Novel Approach for Isolation of Sink hole attack in WSN

[1]Minakshi, [2]Satnam Singh, [3]Mr. Navjot Singh
[1]*Research Scholar, Sri Sai College of Engineering and Technology, Badhani, Pathankot, India*
[2]*Head of Department, Sri Sai College of Engineering and Technology, Badhani, Pathankot, India*
[3]*Co-Guide*
([1]sharmaminakshi.ms143786@gmail.com,[2]jeevanjot1999@gmail.com)

Abstract-A network that does not contain any central controller within it and is self-configuring in nature is known as a wireless sensor network. It is difficult to maintain the security and energy consumption of these networks due to such properties. This research work is based on an active type of attack which is commonly known as sinkhole attack. In the sink hole attack the malicious nodes spoof identification of the base station and act like base station. The sensor nodes start transmitted data to malicious nodes instead of base station. In order to identify and eliminate such malicious nodes, this research proposes a new technique that uses identity verification in order to provide a secure environment for communication in the network. Simulations are performed by implementing the proposed technique in NS2. The proposed technique give results better as compared to existing techniques in terms of certain parameters.

Keywords-*Sink Hole; WSN; Unique Id.*

I. INTRODUCTION

The collection of numerous sensing devices such that the information related to the surrounding environment of a specific region can be known is called a wireless sensor network (WSN). The sensing devices which are otherwise known as nodes are very small in size and also have least cost. Initially, these networks were only deployed within the military regions in which keeping a track on the activities of opposite parties was very important. Each of their movements was tracked and the important information was used by authorities to take appropriate actions [1]. There are several such applications in which it is very difficult to monitor the activities or mobility going on in such wide regions. Thus, the deployment of WSNs is very helpful in such applications. Today, there are large numbers of applications in which WSNs have been deployed. They have been performing certain operations such as sensing, processing and communicating of the data within the regions. The region that is to be monitored is deployed by WSN such that the sensor nodes are randomly dispersed all across the region. Mainly the applications of WSN are large and hostile due to which certain constraints also arise for them [2]. WSNs are deployed within regions that are not suitable as well as do not require any infrastructure. The deployment of around hundreds to thousands numbers of sensor nodes is done such that the tasks that are required to be performed can be accomplished [3]. Since the WSNs are heterogeneous is nature, it is important to study the manner in which it is possible to deploy them in several regions. There are several types of operations performed by the sensor nodes deployed within WSNs. In order to gather the information from certain regions, it is important to ensure that the network is distributed all across it. For performing the overall analysis, it is important to monitor the areas in cooperative manner such that all the relevant data is collected [3]. WSN consists of two important components within it which are aggregation and base station. From the sensors present around the regions, the information is collected and it forwarded to other nodes such that it can be passed on to authorities. The base station is known as the device towards which all the collected data is passed on. The base station is responsible to transfer the information further. WSNs are known to be very different from other networks since they have highly unique properties from others. The possibility of attacks to enter these networks is also high [4]. The vulnerability and susceptibility of these networks to other security attacks is very high since they include broadcasting communication. The entrance of attacks is higher in the networks since they are deployed in higher and dangerous regions. Several attacks can occur at various layers of the network since all these layers work in different manner and perform different functions. Several routing protocols are included here in which the security mechanisms are not provided. Therefore, it is very easy for the attackers to breach the security of networks. Collision attack occurs when the channel arbitration faces neighbor-to-neighbor communication within the link layer. There will be disruption of complete packet in case when collisions occur in any region of the deployed network. Therefore, there is a need to retransmit the packet since single bit error is caused. In the networks, a low-latency link is

created due to which at huge speeds using multi-hops the packets are forwarded. This results in causing a wormhole attack in the network [5]. This attack is known to be a huge threat for any routing protocol available in the networks. It is very difficult to detect or prevent such attack. An attack uses a malicious node to create an influence on the network's traffic. Thus, numerous entities are created in the network which results in causing Sybil attack. An ID is generated in case when any fake additions are made or the duplicates of already available legitimate identities are created. DoS completely interrupt the efficiency of networks here. The physical disruption of network components is seen here when this attack occurs [6]. Further, this attack also results in destroying the wireless transmission. This attack generates noise, collision or interference at the receiver's end. The attacker has certain targets to be focused on amongst which few are the infrastructure of network, the server application as well as the network access. The victim node transmits the extra un-required data in DoS attack.

II. LITERATURE REVIEW

Jianpo Li, et.al (2018) studied about the wormhole attack and reviewed what kinds of aftereffects are caused when it occurs. They proposed AWDV-hop that is a secure mechanism, using which the above mentioned issues can be minimized easily and also the effects of the wormhole attack [7]. They created the neighbor node relationship list (NNRL) by utilizing the broadcast flooding used by the first algorithm. NNRL helps in assigning certain IDs to the nodes that surround each other. With the help of this imagined beacon node, the distance to other beacon is calculated within the NNRL. It is possible to recognize the attack that was actually performed. Here, marks are placed in the scenarios. There are few unknown nodes available as well which also mark themselves as beacon nodes. The outcomes are achieved by simulating the proposed technique.

RanuShukla, et.al (2017) presented the wireless Sensor Network (WSN) an emerging technology due to which it has been utilized in almost every field [8]. It is important to include a secure routing protocol in these networks. Designing an appropriate protocol for a particular scenario is also very challenging. In order to provide the security to the WSN, the technology of the cryptography is not possible to utilize as it is heavy. Therefore, to overcome this major issue they proposed an optimal solution in this paper called as TESRP. Even though the attack is not prevented from occurring here, this is known as the best trust based protocol available. The sequence number is used with the trust algorithm to provide secure scenario within the networks.

Bharat Bhushan, et.al (2017) discussed that it is possible to compute few physical constraints of a specific region by deploying a sensor network that uses wireless communication mode to transmit the data across its nodes. However, the communication being performed is free due to which this network is not much secure [9]. An attack in which no nodes are affected but the important information is stolen is known as wormhole type of attack. The bits that are being forwarded across the network are tracked down by a malicious user and then replayed. There is only one path available through which it is possible to transmit the data across the network. This path is however, wormhole. The user however, transmits the data through this path and the data is no longer secure. To provide a secure scenario in these networks, it thus becomes necessary to propose a novel design. This design helps in providing an environment in which data can be exchanged securely.

Mayank Kumar Sharma, et.al (2016) presented the wireless sensor network is termed as the scenario that provides communication by linking nodes amongst themselves [10]. The communication mechanism followed here is open due to which it is affected by various different attacks. They discussed the wormhole attack in this paper and considered it as major attack as compared to all other issues. Therefore, they utilized the routing protocols in order to minimize effects of this wormhole attack. To make sure that the rink is minimized, comparative analysis is made amongst the techniques that were designed earlier and the new designed approach. This paper aims to reduce the effects of high transmission power which are resulted because of the occurrence of attack. They also introduced more methodologies using which all these issues can be minimized easily.

Ali Modirkhazeni, et.al (2016) presented there are various major area has been covered by this technology. It is growing technology, has been utilized in various application [11]. In this WSN network, the conventional security mechanisms have been not utilized as they are heavy and have limited nodes. They discussed the wormhole attack in this paper and considered it as the major attack among others as it breakdown the functionality of whole network. The attack scenario results in creating a tunnel from which the data is transmitted. Within the networks, it becomes very difficult to identify this kind of attack. This paper designs a new distributed network discovery mechanism which can be applicable easily. The outcomes achieved after conducting experiments clearly depict that the new designed approach is highly secure and keeps the attacks away from private data transmissions.

Swati Bhagat, et.al (2016) presented the widespread application of this technology, has been widely utilized in almost every application nowadays. Today, diverse fields have been deploying these networks to ease their work and provide improvements in their technologies.

However, it is also important to ensure that these scenarios are secure. To do so, the various attacks which can possibly occur in the network are studied and solutions are provided to prevent them from making any destruction. A wormhole type of attack also results in degrading the overall performance of network due to which solutions are present by applying which it is easy to remove it [12]. A wormhole can be recognized using a powerful transmission as per this proposed approach.

III. RESEARCH METHODOLOGY

The different steps of proposed approach are explained below:

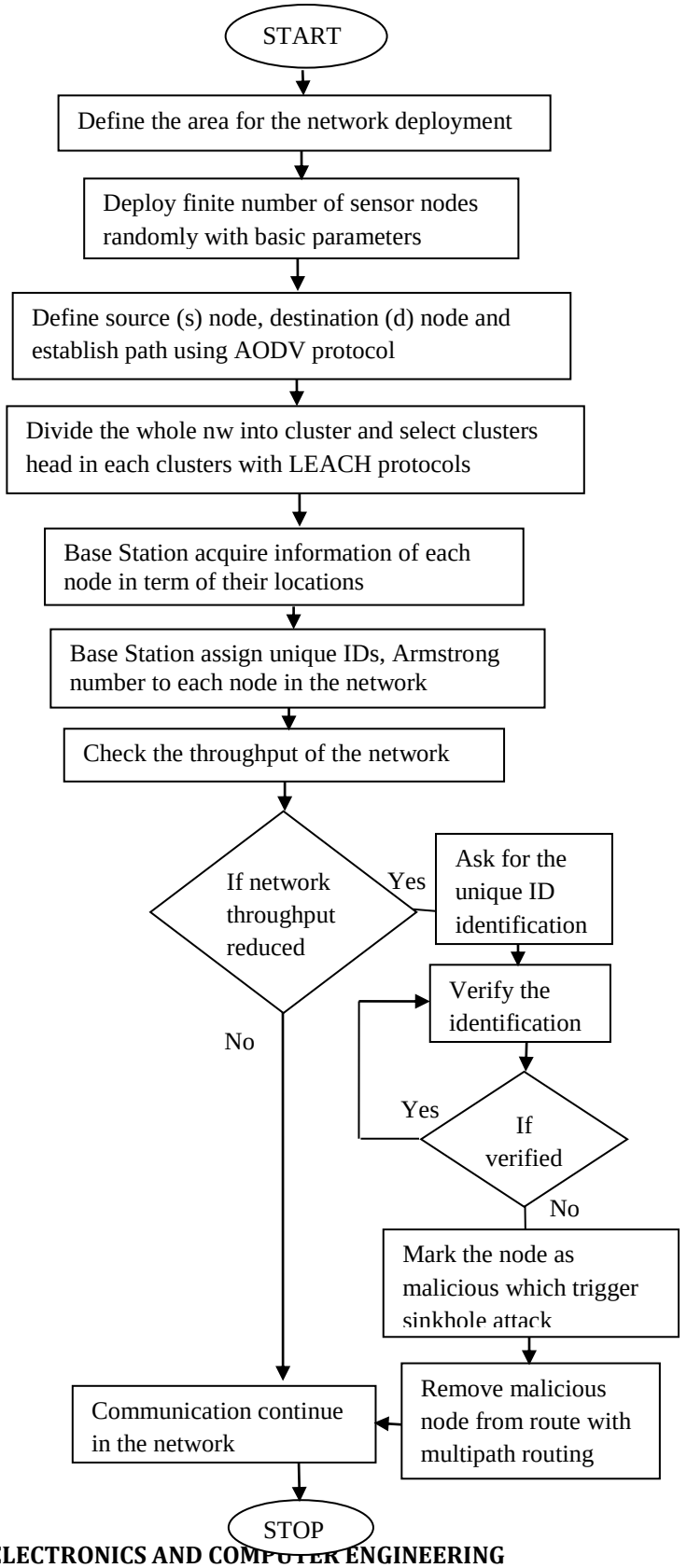
A. Network Deployments:-

The wsn is the self configuring types of nw in which sensors node sense the information and passes the information to base station. Such types of networks, various type of active attacks are possible in the network. Among all the type of attacks the sink hole attack is the attack which is difficult to detection and isolation from the network due to its unique properties.

B. Key Distribution of the Base station:-

The novel approach is implemented in this research work for the detections of malicious node. In techniques of intrusion detection system, require extra software for the detection of malicious nodes which affect performance of technique for the detection of malicious nodes. The second technique which is popular for the detection of malicious nodes is the Delphi technique. This technique do not has any parameters of quality of service due to which we are not able to detect malicious nodes accurately. The technique which is proposed in this research work donot required any extra software and also includes the quality of service parameters for the detection of malicious nodes.

In the proposed technique, the sensor nodes are deployed in the finite area with the basic configuration. In the network, the source and destination nodes are defined randomly and also the path from source to destination is selected with AODV protocol. The AODV protocol is the reactive routing protocol; in which source node send the route request packets and nodes which are adjacent to destinations replies back with the routes replies packet. The paths from sources to destinations are selected on the basis of hop count and sequence number. In the communication, the malicious node spoof the identification of the base station and sensor nodes pass data to malicious node instead of base station. the bases tations perform the task of node localization and key distribution. The base station distributes keys to all sensor nodes in the network and also defines the virtual keys. The sensor nodes when transmit the data to the base station, it will ask for the unique key of the base station. The base station calculates the key with Armstrong number.



Fig,1: Proposed Flowchart

C. *Detection of Malicious node:-*The original base station is able to provide its identification but the malicious node is not able to provide its identification. When the malicious node is not able to provide its identification, it is detected as the malicious node. The keys which are distributed in the network, to generate such keys the concept of Armstrong number is applied in this work. The Armstrong number is the unique number 16 bits which is generated from the various color combinations. The 16 bit Armstrong number of hard to crack and also the unique identification of each node is concatenated with the key to form final key.

D. *Isolation of Malicious nodes:-*Multipath routing is performed at the end which helps in removing the malicious node completely from the network. An echo message is sent to all of the nodes that exist in the network in case when a malicious node is recognized. It will remove malicious node from the network through the multipath routing.

IV. EXPERIMENTAL RESULTS

The proposed work is implemented in NS2 and the results are evaluated by making comparisons against existing work in terms of several parameters.

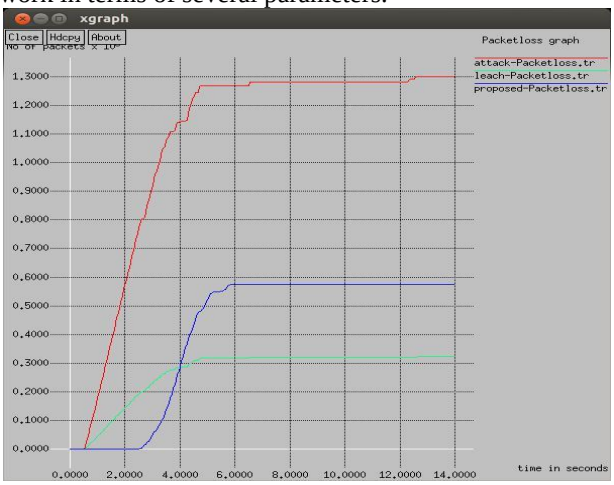


Fig.2: Packet loss comparisons

In figure 2, the LEACH protocol shows the maxi effect and reduced packet loss in the network after the isolation of the sinkhole attack.

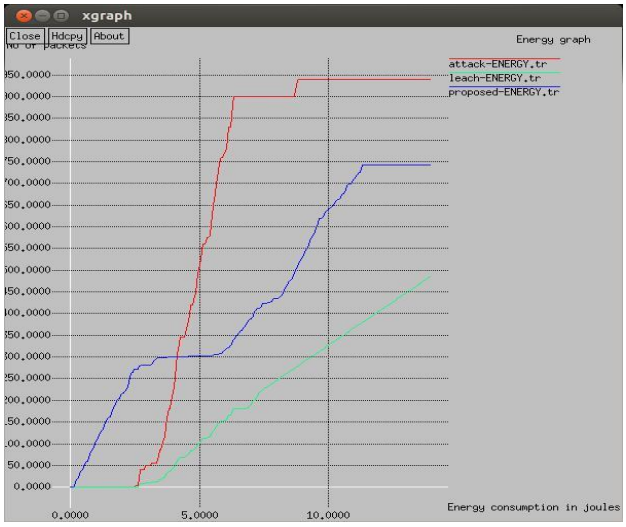


Fig.3: Energy Comparison

Figure 3 shows that the energy consumption of the scneario that includes attack is the highest. The implementation of proposed protocol in the network reduces the amount of energy being consumed here.

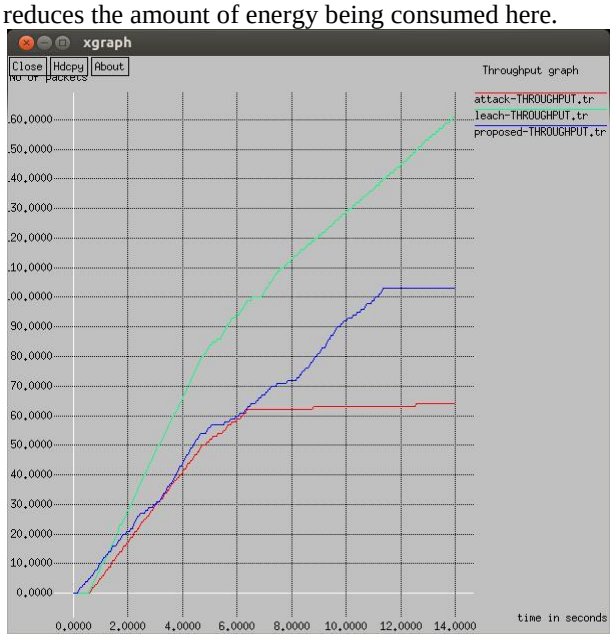


Fig.4: Throughput Comparisons

Figure 4 compares three scenarios which are the proposed, attack and existing genuine scenario and it has been analyzed that the network throughput is increased by steady rate after the isolation of the attack.

V. CONCLUSION

In this work, it is concluded that the LEACH protocol is most effective technique used to reduce energy consumption of the wireless sensor networks. it is the network. The small sizes of sensor nodes are responsible

for the reduced life time of these sensor nodes. The sinkhole attack is one of the active types of attack which reduces the LEACH protocol's performance. The technique of mutual authentication has been proposed in this thesis work, which detects and isolates the sinkhole attack. The outcomes achieved show that there is minimum packet loss and energy consumption rate achieved when the proposed approach is implemented. Thus, the proposed technique helps in reduction of energy consumption, increment in the throughput and reduces the delay time.

REFERENCES

[1] Xun Li, Guangjie Han, Aihua Qian, Lei Shu, Joel Rodrigues, "Detecting Sybil Attack based on State Information in Underwater Wireless Sensor Networks", 2013

[2] James Harbin, Dr Paul Mitchell, "Reputation Routing To Avoid Sybil Attacks In Wireless Sensor Networks Using Distributed Beamforming", 2011 8th International Symposium on Wireless Communication Systems, Aachen

[3] BinZeng, Benyue Chen, "SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless Sensor Network", 201O International Conference on Computer and Communication Technologies in Agriculture Engineering

[4] Shanshan Chen, Geng Yang, Shengshou Chen, "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks", 2010 International Conference on Communications and Mobile Computing

[5] Ren Xiu –li, Yang Wei, "Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network", IEEE, 2009

[6] 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

[7] Jianpo Li1 , Dong Wang1 , Yanjiao Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network", IET Wirel. Sens. Syst., 2018, Vol. 8 Issue 2, pp. 68-75, the Institution of Engineering and Technology 2018

[8] RanuShukla, Rekha Jain, P. D. Vyavahare, "Combating against Wormhole Attack in Trust and Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network", Proceeding International conference on Recent Innovations is Signal Processing and Embedded Systems (RISE -2017) 27-29 October,2017

[9] Bharat Bhushan, Dr. G. Sahoo, "Detection and Defense Mechanisms against Wormhole Attacks in Wireless Sensor Networks", IEEE, 2017

[10] Mayank Kumar Sharma, Brijendra Kumar Joshi, "A Mitigation Technique for High Transmission Power based Wormhole Attack in Wireless Sensor Networks", ieee, 2016

[11] Ali Modirkhazeni, Saeedeh Aghamahmood, Arsalan Modirkhazeni, Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE, 2016

[12] Swati Bhagat, Trishna Panse, "A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network", IEEE, 2016