ISSN:0975-9646

Efficient Routing Algorithm for Wireless Networks based on Bandwidth and Clock Rate

Anto Premkumar [#1], Shijo James[*2] , Saranya. R[#3]

*Assistant Professor-ECE[#1] ,Assistant Professor-EEE[*2] , Student – ECE[#3]*
CSI College of Engineering -The Nilgiris

Abstract- **The algorithm inculcates the use of dynamic – distance vector routing protocols such as RIP, RIPV2, IGRP, and EIGRP to determine the path. These routing protocols will determine the best path by analysing only the hop count. i.e. if a packet goes through a router it refers to one hop. So the least number of hop counts will be always considered as best path. In such case, those protocols will determine only the shortest path, but not the best path. The reason being on its ignorance of bandwidth (speed of transmitting the data) and clock rate(bits/sec) of the path in which the data has to travel, therefore wastage of time in routing and re-routing occurs. Standard Access Control List (Firewall of the router) which will deny an entire communication between the source and destination on the network. Here LINK STATE ROUTING (LSR) PROTOCOL i.e. OSPF, to determine the path is implemented. An OSPF routing protocol will determine the best path, especially by analysing the bandwidth & clock rate. It does not consider about the least number of hop counts. It will always choose only the path which is having highest bandwidth among the other paths and also to increase the routing and re-routing time. VLSM and DHCP on our networks, which will reduce the wastage of IP address and ignore the inactive hosts on the network to reduce the analysing time has brought into account. A new ACL (Firewall of the Router) which is Extended Access Control List (EACL) is developed. With the help of the new EACL Configuration we are able to deny or allow the communication on protocol basis which means if we require only HTTP Communication with the Destination Network we can deny the rest of the services like NFS, FTP, TELNET, SNMP, etc. So that the users from the destination network can view or access only the HTTP site, the users will be denied immediately if they try to access any of our other services (NFS, FTP, TELNET, SNMP).Hence utilization of bandwidth is efficient in the method.**

Keywords*-EACL (Extended Access Control List), LSR (Link State Routing) Protocol, OSPF (Open Shortest Path First), VLSM (Variable Length Subnet Mask), DHCP (Dynamic Host Configuration Protocol), TELNET (Telecommunication Network), FTP (File Transfer Protocol).*

I.INTRODUCTION

Wireless communication technology is increasing daily with such growth sooner or later it would not be practical or simply physically possible to have a fixed architecture for this kind of network. While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability — the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper, we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from previously-studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work overtime to entirely disable a network. While some of the individual attacks are simple, and power-draining and resource exhaustion attacks have been discussed before [1,2,3] prior work has been mostly confined to other levels of the protocol stack, e.g. medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent. [4] The Ad hoc wireless network must be capable of self-organize and self-configure due to the fact that the mobile structure is changing all the time. Mobile hosts have a limited range and sending the message to the other host, which is not in the sender's host transmission range, must be forwarded through the network using other hosts which will be operated as routers for delivering the message throughout the network. The mobile host must use broadcast for sending messages and should be in promiscuous mode for accepting any messages that it receives. In the ad hoc network there can be unidirectional hosts that can transmit only to the one direction, so that the communication is not bi-directional as in the usual communication systems. [5, 6, 7]. Find an alternate path, after a link failure, from a source node to a destination node. Since reconvergence of an Interior Gateway Protocol (IGP) (e.g., OSPF or IS-IS) can take hundreds of milliseconds, there is a need for a method that will find an alternate path in less time than this. The target application is a small (up to tens of nodes) access sub network of a service provider's network, which is a typical scale encountered in practice a service provider typically has many such small regional access networks. Fast Re-Route (FRR) methods establish a new path from s to d in much less time than required for IGP re-convergence.[8] Network security has become serious business in the past few years. Internet worms and Denial of Service (DoS) attacks impact almost every user on the Internet, especially businesses and governments. While end users may experience slowness in connections or inaccessibility of certain websites, businesses and governments experience a significantly greater impacting [9]. A mobile ad-hoc network (MANET) is a collection of nodes, which are able to connect on a wireless medium forming an arbitrary and dynamic network with “wireless links”. That is, over time the links between the nodes may change due to node mobility, nodes may disappear and new nodes appear in the network. The physical size of a MANET is expected to be larger than the radio range of the wireless interfaces, thus for any two nodes in the network to be able to communicate, routing of traffic through a multi-hop path is necessary. [10] Relying only on link-state information means that no router is aware of the individual communicating pairs in the network or their requirements and yet have to act independently such that the TE objective is optimized. This is a very real restriction as in any large dynamic network like the Internet it is not possible to obtain information about individual communicating peers. [11,12]. Access control lists (ACLs) represent a critical component network security. They are deployed at all points of entry between a private network and the outside Internet to monitor all incoming and outgoing packets. A packet can be viewed as a tuple with a finite number of fields such as source/destinationIP addresses, source/destination port numbers, and the protocol type.[13]

II. Problem Statement

The router was configured by using Distance Vector Routing Protocols which will determine only the shortest path not the best path. There occurs delay and traffic at the time of transmitting the packets. And each time the same path with the least number of hops will be determined as the best path. Routers will not look into the alternate path to reach the destination. So it is easy for the Vampires to know the path in which the packets are transferred and Vampires will try for Data Integrity and Dos (Denial of Service). The delay was the main issue at the time of Routing and Re-routing. At the time of routing, the router look into all the active and inactive nodes in the destination network and hence the delay has occurred. It is not possible to deny the particular TCP & UDP Services like HTTP, FTP, Telnet, snmp, tftp in the existing one. So all the TCP & UDP Services will be denied, in that case there occurs more traffic & more CPU utilization to deny all the services, at the same time the data delivery will get delayed.

III. The Proposed Algorithms

In this section, we describe our proposed algorithm in detail. We first introduce the network model, and then describe the parts of: Estimation of time quantum, efficiency.

A.Network Model

Our algorithm can be applied to diverse network models. However, in order to compare the performance of our algorithm with the existing ones, we adopt a network model. In our scenario, about 13 routers, 16 systems and 2 servers (HTTP and FTP) are deployed in a clustered form fashion. The parameter that is considered for the selection is maximum bandwidth and clock rate.

B.Calculation For Bandwidth & Clock Rate

BANDWIDTH=Amount of data transferred to the interface in (kilobytes) /Total time duration takes to transfer (Sec).

BANDWIDTH=d_i (kilobytes) /$T_{i.}$ -----------[1]

CLOCK RATE= Amount of data transferred to the transmission medium in (bits) /Time duration takes to transfer (Sec).

CLOCK RATE=dT_{xi} (bits) /$T_{i.}$ ---------------[2]

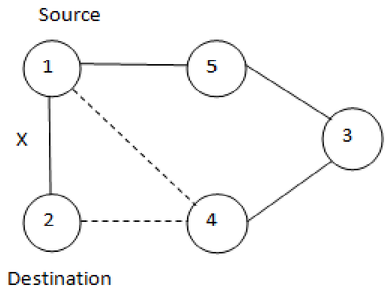


Fig.1.Based on Bandwidth sending the data, even after a link failure.

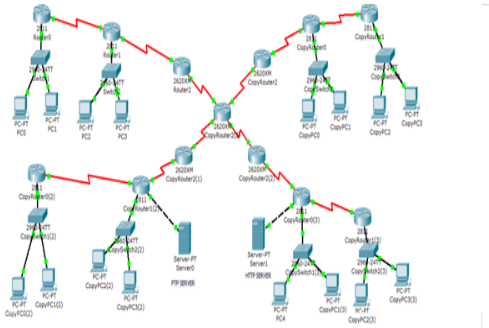


Fig.1.1Cluster based scenario

C.Proposed Algorithm

In the previous techniques which are the main concern of this research is one of the oldest, simplest and fairest and most widely used scheduling algorithms, designed especially for time-sharing systems. It’s designed to give a better response , but the worst turn around and waiting time due to the fixed time quantum concept. The scheduler assigns a fixed time unit (quantum) per process usually 10-100 milliseconds, and cycles through them. In this algorithm, we propose a new algorithm to solve the constant time quantum problem. The algorithm is based on the dynamic time quantum approach where the system adjusts the time quantum according to the burst time of processes founded in the ready queue. This method needs two registers to be identified: - SR: Register to store the sum of the remaining burst times in the ready queue. AR: Register to store the average of the burst times by dividing the value found in the SR by the count of processes found in the ready queue.

When a process in execution finishes its time slice or its burst time, the ready queue and the registers will be updated to store the new data values.

- If this process finishes its burst time, then it will be removed from the ready queue. Otherwise, it will move to the end of the ready queue.
- SR will be updated by subtracting the time consumed by this process.
- AR will be updated according to the new data.

When a new process arrives in the ready queue, it will be treated according to the rules above in addition to updating the ready queue and the registers.

3.2 Pseudo Code and Flow Chart the algorithm described in the previous section can be formally described by pseudo code and flow chart like to follow:

```
-------------------------------------------------------------------
                 Algorithm: Proposed algorithm
-------------------------------------------------------------------
New process P arrives
P Enters ready queue
Update SR and AR
Process p is loaded from ready queue into the CPU to be executed
IF (Ready Queue is Empty)
TQ = BT (p)
Update SR and AR
End if
IF (Ready Queue is not empty)
TQ=AVG (Sum BT of processes in ready queue)
Update SR and AR
End if
CPU executes P by TQ time
IF (P is terminated)
Update SR and AR
BW=DT/TT
CR=TM/TT
End if
IF (P is not terminated)
Return p to the ready queue with
Its updated burst time
Update SR and AR
End if
-------------------------------------------------------------------
```

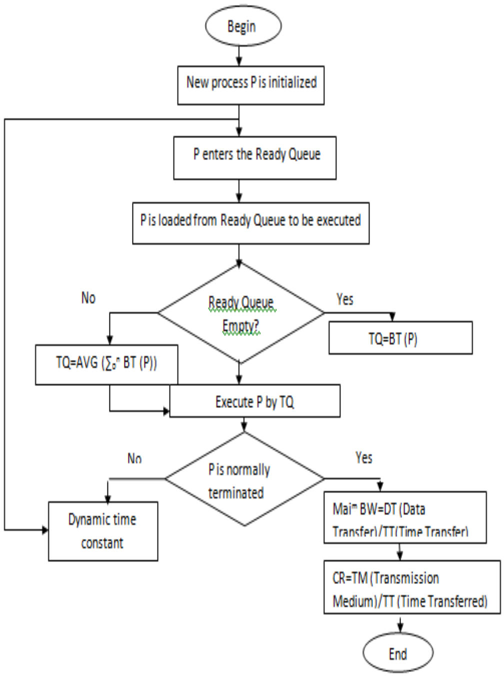

Begin
New process P is initialized
P enters the Ready Queue
P is loaded from Ready Queue to be executed
Ready Queue Empty?
No
Yes
TQ=BT (P)
TQ=AVG (∑₀ⁿ BT (P))
Execute P by TQ
P is normally terminated
No
Yes
Dynamic time constant
Mai™ BW=DT (Data Transfer)/TT(Time Transfer)
CR=TM (Transmission Medium)/TT (Time Transferred)
End

Fig.2. Flow chart for Proposed Algorithm

D.Dijkstra's Algorithm on bandwidth

Assume that in G, all edge bandwidths are nonnegative, i.e., for all $(u, v) \in E$, we have $m(u, v) \geq 0$. In such a graph, Dijkstra's algorithm provides us with the optimal path(s) that solve(s) the single-source shortest-path problem. Internally, the algorithm assigns into a set S all the nodes whose final shortest path bandwidths from the source s have already been calculated.

```
-------------------------------------------------------------------
                 Algorithm For Bandwidth
-------------------------------------------------------------------
 Procedure DIJKSTRA (G, m, s)
for all v ∈V do
N[v] ←∞
Π [v] ←NIL
 end for
Q ←V
N [s] ←0
While Q<∞ Do
u← EXTRACT-MIN (Q)
Q ←Q\u
 for all node v ∈ N (u) do
RELAX (u, v, m)
end for
end while
end procedure
-------------------------------------------------------------------
```

IV. Performance Evaluation

The performance evaluation on energy consumption, packet delivery ratio, and delay and bit error rate was executed and compared with the existing techniques.

TABLE I
EXPERIMENTAL SCENARIO

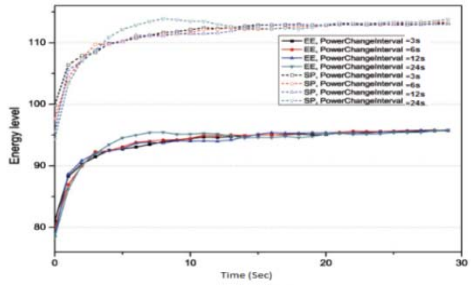
Number of nodes	16
Hops	13
Initial Energy	100joules
Wireless Range	Infinity
Buffer	16 packets

The above experimental scenario is used to evaluate the performance of the proposed algorithm. It uses 16 nodes with hops of 13. The Initial energy of each node is 100 joules, but its stops communicating when it drains to 0 joule.

TABLE II
EXISTING VS. PROPOSED SYSTEMS

	Existing	Proposed
Energy	94 J	78J
Throughput	13900	14500
Hop count	4.7	5.35

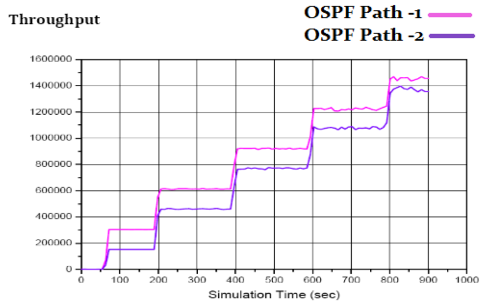
E.Energy Level



EE=Energy Efficiency
SP=Shortest Path
Fig 3. Energy Level

In terms of energy consumption the proposed algorithm performs well. With its initial 100 joules only 20 percent of energy is being consumed.

F.Throughput

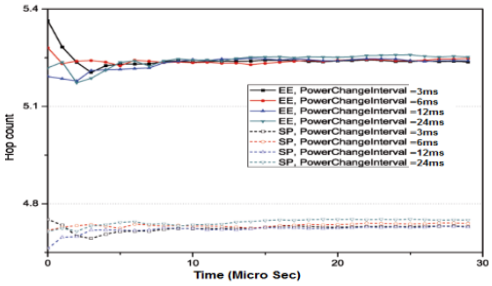


Throughput (bits/sec)

Fig 4.Throughput

Throughput of the proposed algorithm is better when compared to the normal routing strategy because the delivery ratio is extremely high and suddenly increases because of the fast computation of shortest paths.

G.Hop Count



Hop count *vs* Time.

Fg.5. Hop Count

The hop count of the proposed algorithm is very high when compared to existing one since the time taken for hop count is nano second.

V. SIMULATION RESULTS

In this section, the performance of our proposed algorithm is compared using the simulated results and our algorithms show better efficiency in terms of energy, throughput, and hop count time. It achieves high efficiency in energy consumption. Techniques developed for fast recovery from single-link failures to provide more than one forwarding edge to route a packet to a destination. Whenever the default forwarding edge fails or a packet is received from the node attached to the default forwarding edge for the destination, the packets are rerouted on the backup ports. In the authors present a framework for IP fast reroute detailing three candidate solutions for IP fast reroute that have all gained considerable attention. When a forwarding link on a tree fails, the packet may be switched to the other tree.

VI.CONCLUSION AND FUTURE WORK

OSPF Link State Routing protocol, which controlled the delay and traffic by analysing the bandwidth at the time of routing has been implemented. VLSM and DHCP, which are used to reduce the wastage of IP address and ignore the inactive nodes in the network, which will lead to improving the Routing and Re- routing is achieved. Finally the EACL is developed to deny the Vampire attack as well as to deny the unused TCP/IP Services. The above mentioned project deals with the bandwidth to control the delay and traffic, so in future we can work on to improve the bandwidth to get better performance. In future the above completed task can be modified by some other new techniques and algorithms which will reduce the delay time and traffic even more and helps to transmit the packets with high speed and leads to the vampire less networks.

ACKNOWLEDGEMENT

we extend our greatful thank to all the staffs who extend their valuble thoughts to carry out this work successfully.

REFERENCES

[1] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, Context, 2006.

[2] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1

[3] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.

[4]. Eugene Y. Vasserman and Nicholas Hopper "Vampire attacks: Draining life from wireless ad-hoc sensor networks" IEEE transactions on mobile computing vol.12 no.2 year 2013.

[5] Xiaoyan Hong, Kaixin Xu and Mario Gerla "Scalable Routing Protocols for Mobile Ad Hoc Networks.", Los Angeles, August 2002.

[6] Koey Huishan, Chua Huimin and Koh Yeow Nam "Routing Protocols in Ad hocWireless Networks.

[7] P.Jacquet, P. Mühlethaler, T Clausen, A. Laouiti, A. Qayyum and L. Viennot "Optimized Link State Protocol for Ad Hoc Networks." IEEE INMIC Pakistan 2001.

[8] Eric Rosenberg And James Uttaro, A Fast Re-Route Method IEEE Transactions On Networking Year 2013.

[9].Access Control Lists to Protect a Network from Worm/DoS Attacks By Dennis Eck CCNA December 4, 2003 GSEC Practical Assignment Version 1.4, Option 1.

[10] Thomas Heide Clausen, Gitte Hansen, Lars Christensen Gerd Behrmann" The Optimized Link State Routing Protocol Evaluation through Experiments and Simulation".Mindpass Center For Distributed Systems Aalborg University,Fredrik Bajers Vej 7E, DK-9220 Aalborg,Denmark.

[11] Optimal Link-state Hop-by-hop Routing by Nithin Michael, Ao Tang and Dahai Xuy.978-1-4799-1270-4/13/13/ IEEE 2013

[12].R.Gallager, "A minimum delay routing algorithm using distributed computation," Communications, IEEE Transactions on, vol. 25, no. 1, pp. 73 – 85, Jan 1977.

[13]. Compressing Network Access Control Lists by Alex X. Liu Eric Torng Chad R. Meiners IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS-2011.

[14]. Comparing AODV and OLSR Routing Protocols by Aleksandr Huhtonen Sjokulla.2004-04-26/27.

[15]. A Link-state QoS Routing Protocol for Ad Hoc Networks by Anelise Munaretto, Hakim Badis, Khaldoun Al Agha, Guy Pujolle.0-7803-7605-6/0/2 2002 IEEE.

[16]. Using Multiple Metrics with the Optimized Link State Routing Protocol for Wireless Mesh Networks by Waldir A. Moreira Jr. Elisangela Aguiar, Antoniou Abel´em, Michael Stanton.26º Siposio Brasilerio De Redes De Computadores E Sistemas Distribution

[17]. Packet Re-cycling: Eliminating Packet Losses due to Network Failures by Suksant Sae Lor, Raul Landa and Miguel Rio.

[18]. An evaluation of IP based Fast Reroute Techniques by Pierre Francois, Olivier Bonaventure.Copyright is held by the author/owner.CoNEXT'05,October 24-27,2005,Toulouse,France.

[19]. On the Role of Routing in Named Data Networking by Cheng Yiy, Jerald Abrahamy, Alexander Afanasyevz, Lan Wangx, Beichuan Zhangy, Lixia Zhangz. NDN,Technical Report NDN-0016, 2013. http://named-data.net/techreports.html Revision 1: December 7, 2013.

[20]. Hybrid Link-State, Path-Vector Routing by M. Abdul Alim, Timothy G. Griffin AINTEC'10, November 15-17,2010,Bangkok ,Thailand.Copyright 2010 ACM 978-1-4503-0401-6/10/11.