Analysis of Energy Efficient Technique of WSN

Sonam Rana
M.tech
Deptt.of Computer Science&Engg,
PURCITM,Mohali,India

lect.Amandeep Verma
Deptt.of Computer Science&Engg,
PURCITM Mohali,India

ABSTRACT

Large number of nodes is present in the wireless sensor network by which information is sensed and passed to base station. It is also known as decentralized network. The energy consumption of the network is major issue due to far deployment and small size of the sensor nodes. To improve lifetime of the sensor network various techniques are proposed by the various authors. The techniques which increase lifetime of sensor network are the clustering techniques. In this review paper, various techniques are reviewed which improve lifetime of the sensor networks.

Index terms:leach, wsn, head

INTRODUCTION

A network that has large number of sensor nodes deployed within it and also includes one base station is known as a wireless sensor network. The small devices that consume very less energy and are not much costly are known as the sensor nodes. They include within them the computational, communication as well as the memory resources that help in performing various tasks. The information that is present within the surroundings is collected by the sensor nodes present in the network and then forwarded to the base station such that it can be processed. There are several activities going on within the surroundings which need to be observed and then informed to the concerned users [1]. The base station that is present within the network behaves as a gateway within the external environment and the sensor network. The base stations can store large amount of information and for providing several services to the network, various data processing capabilities are included in it. The most important task of base station is to transmit the information that is being received from sensor nodes to the base station. The end users can access the information and can use it as per the demand. Further, if the application needs, the sensor nodes can generate groups amongst each other to perform processing [2]. Due to the smaller sizes of the sensor nodes, the sizes of their batteries are also small. Due to this, the batteries of the sensor not deplete very easily and cannot be recharged easily as they are deployed in very large areas. Thus, the lifetime of the network reduces which is a major concern.

The information that is achieved through the continuous monitoring of the nodes is forwarded to the base station due to which these networks are known as bi-direction wireless sensor networks [3]. Within the scenarios which require continuous monitoring, and it is not possible for the humans to monitor the surroundings, which can be possible by deploying the wireless sensor networks. There are many unique properties of the wireless sensor networks such as the batteries have limited life time; the sensor nodes are heterogeneous in nature, the nodes are mobile and so on. Initially, the military application utilized the WSNs within them in order to monitor the health and military applications. Further, as per the growth in these technologies, various other applications were also involved such as automatic manufacturing, home automation, robot control and so on [4]. On the basis of the information of temperature gathered from the surroundings by sensor nodes, the forest fires were also detected within various applications.

Attacks in WSN

There are two types of attacks are present in wireless sensor network which break the security of the networks [5]. These attacks are as follow:

The passive attack is limited to listening and analyzes exchanged traffic. It is the attacks in which they obtained the data secretly without creating any disturbance in the system. The passive attacks are difficult to detection. In this, operations are not affected. Malicious node is used to perform various functions and used to recover valuable data which is lost in the procedure of channel listen. For Examples, Attacks are snooping and eavesdropping.

Active attacks are the attacks in which attacker modify or remove the transmitted messages on the network [6]. In order to disturb the operation of the network or to cause a denial of service, attacker sends its own traffic and injects old messages.

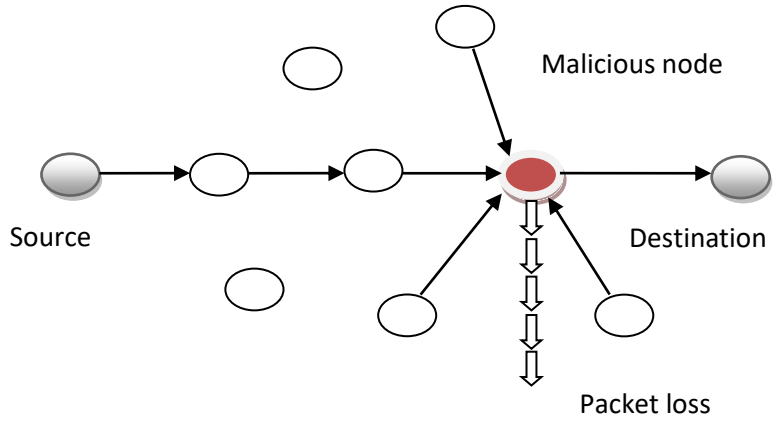

Fig 1 Sinkhole Attack In WSN

Sinkhole Attack: The sinkhole attack is the attack that prohibits the base station to access or sense the correct data and referred as the dangerous attack. This attack occurs in the higher layer application of the network [7]. The main objective of this attack is to attract all the traffic from the area using a malicious node and at the center it creates a metaphorical sinkhole. This malicious node in the network, attack all the present information as well as in the neighbor node. Thus, sensor node listens, information that is being transferred to its neighbor sensor node. In the sinkhole attack, present malicious node attracts other neighboring node with respect to the routing algorithm.

Literature survey

Annie Mathew, et.al (2017) presented the accumulation of large number of sensor nodes are present within a sensor network by which it becomes easy to sense and communicate with in a shortest range [8]. Among various major issues, security is also a major concern in wireless sensor network due to its communication capability. There are various attacks due to which working of sensor nodes is affected such as sinkhole attack, wormhole attack, gray hole attack and many more. Sinkhole is the attack in WSN in which shortest path is shown by the sinkhole node between the sink or destination node. Various methodologies so far are proposed by many researchers for the detection of the sinkhole attack. In this paper, author discussed and studied the sinkhole attack and its classification and methods for the detection of sinkhole attack by using various parameters.

Mahmood Alzubaidi, et.al (2017) presented the main objective of this paper is the clear understanding of types of internal attacks and their affects of sinkhole attacks on RPL. Various mechanism and IDS has been proposed so far for the detection of sinkhole attack [9]. In this paper, each mechanism is studied and analyzed with their advantages and drawbacks in order to highlight false positive rate and resource consumption. They showed a table which provides the previous representation for the detection mechanisms for sinkhole attack. After comparison the most effective method was observed.

Manpreet kaur, et.al (2016) Presented the emerging technology has been utilize in almost wide range of applications in public and military area, this technology is known as wireless sensor network. Large number of tiny sensor nodes with limited resources is present in the sensor networks, for monitoring they are also having a sensor node low in cost and power along with a base station. These networks are more prone to attacks due to small size and large quantity of sensor nodes within a network [10]. The most destructive routing attack among all attack is the sinkhole attack. The sinkhole is the attack in which all the routing information is captured and advertises by the malicious node after which forces the nodes to route the data towards it. Therefore, the performance of the network is degraded by the sinkhole attack. The main objective of this paper is the analysis and detection of the sinkhole attack in wireless sensor network.

Anthonis Papadimitriou, et.al (2009) proposed two new cryptographic protocols to minimize the degradation of network which is caused by the sinkhole attack on tree-based routing topologies within the wireless sensor network. The continuous operation is provided by the both protocols in order to improve the flexible functioning instead of detecting them. It is utilized as functions are operational in the presence of the attacks also [11]. The detection mechanisms are not dismissed by the resilience mechanisms but it minimizes the efficiency of the system due to which it is not utilized properly. In the wsn, they utilize three different routing protocols which contains the classic routing strategies for two protocol according to study of simulation. It is demonstrated, on the basis of simulation results that resilience can be improved further using this proposed method that prevents the affect of sinkhole attack in case of collision.

Gauri Kalnoor, et.al (2016) presented wireless sensor network where large quantity of sensors is present that are distributed spatially. It also monitors the physical or environmental conditions such as, pressure, temperature, motion, sound and many more [12]. All the information throughout the network is passed by the sensors. There is rapid increase in internet traffic when the size

of the network and the number of nodes are increases. The major concern in the WSN network is of security for which an appropriate network is required. A vital role in security of a system is played by the intrusion detection system. The consistent Quality of Service (QoS) assistance is the major challenge of WSN such as reliability, congestion control, efficient energy and end-to-end delay. In order to protect the QoS of WSN, secured routing protocols along with detection of an intruder was applied. Therefore, for the improvement of performance of the network various routing protocols were discussed in this paper.

Kevin Weekly, et.al (2012) presented the implementation of routing protocols for the Low-power and lossy networks due to the sinkhole attacks as it affect the wireless sensor networks. The traffic is captured by the sinkhole attack also known as compromised node as it drops all the incoming packets that result in the degradation of performance. It low the end-to-end delivery due to which numbers of transferred messages are reduced forwarded to the destination [13]. An attractive route to its neighbors is advertised by the captured traffic by the sinkhole using mechanism. In this paper, two countermeasures addressing the sinkhole problem was evaluated. At first, a parent fail-over and second, a rank authentication technique. As per simulation results, it is concluded that single technique do not work well, whereas the combination of the two techniques significantly improves the performance of a network under attack. They also demonstrated that penetration of sinkholes nodes combat the increased density of the network without identifying the sinkholes.

S.Sharmila, et.al (2011) presented the susceptibility of wireless sensor networks to routing attacks. The one-way hash chains were utilized by the protocol for the detection of the exact sink hole [14]. In this proposed method, the attack is detected by the destination node only when there is difference between the digest provided by the trusted path and by the trusted node to the destination. All these transferred messages shows the integrity of the data which is ensured by the optimal path used. In dealing with mutual malicious nodes, this proposed algorithm is robust as it hides the real intruder. MATLAB tool was utilized to test the functionality of the proposed algorithm. Simulation results, demonstrate the performance and accuracy of the proposed algorithm in terms of success rate, false positive and negative rate.

D.Sheela, et.al (2011) proposed an approach which is based on the mobile agent has been utilized in order to provide information to every sensor node in these networks. This information is utilized to avoid the affects of sinkhole attack by not taking the false path. With the help of simulation, the performance of the proposed approach was evaluated [15]. If number of nodes is more in WSN, there is very high overhead in the proposed method. Bloom filter technique or some other reduction technique has been utilized in order to decrease the complexity in storing the information matrix at every node. By using this technique proposed method is very effective and efficient to use.

Author name	Year	Proposed	Conclusion
Annie Mathew and J.Sebastian Terence	2017	Proposed various methodologies for the detection of the sinkhole attack. They also discussed and studied the sinkhole attack and its classification and methods for the detection of sinkhole attack by using various parameters.	Provides the observation about the detection of sinkhole attack.
Mahmood Alzubaidi, Mohammed Anbar, Samer Al-Saleem, Shadi Al-Sarawi, Kamal Alieyan	2017	Presented the main objective of this paper is the clear understanding of different types of internal attacks and affects of sinkhole attacks on RPL.	They showed a table which provides the previous representation for the detection mechanisms for sinkhole attack. After comparison the most effective method was observed.
Manpreet kaur, Amarvir singh	2016	Discussed sinkhole is the attack in which all the routing information is captured and advertises by the malicious node after which forces the nodes to route the data towards it.	Performance of the network is degraded by the sinkhole attack. Main objective of this paper is the analysis and detection of the sinkhole attack in wireless sensor network.
Anthonis Papadimitriou, Fabrice Le Fessant, Aline Carneiro Viana, Cigdem Sengul	2009	Proposed two new cryptographic protocols to minimize the degradation of network which is caused by the sinkhole attack on tree-based routing topologies within the wireless sensor network.	It is demonstrated, on the basis of simulation results that resilience can be improved further using this proposed method that prevents the affect of sinkhole attack in case of collision.

Gauri Kalnoor, Jayashree Agarkhed	2016	Discussed major concern in the WSN network is of security for which an appropriate network is required. A vital role in security of a system is played by the intrusion detection system.	For the improvement of performance of the network various routing protocols were discussed in this paper.
Kevin Weekly and Kristofer Pister	2012	Presented the implementation of routing protocols for the Low-power and lossy networks due to the sinkhole attacks as it affect the wireless sensor networks.	Demonstrated that penetration of sinkholes nodes combat the increased density of the network without identifying the sinkholes.
S.Sharmila, Dr G Umamaheswari	2011	Presented the susceptibility of wireless sensor networks to routing attacks. The one-way hash chains were utilized by the protocol for the detection of the exact sink hole.	Simulation results, demonstrate the performance and accuracy of the proposed algorithm in terms of Success rate, false positive rate and false negative rate.
D.Sheela, Naveen kumar. C, Dr. G.Mahadevan	2011	Proposed an approach which is based on the mobile agent has been utilized in order to provide information to every sensor node in these networks.	With the help of simulation, the performance of the proposed approach was evaluated. If number of nodes is more in WSN, there is very high overhead in the proposed method.

Conclusion

In this paper, it is concluded that present information is sensed by the sensor nodes in the wireless sensor network and forwards it to base station due to its decentralized property. Due to small size of the sensor nodes and far deployment energy consumption is the major issue of network. In this review paper, various energy efficient techniques are reviewed in terms of certain parameters

References:

[1] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, In First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003

[2] J. Qi, T. Hong, K. Xiaohui, and L. Qiang, “Detection and defence of Sinkhole attack in Wireless Sensor Network” in Communication Technology (ICCT), 2012 IEEE 14th International Conference on, 2012, pp. 809-813.H

[3] Modares, R. Salleh, and A. Moravejosharieh, “Overview of security issues in wireless sensor networks” in 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, 2011, pp.308-311.

[4] N. Gandhewar and R. Patel, “Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network” in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, 2012, pp. 714-718.

[5] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey” IEEE Communications Surveys & Tutorials, vol. 10, pp. 6-28, 2008.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. “Wireless Sensor Networks: A survey” Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia institute of Technology, 2001.

[7] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, “A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks” Journal of Security Engineering, 2014, pp.241-250

[8] Annie Mathew and J.Sebastian Terence, “A Survey on Various Detection Techniques of Sinkhole Attacks in WSN”, International Conference on Communication and Signal Processing, April 6-8, 2017

[9] Mahmood Alzubaidi, Mohammed Anbar, Samer Al-Saleem, Shadi Al-Sarawi, Kamal Alieyan, “Review on Mechanisms for Detecting Sinkhole Attacks on RPLs”, 2017 8th International Conference on Information Technology (ICIT)

[10] MANPREET KAUR, AMARVIR SINGH, "Detection and Mitigation of Sinkhole Attack in wireless sensor network", IEEE, 2016

[11] Anthonis Papadimitriou, Fabrice Le Fessant, Aline Carneiro Viana, Cigdem Sengul, "Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks", IEEE, 2009

[12] Gauri Kalnoor, Jayashree Agarkhed, "QoS based Multipath Routing for Intrusion Detection of Sinkhole Attack in Wireless Sensor Networks", 2016 International Conference on Circuit, Power and Computing Technologies

[13] Kevin Weekly and Kristofer Pister, "Evaluating Sinkhole Defense Techniques in RPL Networks", IEEE, 2012

[14] S.Sharmila, Dr G Umamaheswari, "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms", IEEE, 2011

[15] D.Sheela, Naveen kumar. C, Dr. G.Mahadevan, "A non cryptographic method of sinkhole attack detection in wireless sensor networks", IEEE, 2011