A novel approach to avoid intrusion in area monitoring

Amritpal Singh
Assistant Professor
Lovely Professional University

Varun Singla
Assistant Professor
Lovely Professional University

Ravinder Singh
Assistant Professor
Lovely Professional University

Abstract: WSN had become the most popular choice for area monitoring. Many types of sensor nodes are available for monitoring the area like seismic sensors, image sensor, thermal sensor etc. WSN is the most economical method for area monitoring due to which the technique has been adopted by different countries. Use of sensors for this purpose had reduced the cost of monitoring. Thus, security factor has been compromised to some extent. Now, the intruder can easily sense the information being transmitted about an area and he can change it also very easily. Therefore, the paper provides a preventive mechanism against this man-in-the-middle attack so that this confidential information about an area should reach the concerned officials safely and we would be able to prevent the area from accidents.

Introduction

A wireless sensor network is a network which consists of small distributed autonomous device using sensor for monitoring the physical or environmental conditions or in other words wireless sensor network is combine sensing, communication and computing into a single small device. It is a collection of nodes organized in the corporative word where each node consists of processing capability which may contain multiple type of memory like program, data and flash, and have a power source also.

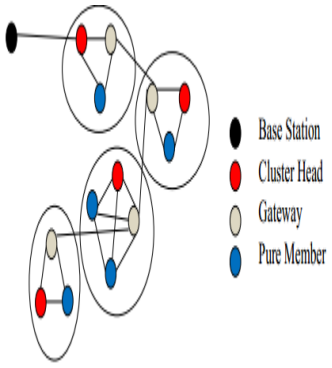

Figure 1. Dynamic Cluster-Based Wireless Sensor Network

A WSN in corporate is a gateway which provides connectivity back to the wired world and distributed nodes .In this network we use different types of protocols. But the protocols which we select depends on the requirements of our application .Such standardare available which includes 2.4 GHz radio based on either IEEE 802.15.4 or IEEE 802.11(is a Wi-Fi standard) .

Topologies in WSN

As the name suggest in star topologies, all the node are directly connected to a common gateway.

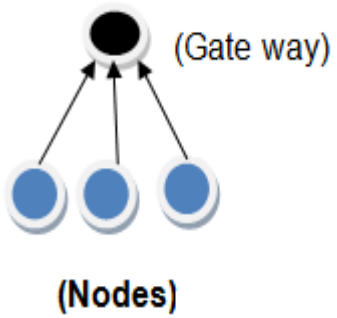

Figure 2. Star Topology

Mesh topologies is most efficient topologies and provide more reliability in this network a node is connected to the multiple node, pass the data through the available path which is more reliable.

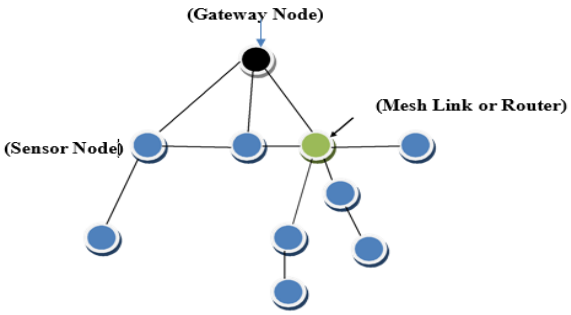

Figure 3. Mesh Topology

Literature Review

Bhaskar Krishnamachari gives the overview of the WSN. In this paper there is an overview of the application of the sensor network, and what are the different topologies are present in the network and which one is good. In this we get the knowledge about the different challenges which comes in the networks and give a short overview of the basic terms and application of the WSN.

YixinJiangand at el have proposed another shared verification and key trade convention. The two principle peculiarities of this convention are personality namelessness and session key reestablishment. This convention gives secure meandering administrations to the true blue client between the home and going to operators or so, this convention gives secure handoff to the real client. The proposed convention is focused around the emit part rule and insisted toward oneself plan. The convention lives up to expectations in two stages: First stage is the common validation with secrecy which conceals the utilization's genuine character when a honest to goodness client is meandering from the home operators to the meeting specialists. This stage utilizes the transient character (TID) rather than the client's genuine personality. Second stage is the session key restoration stage which restores the imparted key which is imparted between the authentic client and the serving operators.

Chen xi, Tian you liang put forward an advancement for deferral tolerant systems and versatile specially appointed systems which is generally utilized as a part of both of nonmilitary personnel and military .Nonetheless, they have the security issues that are progressively genuine because of their characteristic attributes of being great discontinuous and being self-sorted out. In this paper, they have displayed the key issues and difficulties for pioneering systems at system layer with understanding to issues they have given security plans, for example, the key administration, security steering, and trust administration. Based upon all such talks, at last they brought up the potential future exploration limits for the security in sharp systems. In this paper, they have overviewed different sorts of security issues in entrepreneurial systems from different

perspectives. It is clear that the specific attributes of crafty systems make it all the more impeccably fine despite potential assaults and danger. The fundamental key administration instrument that can supply the essential security administrations are still difficult to be accomplished, for situation in regards to pioneering systems. As this system work in a very surprising toward oneself composed appropriated route for an amazing variable situations.

R. Prema1, R. Rangarajan et. al**.** has put forward remote sensor system applications should choose the inborn change between vitality effective communication and the necessity to accomplish favored nature of administration (QoS, for example, bundle conveyance degree, delay and to decrease the force utilization of remote sensor hubs Keeping in mind the end goal to address this test, they propose the Force Mindful Steering Convention (PARP), which achieves application-defined correspondence delays at low vitality cost by alertly adjusting transmission power and directing choices. Broad recreation results demonstrate that the proposed PARP accomplishes better QoS and diminished force utilization.

Problem Formulation

WSN had become the most popular choice for area monitoring. Many types of sensor nodes are available for monitoring the area like seismic sensors, image sensor; thermal sensor etc.WSN is the most economical method for area monitoring due to which the technique has been adopted by different countries. Use of sensors for this purpose had reduced the cost of monitoring. Also, the no of solder and chopper needed to monitor the area for providing security has been reduced. Thus, security factor has been compromised to some extent. Now, the intruder can easily sense the information being transmitted about an area and he can change it also very easily. As an example in military areas or attack-prone areas, it becomes a necessity to get the correct information about an area as a little change in the received information can prove dangerous for the country. Therefore, the paper provides a preventive mechanism against this man-in-the-middle attack so that this confidential information about an area should reach the concerned officials safely and we would be able to prevent the area from accidents.

Working of system

For the area monitoring today we used different types of sensor nodes to deploy together for gathering more efficient data and accurate data. A wireless sensor network consists of large number of sensor nodes to deploy in the area which is to be observed. These nodes are deployed in random topology to cover the area. Sensor has low power battery and low range. So it cannot send data to the process node directly. Therefore, information is transferred by multi hop path to sink node and the data can be send any kind of abstract alarm or aggregated data to base station.

Challenges

The are many challenges in critical mission like border monitoring

a) Energy Efficiency: - Area monitoring is a confidential task. In this the position of deployment of sensor nodes has to be kept confidential. So in this area changing the battery of

a node manually is not a practical or possible task. So it is a great challenge to create energy efficient node. Although some solar power nodes came into existence in the literature but they are also inefficient.

b) Quality of service: - QOS is one of the main issues. The monitoring should be reliable to detect the intrusion and communication between sensor and sink node must be fast, there should not be any kind of delay.

c)Quality of coverage: - To cover the area of monitoring field the deployment of sensor should be in best place.

e) Security Issue: -In area monitoring the major task of sensor node is to send the data confidentially to the destination. Data should be encrypted, secured and protected against any attack. Many types of attacks are possible while data transmission. But most common attack out of them is man-in-the-middle attack. Whenever an intruder tries to attack, it's not an easy task to trace all the routes so instead of tracing all paths it follows a pattern. transmitting over the network.

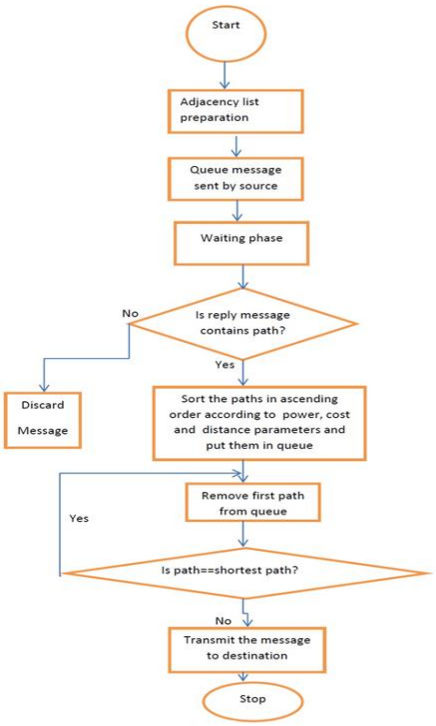

Figure 4. Working of proposed approach

a)Adjacency list preparation: - in this phase each node prepare there its adjacency list i.e. each node find the list of all its neighbour through which data can be sent.

b)Message sending phase :- in this phase source node send an query message or in this algorithm we cancel as help message too , to all its nodes which is present into the adjacency list like ((A0,D0)(A1,D1)……..(An,Dn)).

c)Wait phase :- in this phase on receiving query message or help message, each node prepare its reply message with containing cost and power of the path from the destination in terms of "K" value .

Calculation of "K" value

The "K" factor is calculated in three steps:-

1. Calculation of C (t) :- In this we calculate the transmission cost, which is been calculated by the following equation.

C (t) =T (hop count)…… (1)

In this T is and predefine standard cost which is defined by the use on per unit distance .and „t" is time taken in transmission. The total cost of it C (t) in multiplication of the standard distance cost and time taken in it.

2. Power of battery (P):- second factor in power of battery which we take in as factor Pdf. Pdf is known as a packet discretion factor

Power of battery of node =- Pfd…….. (2)

3. K factor: - In the end by calculation all the values now we calculate the K factor by putting the value in equation

K=mini (-) pdf && min (-) hope count

In this equation (-) sign show that cost must be less than power for the transmission successfully. And in this transmission will be ideal when cost will be minimum and battery power of node will be maximum. So after calculating the K factor of all the nodes the node replies their message with the parameter value of K.

(d) Path selection phase:- in this phase after getting the reply of possible path with k values from all the nodes, source node select the best path based on parameter pdf, hope count and seq no . . .it has with it .

e) Transmission Phase: - Now the information is been transmitted through the securely calculated alternative path.

Column-Number	What Happened	Value of this instance
1	It shows the occurred event	's'SEND, 'r' RECEIVED, 'D'DROPPED
2	Time at which the event occured?	12.000000000
3	Node at which the event occured?	Node id 0
4	Layer at which the event occured?	'AGT' application layer, 'RTR' routing layer,'LL' link layer, 'IFQ' Interface queue, 'MAC'mac layer, 'PHY' physical layer
5	Show flags	----
6	shows the sequence number of packets	0
7	shows the packet type	cbr' CBR packet, 'DSR' DSR packet, 'RTS'RTS packet generated by MAC layer, 'ARP'link layer ARP packet.
8	shows size of the packet	Packet size increases when a packet moves from an upper layer to a lower layer and decreases when a packet moves from a lower layer to an upper layer
9	[….]	It shows information about packet, duration,mac address of destination, the mac address of source, and the mac type of the packet body.
10	show flags	----
11	[….]	It indicates data about source hub ip : port number, goal hub ip: port number, ip header ttl, and ip of next bounce

Figure 5. Trace Format

Results

As per graph showing packet lost rate between alost and klost, where alost is representing the graph of "AODV" algorithm and k lost is showing the packet lost graph of ks algorithm

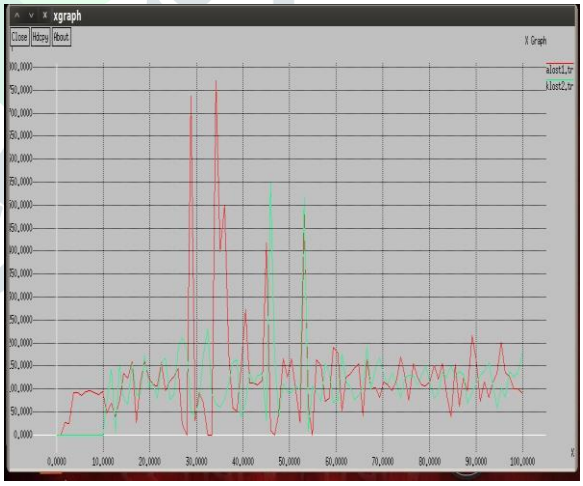

Figure 6. Graph of Packet Delivery Ratio

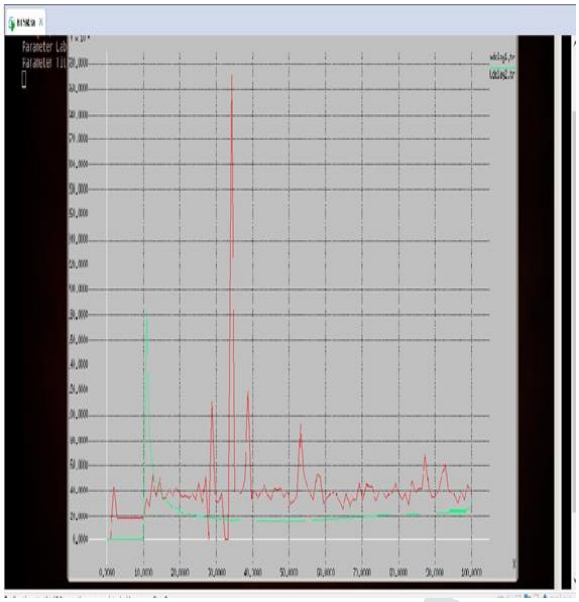

Figure 6. Delay Graph between AODV and KODV

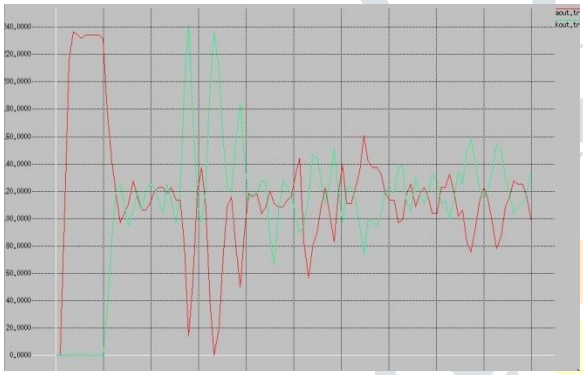

Figure 6. Output Graph

Conclusion

As this algorithm is, we can say an updated version of the AODV but which provide and load balancing or power of nodes and this algorithm provide as the prevention mechanism also by not following any particular path by switch nodes for transmission because of the pdf factor change every time when every any packet go through an node .so the probability of a single node to transmit the data many time continually through it is very less .It provide us less hop count path also which is also improve the cost of the transmission. And dead node problem is also reduced. As we now in AODV protocol the algorithm send the packet through one node until the node don't come in dead state. So this algorithm provides us better power rate, less cost and reduce the probability of man in middle attack by frequently switching there nodes.

Future Scope: - There can be some feature work which we will do. Like we can use time parameter in the place of cost in the formula. if we can do work on there header packet by adding extra field in like power or use we can improve path selecting formula also

References:

[1] M. Erazo-Rodas, M. Sandoval-Moreno, et al., Multiparametric monitoring in equatorial tomato greenhouses (III): environmental measurement dynamics. Sensors 18(8) (2018)

[2] S. Singh, P. Kumar, J. Singh, A survey on successors of LEACH protocol. IEEE Access 5, 4298–4328 (2017)

[3] S. Han, Z. Gong, W. Meng, et al., Automatic precision control positioning for wireless sensor network. IEEE Sensors Journal 16(7), 2140–2150 (2016)

[4] O. Kaiwartya, A.H. Abdullah, Y. Cao, et al., T-MQM: testbed-based multi-metric quality measurement of sensor deployment for precision agriculture-a case study. IEEE Sensors Journal 16(23), 8649–8664 (2016)

[5] T. Alhmiedat, Low-power environmental monitoring system for ZigBee wireless sensor network. KSII Transaction on Internet and Information Systems 11(10), 4781–4803 (2017)

[6] W. Ding, W. Fang, Target tracking by sequential random draft particle swarm optimization algorithm. IEEE Int Smart Cities Conf. 2018, 1–7 (2018)