International Journal of Engineering Trends and Applications (IJETA) – Volume 5 Issue 5, Sep-Oct 2018

RESEARCH ARTICLE OPEN ACCESS

A Security Framework for Detection and Prevention of Misdirection Attack in Wireless Sensor Networks for IOT

Bhavkanwal Kaur [1], Puspendra Kumar Pateriya [2]
School of Computer Science and Engineering
Lovely Professional University
Jalandhar-144402
India

ABSTRACT

Wireless Sensor Networks are resource constrained networks, ad-hoc in nature and prone to various network attacks. Since they are vulnerable to many types of attacks, they need unique security solutions for their protection against different security attacks. In the case of Denial of Service (DoS) attacks possible on wireless Sensor Networks, Misdirection attack is the type of DoS attack, which is very difficult to detect and prevent. Misdirection attack occurs in the network when there is a malicious node present in the network, which misdirects the incoming packet to a different node than the intended one, causing the delay to increase in the network, sometimes infinite. As a result, there is also degradation in the throughput of the network. Thus, the detection and prevention of the misdirection attack is a very critical task. In our research work, we have presented a novel technique to detect and prevent the misdirection attack. The network parameters calculated using this technique shows how the performance of the network degrades by the presence of the malicious node in the network and shows a noticeable reduction of the energy consumption after the isolation of the malicious node from the network.

Keywords :- *Network Delay, Misdirection Attack, Throughput, Packet Loss, Energy Consumption, Detection and Prevention of Misdirection Attack*

I. INTRODUCTION

Internet of Things allows us to think that we will be able to connect to every kind of device in our surroundings using Internet. This will allow us to communicate or connect with any kind of device around us from anywhere in the world. The future of IoT is actually dependent on few of famous and key technologies of today like Wireless Sensor Networks, Miniaturization and Nanotechnology. Wireless Sensor Net- works are always going to be the major component in any sort of IoT applications.[17]In this era, Wireless Sensor Networks is the technology whose growth is increasing drastically and it considered as the most attractive and growing field of research these days. They are a part of many big applications nowadays, like emergency response, management and surveillance of battlefield, analysis and monitoring of the weather information, monitoring in hospitals and inventory management. [1] Wire- less sensor networks is the leading choice these days because of their reliability, facile way of deployment, less in cost and ability to analyze those places which out of reach of human beings.[2]

Providing security to a Wireless Network is a very difficult task. And on the other hand, the main problem is, it is very much vulnerable to attacks. There are numerous attacks possible on Wireless Sensor Networks. Misdirectional Attacks are the most famous type of Denial-of-Service attacks possible on Wireless Sensor Networks. This attack can be done in a number of ways. A malicious node can disrupt a reliable route of packets from source to destination, making the packets from a particular node to not reach the destination. As a result it causes increase in the delay of the packets to reach the destination or it is possible they may not reach the destination at all. This further degrades the throughput of the network. Here, in this paper, we have presented a novel technique to detect and prevent the misdirection attack. In the results it is shown that how the throughput and delay of the network is decreasing when a malicious node is present in the network and how there is considerable decrease in the energy consumption of the network after the detection and isolation of the malicious node from the network. In the Section II, a literature review is done on the different kinds of attacks possible in Wireless Sensor Networks in IoT. In the III section, the novelty of the presented technique is discussed. In the IV section, a brief discussion is done on the Misdirection attack. Section V explains about the proposed technique. The simulation scenario for detecting misdirection attack is discussed in section VI. In section VII consist of the key findings of this work. In section VIII conclusion, future work and applications of the presented approach.

II. LITERATURE REVIEW

Ju young Kim et.al [3] in their paper “A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks” propounded about the study of number of attacks, vulnerabilities and threats for Wireless Sensor Networks. In this paper, a scrutiny is conducted on Wireless Sensor Networks to find out the authorized ways to do attacks and discover various techniques for prevention from such attacks. The various kinds of vulnerabilities, threats and attacks possible on WSNs in a vital or critical situation have been discussed and analyzed in their paper.

Yi Zhing Zang et.al[4] authors presented a different approach in their paper, ”The detection and defense of DoS attack for wireless sensor network”, for an observation technique(MoM) to detect and prevent DoS attack. MoM makes the use of similarity function which is based on the spatial-temporal correlation, to find out the content attack and frequency attack. The MoM uses rekey and reroute countermeasures to isolate the malicious nodes. The security scheme depicts that their solution not only finds out but also prevents the DoS attack, leading to reduction in the energy dissipation.

Kalpana Sharma and M K Ghose [5] presented in their paper ”Wire- less Sensor Networks: An Overview on its Security Threats” that the problem of protection is due to of the sensor network’s nature. They have provided a brief review on the WSNs threats affecting different layers along with their protection techniques. They have used “layer-by-layer” basis as a security scheme for protection purposes. Through this paper they have presented the most occurring security threats in different layers and prevention schemes related to them. Hailun Than et.al [6] presented a new technique in their paper ”A Coincidental and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Network”, for providing confidentiality in multi-hop code dissemination protocol. They combined confidentiality with DoS-attack prevention in a multi-hop code dissemination protocol. The idea is based on Deluge, an open source, state-of-the-art code dissemination protocol for WSNs. In addition, they also have shown a performance evaluation in their proposal in comparison to Deluge and the existing secure Deluge.

Roshan Singh Sachan et.al [7] presented in their paper, “A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN”, wireless media is adhoc in nature when it comes to their deployment and Wireless Sensor Networks has some major threat issues. Numerous variety of attacks can be performed on Wireless Sensor Networks but misdirection attacks are like the type of DDOS attack. In this paper we will discuss about detection and prevention of this attack with small amount of delay and throughput.

You-guo and Ming-fu did an improvement in enhancing the security of the exchange of data among the two parties via Middle-ware techniques. Middle-ware is the new scheme which uses various cryptographic techniques for data privacy and security for instance authentication, data integrity, digital signatures, user identification, communication is happening between reliable devices. But Middle-ware is a newly introduced scheme and a lot of work need to be done in this area.[8] There is another common technique discussed in a number of papers related to adaptive learning. Abie H.et al. presented an Adaptive Security and Trust Management (ASTM) solution with the main scheme that the network notice and adapts to modifying environment dynamically and foresee unknown at- tacks by making non-static changes in the security system and frameworks of the system. The disadvantage of this technique is that, it is a more abstract concept rather than verified and applied for Wireless Networks in IoT environment.[12,13,14].

III. PROBLEM DEFINITION AND NOVELTY

Out of all the attacks possible on Wireless Sensor Networks, Misdirection Attack is one of the most intimidating one. It is one of the most famous Denial of Service attack. Misdirection attack is responsible for increasing delay in the network during transmission of data, thereby reducing the throughput of the network and can even cause congestion. In this paper a novel technique is proposed for uncovering and prohibiting the misdirection attacks occurring in the network.

Wireless Sensor Networks are very much prone to Denial of Service attacks, which is responsible for causing loss of large amount of data accompanying great loss of the energy and power as well. Firstly, a network is set up by deploying a large number of sensor nodes. The network is then divided into finite clusters of equal sizes using the LEACH protocol. LEACH is a ”Low Energy Adaptive Clustering Hierarchy” After the cluster heads are formed, a cluster head is chosen for each cluster in the network on the basis of distance and energy from the base station.

The shortest path by every node to the cluster head, from a particular node to any other node in the network or from cluster head to the base station is chosen on the basis of Ad-hoc On-Demand Distance Vector Routing protocol, since it supports both multi-cast and uni-cast routing. While establishing the path, it is possible that routing protocol may take one or more malicious nodes in its path. These malicious nodes can misdirect the packets to a different path, such that it can cause in the packets to reach the destination. Thus the malicious nodes trigger the misdirection attack, which is really problematic, as it is hard to detect and defend a misdirection attack. Because of this attack, there is an abrupt increase in the high end-to-end delay; as a result the performance of the network is disgraced.

In this paper, a novel technique is proposed, which can detect and isolate the malicious nodes in the network, which are accountable for provoking misdirection attack in the network.

IV. A BRIEF REVIEW ON MISDIRECTION ATTACK

Mis-directional Attacks are the most famous type of Denial-Of-Service attacks. This attack can be done in a number of ways. A malicious node can disrupt a reliable route of packets from source to destination, making the packets from a particular node to not reach the destination. Mis-directional Attacks have various categories:

1) *Forwarding the Packets to a Node nearer to the Destination*: This type of attack is not much more effective, as if the route is misdirected to a node nearer to the destination, the nodes may find an another route to reach the destination. This will only increase the delay, hence reduction in the throughput of the network.

2) *Forwarding the Packets to a Node far away from the Destination*: This is the most destructive type of mis-directional attack because if we are sending the packets far away from the destination node in the network. This can cause the delay to reach to infinity and the throughput of the network to almost zero. Also, if there are malicious nodes or sensors present in the network, they can easily mislead the spectator by sending him the wrong data. This can cause serious danger to the whole of the network and we need to protect our network from all such threats.

III. A NOVEL TECHNIQUE FOR DETECTION AND PREVENTION OF MISDIRECTION ATTACK

A Wireless sensor network is kind of a distributed network, due to which it is very less secure and very much prone to attacks. Sensor nodes themselves act like routers as they route the packets from one node to another. Packets have to pass through multiple hops before they reach the destination. If malicious nodes are present in the path, this can cause the packets to reach the packets with a large delay at the destination or even they can fail to reach the destination. Thus malicious nodes can cause serious vulnerabilities in the network.

A novel technique is proposed which can detect those malicious nodes in the network, which are accountable for provoking misdirection attack in the network. The approach for implementing the proposed technique is as following:

1) Firstly, a network is deployed with a finite number of sensor nodes and the whole network is divided into fixed sized clusters. Location based clustering is used to divide the whole network into fixed size clusters. In location based clustering, the whole network is dissected into cells and one sensor node is selected from each cell as a cluster head. This method of clustering is useful in power consumption as all nodes except the cluster heads are in sleep mode when not in use.

2) In each cluster, the cluster head is selected on the basis of LEACH protocol. LEACH protocol [11] is a hierarchical technique in which all the nodes in a particular cluster transmit all their data to the chosen cluster head and then all the cluster heads in the network aggregate all the data, compress it and then send it to the base station. Each node uses a randomized algorithm in every round, to decide that whether it will become a cluster head or not in that round.

3) Ad Hoc On-Demand Distance Vector Routing Protocol [15] is used to authorize a path from the source to the destination. A route is considered to be found when either the RREQ message itself reaches the destination or it reaches a node which has a valid route entry to the desired destination. When a route is found then a Route Reply messages are uni-casted back to the source node from the valid found routes. The best path is selected on the basis of hop counts and the sequence number. The path which has the maximum sequence number and minimum hop count is decided as the best path for routing.

4) When the data is transmitted from a cluster head through other cluster heads to the base station, the base station or sink node will arrange the packets in the buffer according to their sequence number and the timestamps. The sink node while arranging the packets will see that some of packets are not reaching to it or are arriving after a very long delay. So the sink node will check that the delay is increasing in the network as the packet loss is increasing in the network. Packet loss usually occurs in the network due to increase in the traffic, severe congestion, overflow of the buffer, collision occurring at the link layer. In the wireless sensor networks, the probability of the occurrence of the buffer overflow or severe congestion is very less.

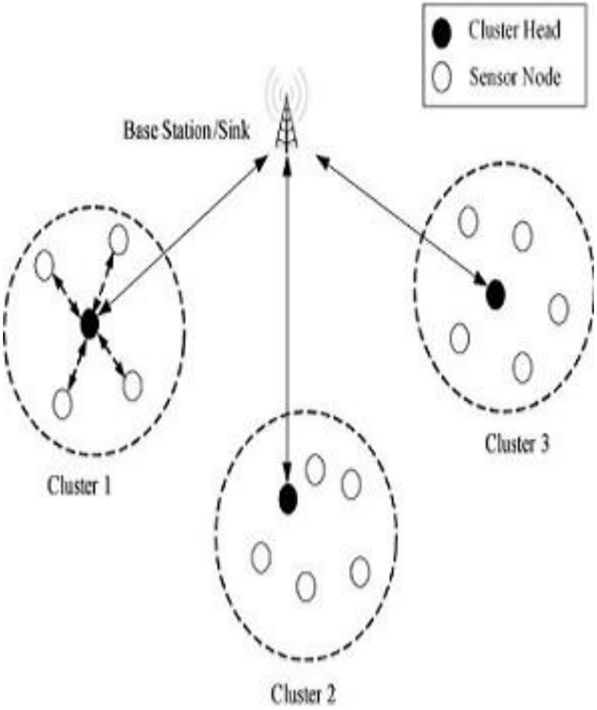
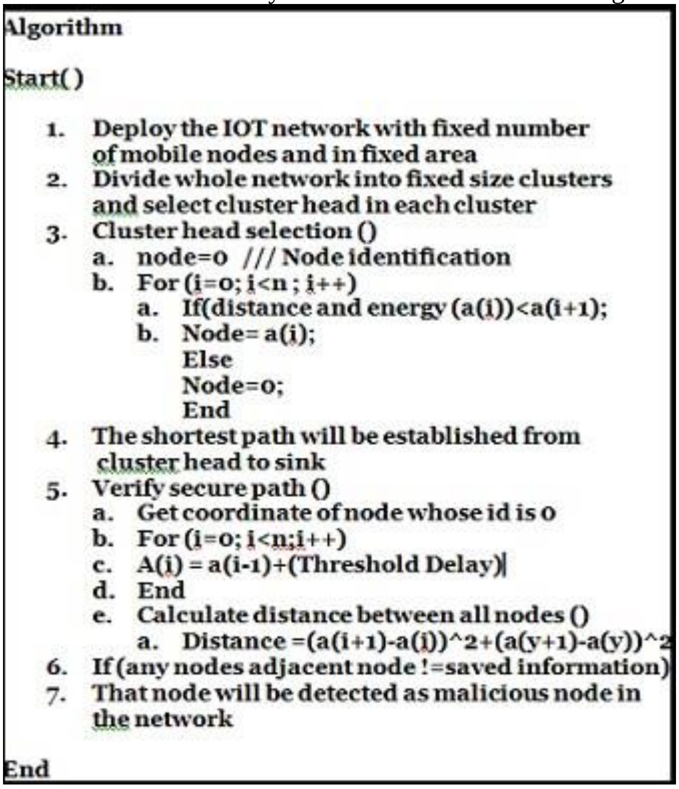


Figure1: Clustering In Wireless Sensor Network

If we consider that we are using a reliable MAC protocol and the rate of increase in the traffic is very low, the reason we are left with which can cause delay in the network due to packet loss occurring in the network due to the presence of malicious node in the network. The malicious node forwards the incoming packets to the wrong routes due to which the Time-to-live(TTL) set inside the packet goes to zero before reaching the destination and the packet gets discarded. Also there could be chance that some of packets reach the sink node with a very long delay, where the delay is actually calculated by subtracting the TTL value at which the packet reaches the destination with the a particular threshold value set before. The threshold value depends upon the size of the packet and the distance traveled by the packet.

5) In order to detect and isolate the malicious nodes in the network, the mechanism of node localization is used. Now the base station will gather the information in terms of their location. The gathered information also contains the distance of each other from the base station.

6) Since now we know the location of the nodes, the unique paths taken for the data transmission in the network can be found. In all the paths, a unique path is found which causes the maximum delay in the network. The path has a malicious node which is responsible for causing increase in the delay by misdirecting a particular packet. When a packet arrives at a node, it's destination address is checked in the forwarding table and the next node is found to which it should be forwarded in order they reach the destination. The misdirecting node changes the address of the forwarding packet and routes it to such a path that barely reaches the destination and the delay in the network starts increasing.

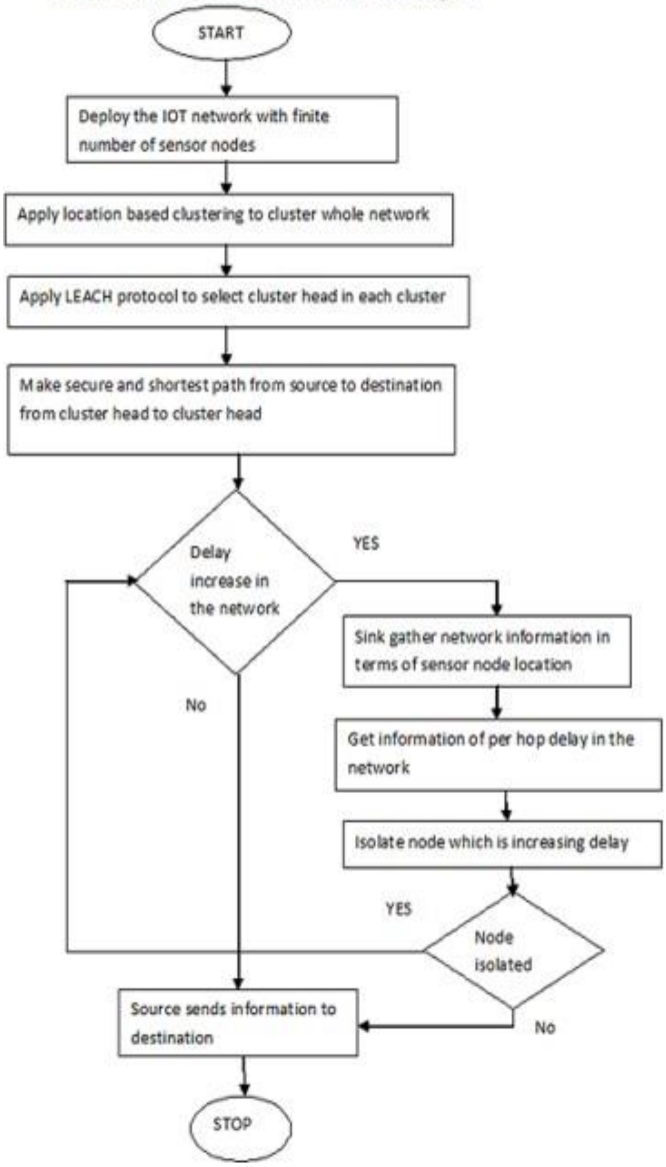


```
Algorithm

Start()

    1. Deploy the IOT 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 coordinate of node whose id is 0
       b. For (i=0; i<n;i++)
       c. A(i) = a(i-1)+(Threshold Delay)
       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
```

7) As the path having the malicious node is found, the distance factor can be used to count the delay on each hop which is on the established path. The base station starts counting delay on each hope. The node which increases the delay in the network is detected as the malicious node in the network.

8) Multi-path routing [14,16] is used to isolate the malicious node in the network. Once, the base station comes to know that which node is malicious, and then it broadcasts the information about the malicious node to the whole network. Once, the base station comes to know that which node is malicious, and then it broadcasts the information about the malicious node to the whole network. The route update packets are forwarded to all nodes except the malicious node. To set up different routing paths, every node keeps the information about the node sending the route update message with the lowest hop as the most nearest node to it, saves its hop count, and re-broadcasts it with a hop count incremented by one.

FLOWCHART OF THE PROPOSED TECHNIQUE


START
Deploy the IOT network with finite number of sensor nodes
Apply location based clustering to cluster whole network
Apply LEACH protocol to select cluster head in each cluster
Make secure and shortest path from source to destination from cluster head to cluster head
Delay increase in the network
YES
No
Sink gather network information in terms of sensor node location
Get information of per hop delay in the network
Isolate node which is increasing delay
YES
Node isolated
No
Source sends information to destination
STOP

If a route update with the identical sequence number is received more than once from the same node, only the previously saved update is considered. When the route setup is completed, each node has its most nearest nodes.
When a particular node forwards data, it forwards it to its one of the nearest nodes in round-robin manner. The data from the same source node would be delivered along the different route to the base station, as each intermediate

node will send it through its nearest hops in round robin manner. Using this different technique of multi path routing [18], packets from the nearby nodes of a malicious node can bypass the data from that malicious node which arbitrarily drops it. Otherwise, data from the nearby nodes of the malicious node will always be forwarded through the malicious node In addition, this different technique of multi path routing also does the load-balancing effect in the network.

IV. SIMULATION SCENARIO OF MISDIRECTION ATTACK IN WIRELESS SENSOR NETWORK

To verify the presented work a WSN under misdirection attack is simulated with the finite number of sensor nodes. The Simulation Scenario is shown in the figure 2.

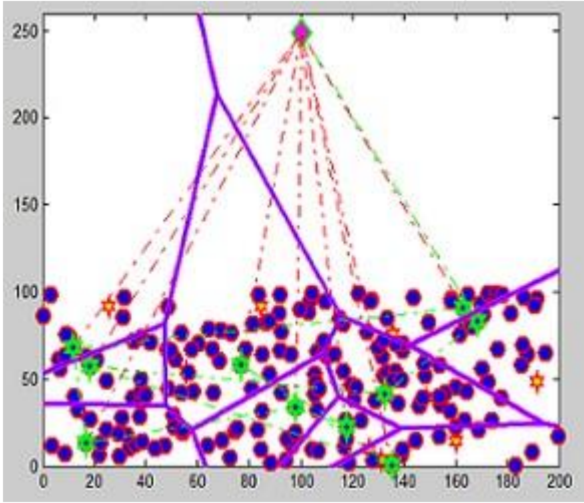


Figure 2:Wsn Under Misdirectional Attack

A. *Experimental Design Parameters*

1) **Throughput**
2) **Packet Loss**
3) **Energy Consumption**

B. *Results*

In a wireless network throughput is the average rate at which the data is successfully delivered to the end user, that is amount of data successfully received as compared to the amount of data send by the source. It is measured in bits per second. In the graph, we have shown the number of packets successfully received, The packet size is taken 1024 bits. The elapsed time is 127.15 seconds. The green colored marks in the figure 3 shows the decrease in the throughput of the network in the presence of malicious node. After the isolation of malicious node the performance of the network has improved and the throughput of the network is increased.

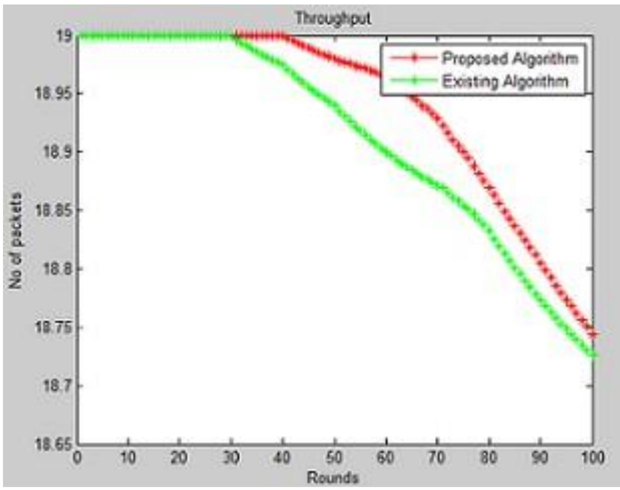


Figure 3: Throughput

Throughput due to Existing Algorithm: 14776.28 bps
Throughput due to Proposed Algorithm: 15254.02 bps
After the detection and prevention of the network from misdirection attack by removing the malicious node from the network, the packet loss is reduced greatly depicted by the red colored marks in the figure 4.

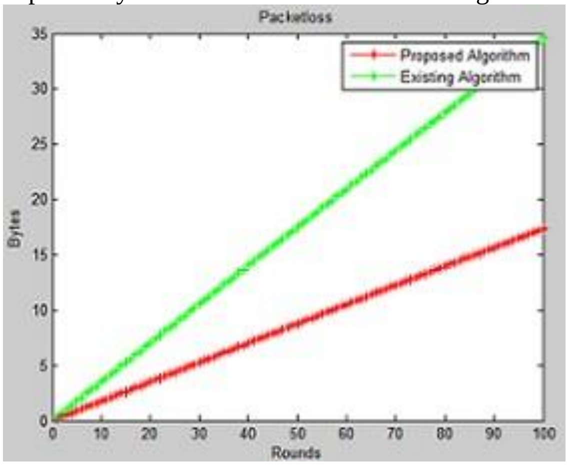


Figure 4: Packet Loss

Packet Loss due to Existing Algorithm: 1873.1067 bytes
Packet Loss due to Proposed Algorithm: 883.0295 bytes
The attacks performed by intruders on the WSN, can lead to increase in the energy consumption of the network, hence leading to reduction in the remaining energy or the lifetime of the network as shown in figure 5 .

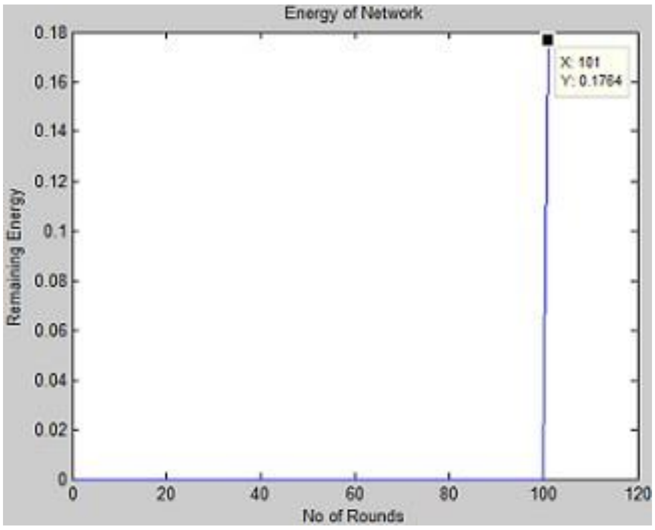


Figure 5: Remaining Energy In The Existing Algorithm

The proposed technique reduces the energy of the consumption in the network as shown in figure 6.

Remaining Energy due to Existing Algorithm: 0.1764 J
Remaining Energy due to Proposed Algorithm: 0.1796 J

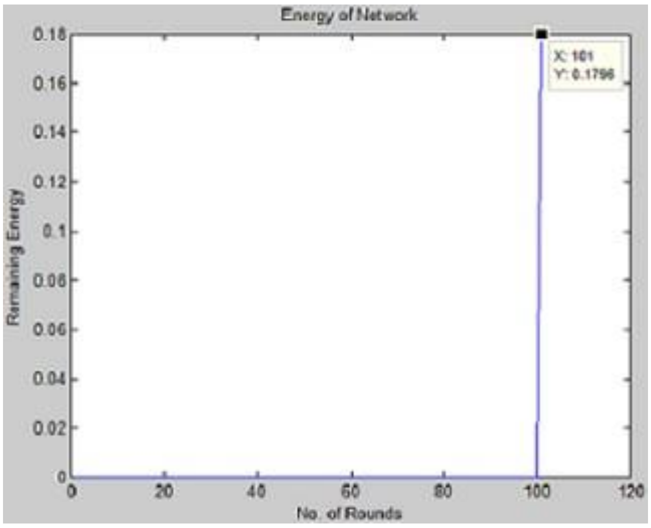


Figure 6: Remaining Energy In The Proposed Algorithm

V. CONCLUSION AND FUTURE SCOPE

1) Misdirection attack degrades the throughput of the net- work and increases the delay in the network, as a result devastating the performance of the network. The proposed technique for detection and prevention of misdirection attack is very effective successful in expelling the misdirection attack and improving the performance of the net- work. Throughput has improved appreciably by proposed technique and packet loss due to delay has reduced.

2) In future, this can be extended to the networks having much complex topology such that the network may have greater density of nodes.

3) This technique can be applied to a wireless sensor net- works that are prone to misdirection attacks such that it will improve the performance of the network and prevent it from misdirection attack.

REFERENCES

[1] C. Castelluccia, E. Mykletun, and G. Tsudik, ”Efficient Aggregation of Encrypted Data in Wireless Sensor Net- works,” Mobiquitous 2005.

[2] J. Horey, M. M. Groat, S. Forrest, and F. Esponda, ”Anonymous data collection in sensor networks,” in Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQ- uitous’07), August 2007.

[3] 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.

[4] Yi-Ying ZHANG, Xiang-zhen LI, Yuan-an LIU, ”The detection and defense of DoS attack for wireless sensor network”, Elsevier Journal of China Universities of Posts and Telecommunications, Vol19, pp. 52-56, Oct-2012.

[5] Kalpana Sharma and M K Ghose, ”Wireless Sensor Networks: An Overview on its Security Threats” IJCASpecial Issue on ”Mobile Ad-hoc Networks” MANETs, 2010, pp.42-45.

[6] Hailun Tan, Diethelm Ostry, JohnZic, SanjayJha, ”A Confidential and DoS-Resistant Multi-hop Code Dissem- ination Protocol for Wireless Sensor Network”, ACM WiSec09, Zurich, Switzerland, March 16-18, 2009.

[7] Roshan Singh Sachan, Mohammad Wazid, Avita Katal, D P Singh, R H Goudar, ”A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN”, International conference on Com- munication and Signal Processing, April 3-5, 2013, India.

[8] L. You-guo and J. Ming-fu, ”The reinforcement of com- munication security of the internet of things in the field of intelligent home through the use of middle-ware,” in Knowledge Acquisition and Modeling (KAM), 2011 Fourth International Symposium on. IEEE, 2011, pp. 254- 257.

[9] Reijo, M, Savola., Habtamu, Abie., Markus Sihvonen., ”Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications”, Proceedings of the 7th International Conference on Body Area Networks, pp. 276- 281, 2012.

[10] An algorithm to detect Malicious Nodes in Wireless Sen- sor Network using enhanced LEACH protocol, Computer Engineering and Applications (ICACEA), 2015(IEEE).

[11] Abie H., and Balasingham I., ”Adaptive security and trust management for autonomic message-oriented middle- ware ”, IEEE 6th Int.Conference on Mobile Ad hoc and Sensor Systems (MASS’09), pp. 810-817, 2009.

[12] S. P. Alampalayam and A. Kumar, ”Security Model for routing attacks in Mobile Ad hoc Networks”, IEEE 58th Vehicular Technology Conference, 2003. VTC Fall 2003, pp. 2122-2126, 2003.

[13] S. P. Alampalayam and A. Kumar, ”An adaptive and predictive security model for mobile ad hoc Networks”, Springer Wireless Personal Communications 29 (3-4), pp. 263-281, 2004.

[14] Ashutosh Bhatia, Praveen Kaushik. A Cluster Based Minimum Battery Cost AODV Routing Using Multipath Route for Zigbee, IEEE International Conference on Networks, 2008.

[15] Murizah Kassim, Ruhani Ab.Rahman, Roihan Mustapha. Mobile Ad Hoc Network Routing Protocols Comparison for Wireless Sensor Network, IEEE International Conference on System Engineering and Technology, 2011, pp, 148-151.

[16] Huang X., Fang Y. Multiconstrained QoS Multipath Routing in Wireless Sensor Networks. J. Wirel. Netw. 2007;14:465478.

[17] L. Atzori, A. Iera, and G. Morabito, The Internet of Things: A survey, in ScienceDirect: Computer Networks, vol. 15, pp. 1-19, May, 2010.

[18] G.H. Raghunandan, B.N. Lakshmi, A Comparative Anal- ysis of Routing Techniques for Wireless Sensor Net- works, Proceedings of the National Conference on In- novations in Emerging Technology, IEEE 2011.