IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. II (Jul.-Aug. 2016), PP 38-42
www.iosrjournals.org

Efficient Network Design Parameters for Packet Switching Using Poisson distribution Methode

L.Sudha[1] , Dr.P.Thangaraj[2]
[1]*Research Scholar, AP/CSE, Navarasam Arts & Science College for Women, Erode,Tamilnadu,India.*
[2]*Professor & Head /CSE, Bannari Amman Institute of Technology,, Sathyamangalam. Tamilnadu,India*

Abstract: *Wireless sensor network is a group of sensor nodes with inadequate processor and partial memory unit embedded with other equipment for communication through the networking banding system. Sensor networks is one of the component of computer network which are used widely in many range of applications, they are Environment monitoring, healthcare, industrial control units of monitoring and system, military applications for security information transformation and many more. This paper defines the basic of security requirements and specification and various attacks on OSI layer network and type of routing algorithm. This paper also review proposed packet switching techniques which is imposed with Poisson distribution for finding the shortest path of the packet switching for specific OSI Layer to liberal the super security mechanisms sending the data or information from one destination to another source of network in WSN.*
Keywords: *Computer Network, Type of attacks, Routing, Packet Switching, Poisson Distribution*

I. Introduction : Routing

A router or a host has a routing table with an entry for each destination or a combined destination for routing the IP packets. The routing table can either be static or dynamic and it contains manually entered information. For each destination, the administrator enters the route into the table. Using one of the dynamic routing protocols like RIP, OSPE or BGP, dynamic routing table will be updated periodically[1].
The vital role of the network layer is to route packets from source to destination and to attain this, it is must selecting a route through the network and in general more than one route is possible. Based on performance criteria, route selection will be done and the simplest one is to select the shortest route that passes through the least number of nodes which results in the least number of hops per packet. To perform this task, a routing algorithm is designed which is a part of network layer software[1],[2].

II. Properties Of Routing Algorithm

Desirable properties of a routing algorithm are Correctness, Simplicity, Robustness, Stability, Fairness, Optimality, and Efficiency. They are Correctness and simplicity are self-explanatory, Robustness supports the capability to cope up with the topological changes and traffic. It requires no hosts to be aborted and network to be rebooted, Stability refers to an equilibrium state of the algorithm and it is the state that reacts to changing conditions such as Congestions, Under any circumstance, the network should neither react too slow nor experience unstable swings from one extreme to another and few performance criteria can either favor the exchange of data packets between nearby stations or confuse the exchange between distant stations[3]. It is to be noted that, always a compromise is needed between fairness and optimality.

2.1 Routing tables

Once the decision making is made, this information or message should be stored in the routing table which let the router knows how to forward a packet. In virtual circuit packet, routing table contains both the incoming and outgoing packet number and determines the output port for the packet to be forwarded. In datagram networks, based on the destination address, routing table contains the next hop to forward the packet.

III. Routing Algorithm Classification

Depending upon the responsiveness, routing algorithm can be classified into two types as: Static (non-adaptive) Routing Algorithm and Dynamic (adaptive) Routing Algorithm

3.1 Static (non-adaptive) Routing Algorithms

In static routing, an initial path will be determined by the network topology and then pre-calculated paths are loaded and fixed for a long time in the routing table. This type of routing suits all small networks and becomes inconvenient for a bigger network. The only disadvantage of this routing is its incompetence to respond quickly to network failure[4][5].

3.2 Dynamic (adaptive) Routing Algorithms

If there is a change in the topology traffic, dynamic routing algorithm will take the routing decision and through neighbor communication, network status will be continuously monitored. Hence, a change in network topology is eventually propagated to all the routers.[6] Each and every router computes the path that suits the destination based on the information gathered. Router complexity is the only disadvantage of this dynamic routing algorithm. The following table are comparison between the static routing and dynamic routing as given in the Table 3.1.

Table 3.1: Comparison between the Static Routing and Dynamic Routing

S.No	Static routing (non-adaptive)	Dynamic routing(adaptive)
1.	Static routing manually sets up the optimal paths between the source and the destination computers.[2]	Using the dynamic protocols, dynamic routing updates the routing table and finds the optimal path between the source and the destination computers.[2]
2.	A router using the static routing algorithm does not require any controlling mechanism if there exists any fault in the routing paths.[2]	Dynamic routers use the dynamic routing algorithms which can locate a faulty router in the network.
3.	While finding the path between two computers or routers in a network, this router would not encounter the faulty computers.	The dynamic router eliminates the faulty router thereby finding out another possible optimal path from the source part to the destination part.
4.	The static routing is suitable only for very small networks and cannot be used in large networks.	Dynamic routing is used for the larger network.
5.	The simplest way of routing the data packets from a source to a destination in a network is done by static routing.	For routing the data packets, the dynamic routing uses complex algorithms.
6.	The static routing has the advantage that it requires minimal memory.[2]	Depending on the routing algorithm, dynamic routers have quite a few memories overheads.
7.	In a case of static routing, the network administrator finds out the optimal path and makes the changes in the routing table.[2]	In the dynamic routing algorithms, the algorithm and the protocol are responsible for routing the packets and making the changes in the routing table[2].

IV. Requirement Of Design Goals

In general, routing algorithm will have one or more of the following design goals like Optimality, Simplicity, Robustness and stability, Rapid convergence and Flexibility[5][6].

4.1 Optimality:

Optimality refers to the ability of the routing algorithm to select the best route. Based on the metrics and metric weightings used to make the calculation, best route will be selected. For example, a routing algorithm can utilize many hops and delay but, it will delay the calculation. By natural, routing protocols should strictly define their metric calculation algorithms.

4.2 Simplicity:

Routing algorithms are designed such a way it must be as simple as possible which offers an efficient function with a minimum of software and utilization overhead. Efficiency is particularly important while the software implements the routing algorithm on a computer with limited physical resources.

4.3 Robustness:

Routing algorithms must be robust as they have to withstand even in unforeseen circumstances such as hardware failures, high load conditions, and incorrect implementations. As the routers are located at junction points, they can cause considerable problems when they fail. The routing algorithms will be the best when they withstood the testing time and proven stable under a variety of network conditions.

4.4 Rapid Convergence:

Routing algorithms must converge rapidly. Convergence is the process of an agreement by all routers, on optimal routes. When a networking event causes either a routes to go down or become available, routing update messages will be distributed by the routers that permeate networks, stimulate recalculation of optimal routes and cause all routers to agree on these routes eventually. Slowly converging routing algorithms can cause routing loops of network outages.

4.5 Flexibility:

Flexibility is most important for the routing algorithms. In other words, routing algorithms should adapt to a variety of network circumstances quickly and accurately.

For example, assume that a network segment has gone down. On becoming aware of this problem, routing algorithms will quickly select the next better path for all routes normally using that segment. Routing algorithms can be programmed in a way such that it can adapt to changes in network bandwidth, router queue size, network delay and other variables.

V. Proposal Methodology: Shortest Route Identification For Packet Switch Using Poisson Distribution

The ISO standard for worldwide communication require the standard protocol to sending the information from one destination to another source destination[3][7]. The following details are type of attacks in computer network which means in OSI layer, the major attacks are available in physical layer, Data link Layer, Network layer and Transport layer is shown in Table 5.1.

Table 5.1 Type of Attacks and its major affecting elements.

Major type of attacks in OSI layer	
Physical Layer	Jamming Attack defense
Data Link Layer	Denial of services
Network Layer	Selective forwarding, Sinkhole, and warm hole, Sybil attack, Hello attack.
Transport Layer	Flooding and De-synchronization

5.1 Packet switched network

Message switching has a number of features and services to other executable devices.

(1) A message may be very long (hundreds of thousands of bits) or very short (of the order of thousands of bits). The large buffer should be available to accommodate the long message. While receiving the short messages, buffer's hardware will be wasted.

(2) A switching computer will not begin to relay a message until the entire message has a first been received even though a line is available. Accordingly, if the message duration is Tm and it must be relayed R times. While ignoring waiting time, the delay will be RTm since at each relay the entire message is stored before being forwarded to the next node. Time becomes inconvenient for long messages and many relays.

(3) To accommodate a very short message, a link must be needed in between the centers but, the link is busy transmitting a very long message. In a message switching system, it would be useful if it is possible to interrupt the long message to allow transmitting feature. Hence, when the system is tied up processing a long message it is possible that short message may be delayed in comparison with the message lengths[7][8].

5.2 Packet switched network responsibility

A packet switched network responsible for circumventing the less desirable features of message switches by subdividing the messages into packets. A typical packet may be 1024 bits long and the message is then transmitted packet by packet. Like the message switching each packet, it must be stored in buffers to store and forward system.In some packet switching system, at destination different packets of a single message may arrive and by differed system, different packets of a message may arrive out of order. Like messages, packet switching may represent a small sequence in the switching computers[8].

Despite that the message may in message switching or in packet switching, each unit of transmission include additional bits referred to as overhead information in addition to the information bits. The overhead bit must identify the destination of the unit so that each switching center will know the further route to the source of the unit where the user can be charged for services.Further, as a part of the overhead, the synchronization bits must be included to identify the beginning and end of the unit. As already mentioned, different packets switching are reassembled in packet switching in proper sequence.

In a message switched system, the information overhead must be annexed to each message accompanied by overhead bits. Thus, if there is more than one packet/message, the packetized message will become more overhead. Accordingly, with respect to message switching packet switching has two disadvantages.

(1) To transmit a given amount of information per unit time, packet switching requires bits to be transmitted at a rapid rate more than is required for message switching.

(2) The switching hardware needed to packetize, add overhead, de-packetize and reassemble is more complicated and it must operate rapidly than the corresponding hardware needed in message switching.

Let assume that a message of B bits is to be relayed from one to another of a series of switching computer using message switching. There is to be a K+1 computer involved in the overall transmission from the source computer C0 to the destination computer CK over K transmission facilities (links).

$$TM = K\,[(B+b) / fb] \cong B/ fb \cong K\,B/fb \qquad (1)$$

Since ordinarily B>> b. next, let us consider that the message has been divided into P packets each with a number of bits per packets B/P, and let's assume that the number of overhand bits needed is again b as before. The total number of bits in the packets is them (B/P) + b. to transmit this packet over the K links will require a time as given except with B replaced by B/P. Hence, the time request for the first transmitted packet to arrive at its destination is K [(B/P) + b]/fb. Since after the first and will arrive after the first by a time [(B/P) + b]/fb. Since after the first there are placed p-1 further packets the total time needed to transmit the entire message by packets is

$$Tp=K[(B/P)+b]/fb(P-1)[(B/P+b]/fb \quad (2)$$

To find the volume of p which minimizes Tp with a set of zero the derivation of Tp with respect to p. Tp will be minimal, when P2 = (K-1) B/b. And that correspondingly(1) & (2) then, Tp is min = b/fb B/b + k-1]2, If B/b>>k then Tp, min b/fb. And this case, referring to Tp, min/Tm=1/K. if there is a finite propagation time association with propagation over a link, then Tp and Tm will be increased by the amount K.

5.2 The Poisson distribution

To determine the probability that m packet occurs in a time τ, P (m, τ); we assume that the transmission of any packet was statistically independent of any other packet. Further, if the probability of no message occurring in the time interval τ1 is P (0, τ1) and the probability of no packet occurring in the time interval. τ2 is P (0, τ2), then since the events are independent the probability that no packet will occur in the interval τ1+ τ2 is P(0, τ1+ τ2)= P(0, τ1) . P (0, τ2), and also took for granted that as τ increase, the probability of a packet occurring in the interval increases[9][10]. Now P (0, τ) is a function of τ alone so we may represent it simply as f (τ) contain in f (τ1+ τ2) = f (τ1).f (τ2).

If we let τ decrease to a small value, Δτ, then reduces to P (0, Δτ) = 1 - λ Δτ, where λ is yet to be determined, which approaches unity as Δτ approaches zero. It, therefore, appears reasonable to assume that in an interval Δτ at most 1 packet can be received.The portability that 'm' packets are received in a time interval τ+ Δτ can then be written as P (m, τ+ Δτ) = P(m, τ). P (0, Δτ) + P (m-1, τ). P (1, Δτ) (3)

Where the first product term is the probability that all m packet were received in the τ seconds interval and none in the interval Δτ and the second product term is the probability that m -1 packets are received in the time in the time interval τ and one packet received in Δτ. Note that we have neglected the possibility of two or more packets in the interval Δτ. Since P (0, Δτ) = 1 - λ Δτ and P (1, Δτ) = 1- P (0, Δτ) = λ Δτ and have using P (m, τ+ Δτ) = P(m, τ) [1 - λ Δτ] + P(m-1, τ) [λ Δτ] ,Transposing, we get

$$P (m, \tau+ \Delta\tau) - P (m, \tau)/ \Delta\tau = \lambda [P (m-1, \tau) - P(m, \tau)] \quad (4)$$

Which, in the limit as Δτ → dτ, becomes, dp (m, τ)/ dτ = λ [P(m-1, τ) - P(m, τ)],The reader can, by direction substitution, verify that the solution of the differential – difference equation given by, is the Poisson distribution (3) and (4),

$$P (m, \tau) = (\lambda\tau) m e\lambda\tau / m! \quad (5)$$

The average value of m is shown in the problem to be $\bar{m}$ = E (m) = λτ.Thus, λ is defined as the average number of packets per seconds

VI. Conclusion

Security has transformed into a key issues in WSN's because they are naturally of the vulnerable to a superior number of attacks than wired networks, so network required the successful security mechanism to minimize the security attacks, security related issues and challenges in wireless sensor system with OSI network layer. Moreover, this research the articulate about the brief dialog on the packet switching with identifying the route of the path of network system to send the data set through layer technology with security manner as well the direction or angle of the path of the routing with the static and computer involved in the overall transmission from the source computer C0 to the destination computer CK over K transmission facilities links on Poisson Distribution to increase trusted system detection and remediation of vulnerability is crucial. Computer network to solve the problem of security and vulnerability to improve the security evaluation procedure.

References

[1]. Ali Dorri, Seyed Reza Kamel and Esmail kheyrkhah, Security challenges in mobile ad hoc Networks: A survey, International Journal of Computer Science & Engineering Survey (IJCSES),6(1), 2015,15-29.
[2]. Emerole Kelechi C and Achumba I, A Critical Review of Techniques for Security and Measurement in a Switched Network, International Journal of Science, Engineering and Technology Research (IJSETR), 4(1), 2015,24-29.
[3]. Fatemeh Soleimani Roozbahan and Reihaneh Azad, Security Solutions against Computer Networks Threats, International Journal of Advanced Networking and Applications,7(1),2015, 2576-2581.
[4]. Lovepreet kaur and Jyoteesh Malhotra , Review on Security Issues and Attacks in Wireless Sensor Networks, International Journal of Future Generation Communication and Networking,8(4),2015,81-88.
[5]. Lovepreet,Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey, International Journal of Computer Applications,100(1),2014, 0975 –0987.

[6]. M. Chowdhury, M. Fazlul Kader and Asaduzzaman, Security issues in wireless sensor networks:A Survey, International Journal of Future Generation Communication and Networking, 6(5),2013,97-116.
[7]. P. L. Chang and P. K. Varshney, Integration of optimal routing and flow control in ATM networks,IEE Proceedings: Communications,145(1), 1998,1-7.
[8]. Ridhi Bhatla, Ashok Kumar and Preeti Khera , Comparative Analysis of Routing Protocols and Security Threats in Wireless Sensor Networks, International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering,4(4), 2016,95-102.
[9]. Sherif A. Abdelrazek, Integrated PV Capacity Firming and Energy Time Shift Battery Energy Storage Management Using Energy-Oriented Optimization , IEEE Transactions on Industry Applications 52(3) ,2016, 2607 – 2617.
[10]. Vandana C.P, Security improvement in IoT based on Software Defined Networking (SDN), International Journal of Science, Engineering and Technology Research (IJSETR), 5(1), 2016,291-295.