MAT JOURNALS
Journal of Electronics and Communication Systems
Volume 1 Issue 2

Analytical Model for Improved QoS and Security in Wireless Ad Hoc Networks

S. A. Arunmozhi, Y. Venkataramani, S. Rajeswari
Department of Electronics and Communication Engineering,
Saranathan College of Engineering, Panjapur, Trichy, India
E-mail: arunmozhi-ece@saranathan.ac.in, deanrd44@gmail.com,
rajeswaris-ece@saranathan.ac.in

Abstract

QoS and Security are necessary features for wide deployment of wireless ad hoc networks. Existing ad hoc networks provide little support for them. In this paper, we have proposed a mathematical model for improving both QoS and Security. We also present a model that takes into account the number of nodes, the Poisson packet arrival process and service process. Here, wireless ad hoc networks are modeled as M/M/1/Q queuing networks and the expressions for the packet loss rate and packet delivery ratio are evaluated. The mean service time of nodes is evaluated and used to obtain the packet delivery ratio. The analytical results are verified by simulations and numerical computations.

Keywords: *QoS, security, ad hoc network, flooding attack, analytical model*

INTRODUCTION

Security is an essential service for network communications. In a wired network, the transmission medium can be physically secured and access to the network can be easily controlled. The risks to users of wireless technology have increased as the service has become more popular. Traditional security mechanisms are generally not suitable for wireless ad hoc network because of limited bandwidth and limited battery lifetime. Hence new security models or mechanisms that are suitable for wireless ad hoc network must be designed to avoid or mitigate the behavior to the networks.

In a QoS context, security is not sufficiently discussed in ad hoc networks research. Mathematical modeling of quality of service security model of ad hoc networking aims at improving the security

in networks with optimal QoS. Due to the open Medium, eavesdropping is easier in wireless ad hoc networks than in wired networks. Dynamically changing network topology allows any malicious node to join the network without being detected. Absence of any centralized infrastructure prohibits any monitoring node in the system. As described by Dmitri *et al.* providing QoS in a wireless ad hoc network is especially challenging due to the lack of fixed infrastructure, the limitations of the wireless channel, and the limited resources of the nodes [1]. According to RFC2386 given by Crawley *et al.* QoS is a set of service requirements to be met by the network while transporting an information flow [2]. The basic requirement of any QoS mechanism is a measurable performance metric.

Typical QoS metrics include available bandwidth, packet loss rate, average end to end delay and packet jitter [3]. QoS can be achieved by utilizing the network resources such as bandwidth and buffers efficiently by means of rate control and admission control. QoS metrics, such as end-to-end delay, packet loss rate and throughput of communication are influenced by security services. In this paper, we concentrate on packet loss rate which is one of the important QoS factors. In a distributed ad hoc network, a node's available bandwidth is decided by both channel bandwidth and also by its neighbor's bandwidth usage. Thus, bandwidth estimation is a fundamental function that is needed to provide QoS in ad hoc networks. However, bandwidth estimation is extremely difficult, because each node has lack of knowledge of the network status and links change dynamically.

Among various security attacks and threats, wireless ad hoc networks are particularly prone to DoS flooding attack [4]. This attack aims to affect the victim by flooding an enormous amount of traffic to exhaust key resources of the network. DoS flooding attack will easily lead to network congestion. Attackers are able to conduct ad hoc flooding attacks by flooding either RREQ packets or false data packets. There is more research works focused on RREQ flooding attacks than data flooding attacks. RREQ flooding attacks are performed during the path finding phase of routing from the source node to the destination node. The data flooding attack is performed only after finding a path. Therefore, an attacker sets up a path to the victim node so as to conduct data flooding

attacks and then forwards useless data packets to the victim nodes along the path. The size of data packets is much larger than that of RREQ packets. Therefore, resource consumption and bandwidth congestion of a node or the entire network are very much increased by such attacks.

In our previous work, we have proposed a defense scheme against a DDoS data flooding attack using flow monitoring table (FMT) [5]. According to this scheme sending rate of each source node is monitored by every intermediate node in the network. The proposed scheme uses bandwidth estimation and rate control mechanism to assign the sending rate. When a source node violates this assigned rate, that node is identified as the attacking node using Explicit Congestion Notification and the attacking node is blocked from the network. In this paper we develop an analytical model for the defense scheme proposed in and also develop a model to compute packet loss rate and packet delivery ratio [5]. We perform comparison between theoretical value and the simulated results.

RELATED WORKS

Cabrera *et al.* have proposed a methodology of utilizing a Network Management System for the early detection of Distributed Denial of Service (DDoS) Attacks [6]. In their methodology, several key variables have been chosen with statistical analysis to detect the attack in the early stage. This scheme is effective only for local test bed and controlled traffic load. Mahajan *et al.* have proposed the aggregate-based congestion control (ACC) to rate-limit attack traffic [7]. The congested router starts with local rate limit, and then progressively pushes the rate limit to some neighbor routers and further out, forming a dynamic rate-limit tree, which can be expensive to maintain. The Flooding Attack Prevention scheme dealt by Yi *et al*. has addressed the malicious flooding attack and defense system [8]. They have proposed the neighbor suppression mechanism for the RREQ flooding attack and the path cut off mechanism for the data flooding attack. Avoiding Mistaken Transmission Table scheme dealt by Li *et al*. has addressed a defense system against the malicious flooding attack [9]. This scheme requires huge memory space and considerable processing time for saving the packets at each node. Xia *et al*. have dealt a scheme that uses the topology information and the public key cryptosystem to detect colluding malicious nodes [10]. However,

it is very hard to utilize the key management and exchange in ad hoc networks. Guo *et al.* have proposed a quantitative model to characterize the flooding attack and a model to detect flooding attack [11]. They have evaluated the number of routing control packets.

ANALYTICAL MODEL FOR WIRELESS AD HOC NETWORK WITH RATE CONTROL

As given by Chiang *et al.* a network is modeled as a set L of links with finite capacities $L_C = (c_l, l \in L)$ [12]. The link capacity L_C is defined as the maximum achievable transmission rate in absence of competing flows. The links are shared by a set N of sources indexed by s. Each source s uses a set $L(s) \subseteq L$ of links. Let $S(l) = \{s \in N \mid l \in L(s)\}$ be the set of sources using link l. The sets {L(s)} define an LxN routing matrix.

$$R_{ls}=\begin{cases}1; \text{ if source s uses link l}\\ 0; \text{ otherwise}\end{cases} \quad (1)$$

Each source s is associated with its transmission rate $x_s(t)$ at time t, in packets/second. Each link l is associated with a congestion measure, $p_l(t) \geq 0$, at time t. The source node adjusts its transmission rate $x_s(t)$ based on the congestion measure, $p_l(t)$. Each source s is associated with an utility function $U_s(x_s)$ which is a function of its rate x_s, end to end delay D(p). This is a function of congestion measure p and packet loss rate L(p) which is again a function of congestion measure. The optimization problem that we wish to solve then becomes as specified by Amine *et al.* [13].

Maximize $\sum U_s(x_s)$

Subject to $R_x \leq c; x \geq 0$

Minimize D(p)

Subject to $p \geq 0$

And Minimize L(p)

Subject to $p \geq 0$

In each period, the source rates $x_s(t)$ and link prices $p_l(t)$ are updated based on flow information. The source rates $x_s(t)$ are updated according to AIMD rate control. We assume that the sender receives a loss feedback from the receiver which implements explicit congestion notification mechanism at least once every round trip time. At the end of each round, the sender adjusts its congestion window W_i based on the loss feedback as specified eqn. 2 and eqn. 3.

$$W_{i+1}(t+1) = W_i(t)+a; \text{ when } f = 0 \quad (2)$$

$$W_{i+1}(t+1) = W_i(t)(1- b); \text{ when } f > 0; \quad (3)$$

Where W_i is the window size of round i, a is the increase constant, b is the decrease constant, and f is the fractional packet loss. According to Arunmozhi *et al.* proposed scheme, we perform the rate control [5].

The rate adjustment depends on the available bandwidth and the capacity of the link.

$$T_{Assigned\ rate} = C_{link} - B_{available} \quad (4)$$

Where $T_{Assigned\ rate}$ is the assigned transmission rate, $B_{available}$ is the available bandwidth and C_{link} is the link capacity. Capacity of wireless networks is discussed by Gupta *et al.* [14].

Estimation of link capacity depends on the type of MAC layer used in the network. For estimating link capacity of IEEE 802.11 MAC layer, Eqn. 5 is used.

$$C_{link} = B/T \quad (5)$$

where B is number of bits transmitted over the time T.

According to this MAC protocol, the time required for one packet being successfully transmitted over one hop is given by the eqn. 6,

$$T = T_{RTS} + T_{CTS} + T_d + T_{ACK} + 3\ SIFS + DIFS \quad (6)$$

Where T_d corresponds to the transmission time of a data packet, T_{RTS} is the time required to send RTS frame, T_{CTS} is the time required to send CTS frame, T_{ACK} is the time required to send ACK frame.

The available bandwidth is estimated via neighborhood bandwidth consumption. That is, for any node i in a MANET, it shares the wireless medium with all of its neighbors. Thus, the total consumed bandwidth in i's neighborhood, $B_{i,consumed}$, can be written as

$$B_{i,consumed} = \sum_{j \in N(i)} B_j \quad (7)$$

where N(i)={node i and all neighbors of *i*}, and B_j is the bandwidth consumed by all the existing connections of node j, $j \in N(i)$. Taking the total bandwidth as B_t, then the available bandwidth for node i is computed as

$$B_{i,available} = B_t - B_{i,consumed} \quad (8)$$

AN ANALYTICAL MODEL USED TO COMPUTE PACKET LOSS RATE AND PACKET DELIVERY RATIO IN THE PRESENCE OF MALICIOUS USERS

DoS attacks are usually characterized by huge packet volumes that lead to network congestion and to an end system overloading. The proposed rate limiting based scheme provides a solution for DoS attacks as a congestion control problem. For every node x, the packets arrive with rate λ and they are served at a rate μ. N_l and N_a are the number of packets used by legitimate users and malicious users, respectively. A maximum number of both legitimate and malicious packets c can be served at the same time. All packets that arrive when the destination node is in a

saturated state will be rejected. λ_l and μ_l are considered for the arrivals and servings of legitimate packets. λ_a and μ_a are considered for the arrivals and servings of false packets. The packet arrival process is the sum of two Poisson processes with rates λ_l and λ_a and thus also a Poisson process with rate $\lambda = \lambda_l + \lambda_a$. The two arrival processes are independent of each other. DDoS flooding attack may cause the degradation of QoS or render the services unavailable to the legitimate users. Packets are dropped due to the unavailability of the bandwidth and time out condition. We will make the assumption that all incoming packets follow Poisson arrival process with exponential inter arrival times. The Probability Distribution Function (PDF) of the legitimate packet's service time $S_l(t)$ will have the form of an exponential distribution for t smaller than the timeout t_{out}, followed by an appropriately weighted delta Dirac function at t_{out}

$$S_l(t) = \begin{cases} \mu_c e^{-t\mu c}, & t < t_{out} \\ \delta(t - t_{out}) P_o, & t = t_{out} \\ 0, & \text{otherwise} \end{cases} \quad (9)$$

$$\text{Where } P_o = \int_{t_{out}}^{\infty} \mu_c e^{-t\mu c}\, dt = e^{-t_{out}\mu c} \quad (10)$$

The mean service time and the service rate for legitimate packets are

$$t_l = \int_0^{\infty} t S_l(t) dt = \frac{1 - e^{-t_{out}\mu_c}}{\mu_c} \quad (11)$$

$$\text{and } \mu_l = \frac{1}{t_l} = \frac{\mu_c}{1 - e^{-t_{out}\mu_c}} \quad (12)$$

Normally, the attacker might want to follow the legitimate arrivals process in order to prevent certain time analysis detection methods. Concerning the malicious packet service process, the strategy of the attacker is to exhaust the resources using the smallest effort possible. As specified by Boteanu *et al*. we take the malicious packet's service rate as $\mu_a = \frac{1}{t_{out}}$ [15]. The utilization factor is defined as the ratio between the arrival rate and service rate. Let the utilization factor of the legitimate users be $\rho_l = \lambda_l/\mu_l$, and the utilization factor of attacker be $\rho_a = \lambda_a/\mu_a$. The overall utilization is computed by approximating the overall mean service time $\tilde{t}$. We consider $\tilde{t}$ to be constant in time and equal to the average of the mean legitimate service time t_l and mean attacker's service time t_a weighted by the legitimate utilization factor and the attacker's utilization factor respectively.

$$\rho = \tilde{t} = \frac{\rho_l}{\rho_l + \rho_a} \cdot t_l + \frac{\rho_a}{\rho_l + \rho_a} \cdot t_{out} \quad (13)$$

The mean service rate is

$$\tilde{\mu} = \frac{1}{\tilde{t}} = \frac{\mu_l \mu_a (\lambda_a \mu_l + \lambda_l \mu_a)}{\lambda_a \mu_l^2 + \lambda_l \mu_a^2} \quad (14)$$

When the flooding attack is launched, large amount of attack traffic is sent to the network, which will easily lead to network congestion. During the malicious congestion, network nodes have to buffer more and more legitimate packets before

they find the shared wireless channel is free. As more and more attack traffic is sent, node's buffer will easily overflow, which may lead to packet dropping. Hence we may say that flooding attack is the direct consequence of packet loss rate. Queue based analysis of DoS attack has been presented by Aissani *et al*. [16].

Our network is modeled as $M/M/1/Q_l$ queue model similar to that of Pham *et al*. [17]. The maximum number of packets that can be accommodated in the queue at any time is given by $K < \infty$. Those packets that arrive when K packets are already present in the system are discarded. The probability that node x has k packets in its queue $[P_k(x)]$ is computed using Eqn. 15.

$$P_k(x) = \begin{cases} \frac{1-\frac{T(x)}{\eta}}{1-\left(\frac{T(x)}{\eta}\right)^{Q_l+1}}\left(\frac{T(x)}{\eta}\right)^k, & 0 \le k \le Q_l \\ 0, & \text{Otherwise} \end{cases} \quad (15)$$

Here, $T(x)$ is the traffic experienced by a node x and η is the node's packet processing rate. Packets are discarded when the queue is full, i.e., $K=Q_l$. Hence, the probability of packet lost due to the congestion, $P_{loss}(x)$ becomes,

$$P_{loss}(x) = P_{Ql}(x) = \frac{1-\frac{T(x)}{\eta}}{1-\left(\frac{T(x)}{\eta}\right)^{Q_l+1}}\left(\frac{T(x)}{\eta}\right)^{Q_l} \quad (16)$$

Hence, the packet loss rate $L_{loss}(x)$ due to the congestion can be computed using eqn. 17.

$$L_{loss}(x) = T(x) \cdot P_{loss}(x) = T(x).\frac{1-\frac{T(x)}{\eta}}{1-\left(\frac{T(x)}{\eta}\right)^{Q_l+1}}\left(\frac{T(x)}{\eta}\right)^{Q_l} \quad (17)$$

The overall packet loss rate L_{loss} in the network due to N nodes is then given by eqn.18.

$$L_{loss} = \sum_{x=1}^{N} L_{loss}(x) \quad (18)$$

When congestion happens, both normal packets and attack packets are lost. In other words, the overall packet loss rate L_{loss} includes both normal packets loss rate and false packets loss rate. This L_{loss} eqn. is used to estimate the normal packet loss rate as $L_{loss\text{-}normal}$.

$$L_{loss\text{-}normal} = L_{loss} \cdot \frac{\rho'}{\rho} \quad (19)$$

This normal packet loss rate $L_{loss\text{-}normal}$ is used to compute attack packets loss rate $L_{loss\text{-}attacker}$ and the packet delivery ratio PDR. Eqns. 20 & 21 are used to compute both $L_{loss\text{-}attacker}$ and PDR.

$$L_{loss\text{-}attacker} = L_{loss} - L_{loss\text{-}normal} = L_{loss}\left(1 - \frac{\rho'}{\rho}\right) \quad (20)$$

$$\text{and PDR} = \frac{C N\beta - L_{loss\text{-}normal}}{C N\beta} .100 \quad \% \quad (21)$$

Here, C is number of flows in the network and β is the packet's sending rate of each flow.

EVALUATION OF THE MODEL FOR COMPUTING PACKET LOSS RATE AND PACKET DELIVERY RATIO

We have evaluated our network model with theoretical results and simulated

results. The ad hoc network is formed with 20 nodes. Constant Bit Rate traffic is taken for analysis. The size of data packet is 512 bytes. The evaluation is performed in two different scenarios. In the first scenario, five data flows with randomly selected sources and destinations are considered. The node's packet processing rate is taken as 4 packets/s. The queue size is 50 packets/s. The source node transmits data packets at the rate from 1 packet/s to 10 packets/s. The attack rate is 5 packets/s. The PDR is computed using Eqn. 21. In the second scenario, Each source transmits data packets at the rate of 2 packets/s.

The attack rate is varied from 1packet/s to 10 packets/s. All the other parameters are as similar to that of the first case. The PDR for this case is again computed. The computation of PDR is described with an example. The packet's arrival rate is 2 packet/s and No. of flows is 5, the traffic experienced T(x) by a node x is then 10 packets/s. Taking Queue length Q_l as 50 packets/s and node's packet processing rate as 4 packets/s, the probability of packet lost is computed using Eqn. 16.

$$P_{loss}(x) = = \frac{1-\frac{10}{4}}{1-\left(\frac{10}{4}\right)^{51}}\left(\frac{10}{4}\right)^{50} = 0.6$$

Then, the packet loss rate $L_{loss}(x)$ is computed using Eqn. 17 as $L_{loss}(x)$ = 10x0.6 = 6 packets/s. Thus the overall packet loss rate L_{loss} in the network due to 20 nodes is 20x6 = 120 packets/s. Taking utilization factor of legitimate user ρ_l as 2 packets/s and utilization factor of malicious user as 5 packets/s, the normal packet loss rate is computed using Eqn. 19, as $L_{loss\text{-}normal} = 120 \cdot \frac{2}{2+5} = 34.28$ packets/s. Finally, PDR is computed using Eqn. 21 as PDR = $\frac{5x\,20\,x\,2 - 34.28}{5x\,20\,x\,2} .100 = 82.85\%$

The network is simulated with the same parameters using NS2 network simulator. Figures 1 and 2 are used to compare the theoretical and simulated values of PDR.

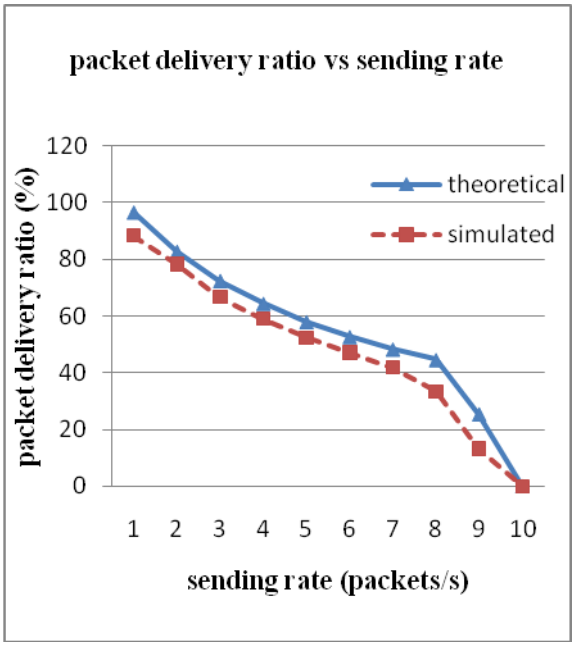

Fig. 1: *Packet Delivery Ratio vs. Sending Rate.*

From Figure 1, it is observed that packet delivery ratio is 96.6% when the source

node transmits data at a rate of 1 packet/s and most packets get to the destination nodes. However, the packet delivery ratio reduces to 0.09% when the source node transmits data at a rate of 10 packets/s. In Figure 2, it is observed that packet delivery ratio is 81.66% when an intruder transmits attack packet at a rate of 1 packet/s. It is also seen that packet delivery ratio decreases as the attack rate is increased. It is finally observed that PDR of simulation is closer to our theoretical results. This validates our theoretical model. However, the simulated values in each case are slightly lower compared to the theoretical values. This is due to the fact that, collision is also taken into account in addition to congestion for simulation.

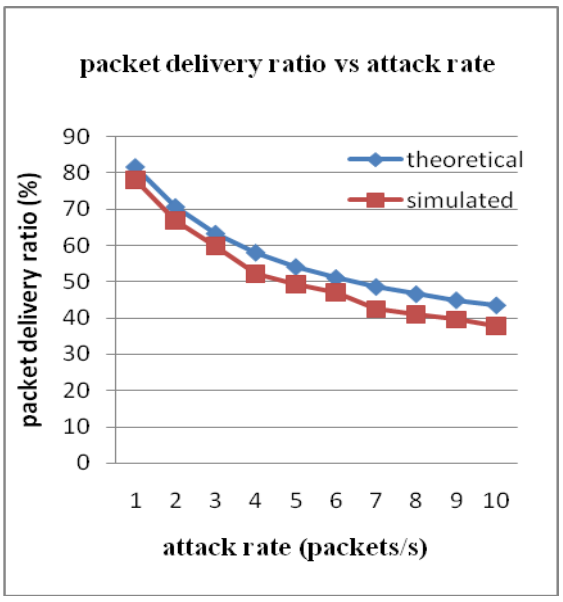

Fig. 2: *Packet Delivery Ratio vs. Attack Rate.*

CONCLUSION

In this paper, we analyze the packet loss rate and packet delivery ratio in wireless ad hoc networks with stationary nodes in wireless ad hoc networks. An analytical model for a wireless ad hoc network is proposed. This provides improved QoS based on rate control. A model which is used to compute packet loss rate and packet delivery ratio with DDoS flooding attack has also been developed. The evaluation of the model is performed with theoretical results and the simulated results. It is observed that packet delivery ratio of simulation results and theoretical results are closer to each other and the simulated values are slightly lower compared to theoretical values due to collision factors considered in simulation. In our future work, we develop the models for our system based on other QoS metrics such as end to end delay and throughput.

REFERENCES

1. Dmitri DP, Herman DH. A survey on quality-of-service support for mobile ad hoc networks. *Wireless Communications and Mobile Computing*. 2002; 2: 503-513p.
2. Crawley E, Nair R, Rajagopalan B, Sandick H. A Framework for QoS

based routing in the internet. *RFC 2386*. 1998.

3. Malik A, Qadir J, Ahmad B, et al. QoS in IEEE 802.11-based wireless networks: A contemporary review. *Journal of Network and Computer Applications*. 2015; 55: 24–46p.
4. Khan S, Traore I. Queue-based analysis of DoS attacks. *In: IEEE Workshop on Information Assurance and Security, United States Military Academy*, West Point, New York; 2005: 266-273p.
5. Arunmozhi SA, Venkataramani Y. Secured system against DDoS attack in mobile Ad-hoc network. *WSEAS Transactions on Communications*. 2012; 11(9): 331-341p.
6. Cabrera JBD, Lewis L, Qin X, Lee W. Proactive detection of distributed denial of service attacks using MIB traffic variables -a feasibility study. *In: IEEE/IFIP International symposium on Integrated Network Management*; 2001: 609-622p.
7. Mahajan P, Bellovin SM, Floyd S, et al. Controlling high bandwidth aggregates in the network. *Computer Communication Review*. 2002; 32(3): 62-73p.
8. Yi P, Dai Z, Zhong Y, Zhang S. Resisting flooding attacks in Ad hoc networks. *In: International Conference on Information Technology, Coding and Computing*; 2005: 657-662p.
9. Li S, Liu Q, Chen H, Tan M. A new method to resist flooding attacks in ad hoc networks. *In: International Conference on Wireless Communications*; 2006: 1-4p.
10. Xia ZY, Wang J. DIMH: A novel model to detect and isolate malicious hosts for mobile ad hoc network. *Elsevier Computer Standards & Interfaces*. 2006; 28: 660-669p.
11. Guo Y, Perreau S. Detect DDoS flooding attacks in mobile ad hoc networks. *International Journal of Security and Networks*. 2010; 5(4): 259-269p.
12. Chiang M, Low SH, Calderbank AR, Doyle JC. Layering as optimization decomposition: A mathematical theory of network architectures. *In: Proc. IEEE*; 2007: 255-312p.
13. Amine K, El Yassini K, El Ouadghiri D. Multicriteria formulation for the quality of service in ad hoc networks. *In: IEEE International Conference on Multimedia Computing and Systems*, Ouarzazate, Morocco; 2009: 395-399p.
14. Gupta P, Kumar PR. The capacity of wireless network. *IEEE Transactions*

on Information Theory. 2000; 46(2): 388-404p.

15. Boteanu D, Fernandez JM, Mchugh J, Mullins J. Queue management as a DoS counter-measure? *In: 10th international conference on Information Security*; 2007: 263-280p.
16. Aissani A. Queueing analysis for networks under DoS attack. *In: International Conference on Computational Science and its Applications*, Part II, Perugia, Italy; 2008: 500–513p.
17. Pham PP, Perreau S. Increasing the network performance using multipath routing mechanism with load balance. *Ad Hoc Networks*. 2004; 2(4): 433-459p.