Periodic Drop Attack in TCP-Mobile Ad-hoc Network

Sunil Kumar
Seeit, Punjab Agricultural University, Ludhiana
India
sunilkapoorldh@gmail.com

Maninder Singh
Department of Computer Science, Punjabi University, Patiala
India
singhmaninder25@yahoo.com

ABSTRACT: *Mobile Ad hoc networks are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure Mobile Ad hoc Network (MANET) is more vulnerable to various attacks since it has no centralized or any pre-existing network structure. At the time of framing of a new security mechanism for MANET various attack variations as well as their characteristics must be known. Jelly Fish periodic drop attack is a new Denial of Service (DoS) attack and passive attack which is difficult to detect as it follows the protocol rules and it works against closed loop flows such as TCP. In jellyfish attack, JF nodes randomly discard some packets over a specified period during communication process over the network. In this paper, periodic drop attack is implemented using AODV and OLSR routing protocols over voice based traffic in MANET. In addition to this, simulation results also illustrate the seriousness of the attacks caused by JF nodes and their effects on data communication.*

Keywords: Jelly Fish, MANET, OLSR, AODV

Received: 18 September 2017, Revised 20 October 2017, Accepted 29 October 2017

1. Introduction to MANET

The wireless ground has been permit exponential growth in the past decade. Mobile Ad-hoc networks are defined as a class of wireless network that handle multi -hop radio replaying and are capable of operating without the foundation of any fixed infrastructure. A MANET is a self-determining setup of mobile nodes. Each node in a MANET is independent to shift independently in any direction of the network and will therefore change its links direction to other devices frequently [1]. MANETs have the process of transmission so that each node has the capability to perform the function of being a host as well as a router. Each packet is forwarded to the nodes which are not in direct communication range following multi hop trend [2-3]. In MANET, Mobile nodes are generating user and application traffic and perform network control and routing protocols. These

infrastructure less mobile nodes in MANET dynamically create routes among themselves to form own wireless network on the fly [4]. Thus, mobile nodes provide an extensible communication method for any place where geographical locations constraints are present [5]. The MANET network is distributed, where all network actions; creating the topology and hand over the messages must be executed by the nodes [6].

2. Routing Protocols

MANET consists of a set of mobile hosts which are connected by wireless links. Network topology in MANET may keep changing randomly due to mobility. Routing protocols that find a way to be followed by data packets from a source node to a destination node used in traditional wired networks that cannot be directly applied in ad hoc wireless networks due to their highly dynamic topology because absence of base station points established infrastructure for centralized administration. An assortment of routing protocols for MANET has been proposed in the recent past.

2.1 Ad hoc On-Demand Distance Vector

Ad hoc On-Demand Distance Vector is a class of reactive routing protocol for MANET; it is refinement to the Destination-Sequenced Distance-Vector (DSDV) routing algorithm [9]. This protocol identifies a route to a destination only when it is required. AODV maintains two managing modes: Route Discovery and Route Maintenance. Illustration of both forms shown in the following Figure 1 and Figure 2.

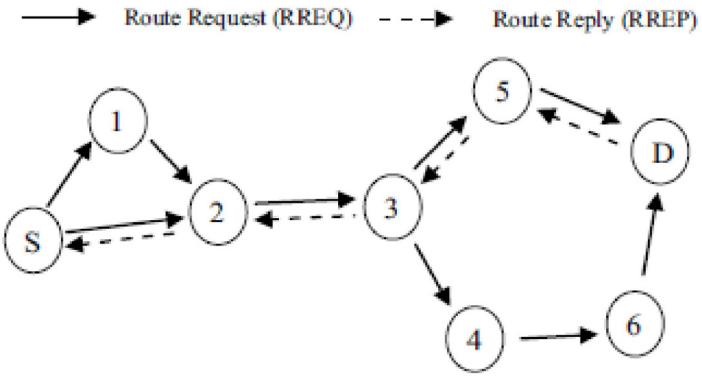

Figure 1. Route discovery process

In AODV, all alive nodes broadcast Hello messages to identified links to any adjoining nodes in the network. These Hello messages are also used to identify link break that occur when the node fails to receive any hello messages from a particular adjoining node. And this is happen only when the source node does not have a valid route to the destination node [9]. If the receiving node is the destination or has a current route to the destination, it generates a RREP. The RREP is unicast in a hop-by-hop fashion to the source.

When the RREQ packet reaches then a central node with a confirmed route to the destination or the destination node. Then, a Route Reply (RREP) packet will be unicaste to the source node.

Once the source node receives the RREP, it starts sending the data packets to the destination.

In route maintenance mode is used to bring feedback about the valid links of the route and to allow the route to be modified in case of any disruption due to movement of one or more nodes along the route.

2.2 Optimized Link State Routing protocol (OLSR)

Optimized Link State Routing protocol is a class of proactive routing protocol designed for large and dense networks [10]. The OLSR protocol is an optimization of the classical Link-State Routing protocol (LSR). At each node it manages topology information during periodic exchange of messages. Fundamental concept of OLSR is the use of multipoint relay (MPR) to provide efficient flooding mechanism by reducing the number of transmissions required. MPR release this information periodically in their control messages [11]. MRP is transmitting the control messages on the concern of other nodes in the network. Each

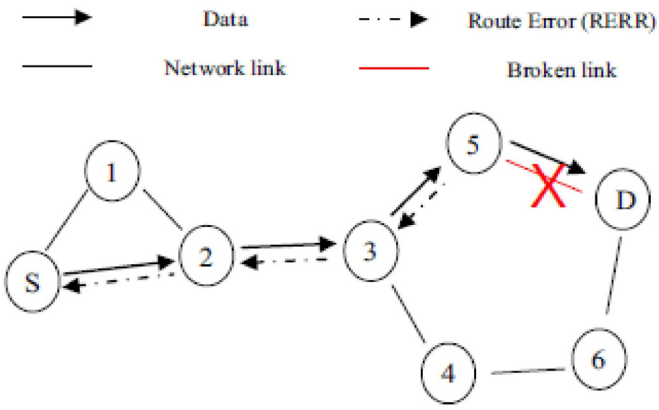

Figure 2. Route maintenance process

node in a network has a list of MPR nodes. Only nodes selected as MPR nodes are responsible for advertising as well as forwarding MPR selector list advertised by other MPRs [12].

In OLSR protocol two types of routing message are used having names, HELLO message and TC message. The working of HELLO message is used for neighbor sensing and MPR selection. In OLSR, each node generates HELLO message periodically in every HELLO interval. A node's HELLO message contains its own address and the list its 1-hop neighbors. A TC message is the message that is used for route calculation. In OLSR, each MPR node display TC message periodically. A TC message contains the list of the sender's MPR selector.

3. MANET Security Attack

In MANET, attacks can be classified into two major categories; passive attacks and active attacks. A passive attack does not disorder the operation of communication over the network. The attacker scout the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to decipher the data collected through snooping [7]. Detection of passive attacks is very challenging since the operation of the network itself does not get affected. An Active attack associate information disruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET [7,8]. Active attacks can be classified further into two categories; external and internal attacks. The dynamic movement of the nodes causes new vulnerabilities that do not exist in a fixed wired network and also the proven security measures used for the wired networks cannot be applicable for MANET [15]. There is no conservation such as fire-walls or access control, thus adding to the vulnerability of MANET to attacks [16].

3.1 Jellyfish Periodic Attack

JellyFish (JF), a kind of denial of service attack which disrupts the whole functionality of TCP. It introduces data drop in the network and reduces throughput and increases delay over the network. TCP is a reliable protocol. It uses acknowledgement (ACK) for each packet. Due to the JF Periodic drop attack, ACK packet which should reach source in time is delayed which makes the source assume that packet is lost. The source retransmits the same packet again. Thus TCP becomes worse to control congestion in the presence of JF attack. Some scenarios have been brought in the functionality of TCP to suit the network under JF attack in this paper.

In jellyfish periodic attack, in which attacking nodes drop all packets for a short time of duration once per retransmission time out. JF node drop for the data only a small fraction of time during transmission [13]. Due to the congestion in the network, a node is forced to drop packets from the network and if the node drops packets from the network periodically then the resulting TCP throughput will reduce to zero [6]. Jellyfish attackers (JF nodes) can severely reduce the good put of all traversing closed-loop flows to near zero by periodically dropping a small fraction of packets.

The JF-node may either choose to banish a piece of packets (e.g., 100 packets from every 1000 packets) or may banish all the packets received during a period of time (e.g., discarding data packets for few milliseconds every second near the TCP sender timeout). This forces TCP to enter the retransmission timeout discard and to increase its RTO value [6].

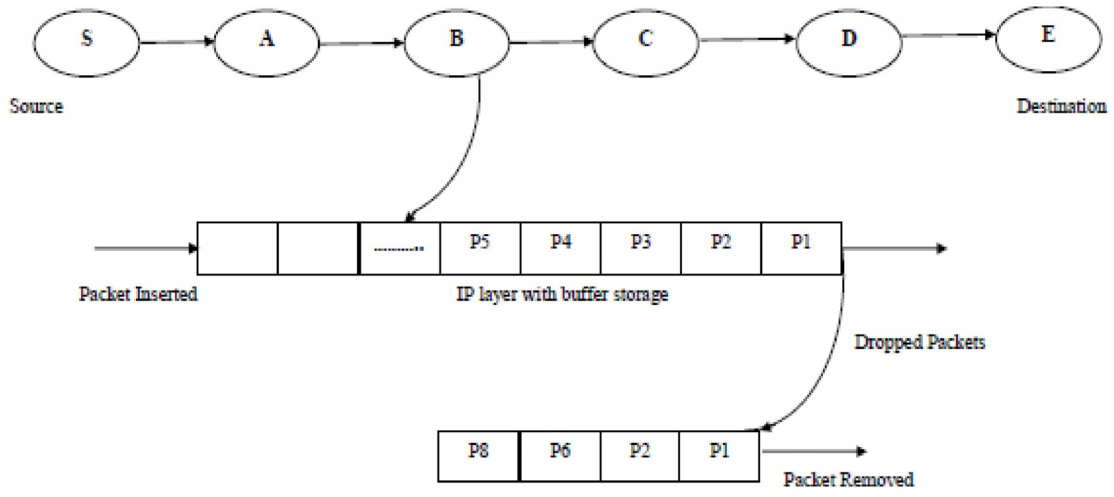

Figure 3. Jellyfish Periodic dropping attack

The sender will ultimately enter in the arena of timeout when JF-node starts remove packets for some duration. This phase leading to decrease in the network throughput and increases the network load. The throughput decreases as the frequency of packets dropped by the attacker node increases. To maximize the impact of the attack, a JF-node will drop packets as soon as the TCP sender exits its slow start phase. Due to this, the flow will always be in a fragile slow-start state. An illustration outline the periodic drop attack is shown in Figure 3.

4. Experimental Setup

In this section, a set of simulation experiments to have been evaluating the performance of routing protocols under JF periodic drop attack. To justify the proposed work, simulations for mobile ad hoc net-work under JF periodic drop attack for two routing protocols i.e. AODV and OLSR has been performed in OPNET [14]. Selection of JF nodes, total number of nodes, mobility speed of the nodes and terrain area as variable parameters have been specified according to the table 1 mention below. Simulate AODV and OLSR routing protocols for different settings and collect the values of performance evaluation metrics in each scenario. In this paper, total four simulation scenarios have been considered depending on the type of data flow (normal or under JF attack), type of routing protocol (AODV or OLSR) and number of MANET nodes (40 nodes). For example, one simulation scenario is MANET with 40 nodes is under JF attack and uses OLSR for routing.

The nodes were randomly placed within certain gap from each other in 12 × 12 km campus environment. Voice traffic with PCM quality was generated in the network explicitly (i.e. user defined) via application configuration node. Fig. 4(a) shows a simulation scenario involving a MANET with 40 mobile nodes and a normal flow (i.e. no JF attacker node) of voice streaming traffic for both AODV and OLSR protocols. Similarly in Fig. 4(b), a simulation scenario has been presented in which out of 40 nodes of MANET, 13 nodes are jelly fish attackers for both AODV and OLSR protocols. Unless explicitly says, all simulation scenarios are configured according to the Table 1.

5. Results and Discussion

In next presents simulation experiments that illustrates the effects of JF on network metrics i.e. throughput, retransmission and network load.

• Retransmission

Retransmissions are necessary for achieving high reliability, given the packet loss rates observed in practical sensor network settings. In figures 5 and 6, a small number of retransmissions is sufficient to achieve high path reliability when used in combination with either blacklisting or a reliability metric. When there are mobile nodes which behave as an attacker node in the network then packets will take time to reach the destination. This affects the performance of the network.

Parameters	Values
Simulator	Opnet Modeler 14.5
Area	11*11 KM
Network Size	40 Nodes
Frame Inter arrival Time	10 Frames /Sec
Frame Size (bytes)	128*120 pixels
Mobility Model	Random waypoint
Traffic Type	Voice Streaming
Simulation Time	10 Minutes
Address Mode	IPv4
Ad Hoc Routing Protocols	AODV and OLSR
Jelly Fish Attacker	Four Scenarios
Packet Size	1024
Frame Interval Time Information	10 frames/sec

Table 1. Experimental design parameters

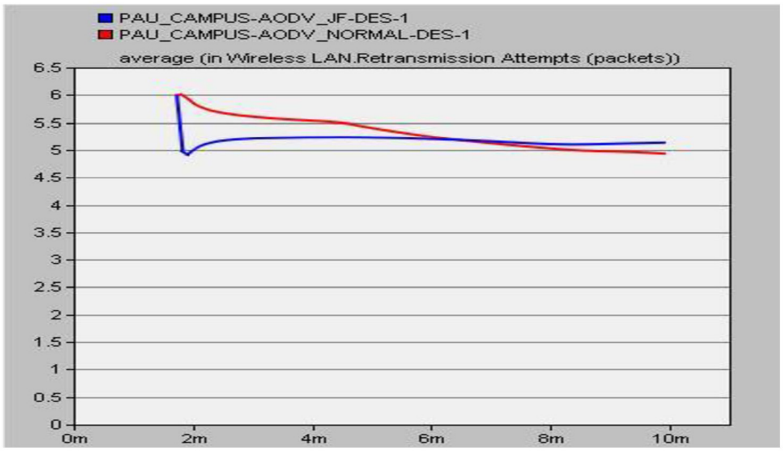

Figure 5. Retransmission of AODV 40 nodes

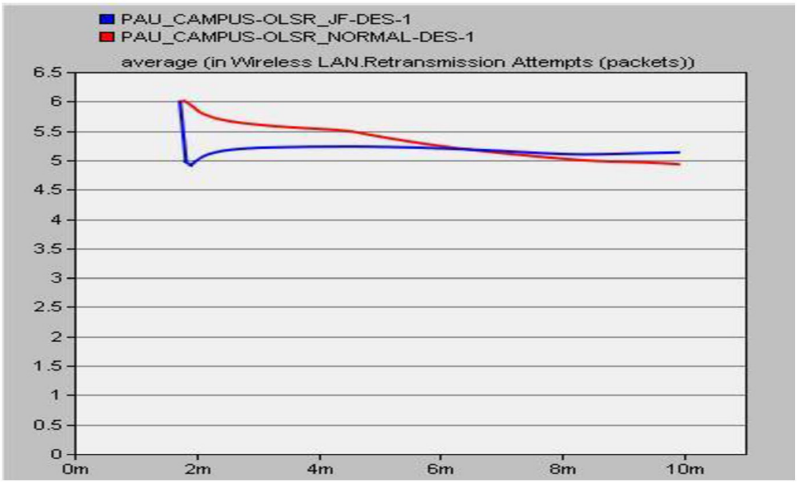

Figure 6. Retransmission of OLSR 40 nodes

	End- to-end Delay (sec)	
	Node Density 40 Nodes	
	AODV	OLSR
Normal Flow	4.9	4.9
JF Attack	5.2	5.2

Table 2. End to end Delay

JF attack increases the retransmission attempts due to packet lost in both cases of AODV and OLSR (Table 2 and Figures. 5–6).

• Throughput

As simulation process, the degradation in throughput to the victim is highly non-linear as a function of the dropping period. According to the result, attack exploiting the slow time scale congestion avoidance procedure of TCP, which flows must infer that multiple packet losses within round trip time are an indication of serve congestion.

Here the malicious node dropped the data rather than forwarding it to the destination, thus effecting throughput. The same is observed in the case of OLSR. A decrease in throughput is an outcome of any JF attack (Table 3 and Figures. 7–8).

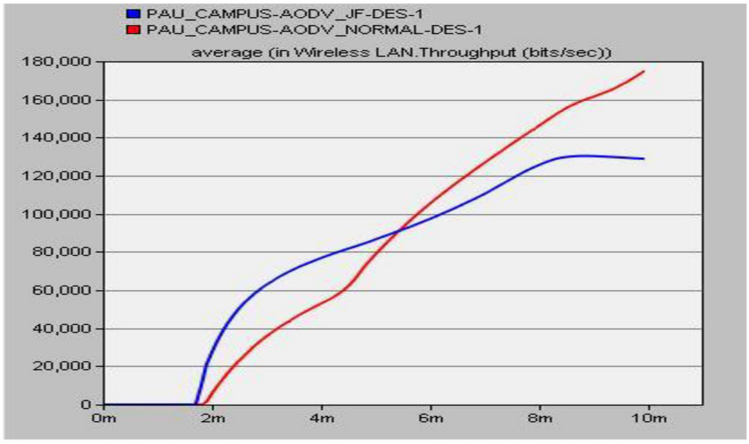

Figure 7. Throughput of AODV 40 nodes

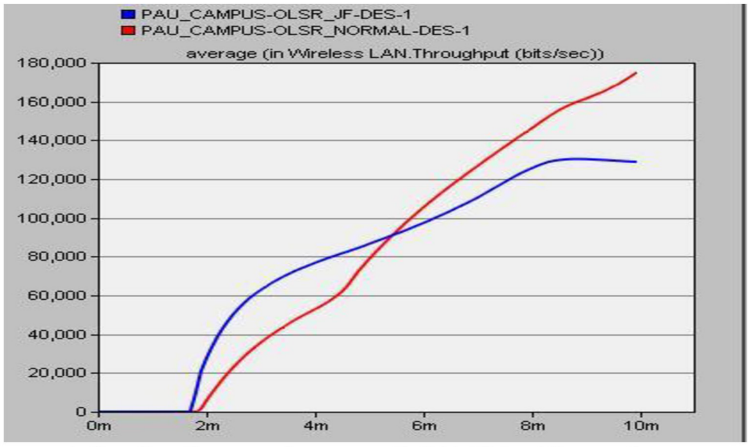

Figure 8. Throughput of OLSR 40 nodes

	Throughput (bits/sec)	
	Node Density 40 Nodes	
	AODV	OLSR
Normal Flow	17,8100	17,8100
JF Attack	13,1400	13,1400

Table 3. Throughput

• Load

The effect of attacker nodes on the network load metrics when varying node mobility during the communication process. It can be observed that flooding attack generated the maximum RRP, which generates the high network load in the network. (Table 4 and Figures. 9–10).

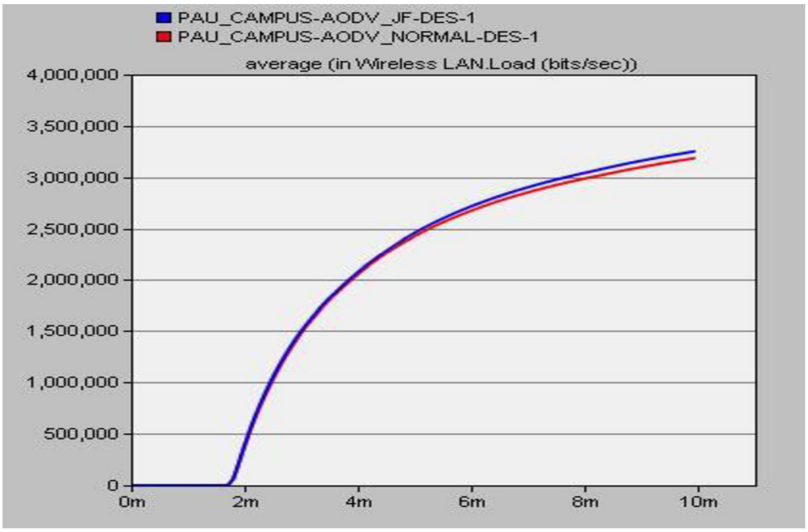

Figure 9. Load of AODV 40 nodes

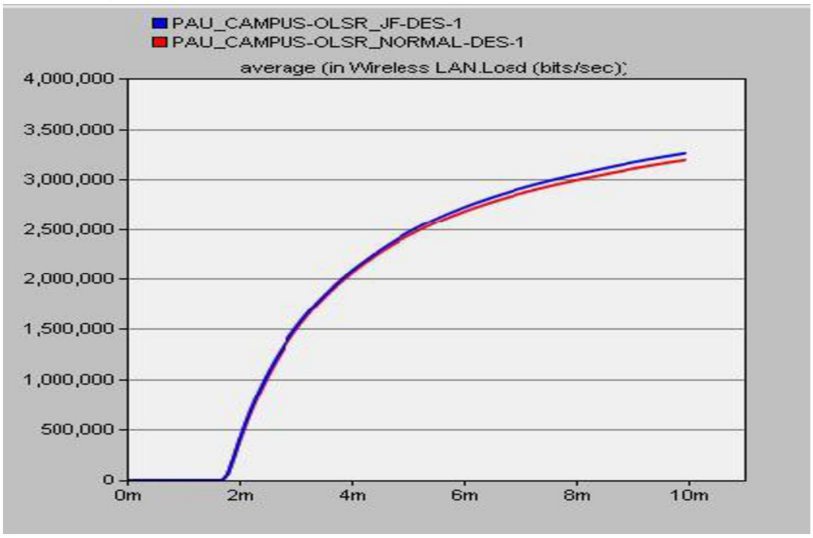

Figure 10. Load of OLSR 40 nodes

	Load (bits/sec)	
	Node Density 40 Nodes	
	AODV	OLSR
Normal Flow	32,95000	32,95000
JF Attack	33,34000	33,34000

Table 4. Load

As per results, maximum load is of AODV. OLSR has the least load in the traffic conditions. This is simply because of the constant mobility of the node; there is a frequent change in the link state and this result in the change in MPR node due to random mobility.

6. Conclusion and Future work

In this paper, a detailed performance evaluation of Jelly Fish attack (JF-drop) over TCP based MANETs is presented. Based on the simulation results generated over various MANET scenarios with varying number of attackers, intermediate hops and attack parameters, it has been observed that Jelly Fish attack causes network performance degradation in terms of network throughput, retransmission and network load.

JF attack is protocol-complaint and has a devastating impact on the throughput of closed-loops flows such as TCP flows. Overall JF periodic drop attack effect the performance of MANET. Finally results goes in the favor of OLSR which has the less effect over the network under the delay variance attack. Jellyfish attack has low trust level and there is no response action taken on the nodes which are attacked by jellyfish attack. Future scope includes efficient detection and prevention method of jellyfish attack with having minimum delay, maximum throughput.

References

[1] Weerasinghe, H., Fu, H. (2007). "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation", *Future Generation Communication and Networking* 2, 362- 367.

[2] Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L. (2004). "Security in mobile ad hoc networks: challenges and solutions.", *Wireless Communications, IEEE*. 2, *p*. 38-47.

[3] Chlamtac, I., Conti, M., Liu, J. I. N. (2003). "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks I, no. I, p. 13-64.

[4] Tamilselvan, L., Sankaranarayanan, V. (2007). "Prevention of Black hole Attack in MANET" , Proceedings of 2nd IEEE *International Conference on Wireless Broadband and Ultra Wideband Communications* (AusWireless 2007), p. 21-21.

[5] Kurosawa, S., Jamalipour, A. (2007). "Detecting blackhole attacks on AODV based mobile adhoc networks by dynamic learning method", *International Journal of Network Security*, 5 (3), 338–346.

[6] Laxmi, V., Mehta, D., Gaur, M. S., Faruki, P., Lal, C. (2013). "Impact analysis of JellyFish attack on TCP-based mobile ad-hoc networks" *In*: *Proceedings of the 6th International Conference on Security of Information and Networks*, SIN '13 p.189-195.

[7] Wu, B., Chen, Wu., Cardei, M. (2007). "A survey of attacks and countermeasures in mobile ad hoc networks *In*: *Wireless Network Security*, Springer US, p. 103-135.

[8] Liu, J., Yu, F., Lung, C., Tang, H. (2009). "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks", *IEEE Transactions on Wireless Communications*, 8(2), 806–815.

[9] Perkins, C., Belding-Royer, E., Das, S. (2003). "Ad-hoc On-Demand Distance Vector (AODV) Routing", Internet experimental RFC 3561, p. 7-24, (July).

[10] Haerri, J., Filali, F., Bonnet, C. (2006). "Performance comparison of AODV and OLSR in VANETs urban environments under realistic mobility patterns", in Med-Hoc-Net 2006, 5th IFIP Mediterranean Ad-Hoc Networking Workshop, June 14-17, 2006, Lipari, Italy, Lipari, ITALY, (June).

[11] Santa, J., Tsukada, M., Ernst, T., Mehani, O., Gómez-Skarmeta, A. F. (2009). "Assessment of VANET multi-hop routing over

an experimental platform", *International Journal of Internet Protocol Technology*, 4(3) (September).

[12] Clausen, T., Jacquet, P. RFC3626: "Optimized Link State Routing Protocol (OLSR)", Experimental, http://www.ietf.org/rfc/rfc3626.txt

[13] Kuzmanovic, A., Knightly, E. (2003). "Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants" *In*: Proceedings of ACM SIGCOMM 2003, Karlsruhe, Germany, August 2003.

[14] Kumar, S., Sengupta, J. (2010). "AODV and OLSR Routing Protocols for Wireless Ad-hoc and Mesh Networks" *In*: *Proceedings of 1st IEEE International Conference on Computer and Communication Technology* (ICCCT), p. 402-407.

[15] Abdelaziz, A. K., Nafaa, M., Salim, G. (2013). "Survey of routing attacks and countermeasures in mobile ad hoc networks" *In*: *Proceedings of* 15*th International Conference on Computer Modeling and Simulation* (UKSim), p. 693-698.

[16] Wazid, M., Kumar, V., Goudar, R. H. (2012). "Comparative Performance Analysis of Routing Protocols in Mobile Ad-Hoc networks under JellyFish Attack", *In*: *Proceedings of 2nd IEEE International Conference on Parallel Distributed and Grid Computing* (PDGC), p. 147-152.