Multipath protected routing in distributed computer systems

As'ad Mahmoud As'ad Alnaser

Department of Computer Science, Al-Balqa' Applied University, Ajlun University College

Asad1_99@yahoo.com

Abstract *In this paper, we give a new solution of a scientific problem, which consists in developing a new approach to the organization of data in distributed computing systems that enhance the security of data during transmission over wireless channels.*

Keywords

Multipath routing, Security, network

1 Introduction

Safety and reliability of information transmission via a data-transfer network are important aspects in distributed computer systems such as Grid-systems and Cloud computing. There are a number of protocols that ensure the protection of information on different network layers. Multipath routing protocols refer to these protocols. They provide safety on the physical layer by dividing transferred data between a number of different paths, that considerably complicates an attacker's goal. Multipath routing also lets to significantly increase the reliability and fault-tolerance of data transmission.

In this work the analysis of the basic methods of multipath routing was carried out[1]:

1) split multipath routing;
2) diversity injection technique;
3) on-demand multipath routing.

2 Method of split multipath routing

The method of split multipath routing was chosen on the grounds of analysis of the advantages and disadvantages of each method.

The way to secure multipath routing proposed in this article is based on A. Shamir's threshold message sharing algorithm. The idea of the algorithm is that some secret K is divided into N unique parts[2]. Herewith it is necessary to get at least T of N parts to recover the original text. And, accordingly, the presence of $T-1$ and less parts does not allow recovering the secret. Such sharing is called threshold (T, N)-sharing where $T \leq N$. In the process of sharing a secret on the sender's side the massage sharing algorithm is executed, on the receiver's side the message recovering algorithm is executed. Both algorithms consist of linear operations, because all the calculations are done on polynomials. The method is based on the following statement: during sending a secret message through one of the paths, an attacker, intercepting one of the nodes on this path, intercepts the message. Thus, if message is divided into several parts, and each of these parts is sent through the different independent paths, then in general, an opponent has to intercept all the paths to recover the message. To intercept the message an attacker has to do at least two things. First he has to intercept all parts of the message physically. This can be done by eavesdropping or intercepting of nodes. Anyway, in case of sending the message via the different paths it will be difficult for an attacker to gather all parts of the message. Secondly, encoding of the connection between nearby nodes is expected, by different keys for each connection.

Within this work the influence of redundancy on the safety of data transmission was analyzed, as well as the search for the optimal value of r for a given level of security in the system was made. It was found that for a given security level such (T, N)-sharing may be found with which the transmission reliability is maximal, while the probability of

compromise will be within the threshold value [3]. Adding the threshold value of security will let to determine the optimal parameters of sharing messages from the point of view of safety and reliability. In the research *N* was chosen equal to the number of independent paths. In the future it is also needed to explore dependencies for $N < m$, herewith the largest number of parts of the message will be assigned to the path with the least probability of compromise. The increase of *N* will let to reduce the augment of variation of redundancy, thus, if y are equal, in the scheme with larger *N* redundancy (reliability) will be higher. Also, with increase of *N* it can be difficult to calculate the values, because there are operations of factorial (Bernoulli trial) and exponentiation (sharing/recovering of the message) in the calculations[4].

In this work a way to improve the security of data transmission in MPLS networks using threshold secret sharing schemes was proposed. Wireless network which is built on the basis of MPLS/VPN protocols with multipath routing protocol will let to protect the data transmitted through the MPLS network if an attacker manages to get the private key of the VPN network and intercepts one of the MPLS network nodes through which data is exchanged in wireless networks.

A threshold secret sharing scheme refers to divide the secret between members of a group, each of whom knows only a part of the secret. The secret can be recovered only by connecting the parts of the secret together. The separate parts are irrelevant themselves. Except providing privacy of data transmitted via a network, by using a threshold scheme, the load of the capacity of the solution and the complexity of data processing should be taken into account.

IP packet entering the MPLS network is divided into *N* parts or MPLS packets, where each new packet has its own feature. Each created MPLS packet is not just a fragment of the original IP packet but mathematical transformation or code. Thus, the part carries information about the IP packet but by itself does not give any representation about the original packet. Having less than *T* parts, the attacker can't recover the original packet. When an IP packet arrives at an incoming MPLS router, the process of secret sharing is used to generate $N = m$ parts of the message (packets) which will be the payload for MPLS packets. The received *N* MPLS packets are distributed between m maximum disjoint switch paths (LSP, Label Switch Path). Multipath routing algorithm is used to find a set of paths. IP packet is divided into blocks *S1*, *S2*, …, *Sm* of *T* bytes in each. The message parts are calculated using *T* different *xi* values according to the agreement between the sender and the recipient. It is important to note that the coefficients (number of each part) should be included in the transmitted packet.

A choice of the optimal values of *T, N* and the allocation of all *N* parts on selected paths for reaching a maximal security are also very important tasks. It is necessary to consider the safety characteristics of independent paths and choose values in order to minimize the probability of interception of the whole message. The (*N, N*)-sharing and sending parts via N independent paths is the most safe and at the same time the least reliable. In this case *N* is taken equal to the number of independent paths, $T = N$, each part is sent via a separate path. Thus, we will get a maximal security with a minimal metric of data processing. So an attacker has to intercept all *N* parts to recover the original message. However, this handling has one significant disadvantage: in case of the loss of one of the *N* parts, the recipient will not be able to recover the message and will have to request a retransmission.

To increase the probability of delivering parts of the message to the recipient some redundancy is added to scheme by choosing $T < N$. In this case, to restore the message it will be enough *T* parts and the loss of *N-T* parts will not affect the result of the transfer. That is, the smaller the *T*, the higher the probability of delivering the message to the recipient. On the other hand, decrease of *T* increases probability of intercepting the whole message by an attacker. Therefore, the main task is to find such values of *T* and *N* to maintain an enough level of security with the highest possible reliability.

3 The algorithm for finding the maximum number of disjoint paths

Being finding the maximum number of non-overlapping nodes is taken into account the probability *qi* that the node *i* intercepted.

To use the modified algorithm for finding the shortest path in a weighted graph, it is necessary to convert the safety performance of individual nodes in the total safety function between nodes, which is defined as metric communication channel between the nodes:

$$m_{ij} = ln\sqrt{(1-q_i)(1-q_j)} \qquad (1)$$

Then, the metric of the path (*s, d*) is defined as:

$$M(s,d) = \sum_{\substack{i=1 \\ j=i+1}}^{n} (ln\sqrt{(1-q_s)(1-q_j)} + ln\sqrt{(1-q_i)(1-q_j)} + \ldots$$
$$+ ln\sqrt{(1-q_i)(1-q_d)}.$$

Considering that the source and receiver are reliable, that is $q_s = q_t = 0$, obtain:

$$M(s,d) = ln\sqrt{(1-q_1)^2(1-q_2)^2\ldots(1-q_l)^2} =$$
$$= ln((1-q_1)(1-q_2)\cdots(1-q_l)).$$

When searching for a set of paths at first is searching the first safe path using a OSPF protocol. After that, the transformation of the graph are prepared as follows: at first, all communication chosen path replaces directed arcs (arc, which is directed to the source is given its initial value with a "-", and an arc directed to the destination, given an infinite value, so that the arc is actually removed . Thereafter, each node in the selected path is divided into two sub-unit connected by a zero value arc directed towards the source node. Then calculated a new set of estimated safety paths, compared with the safety of a paths set obtained in the preceding iteration. If a new set of paths does not provide better security than the previous one, then your search ends with the stored set of paths, otherwise stored found a set of paths and a transition to the initial transformation of the graph.
The following example shows work of the algorithm. Here, after the detection of the first two non-intersecting paths the third is temporarily used elected nodes, but uses the relationship in the reverse direction. After another deletion and rearrangement, found a set of paths, which is compiled from three paths instead of two.
An example of the algorithm for the graph depicted in Figure 1.

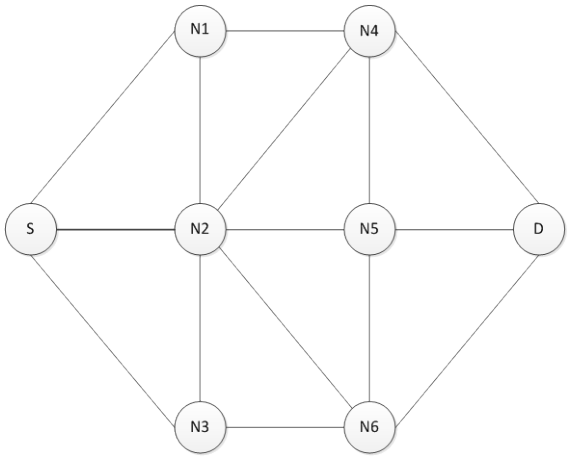

Fig. 1. Graph of network source node S and destination node D

At the first step of the algorithm searches for the path (Figure 2).

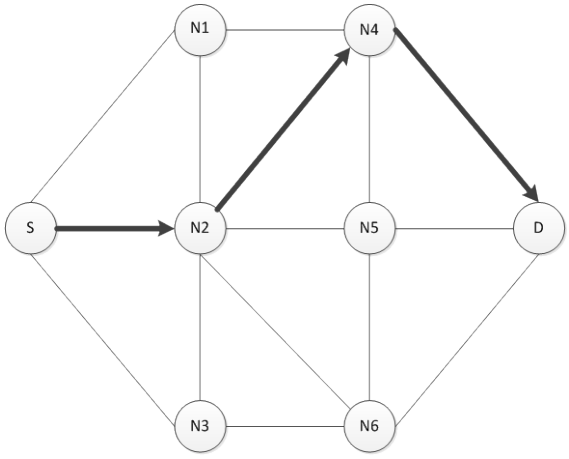

Fig. 2. The first step of the algorithm (searching of the path)

As well is computed the metric of the found path. Assume that the probability of compromise each node is equal to 0.1. In this case, the value found path will be responsible:

$$M(1,2) = ln(1-q_i)(1-q_j) =$$
$$ln(1-0,1)(1-0,1) = 0,092$$

The second step provides to make the transformation of the graph - all connections of the chosen path replace with the directed arcs from the destination to the source (arc directed to the source is given its initial value with "-"), each node is found on the way, except for the source node and the destination node replaces the two sub-assemblies connected by an arc with zero-metric directed to the source, each external communication, combined with these units, replaces the two components of arcs. The result of this step of the algorithm is shown in Figure 3.

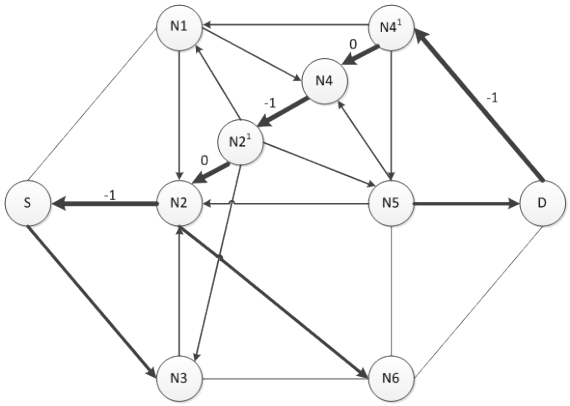

Fig. 3. The transformation of the graph after finding the first path

At the third step performed finding a path at the transformed graph (Figure 4).

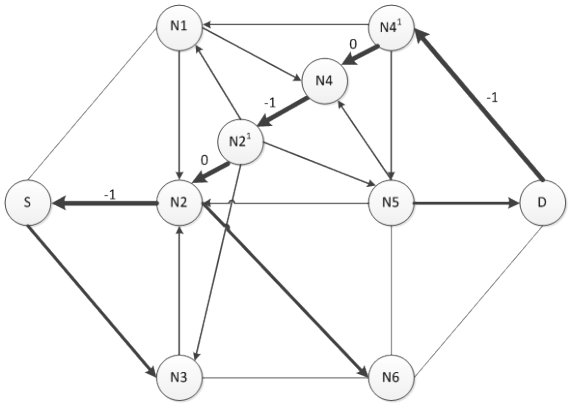

Fig. 4. Searching of the second path at the transformed graph

Calculate the metric of the found path:

$$M(s,t) = ln(1-q_5)(1-q_4) =$$

$$ln(1-0,1)(1-0,1) = 0,092$$

At the fourth step performed the transformation of a graph taking into account found a second pathway (Figure 5).

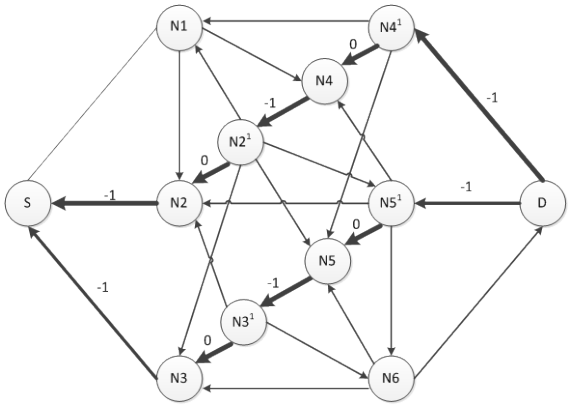

Fig. 5. Transformation of the graph taking into account the second path found

Step 5. Searches the path at the transformed graph (Figure 6).

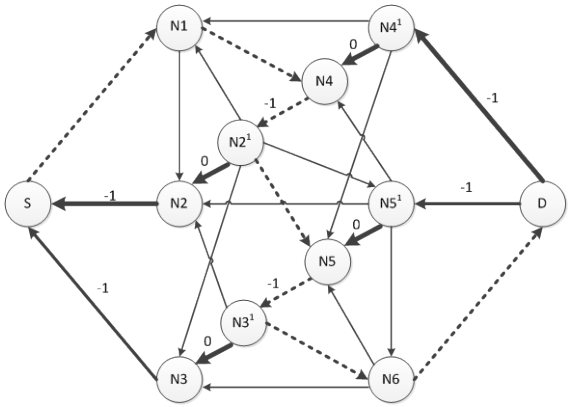

Fig. 6. Searching the second path at the transformed graph

The metric of the found path:

$$M(s,t) = = 0{,}275$$

The third path uses the same components as used in the first and second paths, but connections in the reverse direction is used.

So how else can be found no way of modeling ends with the stored set of paths.

Calculate the total metric of paths found:

$$M(s,t) = = 0{,}459$$

Graph is converted to a primary form found on the box marked path. The edges that connect the 2 nodes and in opposite directions, are removed (Figure 7).

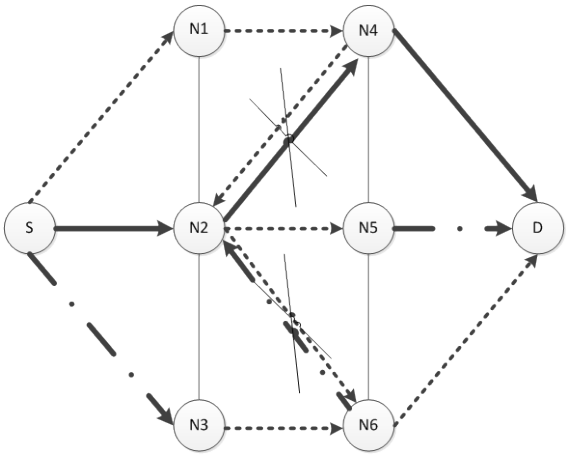

Fig. 7. The transformation of the graph to the primary form

Step 6. Group the edges that stayed to form a new set of non-intersecting paths (Figure 8).

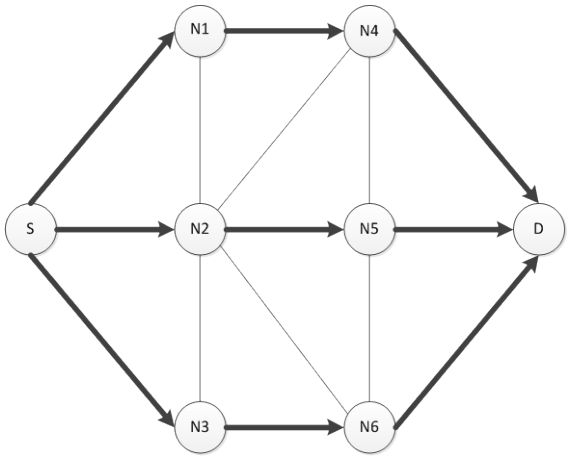

Fig. 8. Formation of a new set of paths

At the last step we calculate the metric of the found a set of paths:

$$M(s,t) == 0{,}276$$

Since the total metric of the new found a set of path < metric of the previous set of paths (0.276 <0.459), then save the new set of paths.

After each iteration, the value *Pmsg*, if this value is less than in the previous iteration, the previous set of acceptable routes, and the algorithm ends.

4 Conclusions

In this work a scheme of sharing with redundancy that allows the loss of some number of packets at the same time providing maximal safety was proposed. In the work it is shown that by choosing the appropriate values of (*T, N*) and the optimal allocation of parts of the message through the different paths it is possible to improve the reliability, that is, to allow the loss of some number of packets, but without neglecting the safety.

Proposed and developed an algorithm for finding an acceptable from the point of view of safety of a set of independent paths for message delivery.

References

[1] As'ad Mahmoud As'ad Alnaser, Y. O. Kulakov: Multipath Routing in Wireless Networks. Contemporary Engineering Sciences,Vol. 5, 2012, no. 6, 251 - 264

[2] Adi Shamir: How to share a secret. Communications of the ACM 22 (11), 1979, pp. 612–613.

[3] As'ad Mahmoud As'ad Alnaser, Y. O. Kulakov : Reliable Multipath Secure Routing In Mobile Computer Networks. Computer Engineering and Intelligent Systems,ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.4, No.2, 2013 , 8-16.

[4] Wenjing Lou, Yuguang Fang: A Multipath Routing Approach For Secure Data Delivery. 0-7803-7225-5/01/ (c) 2001 IEEE.