ISSN 2319 - 6629
Volume 8, No.3, April - May 2019
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt09832019.pdf
https://doi.org/10.30534/ijwcnt/2019/09832019

Improving Throughput of WSN through Blackhole Identification and Elimination

Sneha Sebastian, Dr.Vinodh P Vijayan
PG Scholar –CSE, Associate Professor-CSE
Mangalam College of Engineering Mangalam College of Engineering
snehamehasebastian16gmail.com,vinodh.pvijayan@mangalam.in

ABSTRACT

Some wireless sensor network is traditionally is used to gather information form remote/unmanned area. Always focus on network insist on precisions data collection. Traditionally all sensor network design address challenges like coverage, lifetime and routing related issues. Due to the wide spread application of senor network, it is started using in many critical application like defence, atomic reactor, national security etc. where data security become important than other parameters. Blackhole attack is one of the attack attack which can spread the system with improper information, hence the entire system become obsolete. A trust score based blackhole attack identification can be implemented and affected nodes can be identified. Eliminating such black hole nodes from network may increase routing overhead but it always enhance throughput of network since the network carry any fruitful information.

Key words: Blackhole Identification, classification, throughput, routing overhead

1. INTRODUCTION

Incredible growth in information technology can lead to generation of large volume and variety of data. In this decade, there is huge increase in the data which gives to rise of new technology called big data. Based on an IDC report prediction, the global data volume will grow exponentially from 4.4 zettabytes to 44 zettabytes between 2013 and 2020. By 2025, IDC predicts there will be 163 zettabytes of data. It is very hard to store, analyse and process this huge amount of data using the current methods because it is comprised of high velocity, highly dynamic, immense volume and numerous types of information. Big Data speaks to new research in information processing and examination and different utilizations of businesses are revolving around it [5].Big data was originally associated with three key concepts: volume, variety, and velocity the figure 1 shows these three characteristic of big data.

Numerous industrial ventures present strict requirements on the quality parameters of the assembling procedure of the products. Data about working conditions and manufacturing machines should be gathered continuously way. To ensure the proper working and collection data from various machines, there is need for the collection of real time data. Gathering of real time data is one of the major challenge. As a solution to problem wireless sensor network (WSN) is introduced. Wireless sensor network is utilized for collecting different spatially dissipated data from an assortment of ecosystem through dedicated sensors to monitor and handling at a central location [7].

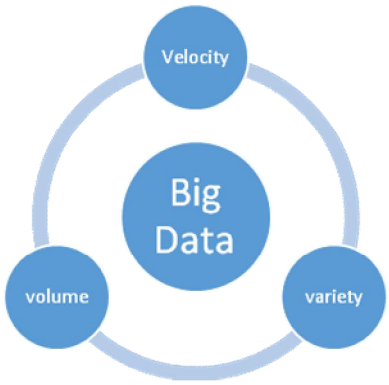

Figure 1: Big Data

Gathering of real time data from environment and sending the data to a central base station for processing. There were many variety of sensors that are used for transmitting the sensed data such as proximity sensors, humidity sensors, thermal sensors, magnetic sensors, position sensors, flow sensors, etc. [1]. A WSN framework consolidates data through data aggregation for gateway that enables remote monitoring [6]. For an effective monitoring and sensing coverage of sensor is very important but this coverage adversely affect the lifetime of a sensor [7, 8]. It very important to transmit the data to base station with full authentication. There were many intruders are there to penetrate and acquire the data that are sent through the network. It is necessary to add some sort of security mechanism to protect the data sent through the network. Black hole attack is the one type of attack that affect the data authentication. The external adversary capture a node or a subset of sensor nodes and manipulate the sensor node based on their desire [9,10]. The sensor nodes that perform actions based on the external adversary are called black hole nodes. The malicious node affect the route discovering technique. When source node broadcast a routing request then malicious node mislead routing information to destination [10].

2.BACKGROUND

Increasing network size poses significant data collection challenges, for what concerns sampling and transmission coordination as well as network lifetime. In this approach each node autonomously takes a decision about the compression and forwarding scheme to minimize the number of packets to transmit [1, 2]. Energy efficiency and energy balance are two important aspects in wireless sensor networks.

Flow-partitioned unequal clustering routing(FPUC)algorithm to achieve better energy efficiency and energy balance [3]. FPUC consists of two phases: clustering and routing. In the clustering \phase, the competition radius is computed according to the node density and the distance from sensor nodes to the sink. The sensor nodes that have more residual energy and larger overlapping degree have higher probability to be selected as cluster heads. In the routing phase, each cluster head first finds the gateway nodes andthendistributesthedataflowtoeachofitsgatewayno desdependingonresidualenergy. In the routing protocols that are specifically designed for the applications used by sensor networks, the limited available power of the sensor nodes has been taken into consideration in order to extend the lifetime of the networks [4].Wireless sensor networks (WSNs) are increasingly being deployed in security-critical applications. Because of their inherent resource-constrained characteristics, they are prone to various security attacks, and a black hole attack is a type of attack that seriously affects data collection [11].

3.PROPOSED SYSTEM

In the network the main objective is to transmit the data to the base station with full authenticity. The network is divided into clusters and each cluster contains a sub cluster head (SCH). The sub cluster head selection aim to reduce the energy consumption and increase the life time of a network. If few sub-cluster nodes are heavily loaded, it leads to faster energy consumption and to get normal depletion of energy so it is necessary to select the sub cluster head very properly. The distance between the normal child nodes and the sub cluster head plays a major part in energy consumption.

In the network, the SCH nodes sends hello packets to all the nodes which are present in the surrounding area and the nodes send back the acknowledgement. TDMA MAC scheduling technique is introduced here to avoid collision. According to the receipt of an acknowledgment all SCH nodes compare the distance between itself to the child nodes with the threshold distance. At the end of the distance calculation, each SCH nodes sends the message to the concerned child nodes, which are link with it. If the child receives more than one number of copies then it will randomly select the SCH node which it has to coordinate.

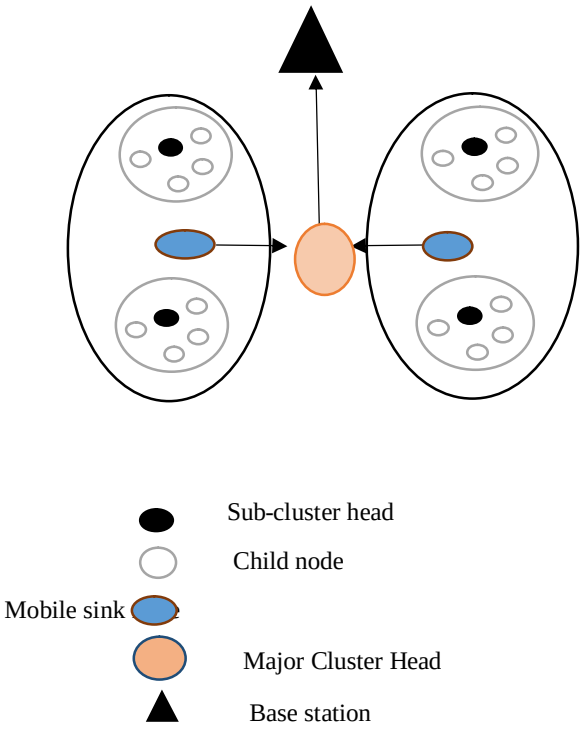

Figure 2: Architecture of System

Along with the network, the balanced load concept is applied to SCH nodes, where the balanced load SCH is formed in each clusters according to the figure 2 shortest distance between the SCH nodes and the child nodes and the distance is calculated using the equation 1. Mobile Sink Nodes (MSN) is introduced to collect the information from the SCH and it will transfer it to the MCH node.

$$DISTANCE_{(SCH,\,CH)} = \sqrt{SCHi(x,y) - CNj(x,y)} \quad (1)$$

Where i – 1,2,3,…… 10% of the total nodes

j – 1,2,3,……80% of the total nodes

SCH – sub cluster head

CN – child node

Once the cluster is formed, the next aim is to transmit the data to the base station. Child node will transmit the information to the sub cluster head. The sub cluster head node cannot able to transfer the information directly to the major cluster head due to the distance. To address this issues mobile sink nodes are introduced. The

mobile sink mode will act as the intermediate between the sub cluster head and the major cluster head. It moves from one place to another and collects the information from the sub cluster head and transmits that to the major cluster head. Each sub cluster consists of one or more mobile sink nodes according to the number of child nodes present in the sub cluster head. If any of the mobile sink efficiency is reduces in that case that sub cluster head will get the help of the neighbour sub cluster head's mobile sink node to transfer the data to the cluster head.

Data that are to send from child node and the base station needed to receive the same data that are sent. To provide the data authenticity HMAC is used.ECC algorithm and SHA-5 algorithm is combined to provide duel authentication mainly to concentrate the integrity and confidentiality. If an intruder get into the network and get access to a node then that node is called as black hole node. The node acted according to the will of the intruder. During the transmission of data to the destination through the malicious node and that node either dump the data or transmit false data. Before transmitting data to a node the sending node will sent a request and after receiving the acknowledgement that data is sent to that node, if it is a malicious node then it may take more time to send acknowledgment. Along with time of acknowledgment the trust value is also considered to detect malicious node.

Trust in a node explain about the scienarity of the node. For a malicious node, the trust value is very different from other node hence it is possible to detect the malicious node.

4.RESULT ON DISCUSSIONS

Testing is done on the standard NS2 platform and AODV is the routing protocol is used. The below table shows the typical configuration used in NS2 to trace file. Based on these configurations the network is simulated. Various configuration used for simulation is indicated in the table 1

Table 1: Configuration of NS2

Network Parameter	Value
Antenna type	Omni antenna
Channel	Wireless Channel
Routing Protocol	AODV
Energy unit	Joule
Queue type	Drop Tail
Address type	Hierarchical

Figure 3. shows that after the identification of blackhole node the throughput is improved considerably.

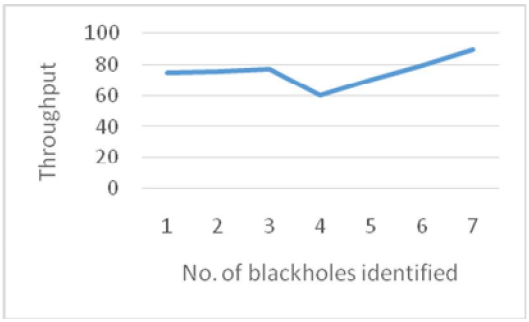

Figure 3: Throughput

The figure 4 indicate that as the number of black nodes are identified then the routing overhead is increased. Once the black node is identified then that node is dropped hence it is necessary to find a reroute for the data transmission.

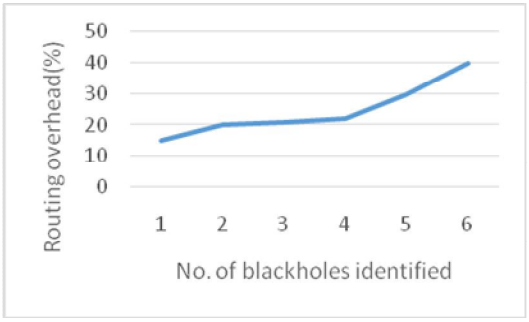

Figure 4: Routing overhead

Figure 5 shows due to the identification of black nodes the unnecessary data transmission can be avoided and thus can improve the energy efficiency.

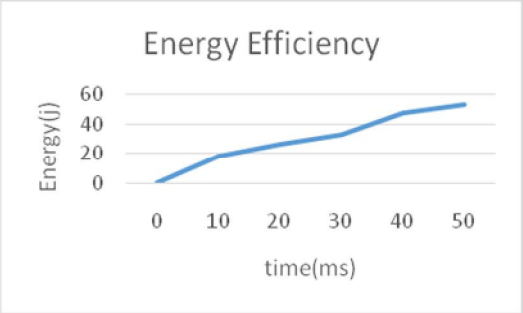

Figure 5: Energy Efficiency

5.CONCLUSION

Black hole detection using classification and elimination using threshold based method improves the overall performance of the system in terms of security and throughput. The large number of false data produced by black node always flood the network but at the same time it adversely affect the performance of the network. As the route with black node is eliminated, the requirement of new route arises and such dynamic routing algorithm always yield slightly high routing overhead. As the black nodes are eliminated the average energy usage of the networks improved at the same time due to the elimination of false data, the packet delivery ratio and throughput over a times also improved.

REFFERENCES

[1]. Shalli Rani, Syed Hassan Ahmed, Rajneesh Talwar, and Jyoteesh Malhotra, "**Can Sensors Collect Big Data? An Energy Efficient Big Data Gathering Algorithm for WSN**", IEEE Transactions on Industrial Informatics Volume: 13, Issue: 4 , Aug. 2017,Page(s): 1961 – 1968
https://doi.org/10.1109/TII.2017.2656899

[2]. C. Caione, D. Brunelli, and L. Benini, "**Distributed compressive sampling for lifetime optimization in dense wireless sensor networks**", IEEE Trans. Ind. Informat. vol. 8, no. 1, pp. 3040, Feb. 2012.
https://doi.org/10.1109/TII.2011.2173500

[3]. J. Peng, X. H. Chen, and T. Liu, "**A flow-partitioned unequal clustering routing algorithm for wireless sensor networks**", Int. J. Distrib. Sensor Netw., vol. 2014, 12 pp., 2014, Article ID 875268
https://doi.org/10.1155/2014/875268

[4]. A. E. Tmer and M. Gndz,"**Energy- efficient and fast data gathering protocols for indoor wireless sensor networks**", Sensors, vol. 10, pp.80548069, 2010.
https://doi.org/10.3390/s100908054

[5].S.Rani, S.H.Ahmed, "**Multi-hop Routing in Wireless Sensor Networks An overview, taxonomy and research challenges**", ISBN. 978-981-287730-7, 2016
https://doi.org/10.1007/978-981-287-730-7

[6]. Nikolaos A Pantazis, Stefanos A Nikolidakis and Dimitrios D Vergados, "**Energy Efficient Routing Protocol in Wireless Sensor Network: A survey**", IEEE Communications Surveys & Tutorials, Vol. 15, 2013.
https://doi.org/10.1109/SURV.2012.062612.00084

[7].Sneha Sebastian, Dr.Vinodh P Vijayan, "**Energy Aware Routing Through Optimum Load Balancing and Evolutionary Algorithm in WSN**"International Journal of Advanced Research, Idea and Innovations InTechnology, Volume 4, Issue 2, March-April 2018

[8]. Notom Ajaykumar, Mrinal Sarvagya, "**Secure and Energy Efficient Routing Protocol in Wireless Sensor Network: A Survey**", IEEE Conference, 2017
https://doi.org/10.1109/ICACCI.2017.8126192

[9].Mandeep Thakur,Amninder Kaur, "**Blackhole Attack Detection Techniques in WSN: A Review**",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 4, April 2017
https://doi.org/10.23956/ijarcsse/V7I4/0225

[10]. Sachin Lalar,Monika,Arun Kumar Yadav, "**Effect of Black Hole Attacks on Wireless Sensor Networks**"International Journals of Advanced Research in Computer Science and Software Engineering Volume-7, Issue-7
https://doi.org/10.23956/ijarcsse/V7I7/0189

[11]. Yuxin Liu, Mianxiong Dong, Member, Kaoru, Ota, Anfeng Liu,"**ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks**"IEEE Transactions on Information on Forensics and Security, Vol: 11 Sept. 2016, Page**(s):** 2013 – 2027
https://doi.org/10.1109/TIFS.2016.2570740