© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Detection of Blackhole Nodes Categories Based on Trust Values for Securing Wireless Sensor Network Using Matlab

Prof. Sidharth Bhalerao, Rakesh Kumar Yadav
Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

Wireless Sensor Networks consists of hundreds and thousands of micro sensor nodes that monitor a remote environment by data aggregation from individual nodes and transmitting this data to the base station for further processing and inference. The energy of the battery operated nodes is the most vulnerable resource of the WSN, which is depleted at a high rate when information is transmitted, because transmission energy is dependent on the distance of transmission. In a clustering approach, the Cluster Head node loses a significant amount of energy during transmission to base station. So the selection of Cluster Head is very critical. An effective selection protocol should choose Cluster Heads based on the geographical location of node and its remaining energy. In this work a centralized protocol for Cluster Head selection in WSN is discussed, which is run at the base station, thus reducing the nodes energy consumption and in- creasing their life-time. The primary idea is implemented using a trust model based selection of Cluster Head from among the nodes of network, which is concluded depending on two parameters, the current energy of the node and the distance of the node from the base station. The protocol is named AODV based on Energy and Distance, and is run periodically at the base station where a new set of cluster heads are selected at every round, thus distributing the energy load in the network and increasing the network lifetime. The simulation results show that the proposed approach is more effective than the existing DSNT protocol.

Keywords: Wireless sensor networks, Cluster Head, micro sensors, network lifetime, DSNT, AODV.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are networks that comprise of sensors that are distributed in an ad hoc fashion over a defined geographical area, aimed at sensing some predefined information from the surrounding, processing them and transmitting them to the sink station. The sensors work with one another to capture some physical event. The data assembled is then transformed to get important outcomes. Remote sensor systems comprise of protocols and algorithms with self-arranging capabilities. WSNs can be widely divided into two types-Unstructured WSN and Structured WSN. While Unstructured WSN have a large collection of nodes, put up in an ad-hoc fashion; Structured WSN have few, scarcely distributed nodes with pre-planned deployment. The Unstructured WSNs are difficult to maintain, but it is relatively easy to maintain Structure WSNs.

Comparison of WSN with ad-hoc networks

i. Wireless sensor networks primarily use broadcast form of communication while ad-hoc networks use point to point communication.

ii. Wireless sensor networks are restricted by sensors limited power, energy and computational capability; whereas ad-hoc networks are not.

iii. Sensor nodes may not have global ID owing to the huge volume of overhead, tremendous number of sensors and geographically constrained dosage.

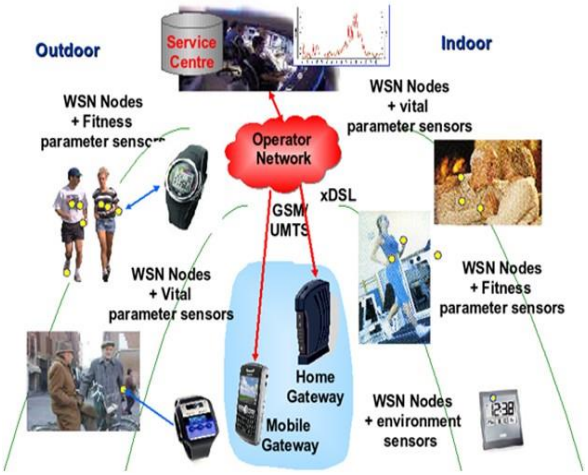


Figure 1. Uses of Wireless Sensor Network [4]

The Sensor Node

Wireless Sensor Networks mainly consists of nodes known as sensors. Sensors are devices with low energy as they operate on battery, having limited memory and pro cessing ability and are designed to survive extreme environmental conditions. These are mostly due to their small size. They are also featured with self-organizing and self-healing power. Three basic parts of a SENSOR NODE can be seen as:

A sensing subsystem that is used for data capturing from the real world.

A subsystem for processing that is used for local data processing and storage.

A subsystem consisting of wireless communication to be used to for data receiving And transmission.

II. RELATED WORK

[1] Black Hole Attack detection in Zone based Wireless Sensor Networks IJRITCC | April 2017, Available @ http://www.ijritcc.org.

The Wireless Sensor Networks (WSNs) became an emerging promising technology deployed in an area for specific purpose and in the wide range of application area such as military application, control and tracking application, habitat monitoring, industry, medicine, health care, agriculture etc. Wireless sensor networks are prone to various attacks. One such type of attack is a black hole attack. A black hole attack is a type of denial of service attack where the node drops the packets fully or selectively, routed through this node which discards the sensitive data packets. This paper deals with the detection of black hole attack in zone based wireless sensor network using the mobile agents.

[2] Detection and Prevention of Blackhole Attack in Wireless Sensor Network Using Ns-2.35 Simulator Abhinav Kaurav, Kakelli Anil Kumar Department of Computer Science and Engineering, Indore Institute of Science & Technology, Indore, Madhya Pradesh, India CSEIT1723234 | Received : 29 May 2017.

Wireless sensor network (WSN) is a network consists of tiny sensor nodes made of semiconductor device distributed over a large geographical area which is used to measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. These networks are easily prone to security attacks. Unattended implementation of sensor nodes in a geographical area causes many security threats in the wireless sensor networks. There are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Black Hole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. This can ultimately is drop of some important data packets and can disrupt the sensor networks completely. In this paper we have introduced prevention mechanism against the black hole attack in WSN. We have used the popular AODV protocol mechanism to detect and prevent this attack in NS-2.35 simulator.

[3] Blackhole Attack Detection Techniques in WSN: A Review Er. Mandeep Thakur M.tech Scholar, Deptt.of CSE, Punjabi University Regional Centre for Information Technology and Management, Mohali, Punjab, India Asst. Prof. Amninder Kaur 2017, IJARCSSE.

The wireless sensor network is the decentralized type of network, the size of the sensor networks is very small due to which battery power of the nodes is limited. Due to self-configuring nature of the wireless sensor networks, various type security attacks are possible in the network. The security attacks are broadly classified into active and passive attacks.

III. PROPOSED WORK AND RESULTS

ALGORITHM:

(I) Initialization Phase:

Step1: Sensor nodes are deployed randomly in a rectangular plane of area and classified these nodes in the form of cluster by calculating distance from nearest relay nodes. The relay nodes are fixed position nodes.

Step2: Cost of link is calculated by using cost estimation function and assign cost value, delay and initial energy to each sensor node.

(II) Setup Phase:

Step3: Now choose the cluster head based on two parameters with maximum energy and minimum delay. The energy of relay nodes are greater than the sensor nodes.

Step4: Each member node sends the data to the cluster head and reduce certain amount of energy. The nodes which have less energy than the threshold energy are considered to be dead.

Step5: All the cluster head nodes send the aggregated data to the nearest fixed position relay node and energy is consumed during transmission. If the energy of relay node is equal then the transmission energy the node is removed from the network.

Step6: Relay nodes are very far away from the base station so each node sends the data to the nearest relay node for sending the data to the base station and reduce the energy consumption.

Step7: If the Relay nodes are dead then a new cluster are formed and for choosing the head node go to step 3. This process repeat until the threshold value is not equal to dead energy which means the network is dead.

Step 8: Calculate Indirect and direct trust, trust values of each node and compare it with threshold value based on above specified formulas.

Step 9: Make decision on the bases of comparison of trust values with threshold value that which node is trusted, entrusted and uncertain.

Step 10: stop

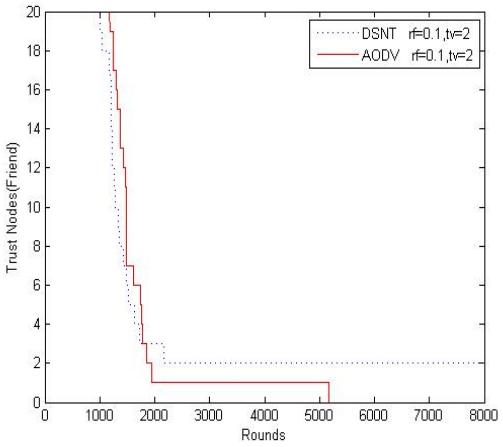
We have done simulation of AODV and DSNT Protocol in MATLAB and MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language. A proprietary programming language developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, Fortran and Python.

COMPARISION GRAPH WITH EXISTING DSNT PROTOCOL

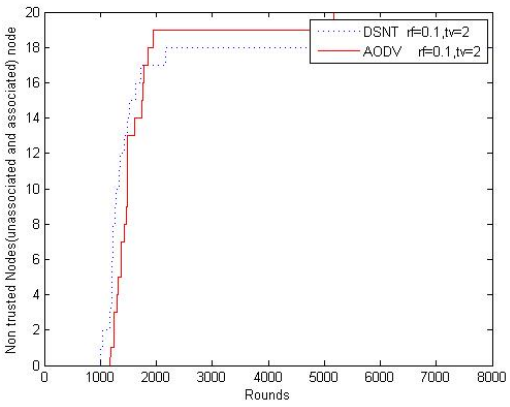
Table 1. for 100X100 Simulation Area:

Parameter	**DSNT Protocol**	**AODV Protocol**
Simulation Dimension	100X100	100X100
Number of Nodes	20	20
Efficiency	45%	57%
Non Trusted Nodes	14	17

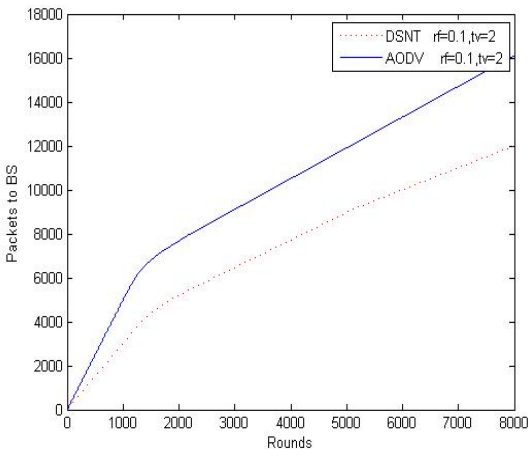
(a)This graph represent number of packets send to base station using AODV protocol which shows better performance as compare to DSNT protocol.



(b)This graph represent performance of identification of trusted nodes using Our AODV and compare with existing protocol DSNT.



(c) This represent identification of no of non-trusted nodes with AODV and DSNT protocol



IV. CONCLUSION AND FUTURE WORK

The organize life-time, which is in danger to significance remaining in the sensor center concentrations, is an essential issue to be considered while plotting WSNs. For an imperativeness capable WSN, diverse WSN structures and collecting estimations have been proposed among which Leach is a change. Channel impacts utilization of the probabilistic model for passing on centrality to usage of the CHs among within centers. The tradition does not guarantee for the procedure and check of number for CH center core interests. In this manner a poor social event if set-up for a round, may influence the all completed execution [38]. Channel C is a for the most part controlled custom and enhances bundle shapes by spreading the CH concentrates all through the structure. Near to picking better social events, the BS what's more ensures that significance diffusing is correspondingly restricted among all the sensor center core interests.

This work, named AODV proposes a headed together approach for Cluster Head affirmation in setting of Trust appear for massiveness and bundle. The essential inspiration driving the proposed figuring is to broaden the security of the Wireless Sensor Network by informing disconnecting, to lessen the execution time at the base-station. To accomplish this goal, we have concentrated on presuming these inside concentrations fit the bill for CH decision in light of current importance and portion of center from BS, in like way decreasing the measure of cycle and subjective CH affirmation winds in AODV estimation. As a future work, this custom can be related for managing versatile sensor center point structures. In like way, future updates for this work is to join this Cluster Head insistence approach with multi ricochet Leach.

V. REFERENCES

[1]. Y.G.Iyer,S.Gandham,andS.Venkatesan.Stcp:a generic transport layer protocol for wireless

sensor networks.InComputerCommunicationsandNetworks,2017.ICCCN2017.Proceedings. 14thInternationalConferenceon,pages449-454,Oct2017.

[2]. Yangfan Zhou, M.R. Lyu, Jiangchuan Liu, and Hui Wang. Port: a price-oriented reliable transport protocol for wireless sensor networks. In Software Reliability Engineering, 2017. ISSRE 2017. 16th IEEE International Symposium on, pages 10 pp.-126, Nov 2017.

[3]. ChiehyihWanandShaneB.Eisenman.Coda:Congestion detection and avoidance in sensor networks.pages266-279.ACMPress,2016.

[4]. V.C. Gungor and O.B. Akan. Dst: delay sensitive transport in wireless sensor networks. In Computer Networks, 2016 International Symposium on, pages 116-122, 2016.

[5]. Chieh yih Wan, Andrew T. Campbell, and Lakshman Krishnamurthy. Pump slowly, fetch quickly(psfq):areliabletransportprotocolforsensornetworks.InIEEEJournalonSelected AreasinCommunications,pages862-872,2015.

[6]. O.B. Akan and I.F. Akyildiz. Event-to-sink reliable transport in wireless sensor networks.Networking, IEEE/ACM Transactions on, 13(5):1003-1016, Oct 2015.

[7]. R.A.Santos,A.Edwards,O.Alvarez,A.Gonzalez,andA.Verduzco.Ageographicrouting algorithm for wireless sensor networks. In Electronics, Robotics and Automotive Mechanics Conference,2016,volume1,pages64-69,Sept2016.

[8]. RuiZhang,HangZhao,andMiguelA.Labrador.The anchorlocationservice(als)protocol for large-scale wireless sensor networks.InProceedings of the Firs tInternational Conference on Integrated Internet Ad Hoc and Sensor Networks, InterSense '16, New York, NY, USA,2016. ACM.

[9]. Xiaojiang Du and Fengjing Lin. Secure cell relay routing protocol for sensor networks. In Performance, Computing, and Communications Conference, 2015. IPCCC 2015. 24th IEEE International, pages 477-482, April 2015.

[10]. Injong Rhee, A. Warrier, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-mac: A hybrid mac for wireless sensor networks.Networking,IEEE/ACMTransactionson,16(3):511-524,June2014.

[11]. MehmetC.VuranandI.F.Akyildiz.Spatial correlation-based collaborative medium access control in wireless sensor networks.Networking,IEEE/ACMTransactionson,14(2):316-329,April2016.

[12]. Chunlong Guo, Lizhi Charlie Zhong, and J.M. Rabaey. Low power distributed mac for ad hoc sensor radio networks.InGlobalTelecommunicationsConference,2012.GLOBECOM'12. IEEE, volume 5, pages 2944-2948 vol.5,2012.

[13]. V.Geetha,P.V.Kallapur,andSushmaTellajeera.Clusteringinwirelesssensornetworks:Performance comparisonof{LEACH}and;leachcprotocolsusing {NS2}.ProcediaTechnology, 4(0):163 - 170, 2012. 2nd International Conference on Computer, Communication, Control and Information Technology(C3IT-2012) on February 25 - 26, 2012.

[14]. W.B. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. Wireless Communications, IEEE Transactions on, 1(4):660-670, Oct 2012.

[15]. WuXinhuaandWangSheng.Performance comparison of leach and leach-cprotocolsbyns2. In Distributed Computing and Applications to Business Engineering and Science (DCABES), 2014 NinthInternationalSymposiumon, pages254-258,Aug2014.