RESEARCH ARTICLE OPEN ACCESS

A Novel Energy Efficient Security Protocol In WSN

Chandan Kumar Trigunait[1], Shashi Prabha[2]
Mechanical Engineering [1], Biju Patnaik University of Technology(BPUT), Rourkela,Odisha, India-769004
Computer Science and Engineering [2], Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, MP, India-462033

ABSTRACT
Wireless sensor networks are the resource constrained networks that are prone to various attacks. In this paper, we have mapped biological immune system to the WSN to develop the security protocol. Various attacks on network layer can lead to energy loss to dead network. This paper applied timely sensing concept to save network from network layer attacks. This paper designed an algorithm Improved-PEGASIS that saves the WSN from network layer attack and performs routing of data in the network. This paper also represents implementation using MATLAB and verification of different performance measures like throughput, energy loss and cost effectiveness. The simulation of the proposed algorithm over WSN shows better results as compared to existing PEGASIS protocol.

Keywords :— Improved-PEGASIS PEGASIS,WSN.

I. INTRODUCTION

Wireless sensor network is a collection of thousand nodes where each node can sense environment, i.e. temperature, pressure, etc. The WSN is basically a battery operated network, so the power supply is very limited. WSN also suffers from limited availability of different other resources. Various attacks in WSN consume these resources rapidly that leads to the dead network [1].

Biological immune system is a complicated versatile system that has developed in vertebrates to protect them from attacking agents. The immune system performs its tasks by using pattern recognition mechanism. The main characteristic of the biological immune system is that it reacts according to attacking agent features. In other words, biological system either destroy an invader or neural its effects depending upon its source, reproduction rate, etc [2].

Aickelin, U. et al. [6] improves the security by introducing an AIS based technique for the intrusion detection. The author uses the danger theory of immune system to recognize the intrusion. The author investigates the relation between DT and the computer security. Ma, Z. et al. [7] introduce a novel multi-layer defense mechanism based on immunity.

The system is capable to recognize the known as well as unknown intrusions. The defense mechanism uses the adaptive capability of BIS to improve its response. Fu, R. [8] proposed a framework that uses the AIS and fuzzy for the anomaly detection. The simulation results shows higher detection rate and lower false detection rate of the proposed technique as compared to watchdog method. Nikdel, A. et al. [9] described a mechanism that provides the proper nodes distribution in each cluster using virtual clustering concept. The results of simulation show the effectiveness of the proposed mechanism.

Nishanthi, S. et al. [10] introduced an algorithm WCSA for the intrusion detection in the network. The phenomenon uses the clonal selection algorithm and the watchdog algorithm for the intrusion detection.

We have mapped human body with the WSN. The human body can be treated as the network. The body consists of the nervous system. Nervous system contains two parts, i.e. Central nervous system and the peripheral nervous system. The central nervous system consists of Brain and the spinal cord. The peripheral nervous system consists of nervous to connect the body with the brain. In WSN, we treated sink node as the brain and nodes as the nervous. Nodes are used to connect the network with sink node. The nodes transfer the data packets to the sink node using multi hop network. In other words, the data packet is transferred from the source to the destination using different nodes. Similarly, in the body the information is transferred to the brain using various nervous. The useful data packets are the antibody while the waste data packets are treated as the antigens. Following table shows the mapping of WSN with the Human Body.

Attacks are classified in two categories active and passive attacks. Passive attacks don't affect the network directly but these attacks are information seeking, which may be critical in the operation of a protocol. Active attacks can affect the working of a particular node as well as the working of the whole network. A passive attacker extracts the packets containing information like location of nodes etc. from the channel which outrages confidential criterion. Active attack includes eavesdropping, traffic analysis, snooping, monitoring while passive attack includes Wormhole, information disclosure, gray hole, resource consumption, routing attacks [3].These attacks on the networks layer lead to wastage of energy. In other words, energy consumption increases due to attacks and it decrease the lifetime of the network. So early sensing of attack and its recovery can save the energy and increase the network lifetime. This paper proposes AIS based PEGASIS algorithm named as Improved-PEGASIS that identify and recover the network layer attack in WSN

II. PEGASIS ROUTING PROTOCOL IN WSN

PEGASIS is chain based routing protocol that transmit data packet form source node to the base station. The farthest node from the base station is chosen as the source node. The source node transfers the data to its closest neighbor[4].

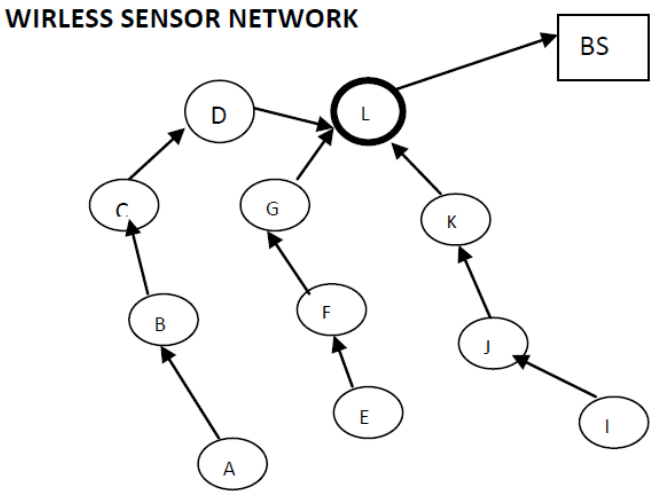

Fig.1 . Data Transmission Using PEGASIS in WSN

The node further transmits data to its nearest neighbor and process continues until data is reached to the base station. The node that transfer data to the base station needs extra energy as the base station has greater distance as compared to other nodes. This node is known as chain leader. Thus the data is transmitted from the source node to the destination. Multiple numbers of chains can exist within the network to transfer the data. The whole process can be explained by figure 2.In figure 2 the nodes A, E, I are distant from base station so they are chosen as the source nodes. Three chains formed by selecting closest neighbor node corresponding to source node. The chains are A-B-C-D-L and E-F-G_L and I-J-K-L where L is the leader node that transmits data to the base station. The leader node i.e. L needs greater amount of energy as compare to other nodes due to the larger distance between the base station and the L.

A. Energy model

The model for the consumption [5] of energy is as follows. Assume Ei is the initial energy of each node. The Ed is the energy dissipated while transmission and retrieval of data. The energy for amplification at the transmitter is Ea. When a node transmit N data packet and each data packet consist of m bits to the other node at distance say d. Then amount of energy

consumed at transmitter end can be given as The amount of energy consumed at receiver end is

III. PROPOSED TECHNIQUE

The base station has the sensing capability and it know details of all nodes. In other words, the base station knows the location, energy level, packet forwarding ratio and life time, etc. all the properties of the nodes. The nodes send this information to the base station at the constant interval of time. The base station also knows the maximum delay possible for a packet to deliver due to known location of nodes. If any node or data packet is marked as the antigen, then it is discarded by the network. The decision that any data packet is an antigen or antibody is taken by the base station. The base station takes the decision by analyzing the information of all the nodes stored in it. The whole can be explained by the following algorithm.

A. Proposed Algorithm

Various terms used in the algorithm are as follow:

data- data packet, Adata- Anti-gen data packet, Ninumber of neighbor of ith node, BS-base station, MD-maximum delay possible for a packet, Ei-energy level of ith node, n-number of nodes, xi,yi- x,y coordinate of ith node, DN- discarded node. SNsource node, CL-chain leader , TN-transmitting node , Di is the distance of ith neighbor from TN.

1. Select the distant and nearest node as the SN and CL respectively.
2. Take source node ad the transmitting node initially i.e.TN=SN.
3. Distance=inf.
4. Delay=0;
5. While TN != BS
6. If delay > MD
7. If queue contains CL
   Then
   Mark data as Adata.
   else if any node in queue has forwarding
   ratio below threshold forwarding ratio
   then mark node as DN.
   else
   Mark Node with lowest energy in queue as
   DN.
   End if.
8. Insert TN to queue.
9. For i=1 to Nth repeat step 4
10. If Di<Distance and Ni!=DN
    Then
    Di=distance.
    Temp=Ni
    End if.
11. Transmit the data from TN to Temp.
12. If data != Adata and Temp != DN
    Then
    TN=Temp
    End if
13. Delay=delay + current delay.

End while

The algorithm can detect and recover various network layer attacks like resource consumption attack, Black hole attack. The algorithm also increases the network life time by discarding the node having energy lower than the threshold energy.

The CL nodes can communicate directly with the base station and in the direct communication , delay is much lower as compared to Multihop communication, because in Multi-hop communication, each intermediate node receives, processes and then sends data to next node. The single-hop communication is used to minimize this delay.

Energy consumed in single-hop communication is:

Ecs=Et

where Et is the transmission energy and can be computed as:

$$E_t = k \times (E_{elec} + E_{amp}) \times d^2$$

Where Eamp is the energy needed for transmit amplifier upto a distance of d and packet size k. The energy consumption due to multi-hop communication is:

$$E_{CM} = n \times k \times E_t + (n-1) \times k \times (E_r)$$

Where Er is the energy required for reception and n is the number of hops. Also it is assumed that Er = Et. This work transmits the data in multi hop manner as base station is not in the range of the source node. That's why the only way for transmission is the multi-hop. In the total amount of the energy consumption in the transmission of data packet from source node to the base station is as follow:

$$E_C = (2n - 1) \times k \times E_t$$

Here the Er=Et and the total energy consumption clearly depends upon the n that is number of hops. In the Pegasis routing protocol when any attack occur then the value of n gets increased that leads to the higher energy consumption while the proposed phenomena doesn't increase the value of n even in the presence of attack so the energy consumption is less. The performance of the algorithm discussed in the next section.

IV. RESULT ANALYSIS

Simulation is performed for PEGASIS protocol as well as for the improved-PEGASIS (proposed) protocol. The comparison is done the different size networks by using the parameters average energy consumption, Cost, end 2 end delay and the throughput.

The end 2 end delay is the time taken to transmit the packet from source to the base station, lower the delay better the performance. The average energy consumption is the total energy consumed by the entire node divided by the number of nodes. Throughput is the output in the given time. The energy consumption must be reduced, and throughput must be enhanced. The cost is the transmission cost calculated by energy*delay.

TABLE 1 PERFORMANCE OF PEGASIS PROTOCOL

Number of Nodes	Delay	Throughput	Energy Consumption	Cost
50	0.525	11.21	0.389	0.204
100	0.720	12.21	0.394	0.283
150	0.915	12.51	0.392	0.358
200	1.02	13.0	0.395	0.402

TABLE 2 PERFORMANCE OF improved-PEGASIS PROTOCOL

Number of Nodes	Delay	Throughput	Energy Consumption	Cost
50	0.482	11.65	0.342	0.1648
100	0.654	12.71	0.369	0.2413
150	0.851	13.21	0.368	0.3132
200	0.97	13.54	0.368	0.3570

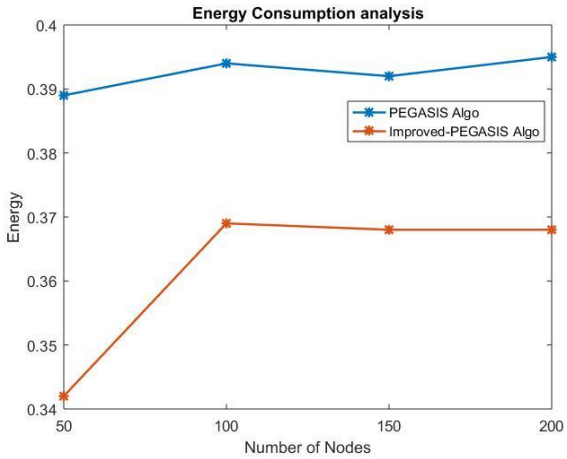

Fig.2. Energy consumption comparison

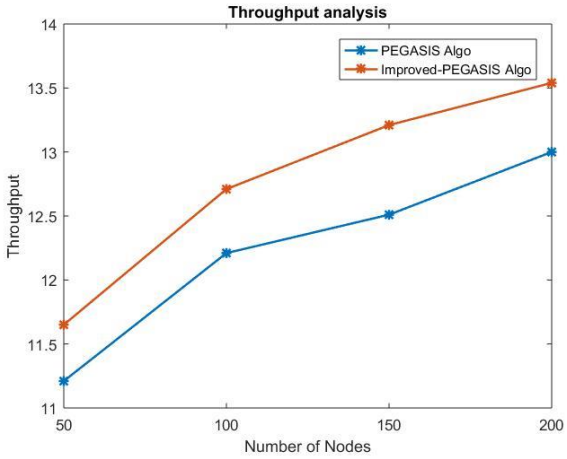

Fig.3.Throughput Comparison

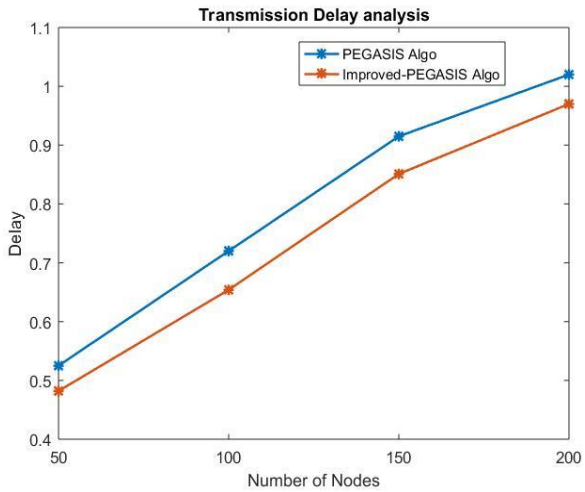

Fig.4. Transmission Delay Comparison

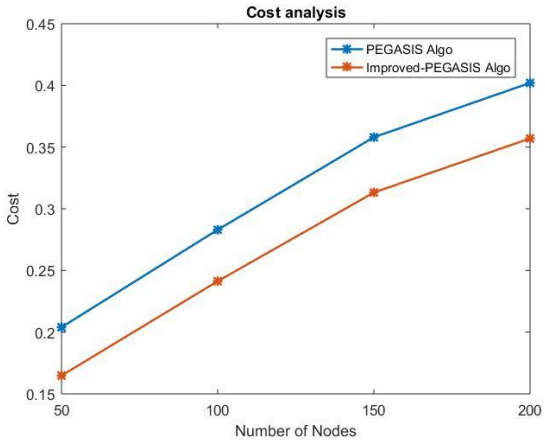

Fig.5. Cost Comparison

Table 1 and Table 2 shows the performance of the PEGASIS and the Improved-PEGASIS protocol over the network having 50,100,150 and 200 nodes respectively. The graph shows that the energy consumption , end 2 end delay and the cost of transmission has been decreased in the improved-PEGASIS protocol as compared to the PEGASIS protocol.

V. CONCLUSION

The paper mainly focuses on the mapping of the human body with the sensor network and implementation of the AIS to enhance the network performance. This paper proposes an algorithm named improved-PEGASIS by introducing the AIS in the PEGASIS algorithm. improved-PEGASIS is a secure and efficient algorithm which can detect and recover various network layer attacks. The simulation is done using the MATLAB, and the results conforms the better performance of improved-PEGASIS protocol as compared to PEGASIS protocol. In future, the AIS can be implementing on various other protocols of WSN to enhance the network lifetime.

REFERENCES

[1] Saleem, K., & Fisal, N. (2013, April). Energy efficient information assured routing based on hybrid optimization algorithm for WSNs. In ITNG (pp. 518-524).

[2] Dasgupta, D. (2006). Advances in artificial immune systems. Computational Intelligence Magazine, IEEE, Volume 1, Issue 4, pp. 40-49.

[3] Mamatha, G. S., & Sharma, D. S. (2010). Network Layer Attacks and Defense Mechanisms in MANETSA Survey. International Journal of Computer Applications (0975–8887) Volume 9, Issue 9, pp. 12-17.

[4] Xie, D., Zhou, Q., Liu, J., Li, B., & Yuan, X. (2013, June). A chain-based data gathering protocol under compressive sensing framework for wireless sensor networks. In Computational and Information Sciences (ICCIS), 2013 Fifth International Confe

[5] Ahn, K. S., Kim, D. G., Sim, B. S., Youn, H. Y., & Song, O. (2011, May). Balanced Chain-Based Routing Protocol (BCBRP) for Energy Efficient Wireless Sensor Networks. In *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on* (pp. 227- 231). IEEE.

[6] Aickelin, U., Bentley, P., Cayzer, S., Kim, J., & McLeod, J. (2003). Danger theory: The link between AIS and IDS?. In *Artificial Immune Systems* (pp. 147- 155). Springer Berlin Heidelberg.

[7] Ma, Z., & Zheng, X. (2008, September). Multi-layer intrusion detection and defence mechanisms based on immunity. In *Genetic and Evolutionary Computing, 2008. WGEC'08. Second International Conference on* (pp. 281-284). IEEE.

[8] Fu, R., Zheng, K., Lu, T., Zhang, D., & Yang, Y. (2012). Biologically Inspired Anomaly Detection for Hierarchical Wireless Sensor Networks. *Journal of Networks*, Volume *7 Issue* 8, pp. 1214-1219.

[9] Nikdel, A., Jameii, S. M., & Noori, H. (2012) A Novel Scheduling Mechanism Based on Artificial Immune System for Communication between Cluster Head and Cluster Members in WSNs. *International Journal of Information and Electronics Engineering, Volume 2, Issue 3.pp.333-337.*

[10] Nishanthi, S., & Virudhunagar, T. (2013). Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm. *IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, pp.1-5.*