# Ant Colony Traceback for Low Rate DOS Attack

M. Hamedi-Hamzehkolaie
Kish international campus
Tehran University
Iran

M. J. Shamani
Kish international campus
Tehran University
Iran

M. B. Ghaznavi-Ghoushchi
School of Engineering
Shahed University
Tehran, Iran

## ABSTRACT
Denial of service is one of the most common threats on the public open networks like Internet which taken up by spoofing in the IP address source and leads to exploit the system resources. This results in a decline in the system performance and normal response. In this paper, the traceback to intruder approach by ant colony algorithm will be applied. And the variance of flow will be used to traceback the Denial Of Service or DOS attack source based on ant colony and metaheuristic algorithms. The simulation results show that the proposed approach can trace the attacks even if the attack traffic intensity is relatively low and by initializing the algorithm parameters correctly. Our simulations show that the probability of errors will reach to its lowest rate or even to zero and this is considered as an effective step in tracing attacks by means of metaheuristic algorithms.

## General Terms
Network security

## Keywords
Denial of Service, Ant Colony, Traceback, Metaheuristic algorithms, Network Traffic.

## 1. INTRODUCTION
According to the annual security infrastructure report [1] in 2010 and the report of cryptic assembly [2] in 2012 the frequency of denial of service attacks has been doubled per year of the decade and related to that damage and threats are increasing every day. Low traffic attacks are almost 80 percent of DOS attacks [1], which mitigating are relatively more difficult [3].

On the other hand, counter techniques are categorized into defense and detection [3]. In order to defend against DOS attacks traffic control mechanism such as packet filtering based on route [4], ingress filtering [5] and rate limiting are proposed. However, rate limiting [6] is not suitable for mitigating attacks having low-data-rate on a link, since these attacks will not trigger rate limiting operation [3].

All the above mentioned approaches are passive since they cannot fully resolve the problem. However, proactive approaches [7] will try to find the attack sources under the control of Internet Service Provider (ISP) or the network administrator supervision. Then it will block the traffic from the source and become able to stabilize the network service and will finally end in arresting the intruders.

Current Internet protocol (IP) traceback approaches like: Probabilistic packet marking [8], Hash [9] and Hop by Hop [10], use the information of the routers along the DOS path. However most of previous approaches, in order to, encrypt the routers information on IP headers or storage of the quantity and amount of package volumes on the routers or IP address traceback aims need to provide infrastructures in the network. In addition to that, to succeed in tracing the IP address of the denial service we need the support of all routers.

Among other approaches of finding the IP address of the DOS attack source, which have been discussed, one is the traceback via considering the network current traffic flow information or applying ant algorithm [11]. For example, in [15] a traceback method that is based on entropy variance has been presented.

Nevertheless, few heuristic algorithms are studied in IP traceback. The heuristic algorithms are naturally very strong at finding the optimal result. The nature of these kinds of algorithms is searching food to survive, similar to the nature of IP traceback [11-13]. Some researchers simulated and designed network topology using their favorite approach [14]. Similarly, most approaches considered by researchers are applied for those networks with intensive traffic attack. Also in [12] using the ant colony algorithm has been proposed where the attacker is placed in the middle hop.

Furthermore, analyzing attacks with low rate traffic has been done in "ITACS" [16]. Nonetheless, this approach which has been developed for fixing others drawbacks still shows drawbacks in this kind of traceback. Low rate traffic attack has also been analyzed by the authors of this paper in [17] by applying level of flows.

The proposed method in this paper has three main differences with other methods in this field. The first one is, it can be applicable for low rate dos attack, apart from being applicable for intensive traffic attacks as usual. The second one is, applying flow variance in our traceback method which to the best of our knowledge has never been used so far. The third one is that, the maximum number of converged ants in summation of all algorithm iterations has been considered to find the target node.

The outline of the paper is in the following manner: In section 2, we describe the proposed model. In section 3, the algorithm flowchart has been presented. In section 4, simulation and result have been shown, finally in the last section, we conclude the paper.

## 2. PROPOSAL MODEL
In this model we tried to improve ant colony trace back algorithm [11] in order to trace not only high traffic attacks which are easy to traceback but also low traffic attacks which are important because of their current growth and apart from it are difficult in case of quantity and complexity.

### 2.1 Schematic system of ant colony algorithm
When a large number of ants follow a sequence, it usually attracts more ants. In the proposed IP finding plan, we have used the average number of existing octet belong to denial of service as Pheromone effect. Therefore, the router with more traffic and more flow of denial of service will be selected by

more ants to pass through next node. Eventually majority of ants will converge to one way of passing through [11].

In the primary format ants are placed on the initial router, and initializing for intensity of Pheromone sequence is adjusted on each router. Once an ant starts from a target, topological information is applied to find neighboring routers. Then it begins reading the information of sequence Pheromone remained on the neighboring node in order to calculate the target probability [11].

## 2.2 Applying additional flow variance

In order to be able to trace low traffic attacks, normal flow rate nodes must also be searched. Once there are more normal flow nodes in searching space, the problem gets more complicated. Defining an index for searching the final node is necessary.

According to our study on simulation information, we managed to find tangible relation, so that additional flow variance on the node in attacking path is a great deal more than addition flow variance on the node out of the attacking path. This issue is shown in Figure 1 for the attack shown in Figure 3 in the first iteration.

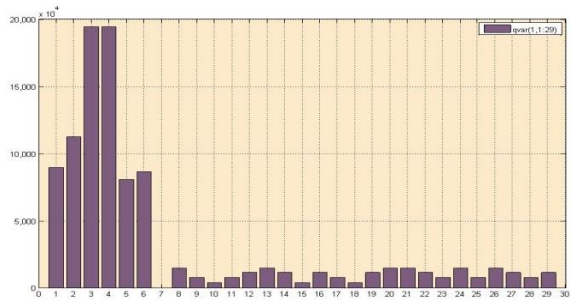

**Fig 1: Flow rate variance entered to router in the first iteration**

Due to downsizing the searching space in the algorithm we define parameter n as the maximum additional output flow from other nodes to the victim node divided to normal flow and a node will be removed from searching space if additional flow variance on it is less than $(\frac{1}{n})^2$ of additional flow variance on the victim flow. Using this characteristic we removed improbable nodes. This results in downsizing searching space and also increasing search speed and accuracy. Indeed searching is still affected by normal flows toward the victim and the attack flow rate. So that if there are more normal flows and less rate of attacks, we will have more complicated search.

## 2.3 Selecting the end node

An important base on metaheuristic algorithm is their randomness. Because of existence of attacks with low rate flow the probability of wrong converging to a relatively strong flow is higher than the attack flow. The existence of a node with the same characteristics next to or behind the end node is sufficient for all ants to converge.

However, the problem is that active nodes in attack due to the additional flow existence are passed by ants in most tracings and their existence probability as the end node is logically more than other nodes. If we take the maximum number of converged ants in summation of all algorithm iterations as the result along with a slight increase in number of algorithm iteration, the error probability will be minimized. In old approaches the maximum number of converged ants to the target in the last iteration was taken as the result. However, we took the maximum number of converged ants in summation of all algorithm iterations as the target node.

## 2.4 Adjusting the parameter of output additional flow limit

In defining additional output limit for a router, it is considered that the determined limit must definitely be less than input flow to victim node. And it's better to have a number between slightly less than the router normal limit and precisely close to additional input flow on victim node. Otherwise, the probability of wrong tracing will rise.

# 3. PROPOSED TRACING ALGORITHM

In Figure 2 the flowchart of proposal algorithm has been drawn. It's worthy mention that permitted nodes are the nodes after the filtration, which has done to reduce the search space

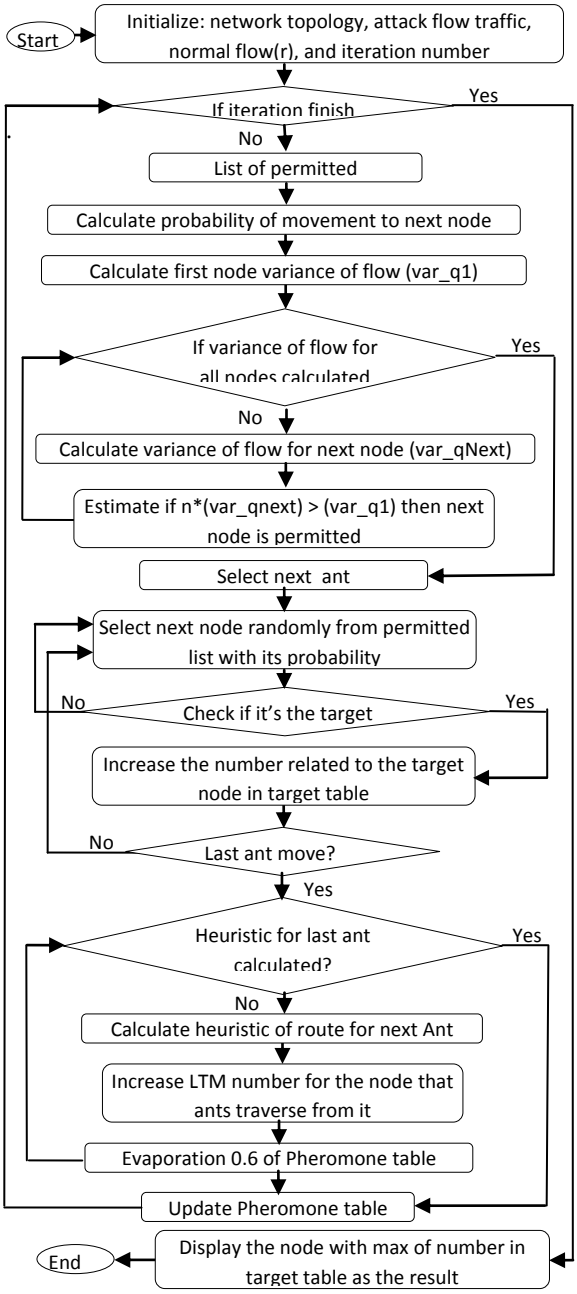


**Fig 2: Low rate attack traceback Ant colony algorithm**

## 4. SIMULATION

In order to evaluate the efficiency of the problem we have selected an attack from a shorter path which can be seen in Figure 3. Node 7 is as the intruder and node 1 is as the victim node. The attack from three different paths has been selected to increase the complexity of the problem. Also the traffic of attack flow for each path is assumed to be 330. In any iteration of outer loop 7 normal flows have been taken into account, which flow with the traffic of 110 with random length and randomly among other nodes. Also in order to increase complexity of the problem, full mesh network topology is assumed.

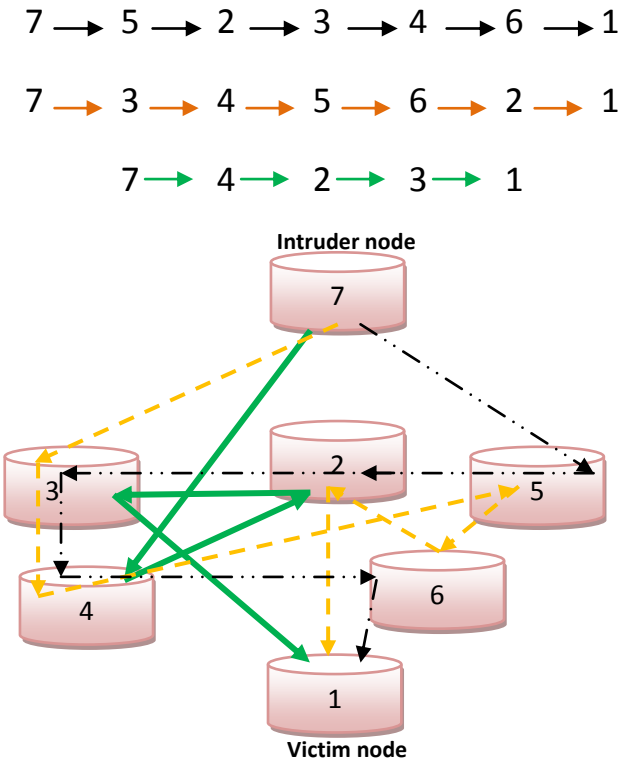


**Fig 3: Three attacking paths from node 7 to node 1**

In the first iteration the probability of movement from victim router is shown in Figure 4. It is clear that movement to 5 nodes including 2-3-6-22-29 is more probable than to the other nodes. According to Figure 3, among these probable nodes only 2, 3 and 6 take part in the attacking path as active nodes and these nodes get more remarkable gradually in next iterations according to more remained Pheromone on nodes of the attacking path. This is shown in Figures 4, 5, 6 and 7.

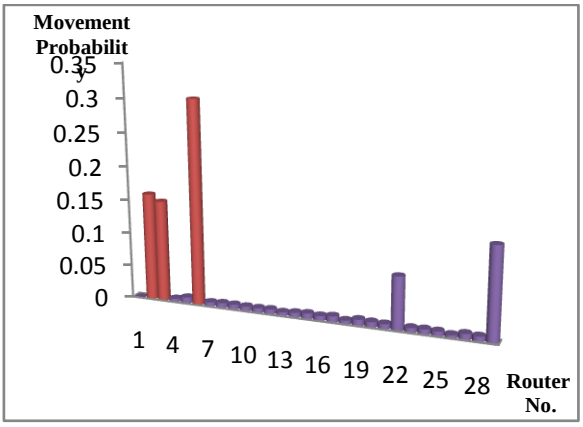


**Fig 4: Movement probability from router 1 to other routers in first iteration**

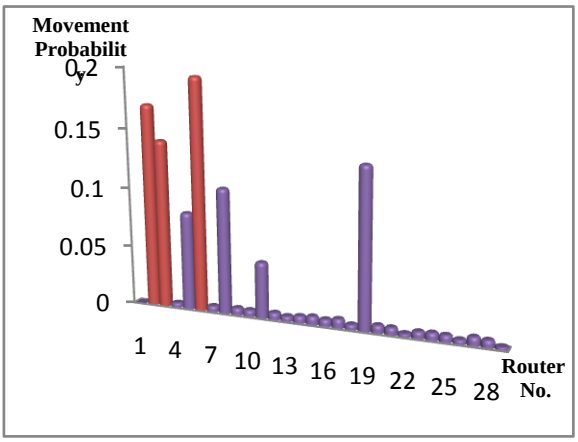


**Fig 5: Movement probability from router 1 in third iteration**

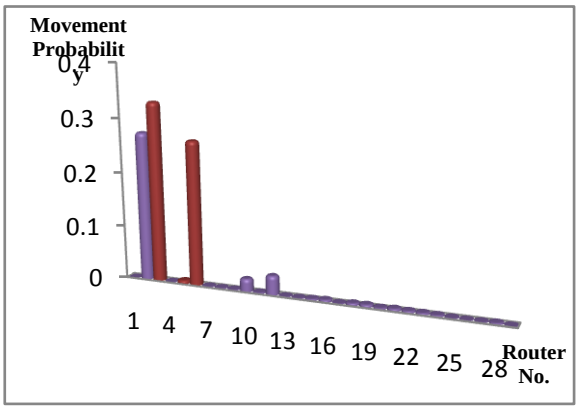


**Fig 6: Movement probability from router 1 in 11th iteration**

According to Figures 4 - 7 it's clear that 2, 3 and 6 nodes, as active nodes on the attacking path to first node, always in all iterations exist as probable nodes and little by little with more consecutive iteration, their existence gets more highlighted. But probable nodes which are not on the real attacking path don't last long. Problem divergence and searching between normal rate nodes make their temporal existence among probable nodes possible.

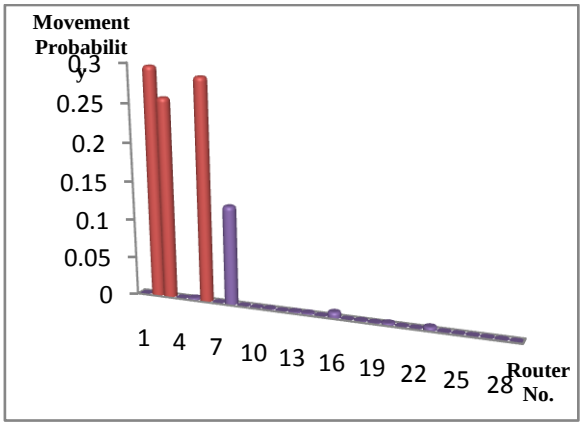


**Fig 7: Movement probability from router 1 in 23rd iteration**

In order to find the end nodes and downsize the searching space in the algorithm, we define n parameter and the condition which is described in section two. Using this characteristic we removed improbable nodes. This leads to smaller searching space and also faster and more accurate search.

Figures 8, 9 are stating this issue. In this example according to input flows, the quantity of $(\frac{1}{n})^2$ is approximately 1/10. (n) Parameter extremely depends on strength of attacks from other nodes to the victim. The bigger the attack is the bigger (n) will be gained.

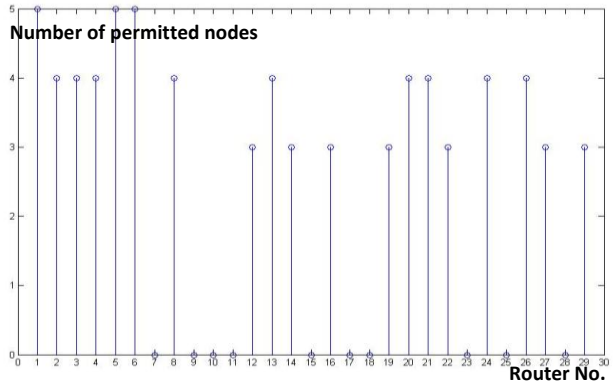


**Fig 8: Number of permitted nodes from each router in first iteration**

As seen in Figure 8 among 29 routers, 19 were selected as permitted nodes and the rest ten routers were removed from searching space. Among these 20 routers and among 8*29=224 paths only 72 paths were selected and the rest were removed from searching space. This way among 28*29=712 probable options we selected only 72 paths. It means that 0.0088 of primary searching space is only searched and the rest is removed from the problem in the first iteration as waste space. According to the obtained results of rate flow summation, it's seen that searching space is approximately doubled and it results in increasing searching time though searching accuracy has risen up.

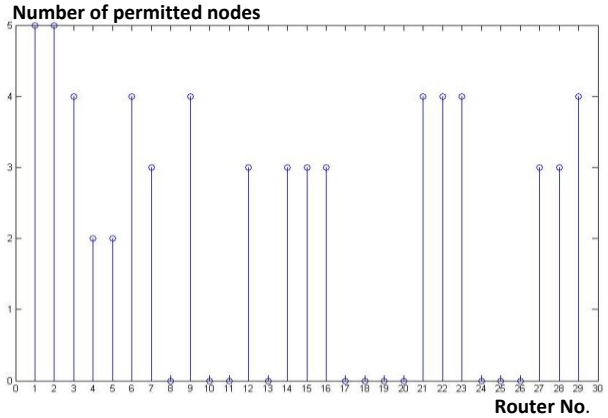


**Fig 9: Number of permitted nodes from each router in 11th iteration**

Also according to algorithm reversed characteristic, by searching space downsizing little by little we reach to the point where there are no permitted nodes for searching. We have already passed the node from which there is no permitted searching path or if exists, by passing it a new loop will be made.

The end node is the one in the end of algorithm introduced as the end node by the biggest number of ants. It's shown in Figure 10 for the first eleven iterations and in Figure 11, for 23 iterations in the end of algorithm.

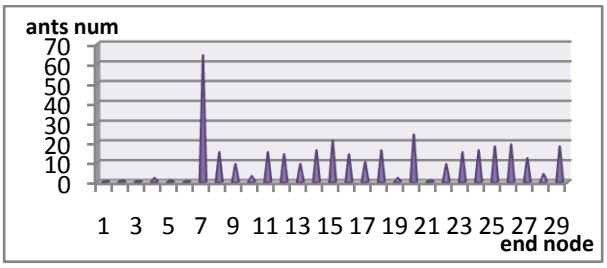


**Fig 10: End nodes in summation of first eleven iterations**

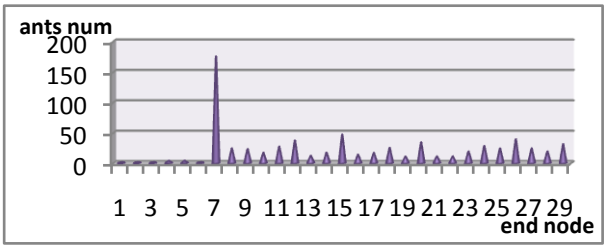


**Fig 11: End nodes in summation of first twenty three iterations**

In Figure 11 node 7 has been correctly selected as end node with summation of 175 ants in 23 runs of algorithms. The node 15 is the probable competitor in the algorithm with the summation of 47 ants. The difference of 128 ants between these two nodes can state the accuracy and the high capability of the algorithm.

## 5. CONCLUSION

Denial of service with low traffic is the devastating kind of denial of service. Detecting and tracing them is relatively more difficult. In this paper the traceback to intruder approach by ant colony algorithm has been applied. And the rates of flow variance have been used to trace back of denial of service source.

The simulation results represent the higher performance of our proposed tracing approach. Therefore, we realized that the proposed solution is finding the main source of effective DOS attack and this can be reached via considering the flow details. Also simulation results show that the proposed approach can trace the attacks even if the attack traffic intensity is really low. The probability of errors will reach to its lowest rate even to zero and this is considered as a big new step in tracing attacks by means of metaheuristic algorithm.

It is necessary to invest more on ant colony algorithm and producing other artificial intelligence approaches for problems related to IP tracing, or we can study highly distributed denial of service attacks. The flow management for complicated networks can be more scalable. In addition practical studies and development in huge networks can be taken up in order to evaluate the scalability of this proposed solution.

## 6. REFERENCES


[1] Anstee, D. 2010. DDoS Attack Trends through 2010. Infrastructure Security Report & ATLAS Initiative.

[2] Shinoda, Y. 2012. Global Information Security Threats Trend. In Proceedings of the Cryptrec Symposium.

[3] K. Lu, D. Wu, J. Fan, S. Todorovic, A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet", Computer Networks, vol. 51, no. 9, pp. 5036-5056, 2007.

[4] Park, K., Lee, H. 2001. On the efectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets. In Proceedings of ACM SIGCOMM.

[5] Ferguson, P., Senie, D. 1998. Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing. RFC 2267.

[6] S. Chen, Q. Song, "Perimeter-based defense against high bandwidth DDoS attacks", IEEE Transaction. Parallel Distribut System. 16 (6) 526–537, 2005.

[7] A. Shahzad, R. Naseem, F. Aadil, Sh. Khayyam, "Trends in defensive techniques against Denial of Service (DoS) Attacks", Canadian Journal on Network and Information Security Vol. 1, No. 1, April 2010.

[8] H. Aljifri, M. Smets, A. Pons, "IP traceback using header Compression", journal of Computers & Security, 22(2), 136–151, 2003.

[9] A. C. Soneren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tachakountio, B. Schwartz, et al, "Single-packet IP traceback", IEEE/ACM Transactions on Networking, 10(6), 721–734, 2002.

[10] T. Baba, S. Matsuda, "Tracing network attacks to their sources", IEEE Internet Computing, 6(3), 20–26.2002.

[11] M. Chen, B. C. Jeng, W. Chao, "Ant-based IP traceback", Expert System Systems with Application journal, vol. 34, pp. 3071-3080, 2008.

[12] Hamedi-Hamzehkolaie, M., Shamani, M.J., Ghaznavi-Ghoushchi, M.B. 2011. DoS-Traceback with Ant Colony Algorithm. In Proceedings of the Iran Electronic War Conference, In Persian.

[13] Dorigo, M., Maniezzo, V., Colorni, A. 1991. Positive feedback as a search strategy. Milan, Italy: Politecnico di Milano, Dipartimento di Elettronica, Tech. Rep. 91-016.

[14] M. Goodrich, "Probabilistic packet marking for large-scale IP traceback," IEEE/ACM Transactions on Networking, vol. 16, pp. 15-24, 2008.

[15] S. Sreenivasulu, S. S. Raja Kumari and V. Chandra Sekhar, "Defense of DDoS Attacks using Traffic Analysis at Router Level", International Journal of Computer Applications, Volume 51– No.10, August 2012.

[16] Chen, H., Yang, W. 2010. The Design and Implementation of a Practical Meta-Heuristic for the Detection and Identification of Denial-of-Service Attack Using Hybrid Approach. In Proceedings of the Second International Conference on Machine Learning and Computing.

[17] Hamedi-Hamzehkolaie, M., Shamani, M.J., Ghaznavi-Ghoushchi, M.B. 2012. Low Rate DOS Traceback Based On Sum of Flows. In Proceedings of the Sixth International Symposium on Telecommunication, IST 2012.