ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2012. No. 3(119)*
ELEKTRONIKA IR ELEKTROTECHNIKA

TELECOMMUNICATIONS ENGINEERING
T 180
TELEKOMUNIKACIJŲ INŽINERIJA

The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks

M. Stojanovic, V. Acimovic-Raspopovic
University of Belgrade, Faculty of Transport and Traffic Engineering,
Vojvode Stepe 305, 11000 Belgrade, Serbia, phone: +381 11 3091225, e-mail: m.stojanovic@sf.bg.ac.rs
V. Timcenko
University of Belgrade, Mihailo Pupin Institute,
Volgina 15, 11000 Belgrade, Serbia, phone: +381 11 2774959, e-mail: valentina.timcenko@institutepupin.com

crossref http://dx.doi.org/10.5755/j01.eee.119.3.1358

Introduction

A mobile ad hoc network (MANET) is a multi-hop, wireless, self-configuring network that can be formed without the need of any pre-established infrastructure or centralized administration. All nodes in the network act at the same time as hosts and packet-forwarding routers. Wireless links, node mobility and lack of central administration make MANETs far more vulnerable to security attacks than conventional networks [1, 2]. Taxonomy and comprehensive survey of MANET security attacks can be found in the literature [2, 3].

In a denial of service (DoS) attack, legitimate users are prevented from access to services or network resources. DoS attacks can be launched at any layer of the protocol stack causing physical jamming, disconnection, and malfunction of routing, transport and application protocols. The attacks become extremely dangerous and hard to prevent if a group of attackers coordinate in DoS. This type of attack is called distributed DoS (DDoS) attack. When a DDoS attack occurs in MANET, the attacker actually compromises a number of mobile nodes, which can follow different mobile patterns and have different speeds.

MANET simulation studies have mostly assumed the random waypoint (RW) mobility model. In the basic RW model, at every instant, a node randomly chooses a destination and moves towards it with a speed chosen uniformly randomly from the interval between the minimum and the maximum allowed speed. However, the RW model is not sufficient to capture some realistic MANET scenarios, including temporal and spatial dependencies as well as geographical restrictions. A realistic mobility model must take into account topological maps, traffic generation model, and node preferential movement or destination [4, 5]. Several studies have considered different mobility models, mainly concerning performance of ad hoc routing protocols [6–8].

The objective of this work is to explore the influence of mobility models, node speed and attack duration on the MANET vulnerability to bandwidth attacks, performed as DDoS attacks. We explain the attack model and present the results of a comprehensive simulation study, carried out by the network simulator *ns*-2 and its associated tools for mobile scenario generation, network animation and trace files analysis. Possible countermeasures against this type of attack have also been outlined.

Background and related work

According to [9], DoS attack can be launched in two forms. The first form aims to break down the target by sending one or more carefully constructed control packets that make use of the protocol or operating system vulnerabilities. The second form is to overflow the target with a huge amount of rubbish data, which leads to exhaustion of network bandwidth or computer resources.

In this article, we investigate the second aforementioned form of attack. Therefore, the term "DoS attack" refers to the threat that generates large amount of useless traffic. For that purpose, the attacker has to control more than one node to generate the attack traffic, i.e., such attacks are usually DDoS attacks. Examples of DDoS attacks in MANETs include routing table overflow attacks, packet-forwarding attacks, SYN flooding, and application-based attacks.

In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes [3], [10]. As a consequence, routing loops may appear and introduce severe network congestion. Multiple attackers may completely isolate a victim, by preventing it from finding

any route to the destination. Packet forwarding attack is performed via network-layer packet blasting [2]. The attacker injects 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 and network congestion in the MANET. In a SYN flooding attack, the attacker creates a large number of half-opened Transmission Control Protocol (TCP) connections with a target node, but never completes the handshake to fully open the connection [3], [9]. Application-based attacks force the victim to perform CPU and memory-intensive database operations and leave few resources to serve legitimate users. This type of attack may be closely related to the sleep deprivation attack, which aims to consume the energy of a victim node [3].

So far, simulation studies have not widely addressed the impact of different mobility patterns on MANET vulnerability to security attacks, including DDoS attacks.

The study presented in [10] investigates the influence of flooding attacks with Dynamic Source Routing (DSR) protocol messages to network performance. The packet delivery ratio and packet delay have been evaluated under different flooding frequencies and different numbers of attack nodes. The analysis assumes only the random waypoint mobility model.

In [11], a notion of dynamic DoS attack has been introduced and analyzed, considering Ad hoc On-demand Distance Vector (AODV) routing protocol. The attack propagation has been modeled by a semi-Markov process. The analysis indicates that the impact of DoS attack may be spread by the mobility of malicious nodes; this is faster in dense networks than in sparse networks.

A simulation study on anonymity threats against MANETs [12] considers a sparse mode inference attack where a target node moves straightly across a network from the left side to the right.

Solutions to locate malicious packet dropping using an unobtrusive monitoring technique have been proposed in [13]. Performance evaluation has indicated that the detection effectiveness depends on the node speed and the applied mobility model.

The attack model and problem statement

The attack model proposed for purpose of this analysis is presented in Fig. 1. First, the attacker compromises a number of mobile nodes by installing a malicious code into them (e.g., by means of worms [11]). It should be noted that the attacker itself could be an insider, i.e., a MANET node (as illustrated in Fig. 1) or some external device. Compromised mobile nodes become "zombies", which simultaneously generate junk packets and forward them towards the target. The attack traffic from each zombie is similar to the legitimate traffic, in the sense of bit rate and packet size. In other words, the traffic from each attack source does not need to be specific or voluminous to constitute a powerful attack.

The main consequence of such attack is bandwidth exhaustion due to large amount of useless traffic; hence, this is a bandwidth attack. This type of attack may look similar to a situation when multiple legitimate users try to access to a particular server node. This is known as a "flash crowd" phenomenon [9]. Unlike the flash crowd, the bandwidth attack is unpredictable and unresponsive to traffic control mechanisms, like TCP flow control or network congestion control mechanisms.

Further, we assume that the ad hoc routing protocol is operating correctly. This means that there is no routing table poisoning; however, packet forwarding attack occurs due to blasting of huge amount of rubbish packets.

The attack power may change dynamically depending on the speed and direction of node movement.

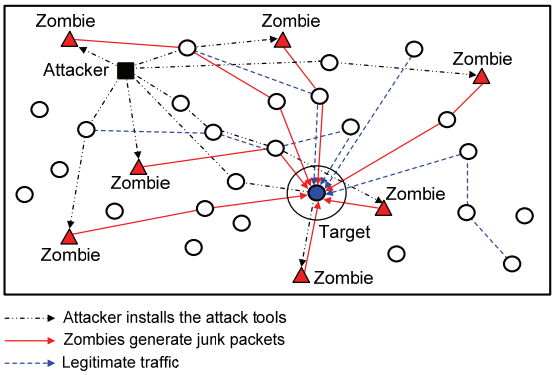


Fig. 1. The proposed model of a DDoS attack in MANET

The motivation for this work is to investigate the effects of DDoS bandwidth attacks under the following conditions: (1) different mobility models; (2) different speeds of the mobile nodes; (3) different number of zombies and (4) different attack duration.

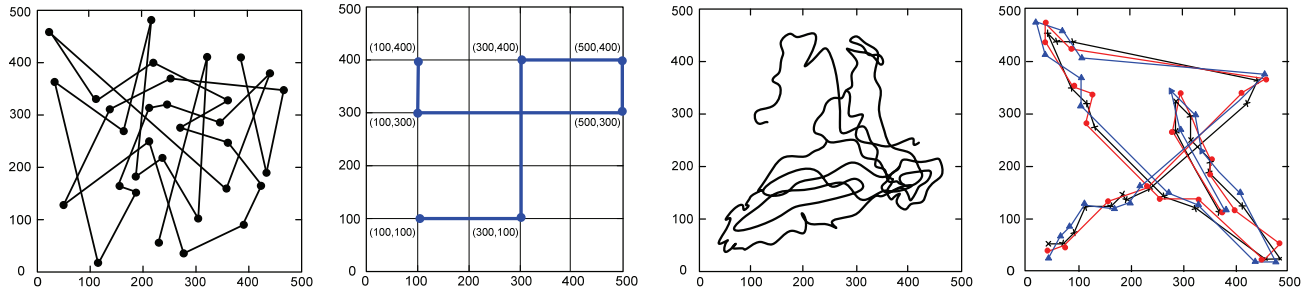
An overview of the investigated mobility models

Mobility models can be classified to entity and group models [4, 5]. Entity models represent mobile nodes whose movements are independent of each other. Group models represent mobile nodes whose movements depend on each other or on some predefined leader node. In this Section, we present a brief overview of the four mobility models that have been analyzed in our simulation study. Examples of trajectories for considered mobility models are presented in Fig. 2.

The *Random Waypoint (RW) model* (Fig. 2, a) assumes that each node selects a random destination in the simulation area and a speed that is uniformly distributed between the minimum value and the maximum value. After reaching the destination, the node waits for a predefined pause time, before selecting a new destination. The basic RW suffers from several drawbacks. First, it supposes that the speeds at two different time slots are independent. Although the pause time is used to mitigate the effects of abrupt stopping and starting, in most cases the current speed may depend on the previous speed. Second, the RW model assumes that each mobile node moves independently of other nodes. However, the movement pattern of a mobile node may be correlated with the nodes in its neighborhood. Finally, in many cases, the movement of a mobile node may be restricted depending on a geographical map, e.g. along the street or a freeway.

The *Manhattan Grid (MG) model* [6] is a representative of city section models, in which the simulation area emulates a block of city streets, typically

through a set of intersecting lines. The MG model has originally been developed by Maxemchuk (1985), for purpose of simulating streets in the area of Manhattan, i.e., a city section, which is only crossed by vertical and horizontal streets. Each mobile node begins its movement from a randomly selected position in the grid (Fig. 2, b). The node further moves towards the next position over the shortest path. When the node reaches the desired position, it pauses for a certain time before continuing to move over the grid, in a randomly selected direction.



a) b) c) d)

Fig. 2. Mobility patterns of different models: a – RW; b – MG; c – GM; d – RPGM (adapted from [4])

The *Gauss-Markov (GM) model* captures temporal and spatial dependencies of node mobility and represents random movement without sudden stops and sharp turns (Fig. 2, c). For a particular time period t, the node speed s_t and direction d_t are calculated on the basis of their values in the time period $t-1$ (s_{t-1} and d_{t-1}) and a random variable, according to following equations:

$$s_t = \alpha s_{t-1} + (1-\alpha)\bar{s} + \sqrt{(1-\alpha^2)}s_{t-1}^G, \quad (1)$$

$$d_t = \alpha d_{t-1} + (1-\alpha)\bar{d} + \sqrt{(1-\alpha^2)}d_{t-1}^G, \quad (2)$$

where α is the adjustable parameter used to vary the randomness by taking values from the interval [0,1]; $\bar{s}$ and $\bar{d}$ are constants representing the mean value of speed and direction, and s_{t-1}^G and d_{t-1}^G are random variables from a Gaussian distribution with mean 0 and standard deviation 1. The location of node at time t, represented by its coordinates (x_t, y_t), is calculated on the basis of parameters from the time slot t–1. In order to avoid that a node remains too long near any area boundary, it is forced away from an edge by modifying the mean value of direction, $\bar{d}$, in Eq. (2) [4]. The GM model is well suited for simulation of personal communication systems and event coverage scenarios.

In the *Reference Point Group Mobility (RPGM) model,* all nodes that belong to a particular group follow a reference point that determines the group motion behavior. Suppose that $RP(t-1)$ represents a group reference point at time $t-1$. A randomly chosen or predefined group vector $\overrightarrow{GM}$ is used to determine the node's new reference point $RP(t)$ at time t. The new position of each node is then calculated by summing a random motion vector, $\overrightarrow{RM}$, with the new reference point. The length of $\overrightarrow{RM}$ is uniformly distributed within a specified radius centered at $RP(t)$ and its direction is uniformly distributed in the interval [0, 2π]. Different mobility applications can be represented by the RPGM model [4]. They include battlefield scenarios, rescue operations, movement in a column, movement of tourist group with a guide, etc. For example, RPGM can emulate movement and behaviors of different expert teams in the same geographical area during a rescue operation (overlap mobility, Fig. 2, d).

Simulation and results

Extensive simulations have been carried out by the network simulator *ns*-2 (version 2.34) [14] under Linux Fedora Core 8 OS. Mobility scenarios are generated by the software package BonnMotion (version 1.4) [15]. The obtained results are evaluated using the Trace Graph analyzer (version 2.02) [16].

The simulation area is set to 500m x 500m, on which 100 nodes with transmission range of 250m are initially distributed uniformly and randomly. IEEE 802.11 and AODV are used for medium access control and routing protocol, respectively. The propagation model is two ray ground. Table 1 contains parameters of the investigated mobility models. The aim is to keep as much as possible realistic conditions of nodes movement. Parameters of the RPGM have been selected with respect to a large number of overlapping groups communicating with each other. Parameters of the GM model assure slight changes of movement directions at regular time intervals. Besides, the option "bounce" enforces the mobile node away from the simulation area boundary, with an angle determined by the incoming direction. Realistic aspect of the MG model is achieved by setting minimum street length to 50m, as well as by building a grid of minimum 10x10 blocks.

Table 1. Parameters of mobility models

Model	Parameter settings
RW	Maximum pause=0.1s
MG	(X, Y) axis blocks=(10, 10); update distance=5.0m; turn probability=0.5; maximum pause=0.1s; pause probability=0.5
GM	α=1; update frequency=2.5; "bounce"=true; angle standard deviation=π/8.
RPGM	Overlapping groups; average number of nodes per group=5; maximum distance=2.5m; maximum pause=0.1s

The legitimate traffic has been simulated by two File Transfer Protocol (FTP) sources, each with the ingress rate 0.5 Mb/s. They are attached to the TCP agents, with packet size 1500 bytes and the default window size 20.

Blasting of the attack traffic is simulated by constant bit rate (CBR) sources, with packet size 512 bytes and inter-arrival time 0.005s. Number of attackers (zombies) has been varied from 1 to 15. Initial positions of attackers are selected in such way that there is at least one hop between each zombie and the target.

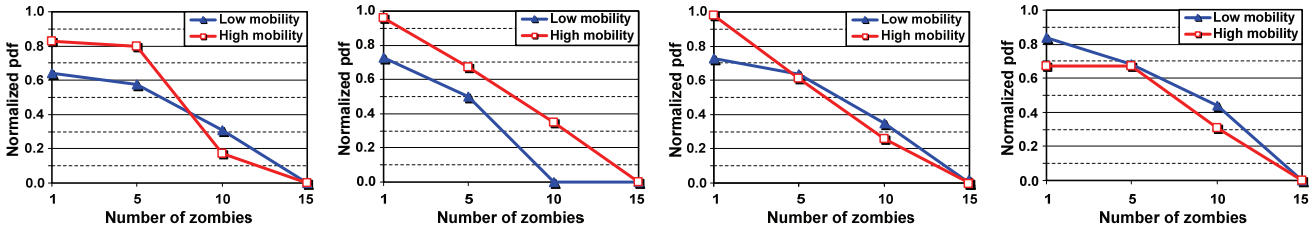


Fig. 3. Normalized *pdf* versus number of attackers (attack duration=10s): a – RW model; b – MG model; c – GM model; d – RPGM model

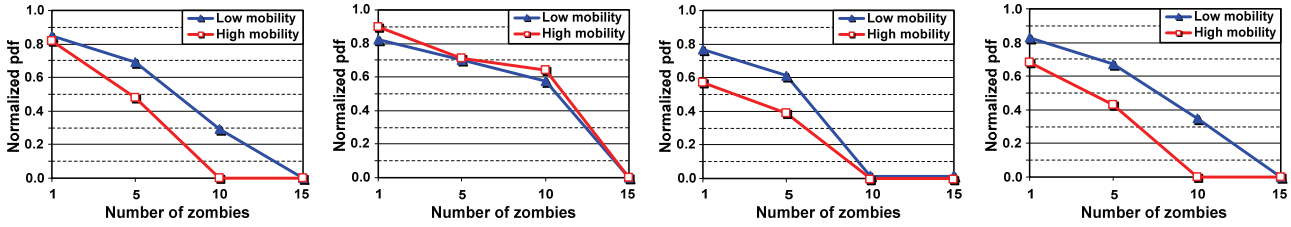


Fig. 4. Normalized *pdf* versus number of attackers (attack duration=20s): a – RW model; b – MG model; c – GM model; d – RPGM model

Low and high mobility have been simulated by setting average node speeds to 1.5m/s and 25m/s, respectively.

First, we assess the attack power through the normalized packet delivery fraction (*pdf*) at the target node. *Pdf* is defined as the ratio of the number of delivered and sent packets. Normalized *pdf* is defined as the ratio of *pdf* for legitimate traffic in the presence of attack and *pdf* in the absence of attack. The amplification of attack power with proliferation of the number of attackers, for attack duration 10s and 20s, is illustrated in Figs. 3 and 4, respectively. If the attack lasts longer (20s), the attackers and the target may approach and move away from each other more times, this may cause very high network dynamics. The MG model is less vulnerable to highly mobile attackers than the other models due to severe restrictions of the attacker movement; this is particularly noticeable for longer attack duration. With all other models and 20s attacks, the target node is not able to respond to legitimate traffic, in the presence of only 10 active zombies. The GM model experiences similar behavior for low and high node mobility; however, it is very sensitive to attack duration. This happens due to slight changes of direction (the angle standard deviation is set to $\pi/8$); hence, it is more resistant if the overall network dynamics is not too high. The RPGM model with low node mobility experiences similar behavior regardless of attack duration. This is a consequence of a rather similar and slow node movement inside each overlapping group. Besides, the RW and RPGM models experience similar *pdf* values for longer attacks.

The second set of results points to the effects of the attack traffic insensitivity to congestion control mechanisms. In our experiments, control of the legitimate traffic flow is provided through the TCP procedures, while the attack traffic is generated permanently, with constant bit rate. The attack duration is 20s, while the number of zombies is 5 and 10. We observe the following metrics:

(1) The ratio of legitimate and attack traffic, sent to the target node (Fig. 5);

(2) The throughput of the legitimate traffic, sent to the target node under attack, which is normalized to its value in the absence of attack (Fig. 6).

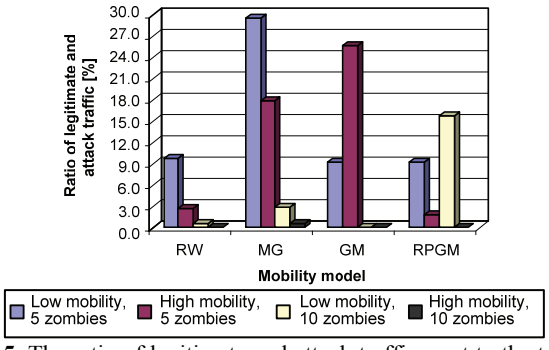


Fig. 5. The ratio of legitimate and attack traffic, sent to the target node, for different mobility models (attack duration=20s)

Differences between the investigated mobility models are clearly highlighted. The worst overall performance of the network with RW model emanates from lack of any restriction in movement of zombies. As a result of high

spatial dependencies, the MG model demonstrates the best overall performance, regarding number of attackers and node mobility. The GM model is less vulnerable than the others for lower number of attackers and high node mobility, mainly because of rather modest alterations of direction. The RPGM performs best for larger number of attackers, but with low node mobility. In a dense network, with large number of overlapping groups, there is a high probability that the legitimate senders and the attackers are located in different groups. This means that the number of intermediate nodes (and groups) may vary. Consequently, although the throughput of both legitimate and attack traffic is rather high, the attack traffic still experiences higher percentage of lost packets. With high mobility and in presence of 10 zombies, there is extremely high percentage of lost packets, regardless of mobility model.

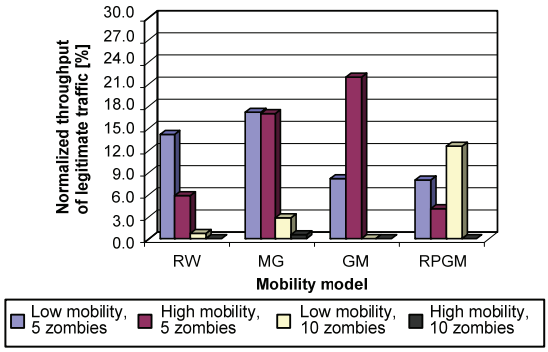


Fig. 6. Normalized throughput of legitimate traffic, sent to the target node, for different mobility models (attack duration=20s)

Finally, we observe normalized average end-to-end (E2E) delay of the legitimate traffic, i.e., the ratio of the average E2E delay with and without the attack. Table 2 contains simulation results for 20s attacks, in the presence of 5 and 10 zombies.

Table 2. Normalized average E2E delay of legitimate traffic under 20s attacks with 5 and 10 zombies

Model	Normalized average E2E delay of legitimate traffic			
	Low mobility		High mobility	
	5 zombies	10 zombies	5 zombies	10 zombies
RW	4.02	5.51	7.06	–
MG	2.66	4.52	2.25	3.77
GM	2.46	–	5.69	–
RPGM	3.45	10.9	13.03	–

Delay performance deterioration is perceived in all investigated cases, because of two factors: (1) frequent TCP retransmissions and (2) exhaustive processing of junk packets at the target node. This is particularly revealed for high node mobility, except for the MG model, which outperforms the other models. In the case of all other models, taking into consideration the results presented in Fig. 4, the target node is not able to respond to legitimate traffic, due to crash in the presence of only 10 zombies. Very high delay values are observed in all situations in which a large amount of junk traffic is received (and processed) at the target node. For example, in the network with RPGM model and low node mobility, the target node receives twice more attack packets, in the presence of 10 active zombies, than in the network with MG model.

Possible countermeasures

By using multiple attack sources, the power of a DDoS attack is intensified and the problem of protection is made more difficult. Besides, the attackers may use false source IP addresses and thus additionally complicate their identification at the target node. These features make IP source traceback and filtering the attack traffic very difficult [9].

Our simulation study indicates that MANET intrinsic features, such as node mobility model and speed, strongly affect the degree of vulnerability to DDoS attacks. Therefore, in some hostile MANET settings, there is a need to protect privacy of node identity and privacy of motion patterns [12]. For example, nodes might communicate only on the basis of their current locations.

In the past few years, intrusion tolerance approaches have gained a strong momentum. They complement preventive techniques (e.g., firewalls, cryptographic systems) and reactive techniques (intrusion detection systems) with mechanisms that afford some essential network services in the presence of malicious actions. Examples of such mechanisms include data replication, redundancy, and content distribution. Joint implementation of preventive, reactive and intrusion tolerance techniques is a basic method for building a survivable MANET [17].

Conclusions

Results of our study clearly indicate that the MANET vulnerability to bandwidth DDoS attacks strongly depends on the mobility pattern and node speed. The effect of attack is intensified with the increase of attack duration and the number of attackers. For all investigated parameters (*pdf*, throughput of legitimate traffic and E2E delay), the MG model is far less vulnerable than the other models, mainly because of its severe spatial restrictions. The RW model demonstrates the worst overall throughput of legitimate traffic. The GM model is highly sensitive to attack duration. The group model (RPGM) experiences the highest throughput of legitimate traffic for low mobility and large number of attackers, but on the count of severely deteriorated delay performance. The obtained results point to the need to maintain node anonymity, to protect privacy of motion patterns, and to apply mechanisms that should assure network survivability in the presence of attack.

Our future work should be focused towards exploring different intrusion detection techniques that would help in reaction to DDoS attacks in MANET environment.

Acknowledgements

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

References

1. **Vindašius A.** Security State of Wireless Networks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 7(71). – P. 19–22.
2. **Yang H., Luo H., Ye F., Lu S., Zhang L.** Security in Mobile Ad Hoc Networks: Challenges and Solutions // IEEE Wireless Communications, 2004. – Vol. 11. – No. 1. – P. 38–47.
3. **Jawandhiya P. M., Ghonge M. M., Ali M. S., Deshpande J. S.** A Survey of Mobile Ad Hoc Network Attacks // International Journal of Engineering Science and Technology, 2010. – Vol. 2. – No. 9. – P. 4063–4071.
4. **Camp T., Boleng J., Davies V.** A Survey of Mobility Models for Ad Hoc Network Research // Wireless Communications & Mobile Computing, 2002. – Vol. 2. – No. 5. – P. 483–502.
5. **Legendre F., Borrel V., Dias de Amorim M., Fdida S.** Reconsidering Microscopic Mobility Modeling for Self–Organizing Networks // IEEE Network, 2006. – Vol. 20. – No. 6. – P. 4–12.
6. **Jayakumar G., Gopinath G.** Performance Comparison of MANET Protocols Based on Manhattan Grid Model // Journal of Mobile Communication, 2008. – Vol. 2. – No. 1. – P. 18–26.
7. **Timčenko V., Stojanović M., Boštjančič Rakas S.** MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison // Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications (AIC '09), 2009. – P. 271–276.
8. **Timčenko V., Stojanović M., Boštjančič Rakas S.** A Simulation Study of MANET Routing Protocols using Mobility Models // Computers and Simulation in Modern Science (Vol. III). – WSEAS Press, 2010. – P. 186–196.
9. **Peng T., Leckie C., Ramamohanarao K.** Survey of Network–Based Defense Mechanisms Countering the DoS and DDoS Problems // ACM Computing Surveys, 2007. – Vol. 39. – No. 1. – 42 p.
10. **Yi P., Zhou Y–k., Wu Y., Liu N.** Effects of Denial of Service Attack in Mobile Ad Hoc Networks // Journal of Shanghai Jiaotong University (Science), 2009. – Vol. 14. – No. 5. – P. 580–583.
11. **Xing F., Wang W.** Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks // Proceedings of the 2006 IEEE Conference on Military Communications (MILCOM'06), 2006. – P. 1047–1053.
12. **Hong X., Kong J., Gerla M.** Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks // Wireless Communications & Mobile Computing, 2006. – Vol. 6. – No. 3. – P. 281–293.
13. **Medidi S., Medidi M., Gavini S.** Detecting Packet Mishandling in Mobile Ad–Hoc Networks // Annual Reviews of Communication. – IEC Publications, 2006. – Vol. 59. – P. 295–301.
14. **The Network Simulator ns–2 and Network Animator Nam.** Online : http://www.isi.edu/nsnam.
15. **BonnMotion**. A Mobility Scenario Generation and Analysis Tool. Online: http://net.cs.uni–bonn.de/wg/cs/applications/bonnmotion/.
16. **Trace graph.** NS Trace Files Analyzer. Online: http://nsnam.isi.edu/nsnam/index.php/Contributed_Code.
17. **Lima M., Dos Santos A., Pujolle G.** A Survey of Survivability in Mobile Ad Hoc Networks // IEEE Communications Surveys & Tutorials. – First Quarter, 2009. – Vol. 11. – No. 1. – P. 66–77.

Received 2011 04 02
Accepted after revision 2011 09 29

M. Stojanovic, V. Acimovic-Raspopovic, V. Timcenko. The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 3(119). – P. 29–34.

In this article, we investigate the influence of mobility models, node speed and attack duration on the MANET vulnerability to bandwidth attacks, which are performed as distributed denial of service (DDoS) attacks. We propose the attack model and present a comprehensive simulation study, carried out by the network simulator ns-2 and its associated tools for mobile scenario generation, network animation and trace files analysis. The following mobility models have been compared: Random Waypoint, Manhattan Grid, Gauss-Markov, and Reference Point Group Mobility. Simulation results indicate that MANET inherent features, such as node mobility pattern and speed, strongly affect the degree of vulnerability to DDoS attacks. Possible countermeasures against this type of attack have also been discussed. Ill. 6, bibl. 17, tabl. 2 (in English; abstracts in English and Lithuanian).

M. Stojanovic, V. Acimovic-Raspopovic, V. Timcenko. Mobilumo modelio poveikis MANET tinklų jautrumui DDoS atakoms // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 3(119). – P. 29–34.

Nagrinėjama mobilumo modelių, mazgų judėjimo greičių ir atakos trukmės įtaka MANET klasės tinklų pažeidžiamumui veikiant pralaidumo juostos atakoms, kurios yra vykdomos kaip paskirstytos „atsisakymo aptarnauti“ atakos (DDoS). Pasiūlytas atakos modelis ir pateikta išsami modeliavimo studija, atlikta naudojant ns-2 tinklo stimuliatorių ir susijusius įrankius mobiliam scenarijui generuoti, tinklui animuoti ir trasavimo failams analizuoti. Palyginti tokie mobilumo modeliai: atsitiktinio mazgo, Manhatano tinklo, Gauso-Markovo ir atskaitos taško grupės mobilumo. Modeliavimo rezultatai rodo, kad būdingos MANET charakteristikos, tokios kaip tinklo mazgų judėjimo modelis ir jų greitis, labai veikia pažeidžiamumo DDoS atakomis lygį. Apžvelgti galimi apsisaugojimo nuo tokio tipo atakų būdai. Il. 6, bibl. 17, lent. 2 (anglų kalba; santraukos anglų ir lietuvių k.).