ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

KS Algorithm: A Preventive Mechanism to avoid Intrusion in Area Monitoring Applications

[1]Kaushal Kumar,[2]Swimpy Pahuja

[1] *M.Tech. Student, Department of Computer Science & Engineering, Lovely Professional University, Phagwara*

[2] *Assistant Professor, Department of Computer Science & Engineering, Lovely Professional University, Phagwara*

Abstract :- Sensor networks now-a-days have wider applicability in various areas whether it is deployment in hostile environments for health monitoring or area monitoring applications. Although the literature has reviewed lots of area monitoring techniques, this paper provides a model for the analysis of unwanted movement in a confidential area. The proposed model would be cost effective and would also provide a prevention mechanism from intruder attacks in data transmission process.

Index Terms - Sensor network, Area monitoring, sensor node, Sensor network applications etc.

I. INTRODUCTION

A wireless sensor network [1] is a network consisting of separate distributed autonomous devices named sensor for monitoring the physical or environmental conditions of an area.

In other words, "The wireless sensor network is a combination of sensing, communication and computing abilities into a single small device called sensor.

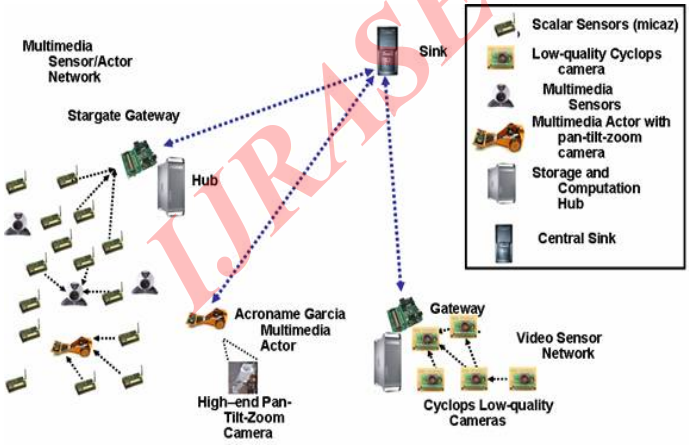


Figure 1.1 Wireless Sensor Network

A WSN in corporate world, is a gate way which provides connectivity back to the wired world and distributed nodes .In this network different types of protocols [2] are used but the protocol selection depends on the requirements of our application like such standard are available which includes 2.4 GHz radio based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi standard) .

Figure 1.2 WSN Components, Gateway, and Distributed Nodes

Applications of WSN

There are several areas where sensors are used [2]:

a) Health Care

In this field, WSN is used for the purpose of remote monitoring. In this, wireless device i.e. sensor makes less invasive monitoring and provides health care to the patients. This application can be of two main types namely wearable and implemented .Wearable devices are used on

ISSN: 2321-9653

the body surface of a human or closer proximity to the user and second type of devices are those devices that are inserted into the human body to analyse the inner sensing of the body. There are many other application too like body measurement and location of the person.

b) Area Monitoring

Area monitoring is also one of the commonly used application of WSN .In area monitoring WSN is deployed over a region or area where some phenomenon or activity is to be monitored. We can take a live example of army or military bases where sensor devices are used to detect the enemy intrusion or interruption. Lots of applications which involves area monitoring activities includes building fire detection system, geo–fencing of jails or schools attendance zones etc.

c) Air Pollution Monitoring

Wireless sensors are also deployed in big cities to monitor the concentration of dangerous or harmful gases for citizens. These ad hoc wireless links are good to use rather than wired installation as it provides better mobility for testing in different areas.

d) Forest Fire Detection

It is one of the useful application of the real word .A WSN node can be installed in forests to detect the starting point of the fire and these node can be equipped with sensors to measure the temperature produced in the tree by the fire and the humidity caused in the atmosphere. It provides a great help to fire brigade officials as they would come to know the cause of fire and its reason to spread which would enable them to act accordingly.

e) Water Quality Monitoring

Water quality monitoring involves analyzing water properties in rivers, lakes, Demand Ocean as well as underground water reserves. In this task, wirelessly distributed sensors enables the creation of a more accurate map of water status and this function allows permanent deployment station in the location of difficult access without any need of manual data retrieval. There are some more application also like “machine health monitoring (MHM)” for machine condition Based Maintenance .

Sensor Node

A sensor node which can also be known as a sensor pod or a mote , is a component of a large network of sensors, where each node is responsible for sensing the needed information and sending that data to the processor in the network via different protocols [3] [4] [5] [6] [7].

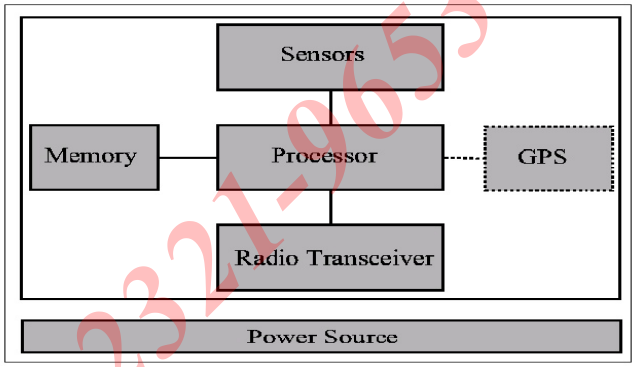


Figure 1.3 Architecture of node in a sensor

Components of Sensor Node

The main components of a node are

Microcontroller

Transceiver

External Memory

Power Source

Sensor

a) Micro Controller

Microcontroller is a small IC (Integrated Circuit) device containing a core processor, programmable in/out peripherals and memory. Program memory can also be used in the form of NOR flash (also known as a NOR gate flash) or OTP Rom (one -time programmable read - only memory) by including a chip as well as a typical small RAM. Micro Controller are designed for embedded application or in generally microprocessor used in personal computer or other general application.

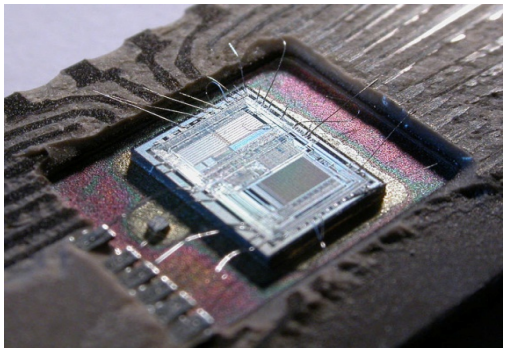


Figure 1.4: Microcontroller chip

Microcontroller are used in automatically controlled products and devices like ASCS(Automobile engine control systems) implantable medical devices , remote controls , office machines appliances , power tools .Other controller which can be used are desktop microprocessor , digital signal processor , FPGA(Field-Programmable Gate Array)

And ASIC (Application-specify Integrated Circuit)

FGPA is a IC which is used in various application like Digital signal processing , Software-Defined Radio , Metal detection , radio astronomy .

ASIC is an IC customized for a particular use , rather than intended for general purpose use like for DVR(Digital Voice Recorder), designed chip is an ASIC.

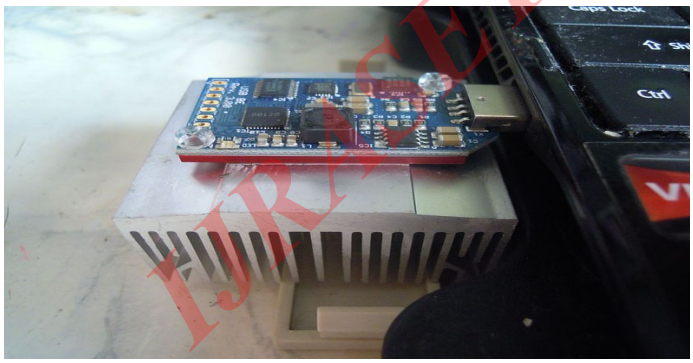


Figure 1.4.3: ASICMINER USB Erupted

A microcontroller is usually used in several embedded systems. Such as sensor node, just because of its flexibility to connect to other device, low cost and less power consumption.

b) Transceiver

Transceiver is device which comprises of transmitter and receiver which shares a common circuitry. In radio terminology, a transceiver means a unit which contains both a receiver and a transmitter.

WSN Node is a device which makes use of ISM Band where ISM stand's for (Industrial Scientific and Medical Radio Band). Wireless transmission media usually are radio frequency, optical communication (laser).

Infrared is like laser, it needs no antenna but it's broadcasting capacity is limited .Radio frequency based communication is most suitable or relevant which fits most of the WSN application. The figure below shows the picture of a transceiver internal and outer part.

Figure 1.4.4 Transceiver

ISSN: 2321-9653

c) External Memory

The most suitable type of memory which can integrate in the microcontroller chip sensor is flash memory and off –chip is RAM . Flash memorisers are used due to their less cost and strong capacity .Mainly the type of the memory to be used depends on the requirement of the application of sensor.

d) Power Source

Sensor node is a great solution of the problem when there is no main supply to the node . Sensor nodes are usually placed at the place where it seems to be difficult to reach. Thus, changing of a battery regularly is also a costly and inconvenient task. At the time of development of wireless sensor node, it was thought that some amount of energy should always be available to power the system in order to work. The sensor node mainly consumes power for sensing, data processing and communication capabilities. But out of these, data communication process takes more energy rather than other tasks. Inside the nodes, power is stored in the capacitor and batteries. Both power sources can be rechargeable or non-rechargeable, now in these days solar source cell have gained more importance.

In order to save the power inside the node, two types of policies are used:

DPM (Dynamic Power Management)

DVS (Dynamic Voltage Scaling)

DVS act as a smart policies in which power saving is done by switching of or shutting down the currently inactive parts while DVS works on the principle of varying the power level according to the non–deterministic work by varying voltage rather than the changing frequency.

e) Sensor

In normal electrical language "Sensor is a converter that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument".[1]

Or in WSN language, "Sensors are hardware devices that produce a measurable response to a change in physical condition like temperature and pressure".

Sensor produce a analogue signal which is converted (analogue-to-digital coverter device) in digital form and then forwarded for processing to the controller.

A sensor node must have :

Sensor node should be a smaller size device.

Sensor node should be consuming extremely low energy.

Sensor operates in high volume density.

Should be autonomous and operate unattended.

Sensor nature should be adaptive by the environment.

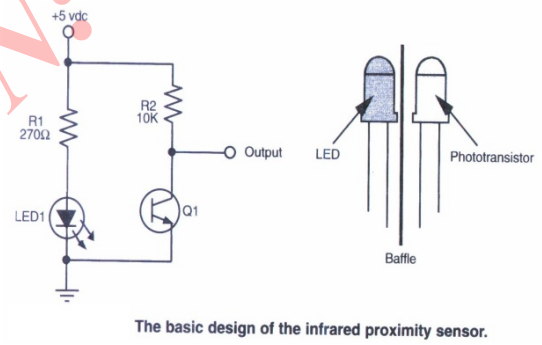


Figure 1.4.5 Basic design of a Sensor

II. EXISTING SYSTEM

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 moniter 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

ISSN: 2321-9653

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 the system :- For the area monitoring today we used different types of sensor nodes to deploy together for gathering more efficient data and accurate data [16].

A wireless sensor network consist large no 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 cant send data to the process node directly. Therefore, information is transferred by multihop path to sink node and the data can be send any kind of abstract alarm or aggregated data to base station.

Challenges or issues :- The are many challenges in critical mission like border monitoring

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.

Quality of service:- QOS is one of the main issue. 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.

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

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, its not an easy task to trace all the routes so instead of tracing all paths it follows a pattern. Usually the intruder follows or selects the shortest path for attack. In man-in-the-middle attack intruder is capable of monitoring all the data which is transmitting over the network. He is also capable of inserting any message to change the monitor data or add any wrong information. The attack can be at any node in the path so its hard to stop that .

III. PROPOSED MODEL

As the interruption while data transmission is a big issue in area monitoring which poses a great affect on data confidentiality. A prevention mechanism has been proposed with the help of an routing algorithm named as "KS Algorithm ", to reduce the probability of attacks [10] while data is transmitted. This new algorithm provides a method for computation of an alternative path [11,12,13,14,15] in order to prevent the confidential data from man-in-the-middle attack. Path computed may not be shortest one and would not include any node from the shortest path which is more prone to intruder attack. In this algorithm, a node would communicate to other node only if that node is authenticated or declared safe node.

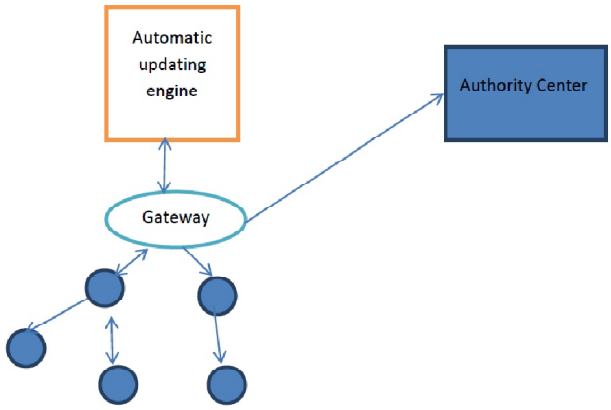


Fig: Proposed Model

ISSN: 2321-9653

The algorithm also involves some assumptions such as:

Source node has the information of residual power, cost to send data as well as minimum distance to be covered for all the nodes present in a particular area.

There is some mechanism named as Automatic Update Mechanism which keeps on updating the information of all other nodes to the source node.

To find the alternative path we consider some parameters.

Low power consumption: - The node to which data has to be transmitted should consume low power and also have enough battery power available to process the next request.

Max Hop Count:- It represents the maximum number of hops or nodes in a path.

Minimum Cost:- The cost of data transmission along the path should be as minimum as possible.

The proposed algorithm which would be used to send the confidential information about an area has been divided into following phases:

Adjacency list preparation phase : In this phase, each node prepares its adjacency list i.e. each node finds the list of all its neighbouring nodes through which data can be sent.

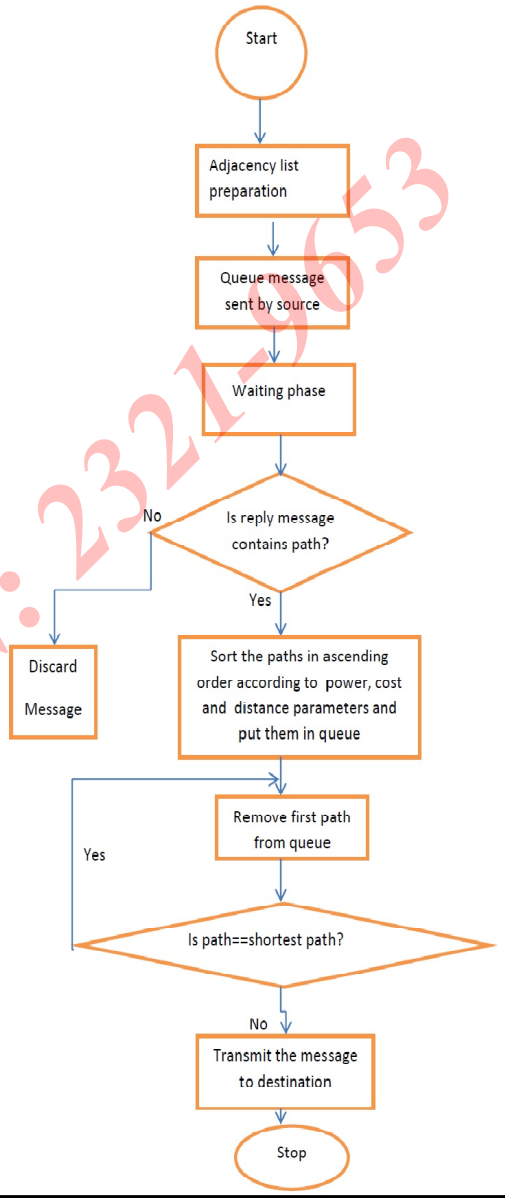
Message sending phase: In this phase, source node send the query message to all the nodes in its adjacency list enquiring about the new way to send the confidential information to the designated node.

Waiting phase: Now in this phase source node waits for a reply from all its neighbouring nodes for a certain period of time.

Path selection phase: In this phase, after getting the reply path from all the nodes, the source node selects the best path based on the parameter values it has with it.

Message transmission phase: Now the information is transmitted securely from this calculated alternative path.

Flow chart of the algorithm…….



IV. CONCLUSION

The shortest route is generally preferred by the sensing devices to transmit sensory data over the sensor networks. The existing algorithm for finding this shortest possible route was given by Dijkstra which is not intruder safe and easily fall prey to intruder attack. In this paper, we have proposed an algorithm to determine alternate route to

destination node in order to send the confidential information over the network while monitoring an area. This route would prove to be highly efficient for data transmission in terms of cost and power parameters.

As the shortest path is more prone to intruder attack, an alternate path which is secure from intruder attack has been

proposed because intruder would be interested in shortest path;

it won't be having any information about the existence of new

path computed by proposed algorithm.

REFERENCES

[1] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam and Erdal Cayirci, "A Survey on Sensor Networks", in Proc. of the IEEE Communications Magazine, vol.40, Issue: 8, August 2002, pp. 102-114

[2] Lewis, F.L., "Wireless Sensor Networks Smart Environments: Technologies, Protocols, and Applications", New York: ed. D.J. Cook and S.K. Das, John Wiley, 2004, pp.1-18.

[3] Qiangfeng Jiang and D. Manivannan, "Routing Protocols for Sensor Networks", in Proc. of the IEEE Conference, 2004, pp. 93-98

[4] Nam N. Pham, Jon Youn and Chulho Won, "A Comparison of Wirless Sensor Network Routing Protocols on an Experimental Testbed", in Proc. of the IEEE International Conference on Sensor Networks, 2006, pp.35-42

[5] S. Hedetniemi and A. Liestman, "A survey of gossiping and broadcastingin communication networks", Networks 18 (4) (1988) 319–349.

[6] J.N. Al-Karaki and A.E. Kamal. Routing techniques in wireless sensor net-works: a survey. IEEE Wireless Communications Magazine,11(6):6 28, 2004

[7] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," In Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking, August 1999.

[8] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, Tech. Rep. F33615-01-C-1895.

[9] A.Perrig, R.Szewczyk, V.Wen and J.D. Tygar, "SPINS: Security Protocols for sensor networks", International Conference on Mobile Computing and Networking (Mobicom 2001), 2001, pp.189-199.

[10] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer 35 (10), 2002, pp. 54-62

[11] T. Korkmaz, M. Krunz, and S. Tragoudas, "An efficient algorithm forfinding a path subject to two additive constraints", in Proceedings of theACM SIGMETRICS '00 Conference, June 2000, vol. 1, pp. 318–327.

[12] Daniel Zappala, "Alternate Path Routing for Multicast" in Proc. of the IEEE INFOCOM, Conference On Computer Communications, March 2000, pp. 1-10.

[13] J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-Tolerant Routing inWSN", in Proc. of the Second International Workshop on InformationProcessing in Sensor Networks (IPSN 03), April 2003, pp. 349-364.

[14] Suk-Bok Lee and Yoon-Hwa Choi , "A secure alternate path routing insensor networks", in Proc. of the Computer Communication 30, pp.153–165 ,2006.

[15] Swimpy Pahuja, A. Verma et al, "An Effective Routing Scheme for Secure Data Dissemination over Sensor Networks", in Proc. of the AICTE Sponsored International Conference on Recent Trends in Computing Mechatronics and Communication (RTCMC 2012) , 2012.

[16] FleGSens — Secure Area Monitoring Using Wireless Sensor Networks Peter Rothenpieler, Daniela Kr¨uger, Dennis Pfisterer, Stefan Fischer Institute of Telematics University of L¨ubeck Ratzeburger Allee 160 23538 L¨ubeck, Germany