*XXIX Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2011**, Beograd, 06. i 07. decembar 2011.*

INTRUSION DETECTION AGAINST DENIAL OF SERVICE ATTACKS IN MANET ENVIRONMENT

Mirjana Stojanović[1],Valentina Timčenko[2], Slavica Boštjančič Rakas[2]
[1] Faculty of Transport and Traffic Engineering, University of Belgrade
[2] Mihailo Pupin Institute, University of Belgrade

Abstract: *In a Denial of Service (DoS) attack, legitimate users are prevented from access to services or network resources. Distributed DoS (DDoS) occurs if a group of attackers coordinate in DoS. When a DDoS attack occurs in a mobile ad hoc network (MANET), the attacker compromises a number of mobile nodes, which can follow different mobility patterns and have different speeds. This paper provides a survey of possible solutions for intrusion detection system (IDS) against DDoS attacks. IDS is a system that supervises network for malicious activities or policy violations and generates reports based on gathered information. Since DDoS attack traffic may appear similar to legitimate traffic, a detection scheme has a high risk of interpreting legitimate traffic as attack traffic, which is called false positive. Particular attention is focused to IDS that minimizes false positives, with respect to different MANET mobility models.*

Keywords: *Mobile ad hoc network, Denial of service, Intrusion detection system, Mobility model*

1. Introduction

Since mobile ad hoc networks (MANET) are autonomous, self-configuring, infrastructure-less distributed systems, these networks are extremely susceptible to large range of security challenges. The increased instances of security threats and attacks have brought the need of providing different defense measures, which unfortunately cannot eliminate all possible intrusions, but can reduce their success probability.

MANET security attacks can be categorized in multiple ways. According to the legitimate status of a node, an attack could be classified as external or internal. External attacks are carried out by nodes that do not belong to the domain and are not legal members of the network, while internal attacks origin from a malicious member inside the network. Internal attacks are more severe than outside attacks since the insider typically knows valuable and secret information, and possesses privileged access rights. These attackers are aware of the security strategies, and are even protected by them.

In terms of interaction, an attack could be classified as passive or active. Passive attacks do not disrupt the communication. They intercept and capture packets to read the

information that they carry. Examples of passive attacks in MANETs include eavesdropping and traffic analysis. In contrast, active attackers inject packets into the network to interfere or interrupt network communication, overload the network traffic, fake the legitimate node or package, obstruct the operation or disconnect certain nodes from their neighbors so they can not use the network services efficiently any longer. Some of the mostly encountered active attacks in MANET are blackhole, wormhole, Byzantine, denial of service (DoS) attack [1, 2].

In a DoS attack, legitimate users are prevented from access to services or network resources. A more destructive attack form is distributed DoS (DDoS), whose assault is coordinated across multiple attackers. DoS attacks can be issued at any network layer causing physical jamming, disconnection, and errors in routing, transport and application protocols.

According to [3], there are generally four extensive categories of defense against DoS attacks: (1) attack prevention, (2) attack detection, (3) attack source identification, and (4) attack reaction.

Attack prevention aims to stop attack before it can reach the target. For example, it may refer to filtering spoofed packets close to or at the attack sources. In that case, one of the most important tasks is to efficiently specify a filtering rule for differentiating accurately legitimate traffic from spoofed.

Attack detection aims to detect DoS attack when it occurs, which precedes any further action. The efficiency of DoS attack specific detection mechanisms can be evaluated in terms of their assumption strength and technical complexity.

Attack source identification intends to locate the attack sources regardless of whether the source address field in each packet contains erroneous information. The main feature of majority DoS source identification techniques is based on applying traceability, and dealing with the widespread problem of IP address forging by attackers.

Attack reaction tries to eliminate or limit the effects of an attack. It is the final step in defending against attacks, and therefore determines the overall performance of the defense mechanism. The challenge for attack reaction is how to filter the attack traffic without disturbing legitimate traffic.

This paper focuses to DoS attacks and systems for their detection, particularly intrusion detection systems (IDS). IDS is a device or application that supervises network or system for malicious activities or policy violations and generates reports based on gathered information. After a brief overview of possible DoS attacks, a survey of intrusion detection techniques is presented. The impact of mobility patters to DoS attacks and the IDS performance has particularly been addressed.

2. An overview of DoS attacks in MANET

DoS attacks can be launched in two basic forms: software exploit and flooding, as illustrated in Figure 1. In the case of the **software exploits attack**, the attacker node will send few packets to exercise specific software bugs within the target node application, disabling this way the victim. They can usually be addressed by adequate software fixes. Flooding tends to inject a large amount of junk packets into the network. Flooding attacks are further classified to single (DoS) and multisource (DDoS).

DDoS attack is typically performed by means of zombies or reflectors. A **zombie** is a node compromised by a cracker, computer virus or Trojan horse worm, and is intended to be used to perform malicious tasks in network or system that belongs to.

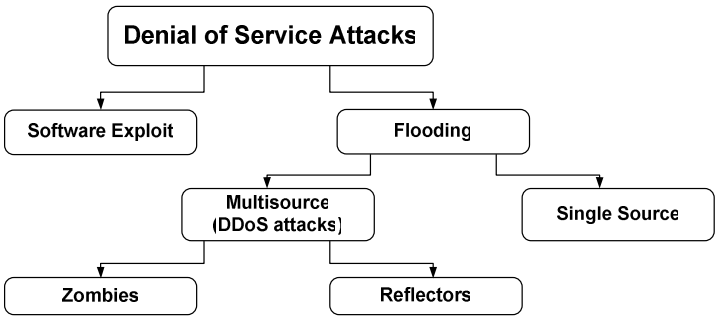

Figure 1. *A basic DoS attacks taxonomy [4].*

Figure 2 describes the process of compromising a number of nodes by means of installing malicious code into them [5]. This process is usually performed by means of an organized worm activity.

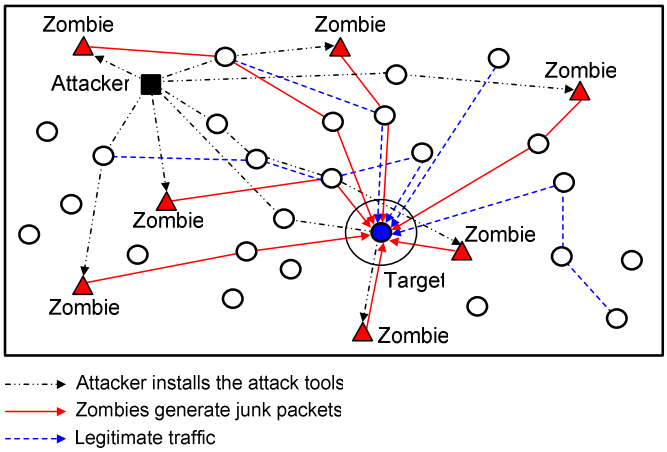

Figure 2. *A model of DDoS attack in MANET [5].*

Reflectors are used to amplify an attack or to hide the identity of the attacker in DDoS attack. A reflector could be any node that takes the role of responding to some requests, e.g. a server that responds to TCP (*Transmission Control Protocol*, TCP) SYN request with a SYN-ACK reply. Reflector nodes can also be used as amplifiers by sending packets to the broadcast address of the reflector network, asking for a response from every node in MANET. Unlike zombies that represent improperly secured nodes, reflectors are usually legitimate nodes that have a task to provide some service.

DDoS attacks can occur in several subforms, as routing table overflow, packet-forwarding attack, SYN flooding, and application-based attacks.

In the case of the **routing table overflow attack**, the attacker is aware of the circumstance that each node in network keeps the needed routing information to further properly route the traffic. This creates the possibility to use this property as disadvantage, since an attacker can easily create and set into the tables the routes to nonexistent nodes [6, 7]. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. As a result, severe network congestion can be produced by the appearance of voluminous routing loops.

Packet forwarding attack is another widely employed attack. Its activity is performed via network-layer packet blasting. It represents a failure to correctly forward data packets in accordance with a data transfer protocol. This attack can cause serious MANET congestions by injecting a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention [8].

The fact is that MANET has a higher channel error rate when compared with wired networks. When considering security at transport layer, there are several problems to take into concern. As TCP does not have any mechanism to distinguish whether a loss was caused by congestion, random error, or malicious attacks, TCP multiplicatively decreases its congestion window upon experiencing losses, which degrades network performance significantly. Though, the mobile node is extremely vulnerable to the classic SYN flooding attack or session hijacking attacks.

In a **SYN flooding attack**, the attacker creates a large number of half-opened TCP connections with a target node, but never completes the handshake to fully open the connection. During the SYN flooding attack, an attacker node sends a large amount of SYN packets to a victim node, spoofing this way the return addresses of the SYN packets [3, 6].

Session hijacking attack takes an advantage of the fact that most communications are protected at session setup phase. In the case of the TCP session hijacking attack, the attacker node spoofs the target's IP address, resolves the expected sequence number, and then performs a DoS attack on the target node. Thus the attacker impersonates the victim node and continues the session with the target.

At the application layer there is a problem of distinguishing the phenomenon "flash crowd" from the **bandwidth attack**. The term "flash crowd" refers to the situation when a very large number of nodes simultaneously accesses a destination node (it is usually some server), which produces a surge in traffic to the server and might cause its virtual unreachability. Bandwidth attacks can occur for multiple of reasons. They can be a product of traffic generation with volumes that exceed the available throughput of network links, or it could be based on simultaneous malicious activity of geographically distributed zombies. Because burst traffic and high volume are the common characteristics of application DDoS attacks and flash crowds, it is not an easy task for current techniques to distinguish them merely by statistical characteristics of traffic. Therefore, application DDoS attacks may be stealthier and more dangerous for the victim node than the general DDoS attacks when they mimic the normal flash crowd. Table 1 shows the brief comparison of a bandwidth attack and flash crowd characteristics.

Table 1. *Comparison between a bandwidth attack and flash crowd [3]*

Comparison aspect	Bandwidth attack	Flash crowd
Network impact	Congested	Congested
Server impact	Overloaded	Overloaded
Traffic	Malicious	Genuine
Response to traffic control	Unresponsive	Responsive
Traffic type	Any	Mostly Web
Number of flows	Any	Large number of flows
Predictability	Unpredictable	Mostly predictable

3. Intrusion detection techniques against DDoS attacks

An intrusion represents a set of actions that compromises confidentiality, availability, and integrity of a system. The IDS mission is to provide a specific security technology against certain threat by identifying potential intruders and proceed with adequate procedure of blocking, denouncing and excluding them from the network.

IDS performance is mainly evaluated through the following two metrics: detection scheme coverage and false positives. **Coverage** represents a proportion of actual attacks that can be detected. Actually, it is a measure of IDS detection effectiveness. In the case of DoS attacks this is relatively easy to measure, as this type of attacks expose themselves with obvious degradation of target's services (e.g. high packet drop rate), though they can be easily detected. **False positive** is each event in the network that is, by mistake, reported as malicious**.** Usually, this metric is represented as value obtained by normalizing number of reported false positives versus the number of reported attacks. According to this, the perfect IDS will have the *coverage* of 100% and 0% *false positives*. In addition to these two metrics, the **intrusion detection time** should be as short as possible.

A detailed survey of all known DDoS defense mechanisms is presented in [3]. This study claims that defending against these attacks is challenging for mainly two reasons. First reason would be the number of involved zombie nodes in a DDoS attack which can be large. The volume of traffic sent by a single zombie might be small, but the volume of aggregated traffic arriving at the victim node is overwhelming. Another reason is that zombies usually spoof their IP addresses under the control of attacker, which makes it very difficult to trace the attack traffic back even to zombies. The problem of DDoS attacks is mostly based on the MANET infrastructure vulnerabilities and the volume of quasi-legitimate attack traffic generated towards the destination points which are crucial obstacles for defense system to overcome the perceptibility to these attacks.

A comparison between different DoS attack detection techniques is presented in Table 2. MULTOPS is a technique that lays on the assumption that a significant, disproportional difference between the packet rate going to and from a source or subnet is a strong indication of DoS.

Table 2. *Basic assumptions for different attack detection techniques [3]*

Detection technique	Basic assumption	Assumption strength	Technical complexity
MULTOPS	Incoming rate is proportional to outgoing traffic rate	Medium	Low
SYN detection	Number of SYN packets ≈ ∑ (FIN and RST packets)	Weak	Low
Batch detection	Attack traffic is statistically unstable	Medium	Low
Spectral analysis	Attack flow is not periodic	Strong	High
Kolmogorov test	Attack traffic is highly correlated	Medium	High
Time series analysis	Attacks are limited to known attacks	Medium	Medium

SYN detection and batch detection apply monitoring of statistical changes as detection algorithm base. Both methods use specified parameter for incoming traffic and model it as a random sequence during normal operation. Spectral analysis uses the obvious difference between the spectral density diagrams in the case of TCP traffic and attack traffic. The Kolmogorov test is based on the assumption that multiple attack sources use the same DoS attack tool, thus forming highly correlated attack traffic. Time series analysis is based on extracting key variables from the target and usage of statistical tools to find the variables from the potential attackers that are highly related to key variables, and than to build a normal profile. Anomalies from potential attackers compared with the normal profile are regarded as a strong indication of an attack.

When coming to MANET, its inherent mobility brings to the light problem of distinguishing between normal and anomalous node/network behavior. As it is uneasy to build normal behavior profiles, the problem of making difference between false alarms and real intrusions becomes even greater.

For instance, the problem of reduction of false positives generated by a cooperative IDS has been considered in [9]. A range of security classes is applicable within the proposed IDS scheme, which is based on the cooperative game theory. The model presumes that every node runs locally the IDS performing local data collection and anomaly detection. The research is related to two common intrusions, cache poisoning and malicious flooding. The proposed model can be a base to study another types of MANET attacks. Simulations (based on GloMoSim tool) assume AODV routing protocol, four different security classes, and the measurement function of the severity of detected intrusions.

A study, presented in [10], has pointed out the need and importance to further investigate the causes of attack occurrences and possible countermeasures related to DoS attacks having into consideration the statistical analysis of IDS log files and flow information. Network forensics provides a means for identifying, preserving, analyzing, and presenting digital evidence for uncovering facts of unauthorized or malicious activities, and is based on several phases: network evidence capture, preservation, examination, analysis, visualization and presentation of the results (Figure 3). Optimal

analysis results can provide answers to critical security questions such as what form of malicious activity has happened, location of malicious event, what nodes have taken the participation in the event, and what was the reason for proceeding with an attack. The whole forensic analysis considers detailed trend analysis, content clustering, data fusion, data correlation, pattern identification and detection of traffic abnormality. Digital evidence is what forensic analysis is based on, and it can be collected in form of captured network traffic, data maintained by network nodes (log files, configuration settings, routing tables and other) or in best case the source of evidence can be the live traffic captured from a network. If an attacker erases all log files on a compromised node, the captured network traffic might therefore be the only evidence available for forensic analysis when dealing with a skilled attacker.

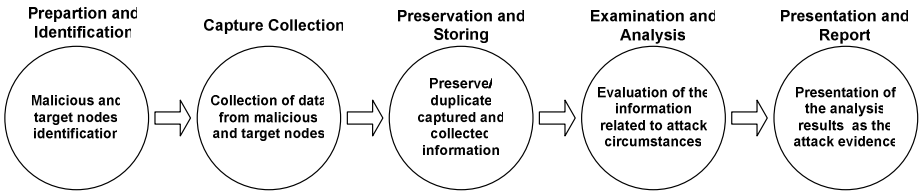

Figure 3. *The network forensics process phases.*

It aims to paralyze the entire network, rather than any particular node, by injecting devastating attack traffic into the MANET. The study has provided the flooding attack model using Dynamic Source Routing (DSR) protocol, based on multiple parameters: number of attackers, each attack node's rate, address spoofing frequency, and attack duration time. When studiously selected these parameters, the difference between attack traffic and normal network traffic is so slight that attackers can evade being detected or tracked. For instance, frequency represents the number of attack packets that use same spoofed address. This parameter is a base of identifying specific form of attack, non-address-spoofing flooding attack (NASF). Once that the value of frequency becomes greater than a value of each nodes rate multiplied with the value of attack duration time, the attack is denoted as the NASF where all attack packets sent out by one attacker have a fixed source and destination addresses.

The analysis is based on source and destination addresses and the time when traffic is received. Proposed analytical model comprehends two detection features. The first detection feature (DF-1) reflects this attributes of NASF traffic, by calculating and examining entries in the IDS log files. This information highly depends on node density, number of connections in the network, packet rate of each connection, and node mobility. The more attack nodes participate in the NASF attack, the more likely they are detected by DF-1. In the case of only a few attackers with abnormally high packet rate, second detection feature (DF-2) is applied. DF-2 supposes that flow rate is the receiving rate of packets belonging to the same flow. As a result, NASF attackers will be identified by the combination of DF-1 and DF-2 regardless of how they adjust the parameters. The analytical model is simulated in GloMoSim environment. Results have confirmed that the integrated use of DF-1 and DF-2 is able to identify all of NASF attacks with 80% coverage.

4. The influence of mobility to DoS attacks strength and the IDS performance

The MANET performance strongly depends on the applied mobility model [11, 12]. A detailed comparison of different mobility model generators such as BonnMotion and SUMO (*Simulation of Urban MObility*) is provided in [13].

In our previous work [5], we have pointed out that when considering MANET performances under DDoS attack, there is strong need to take into consideration the actual mobility pattern and the node speed. We have considered four different mobility models, namely the Random Waypoint (RW), Manhattan Grid (MG), Gauss-Markov (GM) and Reference Point Group Mobility (RPGM) model [14]. Through a comprehensive simulation study, performed with the network simulator *ns*-2 and BonnMotion, we have proved that MANET vulnerability to bandwidth DDoS attacks, strongly depends on the applied mobility pattern and node speed. For example, the obtained results have shown that the MG model, especially in the case for longer attack durations, is less vulnerable to DDoS attack in the presence of highly mobile attackers, due the time and space restrictions that this model imposes. On the other side, the GM model is extremely sensitive to attack duration, but experiences similar behavior regardless of the level of mobility in MANET. On the contrary, appliance of the most widespread RW model would bring the worst performance results. We have also pointed out that the delay performance deterioration is perceived mostly for high node mobility, and especially in the case of RPGM mobility model. Generally, the effect of attack is intensified with the increase of attack duration and the number of attackers.

Although the importance of integrating appropriate mobility model with the MANET IDS has been clearly recognized, an adequate research framework is still missing. For example, an alternative adaptive scheme can be used assuming that proper profiles and corresponding suitable thresholds are adaptively selected by each local IDS node during the process of periodical measurement of its local link change rate, and making a choice of a performance metric that can reflect suitable mobility level [8].

An unobtrusive monitoring technique to locate malicious packet dropping has been proposed in [15]. This study has also shown the possibility of exploring an impact of mobility models on detection effectiveness and obtained false positive rate. The study has evaluated the proposed technique by means of simulation, and proved the difference that applied mobility pattern (RW, GM, RPGM and MG) can cause when analyzing the coverage in identifying malicious behavior. The advantage of this technique is the applicability to multiple network layers. The study has also focused on comparison of normalized value of false positives against specified alert threshold, as well as to finding the best solution to the trade off between the reduced number of reported false positives and reduced efficacy of the detection mechanisms. The proposed mechanism is based on two algorithms: the data collection algorithm and data analyzer. Data collection algorithm is based on making a statistical record on all local data (route requests and route error messages, ICMP time exceeded, TCP timeouts) with an aim to further detect unusual behavior. The information is collected during a certain detection interval, while all stale information is regularly discharged. Data analyzer uses this logged information as input data, extracts the useful information and compares it against the normal behavior profile. The assumption is that the routing protocol functions seamlessly and that packet drops are strictly related to malicious activity or broken links. It is claimed that the choice of the

detection interval plays the main role in obtaining better results. Therefore, in the case of GM and GPRM the values for detection coverage were higher, and for false positives lower than in the case of RW, as these models are more realistic. In contrast to RW, MG experiences higher detection coverage and lower false positives because of its time and space movement restrictions.

5. Conclusion

This paper provides a survey of DDoS attacks and some of the most efficient solutions for IDS. Additionally, our previously presented results have clearly indicated the strong MANET vulnerability to bandwidth DDoS attacks, and noticeable dependency on the mobility pattern and node speed. We have also emphasized the need of providing concrete steps towards appliance of proper forensic analysis, with an aim to more efficiently discourage all future attacks. Besides, it is explicitly pointed out to the need of maintaining node anonymity, protecting privacy of mobility patterns, and integrating adequate mechanisms to applied IDS in way to assure network survivability in the attack occurrences. We conclude this paper by highlighting the impact of diverse node mobility models to the IDS performances, and further to DDoS attacks strength mitigation.

Acknowledgement. The work presented in this article has partially been funded by the Serbian Ministry of Education and Science (project TR 32025).

References

[1] B. Wu et al., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," *Springer Wireless Network Security, Network Theory and Applications*, 2007.

[2] P. Goyal et al., "A Literature Review of Security Attack in Mobile Ad-hoc Networks," *International Journal of Computer Applications*, vol. 9, no. 12, 2010

[3] T. Peng et al., "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," *ACM Computing Surveys,* vol. 39, no. 1, p. 3, 2007.

[4] P. Jain et al., "Mitigation of Denial of Service (DoS) Attack," *IJCEM International Journal of Computational Engineering & Management*, vol. 11, 2011.

[5] M. Stojanović, V. Timčenko, V. Aćimović-Raspopović, "The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks," *Electronics and Electrical Engineering – Kaunas: Technologija* (to be published in April 2012).

[6] P. M. Jawandhiya et al., "A Survey of Mobile Ad Hoc Network Attacks," *International Journal of Engineering Science and Technology,* vol. 2, no. 9., pp. 4063–4071, 2010.

[7] P. Yi et al., "Effects of Denial of Service Attack in Mobile Ad Hoc Networks," *Journal of Shanghai Jiaotong University,* vol. 14, no. 5, pp. 580–583, 2009.

[8] B. Sun et al.," Integration of Mobility and Intrusion Detection for Wireless Ad Hoc Networks" John Wiley & Sons, *Issue International Journal of Communication Systems*, vol. 20, no. 6, pp 695–721, 2007.

[9] H. Otrok et al., "A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks", *International Conference on Distributed Computing Systems Workshops*, Toronto, 2007.
[10] Y. Guo, I. Lee, "Forensic Analysis of DoS Attack Traffic in MANET", *Fourth International Conference on Network and System Security*, Melbourne, pp. 293 – 298, 2010.
[11] V. Timčenko, M. Stojanović, S. Boštjančič Rakas, "MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison," *in Proc. of the 9th WSEAS International Conference on Applied Informatics and Communications*, pp. 271–276, 2009.
[12] V. Timčenko, M. Stojanović, S. Boštjančič Rakas, "A Simulation Study of MANET Routing Protocols Using Mobility Models," *Computers and Simulation in Modern Science (Vol. III)*, pp. 186–196, WSEAS Press, 2010.
[13] V. Timčenko, V. Dulović, "Modeling of Mobility in Urban Environment", *in Proceedings of TELFOR 2011*, Belgrade, Serbia, 2011. (In Serbian).
[14] T. Camp, et al., "A Survey of Mobility Models for Ad Hoc Network Research", *Wireless Communications & Mobile Computing*, vol. 2, no. 5, pp. 483-502, 2002.
[15] S. Medidi et al., "Detecting Packet Mishandling in Mobile Ad-Hoc Networks", *Annual Reviews of Communication- IEC Publications*, vol. 59, pp. 295–301, 2006.

Sadržaj: *Odbijanje servisa (Denial of service, DoS) podrazumeva da je legitimnim korisnicima onemogućen pristup servisima ili resursima mreže. Distribuirani DoS (DDoS) napadi nastaju u slučaju kada koordinirana grupa napadača izvodi DoS napad. U slučaju kada se DDoS napad izvršava u okruženju mobilne ad hoc mreže (MANET), napadač zapravo kompromituje izvestan broj mobilnih čvorova, koji se mogu kretati u skladu sa različitim modelima mobilnosti i različitim brzinama. Ovaj rad sadrži pregled mogućih rešenja sistema za detekciju napada (IDS) u uslovima DoS napada u MANET mrežama. IDS je sistem koji nadgleda mrežu otkrivajući zlonamerne aktivnosti i, na osnovu prikupljenih informacija, generiše izveštaje. S obzirom na to da je DDoS saobraćaj često po svojim karakteristikama sličan legitimnom saobraćaju, postoji visok rizik da se legitimni saobraćaj tumači kao saobraćaj napadača i takvi događaji se nazivaju „lažnim uzbunama". Posebna pažnja je usmerena na IDS koji smanjuju pojavu „lažnih uzbuna", sa aspekta primene različitih modela mobilnosti u MANET okruženju.*

Ključne reči: *Mobilna ad hoc mreža, odbijanje servisa, sistemi za detekciju napada, model mobilnosti*

DETEKCIJA ODBIJANJA SERVISA (DoS)
U MOBILNIM AD HOC MREŽAMA

Mirjana Stojanović, Valentina Timčenko, Slavica Boštjančič Rakas