# Analysis of Attacks and Defense Mechanisms for QoS Signaling Protocols in MANETs*

Charikleia Zouridaki[1], Marek Hejmo[1], Brian L. Mark[1], Roshan K. Thomas[2], and Kris Gaj[1]

[1] ECE Dept., MS 1G5, George Mason University, 4400 University Drive, Fairfax, VA 22030, U.S.A.
{czourida, mhejmo, bmark, kgaj}@gmu.edu
[2] McAfee Research, McAfee Inc.,1145 Herndon Parkway, Suite 500, Herndon, VA 20170, U.S.A.
rthomas@mcafee.com

**Abstract.** Supporting quality-of-service (QoS) in a mobile ad hoc network (MANET) is a challenging task, particularly in the presence of malicious users. We present a detailed analysis of attacks directed at disrupting QoS in MANETs. We introduce a new class of attacks targeted at degrading QoS. We consider attacks on both reservation-based and reservation-less QoS signaling protocols and discuss possible countermeasures. Finally, we identify and discuss the key issues in achieving secure QoS provisioning in MANETs.

## 1 Introduction

Most of the literature related to security in MANETs [1],[2] to date has focused on the problems of key management and secure routing. These problems do not address the issue of protecting the network from attacks on QoS and denial-of-service. Cryptographic techniques for ensuring the integrity and authenticity of routing messages can also be applied to QoS signaling messages. However, cryptographic techniques by themselves can only address a subset of the security problems that exist with current QoS signaling.

QoS provisioning introduces new vulnerabilities that are not addressed by secure routing primitives. Attacks on routing are generally directed toward disrupting network connectivity, whereas attacks targeted at QoS signaling need not affect connectivity. For example, a route that is established by means of a secure routing protocol can still be susceptible to attacks on QoS. If an attacker manages to compromise the key needed for network authentication, it can become part of a "secure" route. Such a node may comply with a secure routing protocol, but at the same time attack and exploit the signaling protocol. Attacks on QoS can be carried out even by nodes that are not part of the route. Securing QoS signaling is also challenging because some attacks against signaling may be difficult to distinguish from legitimate network congestion conditions or loss of connectivity. This paper aims to analyze a representative class of attacks targeted at QoS

* This work was supported in part by the U.S. National Science Foundation under Grant CCR-0209049.

signaling in MANETs and identify the key elements required in a secure QoS signaling scheme.

The remainder of the paper is organized as follows. Section 2 discusses the vulnerabilities of current QoS signaling protocols for MANETs. Section 3 provides an in-depth analysis of attacks and defense mechanisms for QoS signaling in MANETs. Finally, the paper is concluded in Section 4.

## 2 Vulnerabilities in QoS Signaling for MANETs

### 2.1 QoS Signaling for MANETs

The INSIGNIA protocol [3] is an example of a reservation-based QoS signaling protocol for MANETs. The SWAN protocol [4], is a reservation-less QoS signaling protocol for MANETs. While INSIGNIA is based on the IntServ model of QoS in the Internet, SWAN is more closely aligned with the Internet DiffServ model. Ad hoc SRRP [5] is another QoS signaling protocol based on the IntServ paradigm. In this paper, we will illustrate the attacks by applying them to INSIGNIA and SWAN, but the attacks have wider applicability to QoS signaling protocols in general.

**INSIGNIA** In the INSIGNIA protocol, control information is piggybacked onto the header of IP packets in order to reserve, renegotiate, and release resources for traffic flows. When a source node wishes to reserve resources in a connection to a destination node, the source sets a reservation (RES) mode bit in the header of an IP packet. The header of a RES packet also indicates the level of QoS ("base QoS" or "enhanced QoS") and the minimum/maximum amount of bandwidth (e.g., 20/30 kbps) requested by the flow. Upon reception of a RES packet, an intermediate node performs admission control, either accepting or denying the request, based on the availability of local resources. The intermediate node modifies (if necessary) the packet header to indicate whether the request is rejected, accepted at the minimum bandwidth, or accepted at the maximum bandwidth and forwards the RES packet to the next node in the route to the destination. If the request is accepted, the flow ID associated with the packet and the amount of bandwidth reserved is recorded in a state table at the intermediate node. When the destination receives the RES packet, it responds by sending a QoS report back to the source node to indicate the amount of resources reserved for the flow, if any. Reservations are made using "soft state," i.e., the reservation times out after a fixed time period, after which resources are automatically released by all of the nodes on the route. In order to maintain the reservation for longer durations, the source must periodically refresh the reservation with new RES packets.

**SWAN** The SWAN protocol probes for available resources along a route between a source and destination node without explicitly reserving resources for a given flow. The source node sends a special control packet called bandwidth probe request $BPR_{eq}$ to the destination node on a previously established route. The source node indicates its bandwidth requirement in a field of the $BPR_{eq}$ packet called the bottleneck bandwidth

(BB) field. Upon receiving a $BPR_{eq}$ packet, an intermediate node on the route compares the value in the BB field with the available bandwidth on its outgoing field and overwrites the BB field if the available bandwidth value is smaller. When the destination node receives the $BPR_{eq}$ packet, it reads the BB field and sends a bandwidth probe reply packet $BPR_{ep}$ containing this value to the source node. After receiving the $BPR_{ep}$ packet, the source decides whether or not to establish a real-time flow given the rate indicated in the BB field of the $BPR_{ep}$ packet. Since resources are not explicitly reserved for each flow, network congestion may occur. Two mechanisms are provided in SWAN to mitigate the onset of congestion: source-based regulation (SR) and network-based regulation (NR) [4].

### 2.2 QoS Vulnerabilities of MANETs

The main vulnerabilities of MANETs with respect to QoS signaling are listed below:

1. **Open network topology.** In a MANET, the address and identity of a node are independent of the node's location. The open topology and overlaps in radio transmission and reception ranges make it easier for attackers to overhear QoS requests and control messages and to actively interfere with such messages. This makes the signaling protocol vulnerable to attacks on confidentiality and availability.
2. **Node mobility.** In a fixed and wired network, the IP address of a host is considered to be its identity and indicative of its location in a network topology. In a MANET setting, it is difficult to trace and verify the legitimacy of QoS requests.
3. **Intermittent connectivity.** Due to intermittent connectivity, control messages may be lost or protocol timing dependencies may be modulated. Such effects are difficult to distinguish from real attacks.
4. **Limited node capabilities.** Typical nodes in a MANET have stringent resource constraints such as limited energy, memory, and CPU cycles.

## 3 Analysis of Attacks on QoS Signaling

In this section, we analyze a representative class of attacks on QoS signaling. We assume that a secure routing protocol is in place, i.e., a "secure" route between the source and destination nodes has been determined prior to the initiation of QoS signaling. Our analysis is given in terms of an attack template consisting of the following three components:

– *Vulnerability:* the network state or property that the attacker exploits.

– *Attack Step:* the method by which the attacker carries out the attack, the position of the attacker in the network, the amount of effort used by the attacker, etc.

– *Effect:* the observable effects and side-effects of the attack.

We also discuss possible countermeasures to each of the attacks.

### 3.1 Attacks on reservation-based QoS signaling

**OVER-RESERVATION** A greedy node can exploit the signaling protocol and reserve more bandwidth for one of its real-time flows than what it actually needs to use. In

an extreme case, the greedy node could reserve bandwidth for non-existing flows in order to perform a DoS attack or to ensure that its own real-time applications could be supported in the near future.

***Attack analysis**: – Vulnerability:* (i) protocol cannot verify usage of reservations; (ii) naive refreshment of reservations (e.g., INSIGNIA).

– *Step:* attacker (i) acts as the source node; (ii) requests more bandwidth than it uses; (iii) sends one data packet in the specified refresh-time interval to keep the reservation refreshed.

– *Effect:* (i) bandwidth under-utilization; (ii) legitimate sessions are denied service.

Note that in the over-reservation attack, a link could be under-utilized even if no additional real-time flows are initiated. Moreover, since the attacker does not need to send many packets to launch this attack, the attack could be carried out over a long time period.

***Issues specific to MANETs:*** The wireless channel provides smaller capacities than wired mediums. As a consequence, the over-reservation attack can create a DoS condition faster in MANETs than in wired networks. Furthermore, the use of straightforward techniques for rate monitoring is often impractical due to the limited computational power of the mobile nodes. A solution that does not overwhelm the node capabilities should be sought.

***Countermeasure:*** As a countermeasure, we propose that data rate monitoring and rate adjustment should be performed by each node. Rate monitoring prevents the traffic flows from under-utilizing their assigned rates. The data rate of an aggregate traffic stream is measured and compared with the assigned rate recorded in the state table. If the measured rate is lower than the assigned rate by a sufficient margin, the assigned rate is decreased by a certain factor. This is the rate adjustment step.

To successfully apply these techniques in MANETs, they have to be scalable and efficient. To avoid rate monitoring on a per-flow basis, each node could maintain state for active aggregate traffic streams traversing the node per in-hop/out-hop pair. We define the "in-hop" node $i$ to be the upstream neighbor node and the "out-hop" node $j$ to be the downstream neighbor node. An in-out stream through a node may consist of many individual traffic flows. Rate monitoring becomes feasible when the traffic flows through a node are aggregated and managed on an in-hop/out-hop basis such that the node is not overwhelmed with too many rate monitoring computations. A protocol that pursues this scheme is described in [6].

**STATE TABLE STARVATION** The state table starvation attack is another attack specific to reservation-based signaling protocols, as such an attack is possible when the protocol requires flow reservations, e.g., in INSIGNIA. It implies the reservation of state for illegitimate flows and this leads to a state table exhaustion when the storage capacity of a node is exceeded.

***Attack analysis:** – Vulnerability:* (i) node has limited memory and computational power; (ii) reservations are made on a per flow basis; (iii) protocol cannot verify usage of reservations.

– *Step:* attacker (i) acts as the source of the data packets; (ii) requests bandwidth for an illegitimate real-time flow.

– *Effect:* (i) state table is exhausted; (ii) legitimate sessions are denied service.

***Issues specific to MANETs:*** Mobile devices are highly constrained in terms of memory and can store only a limited amount of state information.

***Countermeasure:*** An example of a countermeasure would be for each mobile node to maintain a state table that grows as a function of the number of neighbor nodes, rather than the number of traffic flows traversing the node. To avoid the storage of per-flow state, each node could maintain state for each active aggregate traffic stream traversing it on in-hop/out-hop basis, as discussed in the over-reservation attack. Thus, if a node has $N$ neighbors, the maximum number of in-out flows traversing the node is $N(N-1)$.

### 3.2 General attacks on QoS signaling

**OVER/UNDER-REPORTING OF AVAILABLE BANDWIDTH** In this attack, a malicious node on the path from the source to the destination node falsely represents the available bandwidth on an outgoing link. For example, in SWAN, a malicious node on a path could launch this attack by modifying the bottleneck bandwidth (BB) field of the $BPR_{eq}$ message so as to falsely report the available bandwidth on its outgoing link.

***Attack analysis:*** – *Vulnerability:* (i) bandwidth availability is perceived differently by different nodes due to the shared wireless medium; (ii) link capacities are not fixed due to node mobility and wireless channel characteristics; (iii) protocol is unable to validate the available bandwidth reported by an intermediate node.

– *Step:* attacker (i) acts as an intermediate node; (ii) falsely represents the available bandwidth on its outgoing link in the BB field of a $BPR_{eq}$ packet.

– *Effect:* (i) source node sends at a rate that does not match the available bandwidth on the path.

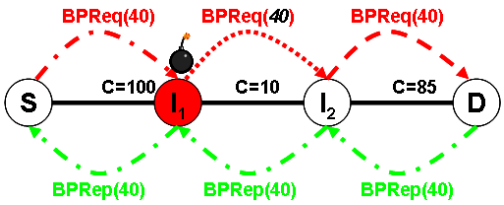


**Fig. 1.** Over-reporting attack

Figure 1 illustrates an example of the over-reporting attack. Here, the source node $S$ requests $40$ kbps for a real-time traffic flow by sending a $BPR_{eq}$ packet with a BB field value of $40$ kbps. Intermediate node $I_1$ performs an over-reporting attack by avoiding the overwriting of the BB field of the $BPR_{eq}$ packet with a value of $10$ kbps, even though the available bandwidth on its outgoing link is only $10$ kbps. Next, the $BPR_{eq}$ message is received by intermediate node $I_2$, which does not overwrite the BB field, since the available bandwidth on its outgoing link is greater than $40$ kbps. The message then reaches the destination node $D$, which creates a $BPR_{ep}$ message with a BB value of $40$ kbps. Upon receiving the $BPR_{ep}$ message, the source node proceeds to send its

data packets with a rate of $40$ kbps, which will cause congestion on the link between $I_1$ and $I_2$, as this can only support a rate of $10$ kbps. The under-reporting attack is similar except the node reports less bandwidth than what is available.

***Issues specific to MANETs:*** Over-reporting/under-reporting attacks are more difficult to detect and isolate in the wireless environment. The link capacities frequently change, due to node mobility and wireless channel characteristics (interference, fading etc). Moreover, several data link layer problems, such as the hidden/exposed terminal problems, exist. As a result, each mobile node perceives the wireless link capacity differently and this can be exploited by malicious nodes to over-report/under-report their available bandwidth. This is in contrast to wired networks, where the links are usually point-to-point and the link capacities are fixed.

***Countermeasure:*** Some MAC protocols for MANETs can reduce or virtually eliminate the effects of the hidden/exposed node problems (cf. [7]). In this case, a node may be able to estimate approximately the available bandwidth at a neighbor node by observing the shared channel. Hence, the over-reporting/under-reporting attacks could be detected by neighbor nodes, assuming they are not colluding as attackers.

Otherwise, the over-reporting attack could also be detected at the application layer. In effect, the destination node could check the percentage of packets that were successfully delivered. Isolating which node committed the over-reporting attack could be done by triggering a search for a new route containing at least one link different from the original path. If an over-reporting attack is detected along the new route, this information could be provided to an IDS. The IDS could then attempt to isolate the attacking node. Such an IDS would have to be "lightweight" enough to be implemented feasibly on MANET devices. A conventional IDS would generally fail to detect this type of attack and would be too computationally expensive to implement in a MANET.

The under-reporting attack cannot generally be detected in direct way. In this case, the default action of the signaling protocol should again be to trigger a search for a new route that has sufficient resources. The main effect of this attack is the extra overhead required in searching for new routes. To mitigate this problem an IDS could log information on the amount of resource that is reported by nodes on different routes and try to detect inconsistencies. The IDS could help to avoid choosing routes (if possible) containing suspect nodes in the future.

**QOS DEGRADATION** QoS degradation represents a new class of attacks in QoS signaling. It involves increase in the delay or jitter of the real-time packets to unacceptable levels.

*Attack analysis: – Vulnerability:* (i) protocol does not verify QoS performance.

– *Step:* attacker (i) acts as an intermediate node; (ii) increases the delay or jitter of the data packets to unacceptable levels.

– *Effect:* (i) QoS for a particular service is degraded; (ii) real-time session needs to be re-initiated.

Increasing the delay or jitter of the real-time packets to unacceptable levels are attacks specific to real-time flows. Conventional DoS mitigation techniques [8] cannot recognize the increase on delay or jitter of the real time packets. Thus, the current

DDoS-aware IDS schemes cannot defend the network against QoS degradation attacks in the Internet or wireless networks.

***Issues specific to MANETs:*** QoS degradation attacks are difficult to distinguish from impairments caused by the mobility of nodes or intermittent connectivity in the MANET. Moreover, monitoring QoS is a particularly difficult task for mobile devices in MANETs due to their limited capabilities.

***Countermeasure:*** A QoS degradation attack could be detected at the application layer by the destination node. As in the suggested countermeasure for the under-reporting/over-reporting attack, detection of QoS degradation should trigger a search for a new route. The presence of QoS degradation on the original route could be reported to an IDS, which could help to avoid problematic routes in the future.

**TIMING ATTACK** The timing attack exploits the sequence in which signaling messages are sent or the timers defined by the protocol, with the objective of disturbing the operation of the protocol. Both reservation-based or reservation-less signaling protocols can be susceptible to this type of attack. However, INSIGNIA in particular, does not have easily exploitable timing dependencies and so is not susceptible to the timing attack.

***Attack analysis:*** – *Vulnerability:* (i) protocol has timing dependencies; (ii) compliance to protocol is not checked.

– *Step:* attacker (i) acts as the source or destination node; (ii) exploits the timing dependencies.

– *Effect:* (i) attacker gains access to the channel at the expense of legitimate flows.

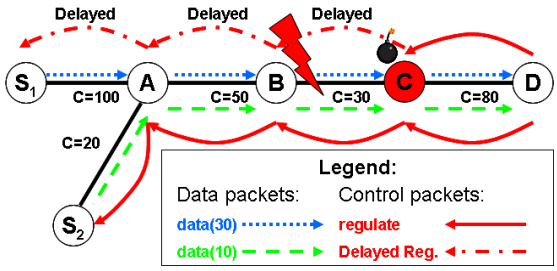


**Fig. 2.** Timing Attack 1.

SWAN implements regulate mechanisms [4] that can be easily exploited. As an example, Figure 2 shows two sources $S_1$ and $S_2$ sending real-time data (at rates of 30 Kbps and 10 Kbps, respectively) to the same destination $D$. The link between the intermediate nodes $B$ and $C$ experiences congestion since it has a capacity of only 30 Kbps. Node $C$ is an attacker node that colludes with $S_1$ so as to give $S_1$ priority over $S_2$. The SWAN protocol requires that the intermediate node $B$ set the ECN (Early Congestion Notification) bit in the IP datagram of all the real-time flows traversing in order to notify the destination $D$ that congestion has occurred. The attack proceeds as

follows. Upon receiving this datagram, node $D$ sends regulate messages to $S_1$ and $S_2$. However, attacker node $C$ is on the path and chooses to delay the regulate message destined for $S_1$. As such, $S_2$ will attempt to re-initiate its session upon reception of the regulate message and when its regulate-timer expires, whereas $S_1$ will continue sending data. Consequently, $S_2$ will be required to probe the channel again to check for the availability of resources, but will receive a $BPR_{ep}$ (Bandwidth Probe Reply) message indicating that the channel is busy, as $S_1$ is still sending data. In summary, by modifying the timing of the regulate messages, the attacker node $C$ allows $S_1$ to preempt $S_2$ and to maintain access to the channel. Clearly this attack can be used as the basis for more sophisticated DoS attacks.

***Issues specific to MANETs:*** The timing attack exploits the sequence in which signaling messages are sent or the timers defined by the protocol. Timing attacks that exploit the sequence in which signaling messages are sent, might not be recognized in MANETs, as the intermittent connectivity and dynamic topology cannot guarantee that a message will arrive at the destination or that it will reach the destination on time.

***Countermeasure:*** The countermeasure here is to implement a QoS signaling scheme that does not present time dependencies and one that does not employ timers to control the protocol's behavior. INSIGNIA, unlike SWAN, is not vulnerable to timing attacks.

**FLOODING** Neither reservation-based nor reservation-less signaling protocols are resistant to flooding DoS attacks.

***Attack analysis:*** – *Vulnerability:* protocol (i) does not verify resource usage; (ii) does not identify the source of flooding; (iii) does not take measures against flooding.

– *Step:* attacker (i) acts as the source node; (ii) floods the network with data traffic.

– *Effect:* (i) network is flooded; (ii) legitimate sessions are denied service..

Flooding the network with data traffic that consumes all of the available bandwidth is a type of a bandwidth depletion attack. However, in INSIGNIA other types of DoS attacks such as over-reservation and state-table starvation attacks can be launched with much less effort.

***Issues specific to MANETs:*** One technique to mitigate flooding is to trace back the attacker and cut off the attack traffic at the source. However, it is much more challenging to trace back an attacker in MANETs than in the wired environment.

***Countermeasure:*** As a countermeasure, the traffic flows should be policed so that they do not exceed their reserved rates. In order to avoid policing on a per individual flow basis, aggregate traffic streams can be policed on an in-hop/out-hop basis as discussed above (cf. over-reservation attack). If an individual flow transmits above its assigned rate, it may experience traffic policing by at least one of the intermediate nodes on the path. Such a distributed traffic policing scheme minimizes the amount of state and processing required in each node of the MANET.

**REPLAY ATTACK** Any protocol that allows the exchange of unauthenticated information is vulnerable to modification and replay.

***Attack analysis:*** – *Vulnerability:* (i) protocol does not protect the integrity of signaling information; (ii) protocol cannot distinguish a replay from an authentic message; (iii) open topology.

– *Step:* attacker (i) duplicates/modifies signaling information; (ii) forwards modified packet to the next hop.

– *Effect:* (i) resources are wasted by illegitimate packets; (ii) legitimate packets are denied service.

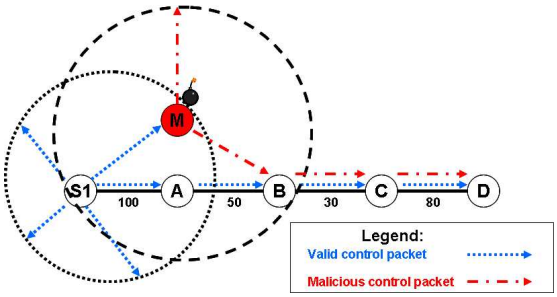


**Fig. 3.** Replay Attack

The replay attack can be performed by a compromised node on the route to the destination by duplicating and modifying the information in a signaling message. In the example shown in Figure 3, the malicious node $M$ receives the control packet sent by the source $S_1$ to the intermediate node $A$. Node $M$ modifies specific fields in the control packet and forwards the packet to the next hop. If the modified packet reaches the destination first, it will be accepted while the original packet that traverses though the route will be disregarded as a duplicate packet.

As an example of a specific replay attack, node $M$ might choose to lower the Bottleneck Bandwidth (BB) field of the control packet to falsely indicate that there is not enough bandwidth for the establishment of the requested real-time session, in order to deny $S_1$ access to the channel. If the routing protocol requires hop-by-hop authentication, node $A$ will authenticate the packet before forwarding it. Since node $M$ does not need to authenticate the packet, it may be able to forward the replayed packet to the destination before node $A$.

***Issues specific to MANETs:*** Since the wireless channel is a broadcast medium, each mobile node hears the transmission of every node in its radio transmission range. In contrast, Internet switches and routers forward packets to destination nodes through designated ports. A node in a wired network can generally only see the packets destined to it.

***Countermeasure:*** As a countermeasure, the number of replayed packets that are processed should be limited over a time interval. If the number of packets with ID $i$, received at the destination within a predefined time interval, is smaller than a threshold value, all the received packets should be processed. Otherwise, only the first received packet should be processed. This limits the number of packets of the same ID that can flood the network.

## 4 Discussion and Conclusion

We have shown that current proposals for QoS signaling in MANETs are highly susceptible to a number of powerful attacks, even when a secure routing protocol is in place. Our investigations suggest that a complete solution to secure QoS signaling solution for MANET should incorporate the following elements: (1) intelligent traffic management, (2) lightweight intrusion detection, and (3) efficient cryptographic primitives.

As discussed, a large class of QoS-based attacks in MANETs can be mitigated via distributed traffic management (cf. [6]). However, some attacks are difficult to mitigate without some means of identifying which nodes have been compromised. Conventional intrusion detection systems are generally impractical for MANETs (cf. [9], [10]), but distributed trust establishment schemes (cf. [11]) could provide sufficient information for nodes to avoid certain types of QoS signaling attacks. While we have not focused on the application of cryptographic primitives to QoS signaling, some form of lightweight scheme is necessary to authenticate the signaling control information.

In ongoing work, we are further developing the DRQoS scheme presented in [6]. We are also investigating computationally lightweight schemes to establish trust measures for MANETs that could be used to make QoS signaling more secure. Our ultimate aim is to design a flexible and secure QoS signaling protocol that can successfully resist attacks which exploit the inherent vulnerabilities of MANETs.

## References

1. Zhou, L., Haas, Z.J.: Securing Ad Hoc Networks. In: IEEE Network Special Issue on Network Security. Vol. 13. (1999) 24–30
2. Hu, Y.C., Perrig, A., Johnson, D.B.: Ariadne: A Secure On Demand Routing Protocol for Ad hoc Networks. In: Proc. ACM MobiCom '02. (2002) 12–23
3. Lee, S.B., Ahn, G., Zhang, X., Campbell, A.T.: INSIGNIA: An IP Based Quality of Service Framework for Mobile Ad Hoc Networks, In: Journal of Parallel and Distributed Computing. Vol. 60. (2000) 374–406
4. Veres, A., Campbell, A.T., Barry, M., Sun, L.H.: Supporting Service Differentiation in Wireless Packet Networks Using Distributed Control (SWAN). In: IEEE Journal on Selected Areas in Communications. Vol. 19, (2001) 2094-2104
5. Yeh, C.H., Mouftah, H.T., Hassanein, H.: Signaling and QoS Guarantees in Mobile Ad hoc Networks. In: Proc. IEEE ICC. (2002) 3284-3290
6. Hejmo, M., Mark, B.L., Zouridaki, C., Thomas, R.K.: Denial-of-Service Resistant Quality-of-Service Signaling Protocol for Mobile Ad hoc Networks. In: Proc. ACM SASN Workshop. (2004) 23-28
7. Haas, Z.J., Deng, J.: Dual Busy Tone Multiple Access (DBTMA): A Multiple Access Control Scheme for Ad Hoc Networks. In: IEEE Trans. on Comm. Vol. 50. (2002) 975–985
8. Mirkovic, J., Reiher, P.: A Taxonomy of DDoS Attacks and Defense Mechanisms. In: ACM SIGCOMM Computer Communications Review. Vol. 34, (2004) 39-54
9. Huang, Y.A., Lee, W.: A Cooperative Intrusion Detection System for Ad hoc Networks. In: Proc. ACM SASN Workshop. (2003) 135–147
10. Tseng C.Y. et al: A Specification-Based Intrusion Detection System for AODV. In: Proc. ACM SASN Workshop (2003) 125-134
11. Eschenauer, L., Gligor, V.D., Baras, J.: On Trust Establishment in Mobile Ad-hoc Networks. In: Proc. Security Protocols Workshop. Vol. 2845 (2002) 47-66