiaole Bai, "Providing end to end secure communication in wireless sensor networks",** IEEE Conference, 2011.

