Novel Technique for Isolation of Misdirection Attack in WSN

Sukhpreet Kaur Er.[1], Abhinash Singla[2]
[1]*Research Scholar, Bhai Gurdas Institute of Engineering and Technology, Sangrur, Punjab, India*
[2]*Head of Department, Computer Science and Engineering, Bhai Gurdas Institute of Engineering and Technology, Sangrur, Punjab, 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. A sensor hub, for the most part, comprises of sensors, actuators, memory, a processor and they do have correspondence capacity. These sorts of networks are much powerless against security attacks. Many kinds of active and passive attacks are conceivable in the sensor network. Among all the conceivable active attacks, misdirection attack is the most widely recognized and destructive attack. This attack debases network execution and prompts denial of service attack. The attack is triggered by the malicious hub which is available in the network. 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 novel procedure is based on Delphi system. 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 - WSN, active attack, misdirection attack, Delphi.

I. INTRODUCTION

Wireless Sensor Network is a combination of tiny light weight wireless sensors with computing elements. These sensor nodes are generally cheaper in price, with limited energy storage and limited processing capabilities. Wireless sensor network consist of 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]. There are two types of sensors nodes in Wireless Sensor networks, sensor node and a Sink node. A large number of sensor nodes are there in Wireless Sensor Networks which collects or sense the data and transmit it to the sink through multiple hops [2]. The sink can use that data locally or globally using internet. Sensor nodes use battery power as an energy source. Battery is a constrained force asset and as wireless sensor networks are normally conveyed at threatening ecological it is about illogical to supplant batteries of the sensor nodes, so control utilization in wireless sensor networks is dependably a noteworthy concern. In this manner it is frequently required to have energy proficient strategies which can build the life of these wireless sensor networks. An inbuilt exchange off system ought to be made so that the end-client ought to decide on dragging out network lifetime at the decrement of lower throughput or higher transmission delay [3]. The movement in Wireless Sensor Network relies on upon number of queries created per Mean time. 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 the quantity of packets to send back to the sink node. Wireless sensor networks are usually installed at unprotected and bitter environments where security is an essential issue [4]. 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. Security issue is the main concern in sensor network. Worm hole Attack occurs in which a malicious node, records packets at a particular location in the network and tunnels them to another location. Black hole Attack is the one in which malicious node captures and reprograms a set of nodes in the network and blocks the packets are received instead of forwarding them towards the base station. In Jamming attack the radio frequencies are inferred that is used by the sensor node. Attacker monitors initially in order to verify frequency at which destination node is getting signal from the sender [5]. In a sinkhole attack, the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node creating a metaphorical sinkhole with the adversary at the center. In Man- in- the- middle attack an attacker sits in between the sender and receiver node. The information being passed by the sender is captured by the attacker sitting in the middle. Misdirection Attack inside WSN is the most popular denial of service attack. This attack can be performed in different ways. A malicious node could deny a substantial course to a specific node in this way denying service to the destination. Misdirection attack can occur in two

ways [6]. Those are which include Packets Forwarded to a Node Near to the Destination and Packets Forwarded to a Node Far Away from the Destination. When the Sink-hole attack occur in the WSN, the performance of WSN starting to decrease in term of some performance metrics such as packet delivery ratio, end to end delay and packet loss.

II. LITERATURE REVIEW

Sneha Kamble et al (2017) discussed in this paper, that within WSN data sending directly to the sink node raise various problems. Information gathering technique is the center of the WSN. In this information aggregation technique is used to decrease the energy consumption as well as enhance the network lifetime. In this paper data aggregation is performed to avoid such problems related to energy. An energy effective system in which data collection nodes are utilized for gathering data from cluster head inside the cluster. The lifetime of the wireless network is improved by forwarding the data in aggregated format [7]. **C. Anand et al (2016)** proposed in this paper because of the scattered way of WSNs, resource constraints, the radio link for multi-bounce communications and their remote region deployment, In the proposed mechanism, a methodology has been created to determine the issue of DoS attacks by actualizing wordings, for example, Intruder Detection System, validating nodes with a key mechanism and retracing routing path as a sly activity from the path required with the victim node as an internal attacker in the network. The essential center of this proposed work is to contribute secure and reliable data transmission over source and destination by determining DoS attack [8]. **Bijan Paul et al (2015)** discussed in this paper, wireless sensor network (WSN), data collecting from the environment and sending that data to be processed and evaluated is the most important issues. Hence the comparison between routing protocols is required because performance of any routing protocol can be changed according to various parameters such as speed, pause time, number of node, and traffic scenario (network topology). In this paper routing protocol AODV, AOMDV, DSR and DSDV has been analyzed by comparing the different performance matrices such as packet delivery ratio (PDR), loss packet ratio (LPR), and average end to end delay (Average End to End) with varying pause time and number of node under TCP & CBR [9]. **Rajendra Prasad Mahapatra et al (2015)** discussed in this paper, Low Energy Adaptive Clustering Hierarchy (LEACH) a well known cluster based protocol. LEACH protocol is used for enhance the life time of the network. LEACH operation is divided into following rounds 1)Set up phase- In this phase nodes are selected as a cluster head(CH) on the basis of energy and distance. 2) Steady state phase- this stage is for data transmission. In this nodes sense data and send this data to their respective CH node. Then processed data will be sending to the base station. So LEACH is a balanced energy consumption protocol for wireless sensor network [10]. **Leena Rani et al (2015)** presented in this paper, when there is a change in the network topology, there is a change in the energy efficiency and the fault tolerance protocols. The maintenance of both of the parameters is very important and so the various methods have been proposed which can prevent the attacks to happen. 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 prevention of all the attacks and will help maintain the network secure [11]. **Ruchita Dhulkar et al (2015)** presented in this article about the security of the wireless sensor networks. There are many attacks which are dangerous for the performance of the network like black hole, jamming, wormhole etc. Misdirection is most dangerous routing attacks network. In this paper they proposed a technique to detect malicious node to work network member in the data routing. Various experiments are conducted in order to analyze the performance of proposed algorithm. On the basis of these experiments it is seen that the proposed algorithm provides better results in terms of various parameters in comparison to existing approaches [12].

III. RESEARCH METHODOLOGY

In this work, network is deployed with finite number of sensor nodes and using leach protocol whole network is divided into fixed size clusters. The cluster heads are selected in each cluster on the basis of distance and energy. DCN (Data Collection Node) node formation is based on the location of CH and connection time. DCN collects the aggregated data from CH and forward towards BS. The shortest path will be established from source to destination on the basis of proactive routing protocol. Some malicious nodes exist in the paths which are responsible to trigger misdirection attack which leads to increase in network delay. In this work, technique will proposed which detect and isolate malicious nodes from the network which are responsible to trigger misdirection attack in the network.

A) Algorithm Steps:

Start( )

1. Deploy the wireless sensor network with fixed number of mobile nodes and in fixed area
2. Divide whole network into fixed size clusters and select cluster head in each cluster
3. Cluster head selection ()

a. node=0 /// Node identification

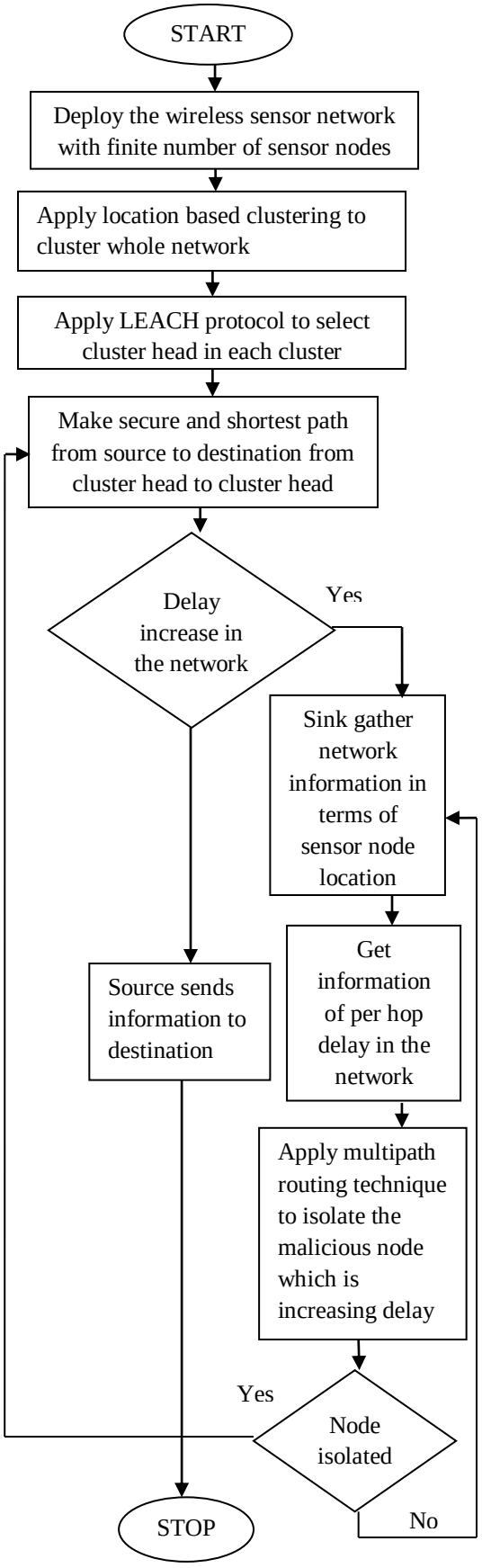
b. For (i=0; i<n ; i++)

a. If

(distance and energy (a(i)
)<a(i+1);
b. Node= a(i);
Else
Node=0;
End
4. The shortest path will be established from cluster head to sink
5. Verify secure path ()
a. Get co-ordinate of node whose id is 0
b. For (i=0; i<n;i++)
c. A(i)=a(i-1)+18;
d. End
e. Calculate distance between all nodes ()
a. Distance =(a(i+1)-a(i))^2+(a(y+1)-a(y))^2
6. If (any nodes adjacent node !=saved information)
7. That node will be detected as malicious node in the network
End

As shown in Figure 1, the whole network is deployed with the finite number of sensor nodes and the whole network is divided into fixed size clusters. The location based clustering is applied to divide the whole network in the clusters. In the each cluster, cluster heads are selected using the technique of LEACH Protocol. In the LEACH protocol, energy and distance of each node is checked, node which has maximum energy and minimum distance from the other nodes is selected as the cluster head. All the nodes in the network will aggregate its data to its cluster head. The cluster head will establish path through other cluster heads and transmit data to base station. To establish path from source to destination, DSDV routing protocol is used. It maintains the information in the form of tables at every node. The source node select best path on the basis of hop count and sequence number. The path which has minimum hop count and maximum sequence number will be selected as the best path to destination. The source nodes start transmitting data to destination on the path. In the selected path, some malicious nodes are their which are responsible to trigger misdirection attack. To detect and isolate malicious nodes, the base station will apply technique of node localization. In the technique of node localization, base station will gather node information in terms of their location. The gathered information also contains the distance of each other from the base station. The distance factor leads to count delay on each hop which is on the established path. The base station when detect that delay is increased on the established path. The base station start counting delay on each hop, the node which increase delay in the network so, it will be detected as the malicious node from the network.

B) Flowchart: Below is shown the proposed flowchart (fugure 1):



IV. EXPERIMENT RESULTS

The proposed algorithm has been implemented in NS2 and the results are analyzed in terms of various parameters such as delay, throughput, energy, jitter and packet loss.

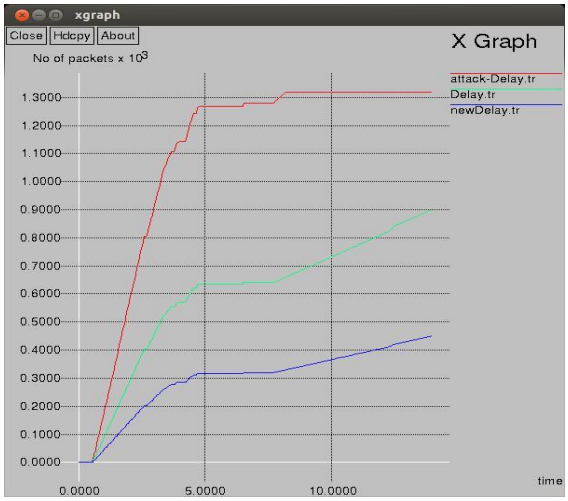


Fig.2: Delay graph

As illustrated in Figure 2, the Delay graph has been plotted. This graph shows the delay of without attack, with attack and the delay observed in the new proposed work. The performances are compared. It has been analyzed that delay in the attack scenario is maximum and delay is reduced in proposed scenario due to isolation of attack in the network.

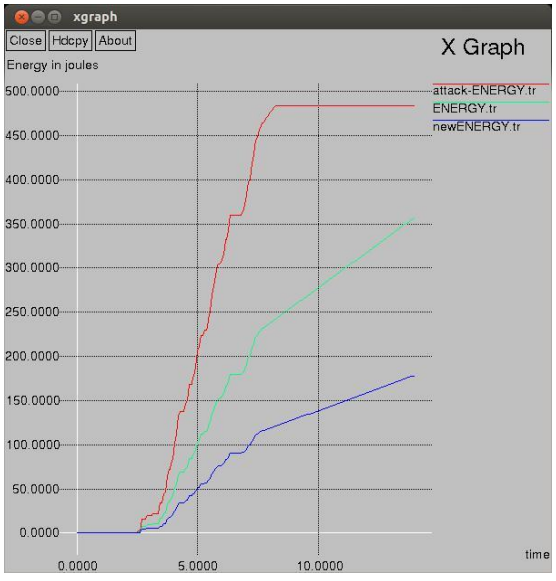


Fig.3: Energy graph

As illustrated in the Figure 3, the energy consumption of the without attack, with attack and new proposed work is compared. Due to the attack in the network, the graph clearly shows that the energy consumption is more in the previous network. When fault is removed from the network, energy consumption is reduced from the network.

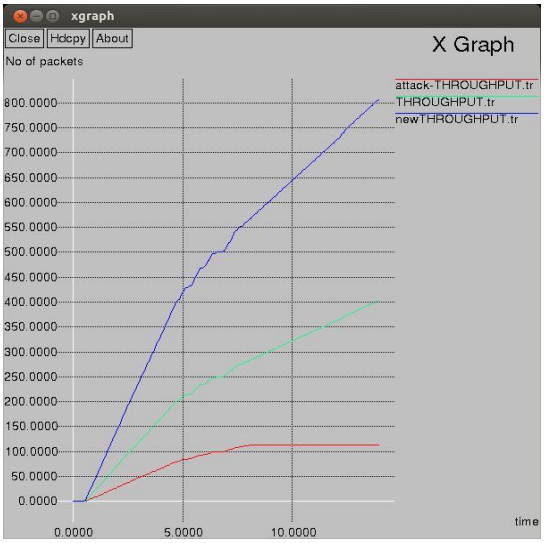


Fig.4: Throughput Graph

As shown in the Figure 4, the comparison of without attack, with attack and proposed scenario is shown in terms of throughput. It has been analyzed that throughput of the proposed scenario is maximum when the malicious node is isolated as compared to other two scenarios.

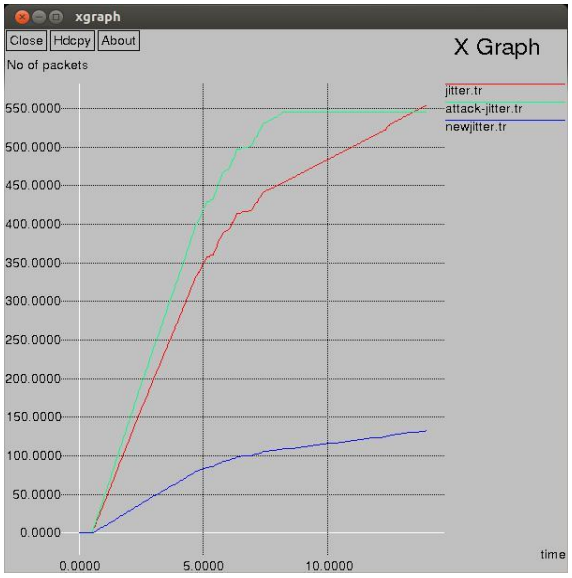


Fig.5: Jitter Graph

As shown in Figure 5, the comparison of without attack, with attack and proposed scenario is shown in terms of jitter. It has been analyzed that jitter of the proposed scenario is minimum as compared to other two scenarios.

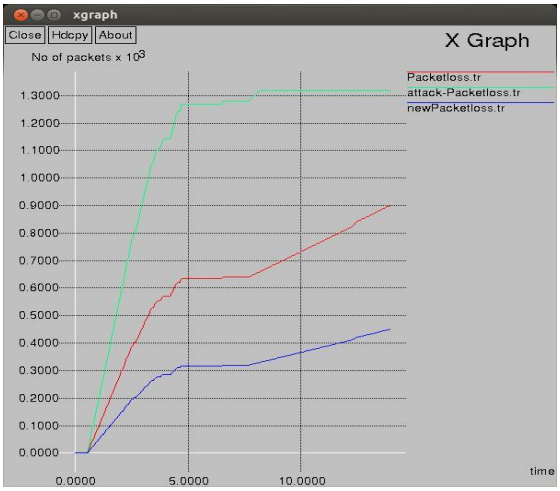


Fig.6: Packet loss Graph

As shown in Figure 6, the comparison of without attack, with attack and proposed scenario is shown in terms of packet loss. It has been analyzed that packet loss of the proposed scenario is minimum when the malicious node is isolated from the network as compared to other two scenarios.

V. CONCLUSION

The wireless sensor networks is the type of network in which sensor nodes can sense environmental conditions and sensed information will be passed to base station. The size of the sensor nodes is very small due to which battery life of the sensor nodes is limited. The wireless sensor networks are the self configuring type of network due to which some malicious nodes may join the network. These malicious nodes are responsible to trigger misdirection attack in the network. In this work, technique is proposed which will detect and isolate malicious nodes from the network. The proposed technique is based on node localization in this technique base station will analyze the delay per hop. The node which can increase delay maximum times will be detected as malicious nodes in the network. It is analyzed that energy consumption of the network get reduced, throughput get increased and delay get reduced in the network.

VI. REFERENCES

[1]. Baviskar, B.R. and Patil, V.N. (2014), "Black hole attacks mitigation and prevention in wireless sensor network", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp. 167-169.

[2]. Salehi, S.A., Razzaque, M.A., Naraei, P., Farrokhtala, A. (2013), " Detection of sink hole Attack in wireless sensor networks", IEEE International Conference on Space Science and Communication (IconSpace), Melaka, Malaysia.

[3]. Mishra, A. , Nadkarni, K. and Patcha, A. (2004), "Intrusion Detection In Wireless Ad Hoc Networks", IEEE 1536-1284/04/.

[4]. Kim, J.Y., Caytiles, R. D. and Kim, K.J. (2014) "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks", Journal of Security Engineering, pp.241-250.

[5]. Karlof, C. and Wagner, D. (2003), "Secure routing in wireless sensor networks:Attacks and countermeasures", AdHoc Networks Journal, vol. 1, no. 2-3, pp. 293-315.

[6]. Krontiris, I., Giannetsos, T. and Dimitriou, T.(2008), "Launching a Sinkhole Attack in Wireless Sensor Networks" in Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, (wimob).

[7]. Kamble, S. and Dhope, T. (2017), "Reliable Routing Data Aggregation using Efficient Clustering in WSN", International Conference on Communication Control and Computing Technologies, IEEE, pp.246-250.

[8]. Anand, C. and Gnanamurthy, R.K.(2016), "Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network", Springer Science + Business Media New York.

[9]. Paul, B., Bhuiyan, K.A., Fatema, K. and Das, P.P. (2015),"Analysis of AOMDV,AODV,DSR, and DSDV Routing Protocols for Wireless Sensor Network", Computational Intelligence and Communication Networks(CICN),IEEE.

[10]. Mahapatra, R.P. and Yadav, R.K. (2015), "Descendant of LEACH Based Routing Protocols in Wireless Sensor Networks", 3rd International Conference on Recent Trends in Computing (ICRTC).

[11]. Rani, L. and Er. Rani, V. (2015), "A Novel Study on Data Flow Routing with Energy Optimization under Different Attacks in WSN".

[12]. Dhulkar, R., Pokharkar, A. and Mrs. Pise, R. (2015), "Survey on different attacks in Wireless Sensor Networks and their prevention system".