Appendix 1

MATLAB CODING

```
attackpegasis
node_number1=30;
flag=0;
%node_number=10;
energy=zeros(1,node_number1);
receive_factor=512*50*0.0001;
send_factor=512*12*0.001;
node_number=100;
malnode=20;
node_x=rand(1,node_number);
node_y=rand(1,node_number);
plot(node_x,node_y,'.')
hold on
plot(node_x(1),node_y(1),'.r')
hold on
plot([node_x(1) 0],[node_y(1) 0])
hold on
p=0.15;n=fix(1/p);
for round=1:n

distance=zeros(1);
max_distance=0;
max_node=0;
for i=1:node_number1,
   distance(i)=sqrt(node_x(i)^2+node_y(i)^2);
   if max_distance<distance(i),
```

```
        max_distance=distance(i);
        max_node=i;
    end
end
plot(node_x(max_node),node_y(max_node),'-')
hold on
average_distance=sum(distance(:))/node_number;
MD=max_distance/10000;

connect_distance=zeros(1,node_number1);
connect_node=zeros(1,node_number1);
connect_node(1)=max_node;
connect_distance(1)=average_distance;

for i=2:node_number1,
    temp_node=0;temp_min_distance=1.5;
    for j=1:node_number1,
        b=0;
        for k=1:(i-1),
            if j==connect_node(k),
                b=1;
                break
            end
        end
        if b==0,
            distance=sqrt((node_x(connect_node(i-1))-
node_x(j))^2+(node_y(connect_node(i-1))-node_y(j))^2);
            if temp_min_distance>distance,
                temp_min_distance=distance;
                temp_node=j;
```

```
        end
       end
    end
   if i==malnode &&
   temp_min_distance=temp_min_distance*100;
   end
    connect_distance(i)=temp_min_distance;
    connect_node(i)=temp_node;

delay=connect_distance(i)/1000
MD
%pause;
    if(MD>=delay&&flag==0)
    plot([node_x(connect_node(i-1))
node_x(connect_node(i))],[node_y(connect_node(i-1))
node_y(connect_node(i))],'-');

    energy(connect_node(i-1))=energy(connect_node(i-
1))+connect_distance(i)^2*send_factor+receive_factor;
    energy(connect_node(i))=energy(connect_node(i))++receive_factor;

    else
    plot(node_x(connect_node(i)),node_y(connect_node(i)),'g');
i=i-1;
flag=1;
    end
hold on
end
t=fix(rand(rand(1,1))*100)+1;
energy(t)=energy(t)+average_distance^2*send_factor+receive_factor;
```

```
end

receive_factor=512*50*0.0001;
receive_consumption=100*receive_factor;
energy_consumption=zeros(1,node_number);
send_factor=512*12*0.001;
for i=1:node_number1,
   energy_consumption(i)=connect_distance(i)^2*send_factor+receive_factor;
end
consumption=receive_consumption+sum(energy_consumption(:))
figure
plot(1:30,energy,'.')
hold on

atckspegasis1n
node_number1=30;
flag=0;
%node_number=10;
energy=zeros(1,node_number1);
receive_factor=512*50*0.0001;
send_factor=512*12*0.001;
node_number=100;
malnode=20;
node_x=rand(1,node_number);
node_y=rand(1,node_number);
plot(node_x,node_y,'.')
hold on
plot(node_x(1),node_y(1),'.r')
hold on
plot([node_x(1) 0],[node_y(1) 0])
```

```
hold on
p=0.15;n=fix(1/p);
for round=1:n

distance=zeros(1);
max_distance=0;
max_node=0;
for i=1:node_number1,
   distance(i)=sqrt(node_x(i)^2+node_y(i)^2);
   if max_distance<distance(i),
      max_distance=distance(i);
      max_node=i;
   end
end
plot(node_x(max_node),node_y(max_node),'-')
hold on
average_distance=sum(distance(:))/node_number;
MD=max_distance/1000;

connect_distance=zeros(1,node_number1);
connect_node=zeros(1,node_number1);
connect_node(1)=max_node;
connect_distance(1)=average_distance;

for i=2:node_number1,
   temp_node=0;temp_min_distance=1.5;
   for j=1:node_number1,
      b=0;
      for k=1:(i-1),
         if j==connect_node(k),
```

```
            b=1;
            break
          end
        end
        if b==0,
          distance=sqrt((node_x(connect_node(i-1))-
node_x(j))^2+(node_y(connect_node(i-1))-node_y(j))^2);
          if temp_min_distance>distance,
            temp_min_distance=distance;
            temp_node=j;
          end
        end
    end
   if i==malnode
   temp_min_distance=temp_min_distance*1000;
   end
    connect_distance(i)=temp_min_distance;
    connect_node(i)=temp_node;

delay=connect_distance(i)/1000
MD
%pause;
    if(MD>=delay)
    plot([node_x(connect_node(i-1))
node_x(connect_node(i))],[node_y(connect_node(i-1))
node_y(connect_node(i))],'-');

    energy(connect_node(i-1))=energy(connect_node(i-
1))+connect_distance(i)^2*send_factor+receive_factor;
    energy(connect_node(i))=energy(connect_node(i))++receive_factor;
```

```
   else if flag==0
   plot(node_x(connect_node(i)),node_y(connect_node(i)),'r*');
i=node_number1+1;
flag=1;
break;

      end
   end
hold on
end
t=fix(rand(rand(1,1))*100)+1;
energy(t)=energy(t)+average_distance^2*send_factor+receive_factor;

end

receive_factor=512*50*0.0001;
receive_consumption=100*receive_factor;
energy_consumption=zeros(1,node_number);
send_factor=512*12*0.001;
for i=1:node_number1,
   energy_consumption(i)=connect_distance(i)^2*send_factor+receive_factor;
end
consumption=receive_consumption+sum(energy_consumption(:))
figure
plot(1:30,energy,'.')
hold on

pegasis1
node_number1=30;
```

```
%node_number=10;
energy=zeros(1,node_number1);
receive_factor=512*50*0.0001;
send_factor=512*12*0.001;
node_number=100;

node_x=rand(1,node_number);
node_y=rand(1,node_number);
plot(node_x,node_y,'.')
hold on
plot(node_x(1),node_y(1),'.r')
hold on
plot([node_x(1) 0],[node_y(1) 0])
hold on
p=0.15;n=fix(1/p);
for round=1:n

distance=zeros(1);
max_distance=0;
max_node=0;
for i=1:node_number1,
   distance(i)=sqrt(node_x(i)^2+node_y(i)^2);
   if max_distance<distance(i),
      max_distance=distance(i);
      max_node=i;
   end
end
plot(node_x(max_node),node_y(max_node),'-')
hold on
average_distance=sum(distance(:))/node_number;
```

```
MD=max_distance/1000;

connect_distance=zeros(1,node_number1);
connect_node=zeros(1,node_number1);
connect_node(1)=max_node;
connect_distance(1)=average_distance;

for i=2:node_number1,
   temp_node=0;temp_min_distance=1.5;
   for j=1:node_number1,
      b=0;
      for k=1:(i-1),
         if j==connect_node(k),
           b=1;
           break
         end
      end
      if b==0,
        distance=sqrt((node_x(connect_node(i-1))-
node_x(j))^2+(node_y(connect_node(i-1))-node_y(j))^2);
         if temp_min_distance>distance,
           temp_min_distance=distance;
           temp_node=j;
        end
      end
  end
   connect_distance(i)=temp_min_distance;
   connect_node(i)=temp_node;
delay=connect_distance(i)/1000
MD
```

```
pause;
   if(MD>=delay)
   plot([node_x(connect_node(i-1))
node_x(connect_node(i))],[node_y(connect_node(i-1))
node_y(connect_node(i))],'-');
   else
   plot(node_x(connect_node(i)),node_y(connect_node(i)),'g');
end
hold on
   energy(connect_node(i-1))=energy(connect_node(i-
1))+connect_distance(i)^2*send_factor+receive_factor;
   energy(connect_node(i))=energy(connect_node(i))++receive_factor;
end

t=fix(rand(rand(1,1))*100)+1;
energy(t)=energy(t)+average_distance^2*send_factor+receive_factor;
end
receive_factor=512*50*0.0001;
receive_consumption=100*receive_factor;
energy_consumption=zeros(1,node_number);
send_factor=512*12*0.001;
for i=1:node_number1,
   energy_consumption(i)=connect_distance(i)^2*send_factor+receive_factor;
end
consumption=receive_consumption+sum(energy_consumption(:))
figure
plot(1:30,energy,'.')
hold on
```

Appendix 2

PROPOSED ALGORITHM

Various terms used in the algorithm are as follow: data- data packet, A data- Anti-gen data packet, Ni-number 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. SN-source 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 + currentdelay.

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 algorithm AIS-PEGASIS is efficient algorithm but the performance of the algorithm in the presence of mobile base station is necessary to be optimized. This optimization can be achieved by little modification to the algorithm. This modification is to select the distant and nearest node again with the change in the position of the base station. The process can be easily understood by following algorithm.

Various terms used in the algorithm are same as of AIS- pegasis.

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. Loc:=Store location of base station
4. Distance=inf.
5. Delay=0;
6. While TN != BS
7. If loc!=location of the base station
8. Select the distant and nearest node as the SN and CL respectively.

9. Take source node ad the transmitting node initially i.e.TN=SN.

10. Loc:=Store location of base station

11. Distance=inf.

12. Delay=0;

13. End if

14. If delay > MD

15. 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.

16. Insert TN to queue.

17. For i=1 to Nth repeat step 4

18. If Di<Distance and Ni!=DN

Then

Di=distance.

Temp=Ni

End if.

19. Transmit the data from TN to Temp.

20. If data != Adata and Temp != DN

Then

TN=Temp

End if

21. Delay=delay + currentdelay.

End while

The performance of the above described algorithm can be easily compared with other existing algorithm by using simulator like MTLAB. The implementation and performance of the algorithm discussed in the next chapter.

attackpegasis
node_number1=30;

Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Immune System Based Architecture to Enhance the Security in WSN

Nipin Gupta
Research Scholar,
Jagannath University, Jaipur, India

Malay Ranjan Tripathy
Professor, ECE Deptt,
Amity University, Noida, India

Abstract: A Sensor Network is one of the most complex networks because of its low power sensing devices. In this present work we are building immunity system based architecture to secure the WSN. In this architecture the security load will be distributed in different intelligent sensor organs over the network. This load is divided in three main stages called prevention, detection and the network reconstruction. The prevention mechanism will be performed by the memory cell nodes. Responsibility of detection process is on T cells and the antibodies will perform the node blocking and the network reconstruction over the network. The whole system will be maintained by the brain cell that will perform the activation of these three security services respective to required security level. The presented architecture is reliable and improves the communication throughput over the network.

Keywords: Immune System, Authentication, Detection, Prevension, Architecture

I INTRODUCTION

A Sensor network is one of the most crucial and complex network because of its heterogeneity in terms of network type, topology, nodes and the application. A sensor network is constructed by the help of wireless tiny sensors with the minimum requirement of transreciving and sensing capability. The major vector in such network is network type, it represents the sensors can be implemented in any kind of network including the mobile networks, vehicular area network, body area network etc. Each kind of network has its own capabilities and the requirements. It means to work of sensor network we need to first understand the network type where it will be implemented. The major concern of the sensor network is the topology. Some of sensor networks can be centralized such as in body area networks and some sensor networks are randomly distributed and we can shape them such as the vehicular area based system. The topological architecture is also based on the application and the network requirement. According to these requirements the node type is also decided. In the simplest sensor type they only perform the transmission and do not have storage element or the processor. There also exist the smart sensors with the capability of the memory and the processors. The sensors also exist that can perform the required decision making in terms of security analysis, congestion control etc. Because of these all reasons there is always the requirement of some such architecture that can be implemented on any kind of sensor network respective to the service distribution. The AIS (Artificial Immune System) gives such kind of architecture.

In this architecture system the complete network is divided in controller nodes. Figure 1 is showing the three levels of the architecture. The level 1 is represented by the brain nodes. This kind of node is having the maximum configuration in terms of memory and the processing requirement. It works as the main centralized node which is responsible for all the communication over the network. All the

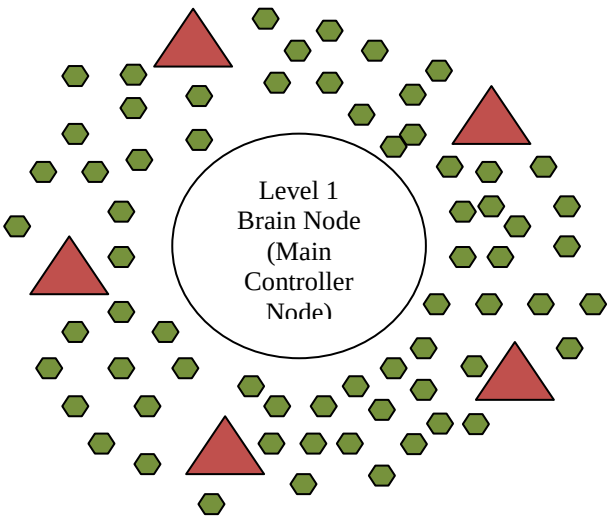

Figure 1: Artificial Immune System

Aggregative work or the decision making regarding the whole system is done by this brain node. It is responsible for the work distribution as well as the allotment of the services. It can also block the services or to prioritize them according to network or the application requirement. Any problem in such node can block or disturb the communication over the whole network. The second level of the categorization is in the form of agent nodes. As the sensor network system is a large system with different kind of services over the network. To control these sub systems over the network some agent nodes are defined with respective capabilities. In this figure 1 the rectangle shape nodes represents the agent or the controller nodes. These agent nodes are intelligent nodes that control the sub system with its defined strength and to report to the brain node. A network system has a few agent nodes depending on the physical distribution or the number of services that required to control over the network.

The third and the lowest level of node are the communicating sensor nodes. In figure 1 level 3 nodes are defined in green circles. These are vast number of nodes that can be homogeneous or the heterogeneous depending on the network type. These nodes have lowest level of physical characteristics in terms of energy, memory and processing capabilities. There also exist such nodes that do not have any memory or the processing capabilities.

II Security Architecture

As we discussed earlier the WSN is one of the most complex network as it can be implemented on other network types. Because of this the capabilities and the requirement such network change according the network type and the application. Because of this for the service capabilities and the network architectures is required to design respective to the system requirement where it will be implemented. To design the generic architecture there is lot of dynamic properties that is required to be discussed. In this work we are basically designing such a generic system that can be implemented on any kind of network system. The presented system is based on the immune system. The work is about to present this system respective to the security requirements of the system.

The security is always the major challenge for wireless or the dynamic network. There are number of factors that influence the security system. This factor includes the physical characteristics of the system, topology and the routing gateways. A network is affected from the internal and external attacks. The internal attacks are performed by some internal node or itself generated by some miscommunication within the network. The reason of these attacks is the high load over some node or the energy loss of a node. The kind of attack is done by the external nodes that are performing by some dynamic node that enter to the system with some fake identity. These attacks basically capture the network information or change the communicating data to add error in data values. To handle these all kind of attacks there are different kind of detection and the prevention mechanisms exist. These all are collectively called the security services.

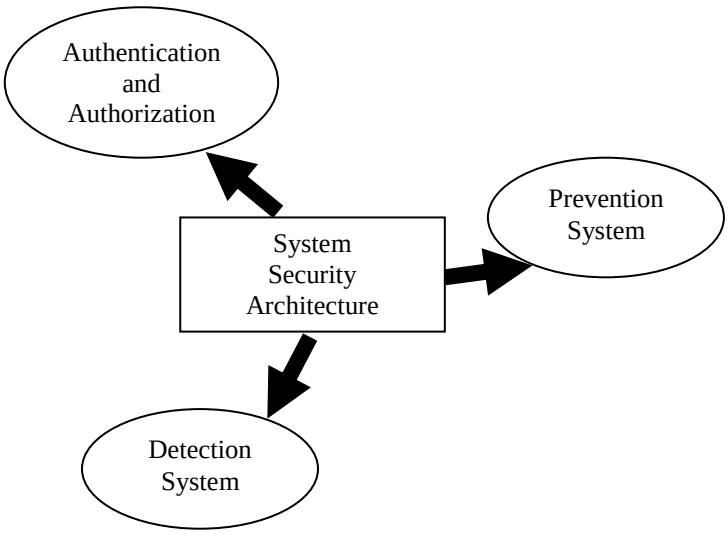

Figure 2: Secure System Architecture

The authentication and authorization service is the major security approach used to distinguish the valid and the attacker node. Each node over the network is assigned a unique id. In first level of authentication system the communicating node is checked for the valid identity. The authentication is verified by the main controller node. In the second level the authorization is performed by the controller node. The authorization is basically used in heterogeneous systems where different communicating capabilities are defined for different kind of nodes. The work distribution respective to the secure communication is done at this level. In the third level of this service the secure communication is performed. For this communication the cryptographic algorithm is implemented. A key distribution and encoding approach is implemented to perform the secure and reliable communication over the network. Here figure 2 is showing the complete authentication and authorization system. As we can see the it is defined as a sequential security process in which the level of security is implemented in a series. With the implementation of all three sub systems the high level secure communication can be achieved. The system is basically to save the network from any kind of external attack. The system is safe in terms in case of different intruder attacks.

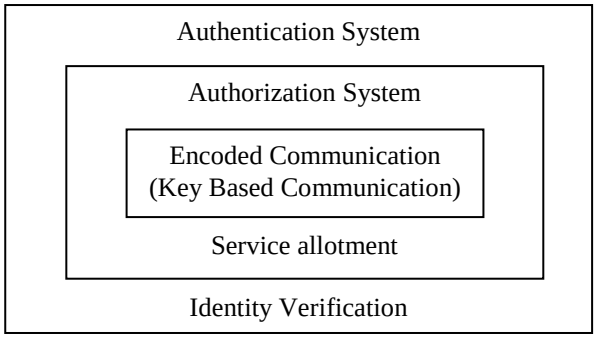

Figure 3: Authentication and Authorization System

The second major aspect of security architecture is prevention algorithm. The prevention approach is based on the existing network communication statistics. It includes the prediction oriented analysis to identify the chances of some attack or the data loss during the communication. Based on this analysis the early decision is taken place regarding the node blockage or the route change. The major concern in this kind of security service is the preventive path generation. According to this approach a compromising path is detected to perform the expected reliable communication. Let we have a network with m nodes called N=N1, N2, N3….Nm. From the initial analysis the list of attacker node list is generated called A=A1, A2….An. In case of preventive analysis the the communication path will be generated on nodes excluding the expected attacker nodes i.e.

SafeNodes=N-A

It means the safe path will node include any node that is in the list of expected attacker. To identify this kind of different algorithmic approaches are used such as ACO, Genetic approach etc. Generally this kind of preventive analysis is performed by the intelligent node with high memory i.e. Centralized nodes. Such kind of preventive mechanism is basically implemented to save the network from internal attacks.

The third and the main key of secure network architecture is the Detection System. This kind of system is the innermost layer of secure system architecture. This layer is called the Detection System. In case, if some smart intruder enter to the system and start to disturb the network in different ways, it is required to analyze the network and to identify the type of attack and the attacker nodes over the network. The work of this layer is divided in three sequential phases shown in figure 4.

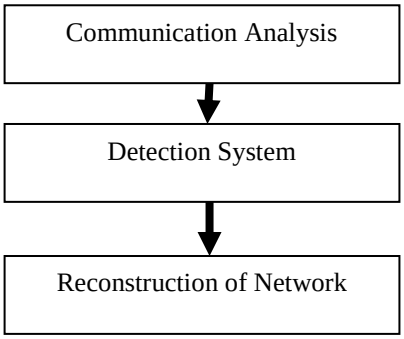

Figure 4 : Detection System

As we can see in the sequential definition of the detection system is shown. In the initial phase the communication analysis is performed. There are number of different approaches for such kind of analysis. These approaches can be centralized or the host based. In the centralized system the approach will be implemented on the main controller node that will perform the decision making on the basis of analysis on all nodes over the network. The analysis can also be performed on each host of the network. This kind of analysis is based on the neighbor node communication analysis. Another analysis type is the agent based analysis. In such kind of analysis we place some agent nodes over the network and these agents perform the analysis on neighboring nodes.

Once the analysis phase is done the detection system starts working. It is about to detect the attack over the network, for such kind of attack detection there are number of approaches. The detection systems are of two types, one is the attack specific detection system and other is the generic detection system. The generic systems are based on the throughput or the loss analysis based system. In both kind of system the most common approach among them is the threshold based analysis. According to this approach the threshold value is set to analyze the communication throughput on the each node on routing path. If the loss is greater than threshold value, it means there is some attack in the network. The threshold analysis can be performed on different communication parameters such as Network throughput analysis, loss analysis etc. The detection phase is performed on some specifc nodes and sometimes periodic to improve the network optimization.

The third and important phase of the detection system is the network reconstruction. The reconstruction includes node elimination, load distribution and the network rerouting. The reconstruction process is actually done by the centralized node or the agent. Once the reconstruction is done the network start behaving normally.

III Immune System Based Architecture

In the above defined security architecture we have defined the system in three security layers. These layers will be executed in a series from outer layer to the inner layers. This architecture is the parallel implementation of all three layers for complete network. But the sensor network has the drawback in the form of energy concern. Implementation of this complete system for the complete network is not efficient in terms of network delay and in terms of energy optimization. In this work we have presented a security system that can be implemented on any kind of sensor network. The presented system is based on the human immune system. In this present work we have divided the complete network system in the form smaller sub system. Each sub system is having a controller agent to manage the security for that sub-system. These all systems are arranged in the form of human immune system. Different systems presented here work as different organs of the human body.

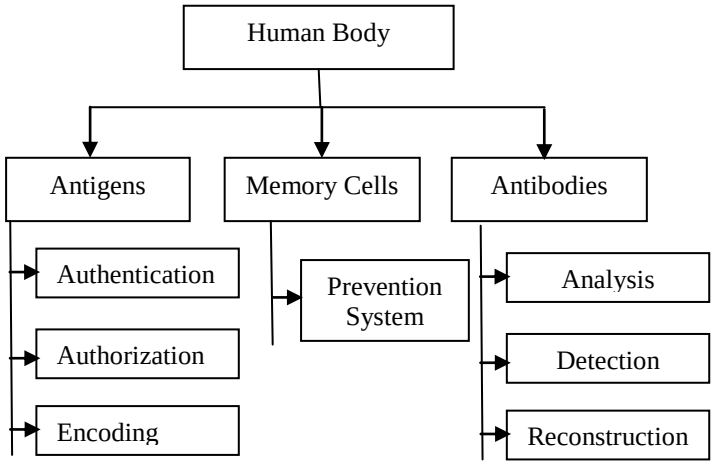

Figure 5 : Secure Immune System

As we can see the complete architecture proposed is shown in figure 5. We have divided the complete network body in three main sub systems called Antigens, Memory Cells and Antibodies. Each sub system is for some specialized task. These sub system further intake some other body components to perform sub tasks related to that system.

IV CONCLUSION

The proposed system is based on a immune system based architecture to improve the network security in wsn. We have divided the network in different clusters according to the work process. Each cluster is defined by some controller. Each controller is assigned by specific task of authentication or security. The presented system will give an enhanced protocol with security.

REFERENCES

[1] Suman Deswal and Sukhbir Singh, "Implementation of Routing SecurityAspects in AODV", InternationalJournal of Computer Theory and Engineering, Vol. 2, No. 1 February,2010.
[2] Chin-Yang Tseng, "A Specification-based Intrusion Detection System for AODV".
[3] Monis Akhlaq, "Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16 2006.
[4] Mariannne. A. Azer, "Wormhole Attacks Mitigation", 2011 Sixth International Conference on Availability, Reliability and Security
[5] Pallavi Sharma Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", 978-1-61284-486-2 IEEE.
[6] Yih-Chun Hu, "Wormhole Attacks in Wireless Networks", I EEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006
[7] Majid Khabbazian," Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS 1536-1276/09@ 2009 IEEE.
[8] Sergio Felperin," A Theory of Wormhole Routing in Parallel Computers", 0-8186-2900-2/92@1992 IEEE
[9] Jong-Pyng Li," Priority Based Real-Time Communication for Large Scale Wormhole Networks", 0-8186-5602-6/904 1994 IEEE
[10] Farid Na¨ıt-Abdesselam," Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol", WCNC 20071525-3511/07©2007 IEEE
[11] Xia Wang," An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks", 31st Annual International Computer Software and Applications Conference(C0MPSAC 2007) 0-7695-2870-8107@2007 IEEE

[12] Viren Mahajan," ANALYSIS OF WORMHOLE INTRUSION ATTACKS IN MANETS", 978-1-4244-2677-5/08©2008 IEEE

[13] Yun Wang," A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE

[14] Sanjay Keer," To Prevent Wormhole Attacks Using Wireless Protocol in MANET", Int'l Conf. on Computer & Communication Technology 978-1-4244-9034-/10©2010 IEEE

[15] E.A.Mary Anita," A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs", ICCCCT-10 978-1-4244-7770-8/10©201 0 IEEE

AIS-PEGASIS:secure routing in wsn

Nipin Gupta*
***Research Scholar, Jagannath University**
Jaipur, nipinsingla@yahoo.com

Malay Ranjan Tripathy**
****Professor, Dept. of ECE AMITY University**
Noida, mrtripathy@hotmail.com

***Abstract* -Wireless sensor networks are the resource constrained networks that are prone to various attacks. In this paper, we have mapped human body to the WSN. The peripheral nervous system is mapped with the network layer. Various attacks on network layer can lead to energy loss to dead network. Similarly, an attack on nervous system can lead to paralysis, etc. A timely sensing of attack can save the person from paralysis. This paper applied this timely sensing to save network from network layer attacks. This paper designed an algorithm AIS-PEGASIS that saves the WSN from network layer attack and performs routing of data in the network. This paper also represents the AIS implementation using MATLAB. The simulation of the proposed algorithm over WSN shows better performance as compared to conventional techniques.**

***Keywords: WSN, AIS, PEGASIS, AIS-PEGASIS*.**

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].

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 system architecture is shown in figure 1.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.

TABLE 1 MAPPING OF HUMAN BODY WITH WSN

Mapping of Human Body with WSN	
Human Body	Network
peripheral Nervous System	Network Layer
Brain	Sink Nodes
Nervous	Nodes
Antibody	Data packets
Antigen	Attack data packet

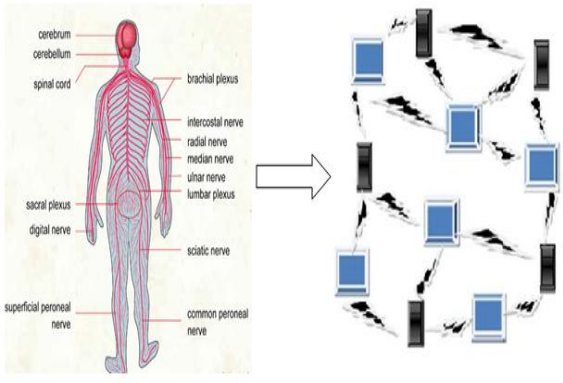

Fig. 1. Mapping Human Body with WSN

Various Attacks on the network layer are Wormhole, black hole, Byzantine, flooding, resource consumption, location disclosure attacks, etc. These

attacks are classified in two categories active and passive attacks.

Passive attacks don't affect the network directly but t hese 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. It is similar to the attack on the peripheral nervous system. The attack on PNS stops the working of PNS, and it leads to paralysis, etc. if the attack on PNS is timely sensed, then early curing can save the person from paralysis similarly 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 AIS-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].

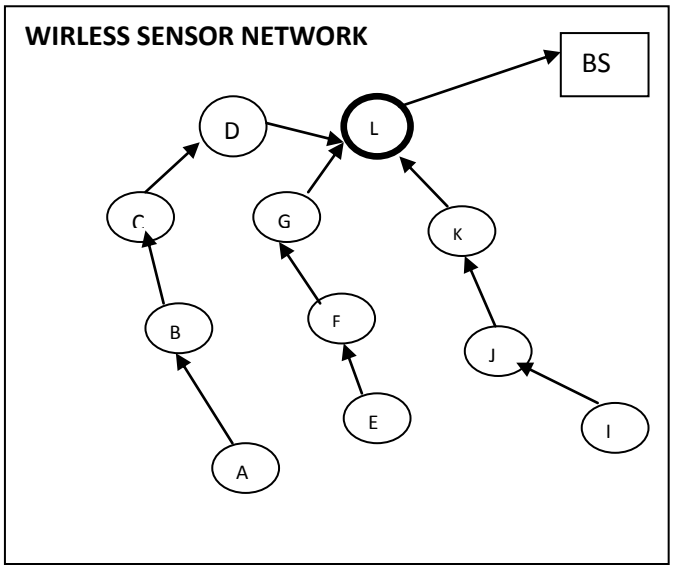

Fig. 2. Data Transmission Using PEGASIS in WSN

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 $Etcon = N * m * Ed + N * m * Ea * d^2$

The amount of energy consumed at receiver end is $Ercon = N * m * Ed.$

III. RELATED WORK

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.

IV. 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, Ni-number 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. SN-source 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 + currentdelay.
    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: $E_{CS} = E_t$

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.

V. IMPLEMENTATION

The proposed algorithm is implemented using the MATLAB. The MATLAB doesn't contain any toolbox for the WSN or for AIS. The m file coding is

done to design the WSN. Simulation is performed for PEGASIS protocol as well as for the AIS-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 2 PERFORMANCE OF PEGASIS PROTOCOL

Number of nodes	End 2 end delay	Throug-hput	Energy consumption	Cost=energy*delay
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 3 PERFORMANCE OF AIS-PEGASIS PROTOCOL

Number of nodes	End 2 end delay	Through put	Energy consumption	Cost=energy*delay
50	0.5000	11.51	0.369	0.184
100	0.696	12.69	0.373	0.259
150	0.890	13.0	0.372	0.331
200	0.99	13.2	0.373	0.369

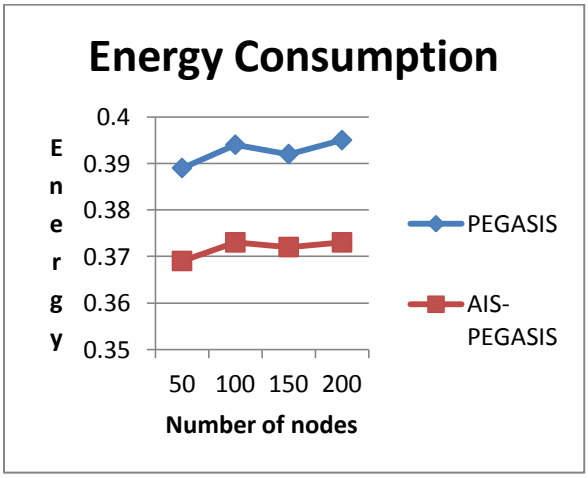

Fig. 3. Comparison of Energy Consumption

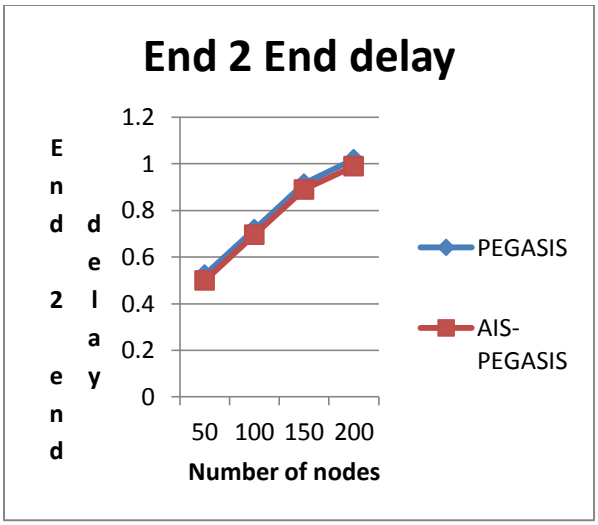

Fig. 4. Comparison of E2E Delay

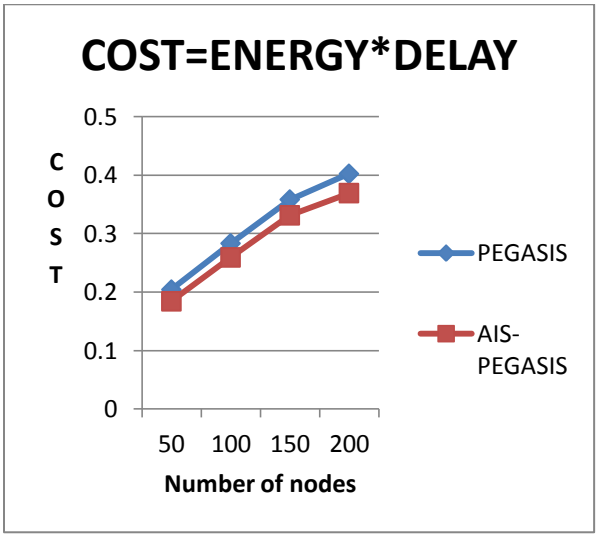

Fig. 5. Comparison of Cost

Table 2 and Table 3 shows the performance of the PEGASIS and the AIS-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 AIS-PEGASIS protocol as compared to the PEGASIS protocol.

VI. 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 AIS-PEGASIS by introducing the AIS in the PEGASIS algorithm. AIS-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 AIS-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 MANETS-A 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 Conference on* (pp. 1479-1482). IEEE.

[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.*