Reliable Multipath Secure Routing In Mobile Computer Networks

As'ad Mahmoud As'ad Alnaser[1*] Kulakov Y. O.[2]

1. Department of Computer Science, Al-Balqa' Applied University, Ajlun University College
P.O. Box 158, Postal Code 21166, Irbid-Aidun, Jordan

2. Department of Computer Engineering, National Technical University of Ukraine
"Kyiv Polytechnic Institute"

* E-mail of the corresponding author: Asad1_99@yahoo.com

Abstract

This paper analyzes the security and reliability of data transmission over wireless networks. We propose a method for determining the optimal parameter of separation message with specified given security level and reliability of data transmission in mobile networks.

Keywords: Multipath routing, Mobile network, Security

1. Introduction

The important aspects of wireless networks are safe and reliable data transmission. There are several methods to ensure the security of information on different network layers [Priyanka *et al*., 2010], which include ways of multipath routing methods to ensure safety at the physical level by splitting traffic between many different ways [Gopinath S., *et al*., 2012 , Yi J., *et al* ., 2011].

Multipath routing also significantly increase the reliability and fault tolerance for data transmission. This is especially relevant for wireless networks with a dynamic infrastructure. In an article [Jaisankar N., *et al*., 2010] a solution to ensure the data security during transmission of information inside the network without encryption was proposed, the solution is to increase reliability of information transfer. This is achieved by separation message with threshold secret schemes to pieces, which are then transmitted to the independent paths. Feature of the secret schemes is that the message can be restored only providing the pre-determined quantity of parts. Each of the parts separately assumes no useful information. It is allowed loss of some parts, there is a possibility of making redundancies in the scheme. However, the authors do not give calculation method for the optimal values quantity of parts according to the different requirements. The purpose of this work is to examine the influence redundancy on data transmission security, considering probability characteristics of the network, and also search for the optimal parameters of the divided message in terms of safety and reliability.

2.A threshold scheme of separation message

This work proposed a method for the optimal partitioning messages into parts based on the threshold separation of the relatively small message (secret) *K* to *N* unique parts. At the same time to reconstruct the original message is enough to receive *T* parts from *N*. Such a division is called the threshold (*T, N*)-separation, where $T \le N$. In the process of exchanging the secret on the sender side, the algorithm of messages division is executed, on the receiver side – the algorithm of message is recovered.

There are several different threshold schemes of separation message, for example, the work [As'ad & Kulakov Y.O., 2012], proposed a modified scheme that used Lagrange interpolation polynomials. Since the actual message is too large to make it into a polynomial as a separate number, it is divided into segments of *T* bytes each. The separation process on the part is a relatively simple - determining the degree of the polynomial (*T* - *1*):

$$f(x) = (a_0 + a_1 x + a_2 x^2 + ... + a_{T-1} x^{T-1}) \bmod p$$

at the points $x = [1 .. N]$ where $a_0,..,a_{T-1}$ - byte segments of the original message, *p* - prime, exceed *max* $(a_0,..,a_{T-1})$, for example, *p* = 257. Obtained the values of *S(xi)* are passed by independent routes to the recipient. If the received is less than *T* units, restoring the segment will not be possible. After receiving *T* or more parts, the receiver performs recovery segment using the Lagrange interpolation polynomial:

$$f(x) = \sum_i l_i(x) y_i \bmod p,$$

$$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \bmod p.$$

Recovery of all the coefficients a_i is performed by calculating the coefficients of the polynomial $f(x)$ modulo *p*.

3. Distribution of the message parts

The choice of optimal values *T, N* is also an important task .It is necessary to consider the safety performance of independent paths and select values in order to minimize the probability of intercepting the message.

The most secure and, at the same time, the least reliable - distribution (*N, N*). In this case we take the *N*, equal to the number of independent paths, *T* = *N*, each part is sent to a particular path. In this case, the attacker must intercept all *N* pieces to recover the original message. However, this approach has one major drawback: the loss of one of the *N* parts, the recipient will not be able to collect the message and will have to request a retransmission. This problem is particularly relevant for wireless networks with dynamic topology and intermittent connectivity.

In the case when $T < N$, to recover the message there will be enough *T* units and losing of $N - T$ units will not affect the transfer result. Namely, that *T* smaller, the more likely were message deliver. On the other hand, the *T* reducing leads to a higher probability of intercept and recover the entire message by attacker.

Thus, the main task is to find such *T* and *N*, to maintain a sufficient level of security at the highest possible reliability.

We will introduce the notion of redundancy as *r* (*T, N*)-distribution:

$$r = 1 - \frac{T}{N} \tag{1}$$

When *T* = *N* distribution has zero redundancy, that is $r = 0.$ This provides maximum security with minimum reliability. To increase the reliability it is necessary to reduce T.

Figure 1 shows the dependence *r* from *N* for different values of *T*, although, the redundancy itself is not of interest. The objective of this article - to assess the impact of redundancy on the probability of message interception order to be able determine the optimal value of *r* in each case. This requires analysis of the compromise way probability and the probability to intercept messages.

4.Estimation of probability interception of message

Consider the mobile computer network in which the number of non-intersecting paths at the vertices in the network is equal to m. Each of the non-intersecting paths consists of a nodes number. Suppose that the node can be captured with a probability, with the way intercepted if intercepted at least one node on the way. Then, the probability of compromise path will be:

$$p_i = 1 - (1 - q_1) \cdot (1 - q_2) \cdot ... \cdot (1 - q_j) \tag{2}$$

Probability of intercept message P_{msg} depends on the choice values of *T, N*, and the number of independent paths. For the separation of (*N, N*) calculation P_{msg} is quite simple - all *N* parts must be intercepted:

$$P_{msg} = \prod_{i=1}^{m} p_i \tag{3}$$

For the case when $T < N$ it is necessary also to calculate the probability of interception of *k* paths from *m*.

In real systems for $T < N$ the calculation of P_{msg} is a daunting task. Compromised probability q_j of individual nodes is not equal, respectively, the probability of each path interception p_i is also different. For example, a look at the calculation of the probability P_{msg} at *m* = 4, *N* = 4, *T* = 3. Let them p_1, p_2, p_3, p_4 - the probability interception of corresponding paths. Then, to restore the message you need to steal at least 3 of the 4 ways. The probability P_{msg} derived from the formula of total probability:

$$P_{msg} = P_{3,4} + P_{4,4},$$

where:

$$P_{4,4} = \prod_{i=1}^{4} p_i = p_1 p_2 p_3 p_4,$$

$$P_{3,4} = p_1(1-p_2)p_3p_4 + p_1p_2(1-p_3)p_4 + p_1p_2p_3(1-p_4) + (1-p_1)p_2p_3p_4.$$

Since all values are random, in general it can’t be obtained depending P_{msg} on certain parameters, for example, $P_{msg}(r)$ or $P_{msg}(p)$. Therefore, we consider the special case of the average, when probability of being compromised paths p_i are equal. At the same time, for calculating $P_{k,m}$ we can use the formula for the Bernoulli:

$$P_{k,m} = C_m^k p^k (1-p)^{m-k} \tag{4}$$

Then, the formula for the probability of messages interception:

$$P_{msg} = \sum_{i=N}^{T} P_{i,m} \tag{5}$$

Figure 2 shows a probability plot of message interception on the probability of individual paths interception for different number of ways. Thus, for *m* = 1 P_{msg} is linearly dependent on p , and already for *m* = 2 is noticeably significant reduction of probability**.**

5. The influence redundancy on probability of message intercept

Previously, it was determined that increasing the redundancy leads to increase probability of message interception. After determining the formula redundancy *r* (1) and the probability P_{msg} (5) out several researches can be carried.

Consider the dependence $P_{msg}(r)$ in Figure 3 and Figure 4. In the first case *r* was calculated for various separation schemes (*T, N*), *p* = 0,5. In the second case, changing *p* and *N, T* is fixed. The diagrams show that, first, the step of redundancy depends on *N*. The larger *N*, the smaller step. Second, redundancy depends on *p*, since for a given fixed level of security and increasing *p* leads to a restriction *r*.

We introduce the notion as a threshold value of security *y*, which is the limiting value of message interception probability for the desired level of protection $P_{msg} \leq y$.

We introduce the notion as a threshold value of security *y*, which is the limiting value of message interception probability for the desired level of protection $P_{msg} \leq y$.

Figure 5 shows the restriction of redundancy for certain values of y and p, *T* = 5.

Stair stepping graph shows change in the pitch of redundancy depending on *N*. Also with the help of these graphs, a rough estimate of the maximum redundancy with average values of probability interception of separate paths p can be given.

6. Analytical Modeling

In the previous sections particular cases with the average value of *p* were cited. Consider the calculation of allowable redundancy for a given threshold *y* and safety of different random values p_i. The survey was developed by a software environment for the modeling of multipath routing in wireless networks.

As shown in Figure 6 , the model uses a network, The nodes are recorded probability of compromise. The threshold value of $y = 0{,}7$.

A result of modeling was obtained five best independent paths (sorted in order of increasing probability):

1. *p* = 0.657 [*SRC*] -> [1] -> [6] ->[15] -> [27] -> [*DST*]
2. *p* = 0.722 [*SRC*] -> [5] -> [11] -> [12] -> [19] -> [24] -> [*DST*]
3. *p* = 0.807 [*SRC*] -> [3] -> [10] ->[13] -> [17] -> [21] -> [25] ->[*DST*]
4. *p* = 0.814 [*SRC*] -> [4] -> [9] ->[18] -> [22] -> [23] -> [*DST*]
5. *p* = 0.816 [*SRC*] -> [2] -> [8] ->[14] -> [16] -> [20] ->[26] ->[*DST*]

Calculation of redundancy for this model:

1. $T = 5, N = 5, r = 0$: $P_{msg} = 0.254$, $P'_{msg} = 0.259 < y$
2. $T = 4, N = 5, r = 0.2$: $P_{msg} = 0.661$, $P'_{msg} = 0.660 < y$
3. $T = 3, N = 5, r = 0.4$: $P_{msg} = 0.913$, $P'_{msg} = 0.910 > y$

Here P'_{msg} - is the theoretical probability of intercept messages for the average value of *p*. As can be seen, the values $P_{msg} \approx P'_{msg}$ coincide with an error, indicating that the correct programming model and implemented algorithms.

Thus, for this model separation (4, 5) is optimal given the level of security *y* = 0,7. Redundancy in this case is 20%. That is, with the loss of one of the message parts can be recovered. With further increase of redundancy on one step, P_{msg} exceeds the limit y.

5. Conclusion

In this work the effects of redundancy on the security of data transmission were analyzed, as well as search for the optimal value of *r* for a given security level in the system. It was found that for a given level of security, it is possible to find a (*T, N*)-distribution, in which the reliability of the transmission is maximized, and the probability of being compromised will be within the threshold. The introduction of a threshold security protocol to determine the optimal parameters divided message in terms of safety and reliability. In the studies *N* was chosen equal to the number of independent paths. In the future it is necessary to research probability $N > m$, with the largest number of the message parts will be assigned to the path with the least likely to be compromised. The increase of *N* will reduce increment of redundancy, so at equal *y*, in a system with a large *N*, redundancy (reliability) will be higher. Also, with increased *N*, it will be difficult to calculate the values, because there are operations in the calculation of factorial (Bernoulli distribution) and the exponent (separation / collection message).

References

As'ad Mahmoud As'ad Alnaser, Kulakov Y. O.,(2012) “Multipath Routing in Wireless Networks” Contemporary Engineering Sciences, Vol. 5, no. 6, 251 – 264.

Yi J., Adnane A., David S., Parrein B. , Radunovic B., Gkantsidis C., Gunawardena D., and Key P. (January 2011) “ Multipath optimized link state routing for mobile ad hoc networks Ad Hoc Networks”, Volume 9, Issue 1, Pages 28-47

Jaisankar N., Saravanan R. An Extended AODV (August 2010) “Protocol for Multipath Routing in MANETs “IACSIT International Journal of Engineering and Technology, Vol.2, No.4,.

Priyanka Goyal, Sahil Batra, Ajit Singh (November 2010) “A Literature Review of Security Attack in Mobile Ad-hoc Networks” International Journal of Computer Applications (0975 – 8887) Volume 9– No.12

Gopinath S., Maragatharaj S., Rajalingam C., (January 2012) “The Modified Routing Protocol for Defending against Attacks in MANET” International Journal of Advanced Research inComputer Science and Software Engineering Volume 2, Issue 1.

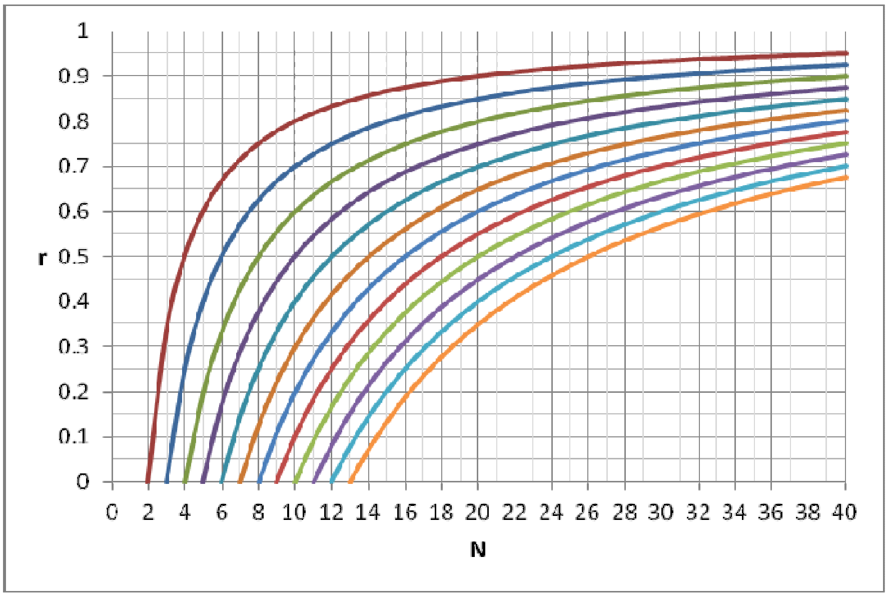


Figure 1. Dependence of redundancy (*r*) from *N* for different *T*

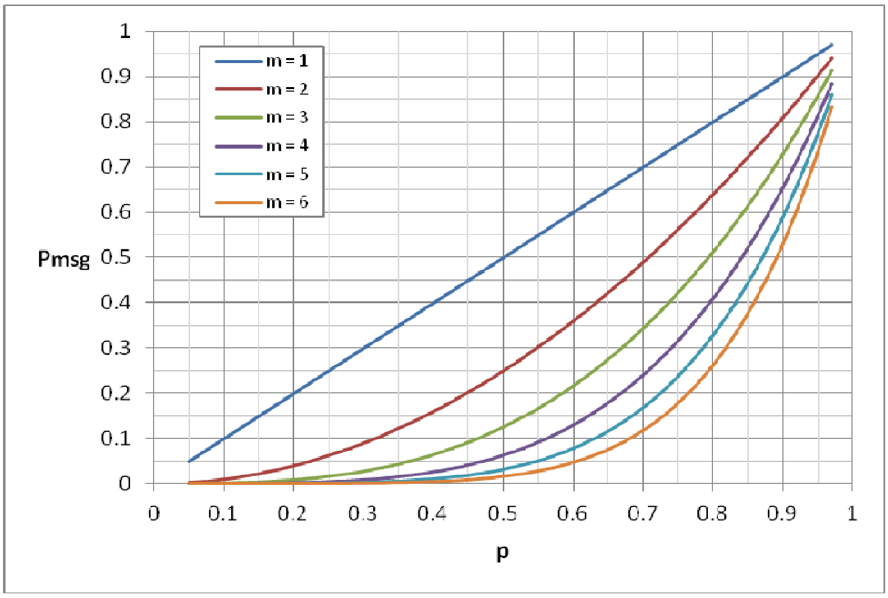


Figure 2. Probability P_{msg} on p for (N, N) – distribution

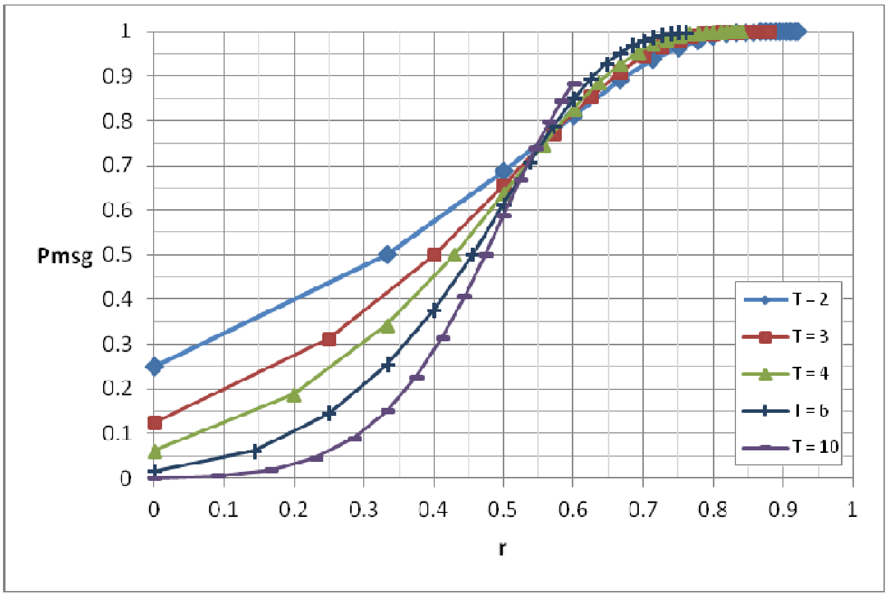


Figure 3. Dependence P_{msg} from r for different T

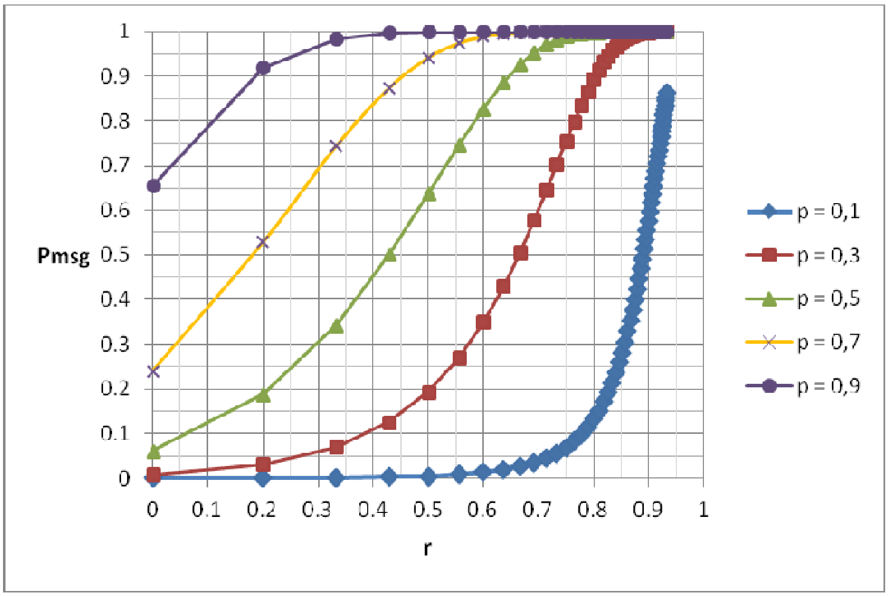


Figure 4. Dependence P_{msg} from *r* for different *p*

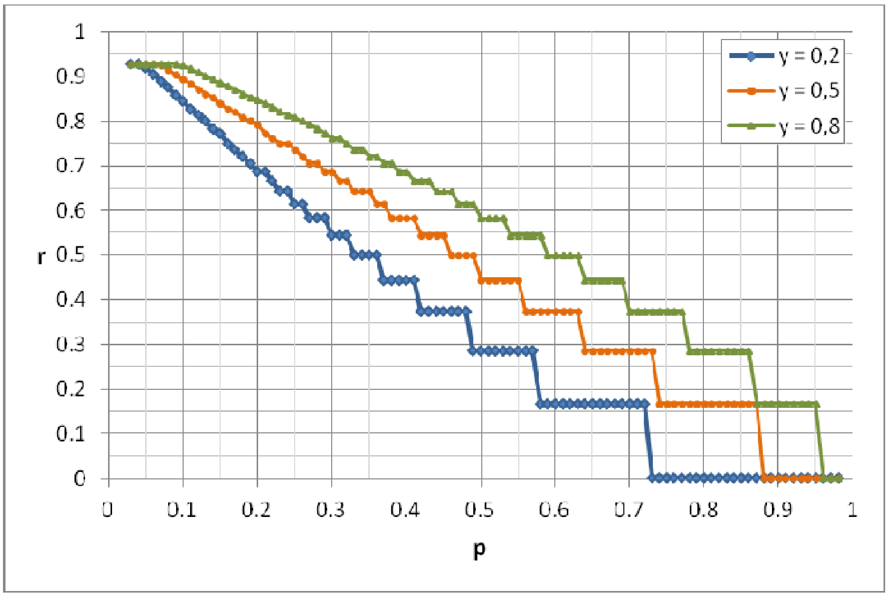
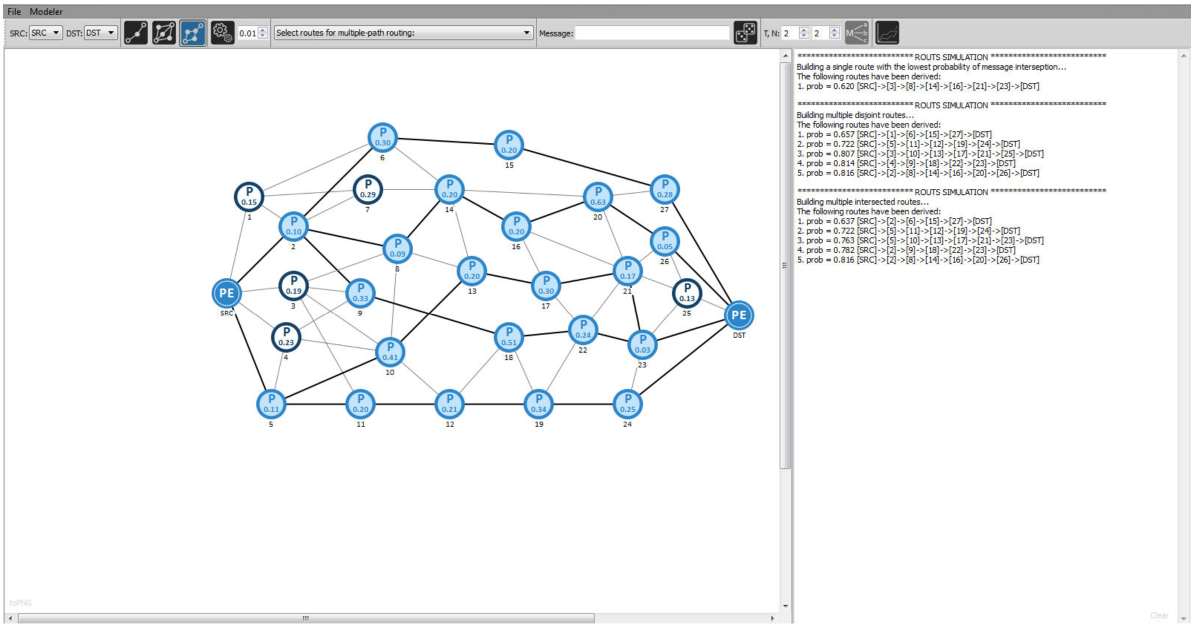


Figure 5. Dependence *r* from *q* for different *y*



SRC: SRC DST: DST 0.01 Select routes for multiple-path routing: Message: T, N: 2 2

```
************************* ROUTS SIMULATION *************************
Building a single route with the lowest probability of message interseption...
The following routes have been derived:
1. prob = 0.620 [SRC]->[3]->[8]->[14]->[16]->[21]->[23]->[DST]

************************* ROUTS SIMULATION *************************
Building multiple disjoint routes...
The following routes have been derived:
1. prob = 0.657 [SRC]->[1]->[6]->[15]->[27]->[DST]
2. prob = 0.722 [SRC]->[5]->[11]->[12]->[19]->[24]->[DST]
3. prob = 0.807 [SRC]->[3]->[10]->[13]->[17]->[21]->[25]->[DST]
4. prob = 0.814 [SRC]->[4]->[9]->[18]->[22]->[23]->[DST]
5. prob = 0.816 [SRC]->[2]->[8]->[14]->[16]->[20]->[26]->[DST]

************************* ROUTS SIMULATION *************************
Building multiple intersected routes...
The following routes have been derived:
1. prob = 0.637 [SRC]->[2]->[6]->[15]->[27]->[DST]
2. prob = 0.722 [SRC]->[5]->[11]->[12]->[19]->[24]->[DST]
3. prob = 0.763 [SRC]->[5]->[10]->[13]->[17]->[21]->[23]->[DST]
4. prob = 0.782 [SRC]->[2]->[9]->[18]->[22]->[23]->[DST]
5. prob = 0.816 [SRC]->[2]->[8]->[14]->[16]->[20]->[26]->[DST]
```

Figure 6. Modeling of ways formation