IDENTIFICATION AND MITIGATION OF SELECTIVE FORWARDING ATTACK IN WIRELESS SENSOR NETWORK

[1]Pushpinder Kumar, [2]Amarvir Singh
[1]Research Scholar, [2]Assistant Professor
[1,2]Department of Computer Science
[1,2]Punjabi University, Patiala,India

Abstract: A wireless sensor network comprises of countless spread over a particular territory where we need to take care of at the progressions going ahead there. Among all the conceivable active attacks, selective forwarding attack is the most widely recognized and destructive attack. In this work, a novel strategy has been proposed to recognize and disengage malicious nodes from the network which are in charge of triggering the attack. The proposed technique is based on the threshold technique for detection of malicious nodes. The exploratory results will demonstrate that proposed strategy detects and separate the malicious nodes from the network proficiently. It will enhance network effectiveness as far as bundle misfortune, defer and expand throughput of the network. NS2 simulator instrument will be utilized as a part of it.

Keywords: **Nodes, Throughput, Energy Consumption, Delay, Protocol.**

INTRODUCTION

Wireless Sensor Network is a combination of tiny lightweight wireless sensors with computing elements. These sensor nodes are generally cheaper in price, with limited energy storage and limited processing capabilities. Wireless sensor network consists of a large number of these sensor nodes (usually hundred or thousand of nodes). These types of networks are highly distributed and deployed in hostile environments [1]. Wireless sensor networks are usually installed at unprotected and bitter environments where security is an essential issue. In such unprotected environments, wireless sensor networks are open to many physical as well as logical attacks. Security of Wireless sensor network is very important as such types of networks are generally causing alerts which require sudden attention. False alerts generated by the wireless sensor networks may lead to unwanted actions [2]. The movement in Wireless Sensor Network relies on upon a number of queries created per Meantime. The sink node transmits the data to be detected by sending a query all through the sensor field. The sensor nodes react to the query by social event the data utilizing their sensors. At last when the sensor nodes have the consequence of the infused query will answer to the sink node through some directing convention. A sensor node likewise totals the answers to a solitary reaction which spares some of the packets to send back to the sink node [3]. The misdirection attack is basically a type of DoS attack which can occur at various instants. A communication that is to occur within the network is denied due to the presence of malicious nodes due to which the service is also further not provided to the destination. There are a number of nodes deployed in the network [4]. There is a source which sends data to the destination. In this attack, one node attack acts as a malicious node which sinks all the packets and drops to forward it. The path is established between source and destination using AODV protocol. Data is transmitted from source to destination. During data transmission, one intermediate node acts as a malicious node which triggers misdirection attack in the network. In the figure, the source node sends data to the destination through AODV. During transmission, the intermediate node becomes malicious and pretends itself as a destination node. Therefore this malicious node sinks all the packets and avoids forwarding it to the original destination. Misdirection attack can occur in two ways [5]. Packets Forwarded to a Node Near to the Destination sort of misdirection attack is less serious, on the grounds that packets compass to the destination however from an alternate course which assists delivers long delay, consequently diminishing throughput of the system (bit exchange every second). Packets Forwarded to a Node Far Away from the Destination is the second type of attack. In order to send the node away from the network, the misdirection attack can be very problematic here [6]. The destination of the nodes is modified and so they never reach the desired destination. This results in continuous delay within the network and negligible throughput is also generated. As these attacks results in degrading the performance of the networks, the misdirection attacks are very harmful for providing reliable networks.

LITERATURE REVIEW

Juby Joseph et.al (2014) presented in this paper [7]that there is a lot of use of the wireless sensor networks in fields which have consumers and in industrial and defense areas also it has its involvements. The networks are vulnerable and prone to the attacks of outsiders. It is very commonly found that the attackers attack the security of the networks. The Denial of Service (DoS) attacks has another kind of attack known as misdirection attacks which mislead the packets of the network. There are various selfish nodes present in the network which perform such activities and they decrease the efficiency of the network. The messages are not forwarded to the intended nodes due to the unexpected behaviors of some nodes.

TarekAzzabi, et.al (2017) proposed in this paper [8] that a communication infrastructure is given for multiple engineering purposes within the wireless sensor networks. This infrastructure is used within numerous applications that are evolving with the emerging trend. It is very important to ensure the security of these types of networks as the data transmitted across these networks

is highly sensitive and private. Thus, the security measures to be taken are very important to be discussed within this work. The various issues are arising within the current applications during the collection and exchange of data within these networks which need to be investigated in proper manner. This paper focuses on all such issues and presents the studies elated to solving all such problems.

Ju young Kim et.al (2014) presented in this paper [9] about the investigation of the distinctive vulnerabilities, threats and attacks for Wireless Sensor Networks. In this paper, the analyzing of network researchers is presented. Further the various network security threats are also studied here for providing solutions to all such related issues being faced. The diverse vulnerabilities, threats, and attacks that could place WSNs in a crucial or basic circumstance have been recognized and talked about in their paper. The diverse classifications for these threats are characterized to distinguish a conceivable countermeasure plan pertinent for every risk characterization.

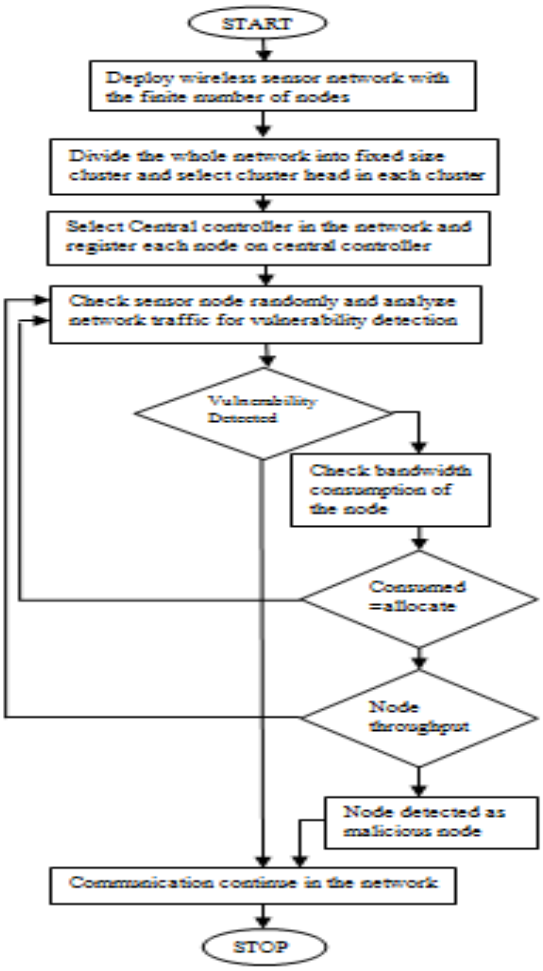
Roshan Singh Sachan et al (2012) [10], presented in this paper that there are various types of attack that the wireless sensor network faces. There are a lot of instances that have been occurring in which the detection of the attack of DoS and misdirection attacks has not been possible. The node in misled in such a way that the node reaches to any other node except for the destination node. The degradation of performance occurs due to such cases. Here in the article, such an attack has been proposed for the topological analysis of the wireless network. An algorithm is proposed which will provide a help for the assistance in throughput and delaying of the packets. Better performance is observed in the tree network topology than in the mesh topology network.

Leena Rani et al (2015) presented in this paper [11] that the main degradation of energy occurs due to the attacks that are caused by the intruders. The misdirection attack, a type of DoS attack has caused a lot of problems as it is difficult to be detected. Approaches like cluster based approach are explained in this article which will prevent the energy from being destroyed. Through this, the maintenance of the throughput is also done. The article has proposed various such methods which will help in the prevention of all the attacks and will help maintain the network secure.

Anita Daniel. D, et.al [12] presented in this paper that there are a lot of applications that have been utilizing wireless sensor networks within them due to their dynamic properties. There is a need to study the security challenge arising within these networks which is presented in this paper. The numerous security methods proposed which also include the methods of preserving energy are presented in this paper. In order to provide an efficient wireless sensor network there is a need to take control of the security methods along with the other limitations present. Only then can the problems be avoided in a proper manner. There is a need of real-time implementation which can be provided by enhanced HMAC protocol within these networks in the future work.

RESEARCH METHODOLOGY

In this work, in order to recognize and remove the malicious nodes from the network, a technique has been proposed. On the basis of traffic analyzer and threshold values present within the network, there is a technique proposed. The central controller is chosen within the network depending on the trust values of the nodes. Depending on the data packets that are re-transmitted within the network, the trust value of the node is computed. There is a central controller node that registers each node according to IP, MAC address and the current data. The bandwidth required for communication related to the base station is assigned using the central controller node. Depending on the hop count and sequence number, a secure and efficient path is generated from sensor node to base station. The data is transmitted from the sensor node. Further the central node checks individually each node in a random manner. The nodes that have threshold unequal to the decided threshold value are to be detected and presented as malicious node within the network. For removing such malicious nodes from the network, a multipath routing method is presented here.



Flowchart of Proposed Work

Experimental Results

The proposed algorithm has been implemented in NS2 and the results are analyzed on the basis of various performance parameters such as delay, throughput and energy consumption.

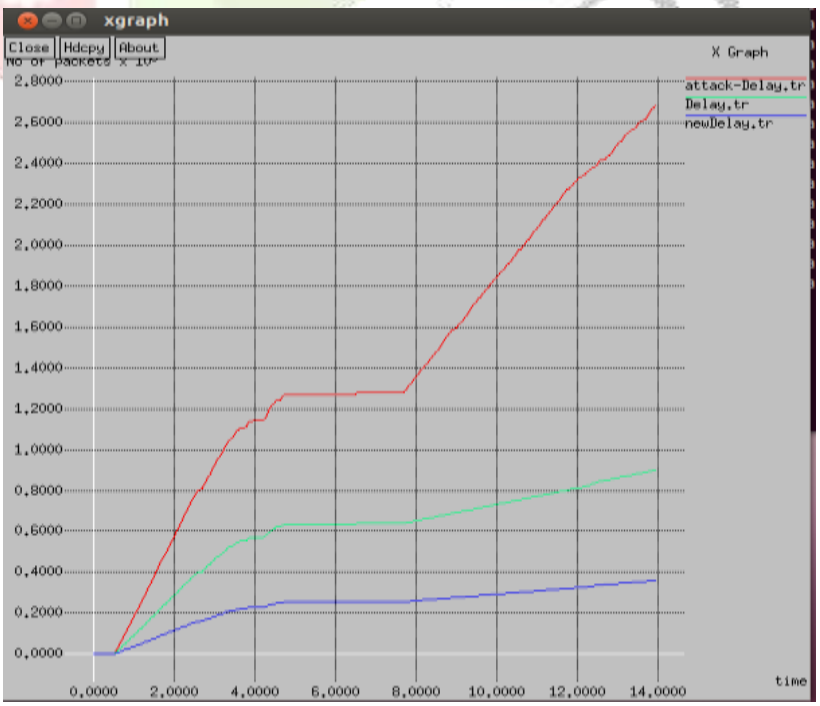


Fig 1: Delay

As shown in figure 1, in terms of the delay parameters, there is a comparison made amongst the LEACH, the attack as well as the proposed technique. There is maximum delay caused during the presence of attacks. There is least delay within the proposed method as there is no attack present in that network.

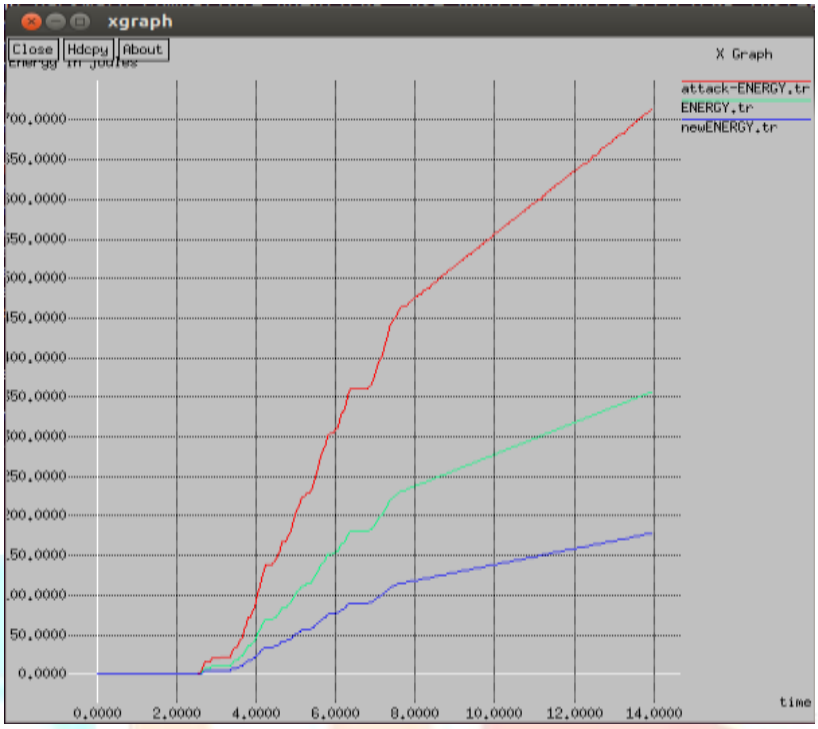


Fig 2: Energy Consumption

As shown in figure 2, the comparison of the proposed, attack scenario is shown in terms of energy. It is been analyzed that energy consumption of the proposed scenario is least as compared to attack scenario.

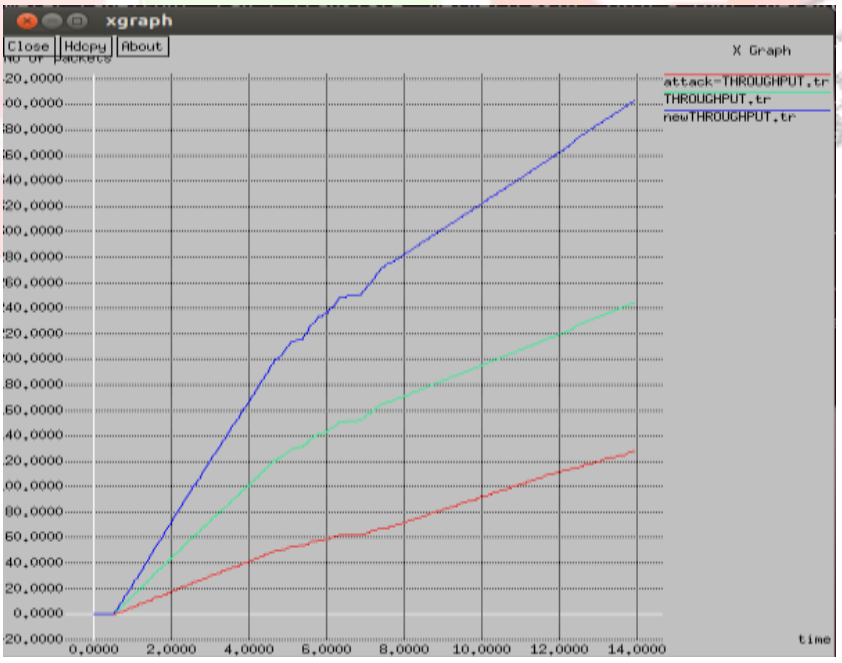


Fig 3: Throughput

As shown in figure 3, a comparison has been made for the attack and the proposed method in terms of throughput. In comparison to the other methods, the throughput of proposed method is the highest.

Conclusion

The technique is proposed in this paper which can identify and separate the malicious nodes from the network. The malicious node is identified on the basis of the delay such that the node that contributes maximum delay will be recognized as malicious node. This helps in minimizing the energy consumption of the network along with the increment in throughput and reduction of delay within the network. It is been analyzed that proposed technique performs well for the detection and isolation of selective forwarding attack in wireless sensor networks.

REFERENCES

[1]Parida, NachiketaTarasia, TulasiAmbashaPatnaik, "Security against Selective Forward Attack in Wireless Sensor Network", 2012, IOSR Journal of Engineering, Vol. 2(5) pp: 1200-1206

[2] W. Z. Khan, Y. Xiang, and M. Y. Aalsalem, "Comprehensive study of selective forwarding attack in wireless sensor networks," 2011, International Journal on Computer Network and Information Security, vol. 1, pp. 1–10

[3]Leela Krishna Bysani and Ashok Kumar Turuk, "A survey on selective forwarding attack in wireless sensor networks", 2011, Devices and Communications (ICDeCom), 2011 International Conference on. IEEE

[4]JyotiShokeen, Palak, Preeti Devi, "A Survey on Selective Forwarding Attacks in Wireless Sensor Networks", 2016, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, pg. 45-50

[5]RachanaSrivastava, InderjeetYadav, "Securing Wireless Sensor Networks from Selective Forwarding Attack", 2016, International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 5

[6]Leela Krishna Bysani, Ashok Kumar Turuk, "A Survey On Selective Forwarding Attack in Wireless Sensor Networks", 2011, International Conference on Devices and Communications

[7]Juby Joseph, Vinodh P Vijayan," Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol", 2014 International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Issue 7, pp- 825-830

[8]Tarek AZZABI, Hassene FARHAT, Prof Nabil SAHLI, "A Survey on Wireless Sensor Networks Security Issues and Military Specificities", 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), volume 19, issue 31, pp- 293-312

[9]Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks", 2014, Journal of Security Engineering, vol 3, issue 2, pp. 241-250

[10]Roshan Singh Sachan, Mohammad Wazid, AvitaKatal, D P Singh, R H Goudar, "A Cluster-Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", 2013 IEEE, Communications and Signal Processing (ICCSP), International Conference, volume 7, issue 12, pp- 31-47

[11]Leena Rani, Er. Veena Rani, "A Novel Study on Data Flow Routing with Energy Optimization under Different Attacks in WSN", 2015, International Journal of Engineering and Technical Research (IJETR), Volume-3, Issue-5, pp- 134-137

[12] Anita Daniel. D, EmaldaRoslin. S, "A Review on Existing Security Frameworks with Efficient Energy Preservation Techniques in Wireless Sensor Networks", 2015, IEEE ICCSP conference, vol 5, issue 16, pp- 793-835