M-PEGASIS: Energy Efficient for Mobile Wireless Sensor Network

PRINKA AGGARWAL
STUDENT
AIET FARIDKOT

SARABJEET KAUR
AP,BCA
AIET FARIDKOT

Abstract : Wireless network has become increasingly popular during the past decades. Most of the researchers have recently started to consider power-aware development of efficient protocols for MANETs. As each mobile node in a MANETs performs the routing function for establishing communication among different mobile nodes the "death" of even a few of the nodes due to power exhaustion might cause disconnect of services in the entire MANETs.It has also been observed that Sybil attacker has increased the End to End Delay as well as energy consumption and reduced the Throughput of the network.we have utilized PEGASIS protocol and neural network to solve network issues. Matlab has been used as the simulation tool for evaluating the performance of PEGASIS protocol.

I. INTRODUCTION

Wireless network has become increasingly popular during the past decades. There are two variations of wireless networks- infrastructure and infrastructureless networks. In the former, communications among terminals are established and maintained through centric controllers. Examples include the cellular networks and wireless Local Networks (IEEE802.11). The latter variation is commonly referred to as wireless adhoc network. Such a network is organized in an adhoc manner, where terminals are capable of establishing connections by themselves and communicate with each other in a multi-hop manner without the help of fixed infrastructures. This infrastructureless property makes an ad hoc networks be quickly deployed in a given area and provides robust operation. Example applications include emergency services, disaster recovery, wireless sensor networks and home networking.
Communication has become very important for exchanging information between people from, to anywhere at any time. MANET is group of mobile nodes that form a network independently of any centralized administration. Since those mobile devices are battery operated and extending the battery lifetime has become an important aim. Most of the researchers have recently started to consider power-aware development of efficient protocols for MANETs. As each mobile node in a MANETs performs the routing function for establishing communication among different mobile nodes the "death" of even a few of the nodes due to power exhaustion might cause disconnect of services in the entire MANETs.
So, Mobile nodes in MANETs are battery driven. Thus, they suffer from limited energy level problems. Also the nodes in the network are moving if a node moves out of the radio range of the other node, the link between them is broken. Thus, in such an environment there are two major reasons of a link breakage: Node dying of energy exhaustion, Node moving out of the radio range of its neighboring node.

APPLICATIONS OF MANETS :

1.Military Scenarios
2.Data Networks
3.Rescue Operations
4. Device Networks
5.Sensor Network
6. Free Internet Connection Sharing

1.2ROUTING IN MANET

Mobile ad hoc networks (MANETs) have become aprevalent research area over the last couple of years. Many research teams develop new ideas for protocols, services, and security, due to the specific challenges and requirements MANETs have. They require new concepts and approaches to solve the networking challenges. MANETs consist of mobile nodes which can act as sender, receiver, and forwarder for messages. They communicate using a wireless communication link e.g. a Wireless LAN adapter (IEEE 802.11).

1.3 SYBIL ATTACKS

It is an unsafe advanced world out there. Security and antivirus programming is essential for any system. Restricted security can separate is in a Sybil attack. Sybil attack is a kind of security risk when a hub in a system guarantees various characters.

1.3.1Specific Types of Sybil Attack

a) Routing

b) Tampering with Voting and Reputation Systems

c) Fair Resource Allocation

d) Distributed Storage

e) Data Aggregation

1.3.2 Taxonomy of Sybil Attacks

Sybil Attacks Taxonomy: To better recognize the implications of the Sybil attack and how to preserve against it, we develop taxonomy of its different forms.
The capability of Sybil attacker can be determined in following ways:

a) Dimension I: Fabricated vs. Stolen Identities

b) Dimension II: Direct vs. Indirect Communication Direct Communication

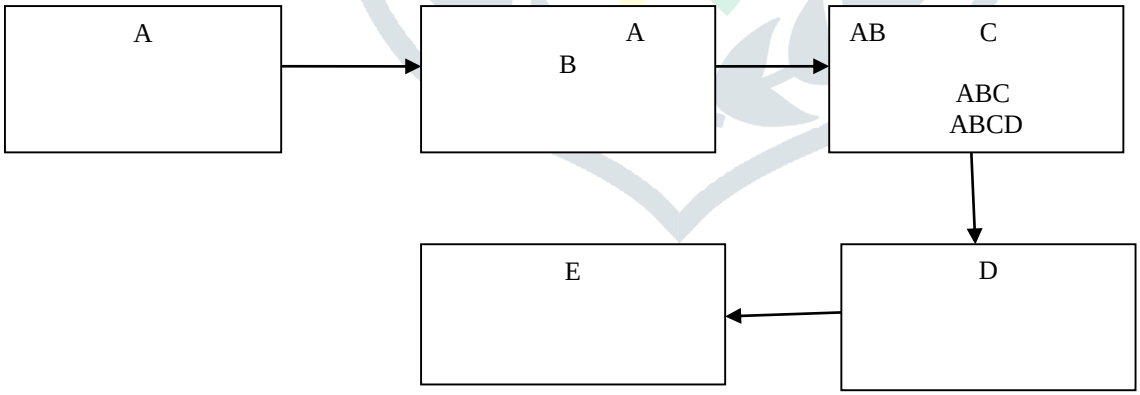
c) Dimension III: Simultaneous Vs Non-Simultaneous

1.4 M.PEGASIS PROTOCOL

M-PEGASIS is a chain based routing protocol for mobile WSN based on PEGASIS protocol to support mobile nodes. In M-PEGASIS nodes move according to random way point mobility model, after moving of the nodes, if node doesn't find close neighbor it goes into sleep mode for random period of time and then wake up. This method is repeated until it finds one in transmission range.

ROUTE DISCOVERY PROCESS

When source S wants to deliver data packet to destination D, then from header destination address can be obtained. Header also contains the source node, that contains the each routing node id.



.

When data packet moves from source to destination, then it is responsibility of each node to take care that right packet has been moved from source to destination. Node A passes packet from Node B, Node C, Node D to Node E, the destination. If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded.

1.5 NEURAL NETWORK

All neural networks take numeric input and produce numeric output. The transfer function of a unit is typically chosen so that it can accept input in any range, and produces output in a strictly limited range. For example of a sigmoid - S-shaped - function, the output is in the range (0,1), and the input is sensitive in a range not much larger than (-1,+1). The function is also smooth and easily differentiable, facts that are critical in allowing the network training algorithms to operate

2.1LITERATURE SURVEY

DSDV is developed on the basis of Bellman–Ford routing algorithm with some modifications. In this routing protocol, each mobile node in the network keeps a routing table. Each of the routing table contains the list of all available destinations and the number of hops to each

WRP belongs to the general class of path-finding algorithms , defined as the set of distributed shortest path algorithms that calculate the paths using information regarding the length and second-to-last hop of the shortest path to each destination.

In GSR protocol , nodes exchange vectors of link states among their neighbors during routing information exchange. Based on the link state vectors, nodes maintain a global knowledge of the network topology and optimize their routing decisions locally.

DSR allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination. In this protocol, the mobile nodes are required to maintain route caches or the known routes.

AODV is basically an improvement of DSDV. But, AODV is a reactive routing protocol instead of proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV.

3.1 PROBLEM STATEMENT

Because of the changing topology special routing protocols have to be proposed to face the routing problem in MANETs. Since routing is a basic service in such a network, which is a prerequisite for other services, it has to be reliable and trustworthy. Otherwise dependable applications cannot be provided over the MANET. This brings up the need for secure routing protocols. A secure routing protocol has to be able to identify trustworthy nodes and find a reliable and trustworthy route from sender to destination node. This has to be realized within a few second or better tenths of seconds, depending on the mobility of the nodes and the number of hops in the route. In the proposed work, the problem of routing can be solved using PEGASIS and Neural Network.

4.1 OBJECTIVE AND METHOLODGY

OBJECTIVES

This paper encompasses a set of objectives that is associated with a set of objectives that is associated with milestone of this process. The objectives are mentioned below.

1. To study the previous implemented routing algorithms.
2. To build the network for deployment.
3. To propose novel routing protocol.
4. To implement the proposed work based on PEGASIS and NN.
5. To evaluate the results.

METHODOLOGY

Matlab has been used as the simulation tool for evaluating the performance of PEGASIS protocol. Matlab has been used to simulate ANN using the inputs from matlab. Attempt has been made to enhance the Accuracy of routing on MANET using Artificial Neural Networks.

TOOLS USED

Table.1 Tools Used

Computer	Core 2 Duo or higher
RAM	3 MB
Platform	Windows 7
Other hardware	Keyboard, mouse
Software	Mat lab 7.10.4

5.1 SIMULATION MODEL

The simulations were carried out by using MATLAB as the language that we use to develop the proposed framework. In the simulation the following steps are to be followed by user:

Step 1 : Firstly initialize the network by entering the number of nodes as well as implement MPEGASIS on the network.

Step 2 : Then the source and destination is chosen by the network and a network is deployed.

Step 3 : After this, number of rounds will run showing different optimal path according to distance for the network.

Step 4 : Then a graph is plotted by the user.

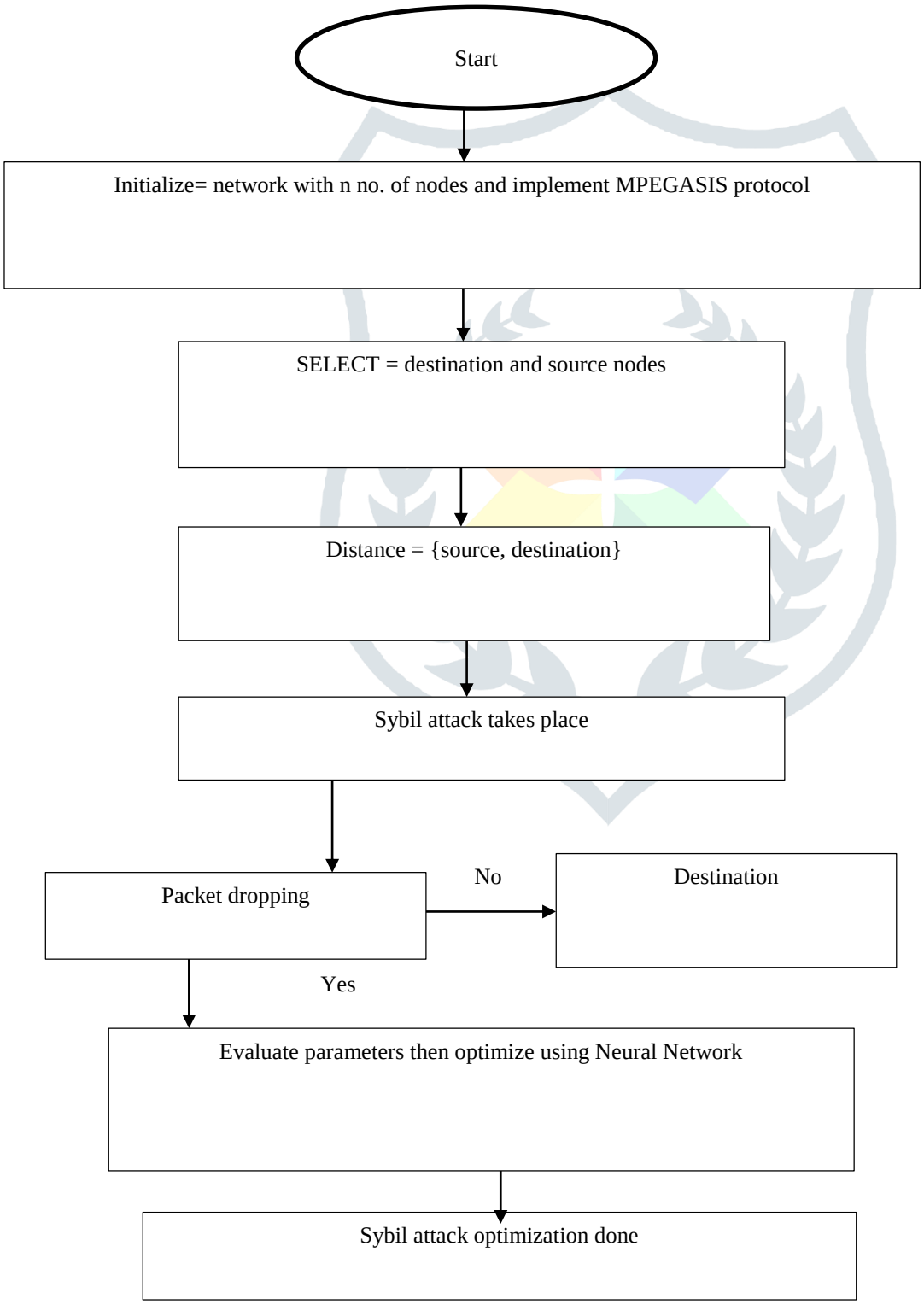
Step 5 : Then the Sybil attack which produces the number of multiple copies in the network which increases the load as well as some of the data packet is dropped due to Sybil attack in the network.

Step 6 : If packet dropping condition take place and some packets are lost. And if not then send it to the chosen destination.

Step 7 : Then, Plot graph for proposed parameters.

Step 8 : Call neural network for optimization purpose.

Step 9 : Then, again Evaluate parameters and plot graph with optimized network nodes. The specific parameters used are throughput, energy optimization, error rate and end to end delay.



6.1 RESULT

initially the network simulation model is formed which contains image while first time 20 nodes as given input and. Length vs breadth of the network is 1000*1000, the channel (CH) captures the routing information from the initiator (source node) and then sends the data from the source to destination node. Then we have Sybil nodes with k number of rounds to get accurate value of Sybil nodes. Initially, it searches nodes in network, then after this source is plotted in the network just after that Sybil Attack take place in the network and then we have Sybil attack nodes that has been found in cache memory

7.1 CONCLUSION AND FUTURE SCOPE

Main concept behind the wireless network is to save energy more and more so that it works last long enough. This is due to fact that the size of a node is expected to be small and this leads to constraints on size of its components i.e. battery size, processors, data storing memory, all are needed to be small. So any optimization in these networks should focus on optimizing energy consumption to enhance network life time.

In the proposed algorithm the energy consumption is more balanced as compared to the other optimization algorithms. The simulation result shows that the network lifetime is improved in case of proposed scheme. As from the simulation results, it has been also concluded that the nodes are balanced in the network.

In this thesis, we advance a simple protocol named as PEGASIS using neural network optimization on the network which is affected by Sybil attack. In this first we run the system by applying MPEGASIS, and once Sybil attack occur in the network then we will apply neural network for optimization purpose which will remove fake individualities/ nodes from the specific network. And results have been evaluated after sybil attack occurs inside the network as well as after Neural network optimization is applied on the network utilizing specific parameter such as: throughput, energy consumption, end to end delay and error rate.
In future combination of other soft computing may be implementing on the same protocol in order to obtain more encouraging

REFERENCES

[1] Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) forMobile Computers. Proceedings of ACM SIGCOMM 1994:234–244.

[2] Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989) A Loop- Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4:224–236

[3] Murthy S, Garcia-Luna-Aceves JJ (1996) An Efficient Routing Protocol for Wireless Networks. Mobile Networks and Applications, Volume 1, Issue 2:183–197.