Application of Forensic Analysis for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks

VALENTINA TIMCENKO[1], MIRJANA STOJANOVIC[2]
[1]Mihailo Pupin Institute, University of Belgrade, Volgina 15, Belgrade, SERBIA
[2]Faculty of Transport and Traffic Engineering and Faculty of Electrical Engineering,
University of Belgrade, Vojvode Stepe 305, Belgrade, SERBIA
[1]valentina.timcenko@institutepupin.com, http://www.pupin.rs
[2] m.stojanovic@sf.bg.ac.rs, http:// www.sf.bg.ac.rs/

Abstract: - This paper addresses a specific approach to resolving the problem of intrusion detection against distributed denial of service (DDoS) attacks in mobile ad hoc networks (MANET). The main function of an intrusion detection system (IDS) is to inspect the network for malicious activities, policy violations and security loopholes integrity, and to generate the appropriate reports. Network forensics concerns examining a network for anomalous traffic and identifying intrusions. It is very useful in decreasing probability of reoccurrence of the same intrusion activities. In the first part of the paper, we provide a comprehensive overview of recent advances in network forensics in MANET environment. In the second part of the paper, we propose a model of IDS that uses network forensics to detect DDoS attacks in MANET. The forensic analysis relies on inspecting simultaneous malicious activities of a group of attackers (zombies). Since DDoS attack traffic can appear rather alike to legitimate traffic in the sense of bit rate and packet size, the applied method should minimize the risk of misinterpreting legitimate traffic as attack traffic (false positives). We propose a flexible IDS model and the associated forensic analysis algorithm based on log file inspection. The performance analysis encompasses 100-nodes network with Manhattan Grid (MG) mobility model, and different numbers of malicious nodes. The study has been carried out by the network simulator ns-2 and its associated tools for mobility scenario generation, network animation and trace files analysis.

Key-Words: - Mobile ad hoc network, intrusion detection system, denial of service, network forensics, network simulation

1 Introduction

Since mobile ad hoc networks (MANETs) are autonomous, self-configuring, infrastructure-less distributed systems, these networks are exceptionally vulnerable to large set of security issues [1]. The increased occurrences of security threats and attacks have motivated the development of different defense mechanisms. These methods unfortunately cannot eliminate all potential intrusions, but can, to a certain extent, reduce their success probability.

MANET security attacks can be classified in accordance to different criteria. Thus, external attacks are performed by intruders outside the network, while internal attacks origin from legal, but malicious network nodes. Since the insider usually knows confidential information and possesses privileged access rights, the internal attacks seem to be more destructive than outside attacks. Additionally, inside attackers are up to date with the applied security policies, and in most cases well protected by these policies.

According to the interaction type, an attack could be categorized as passive or active. Passive attacks, like eavesdropping and traffic analysis, seize and capture packets to read the information that they carry, without any communication disruption. Active attacks refer to injection of junk packets into the network to obstruct or interrupt network communication. Some of the most common active attacks in MANET are blackhole, wormhole, Byzantine and Denial of Service (DoS) [2], [3].

The goal of DoS attack is to prevent legitimate users from access to required services or network resources. DoS attacks can be performed at any network layer producing physical jamming, disconnection, and errors in routing, transport and application protocols. DoS assaults can be performed in two general forms: software exploit and flooding. In the case of the **software exploits**, the attacker node will send a small number of packets to inject specific software bugs within the victim node application. They can usually be addressed by adequate software patches. **Flooding** tends to insert a huge amount of rubbish packets into the network. Flooding attacks are additionally classified to single and distributed attacks.

Distributed DoS (DDoS) is a more harmful then single DoS, because it is based on coordinated activity of multiple attackers across the network. DDoS attack is usually performed by means of two types of malicious nodes – zombies and reflectors [4], [5]. A zombie is a node compromised by a computer virus, cracker or Trojan horse worm, and is determined to be used to carry out malicious tasks in network or system that belongs to. Reflectors are intended to intensify an attack or to cover the identity of the intruder in DDoS attack.

DDoS attacks can appear in numerous varieties, such as packet-forwarding attack, routing table overflow, SYN flooding, or application-based attacks. A comprehensive survey of those attacks can be found in literature [4], [6], [7], [8], [9].

MANETs are prone to frequent link disconnections [10]. In our previous work we have focused on different mobility models, concerning performance of ad hoc routing protocols [11], [12]. In [5] we have considered the impact of mobility models on MANET vulnerability to bandwidth attacks, performed as DDoS attacks. Results of a comprehensive simulation analysis indicate that the MANET vulnerability to such attacks strongly depends on the mobility pattern and node speed. In [13] we have provided a survey of DDoS attacks and a detailed overview of the advanced solutions for intrusion detection system (IDS) against DDoS attacks.

This paper is a step forward in providing the exhaustive intrusion detection model suitable for detecting wide range of different MANET attacks covering specific network parameters. It focuses to IDS against DDoS attacks and, particularly, to application of network forensics in MANET IDS. The objective of this work is to point out the importance of forensic analysis in regular security system cycle, and propose a network forensic based IDS model, considering primarily the detection of DDoS attacks in MANET environment.

The rest of the paper is organized as follows. Section 2 provides an overview of the DDoS attacks and set of the requirements for digital evidence investigation by means of IDS in MANET. Section 3 highlights and briefly describes the methodology of the network forensic analysis with particular attention to its applicability for MANET. In section 4 we have proposed a flexible model of intrusion detection system and forensic analysis algorithm. Section 5 describes simulation environment settings and provides explanation of the obtained results. Section 6 provides concluding remarks.

2 IDS against DDoS in MANET

An in-depth survey of all existing DDoS defense methods is provided in [4]. According to this study, defending against these attacks is challenging for generally two reasons. First, there is a problem of potentially large number of involved zombies in such an attack. The volume of traffic sent by a single zombie might be small, but the aggregated traffic volume accessing the target node can be rather devastating. Second, the fact that zombies might spoof their IP addresses under the control of intruder, makes extremely complicated to trace the attack traffic back even to zombies. Thus, the main obstacles for network defense system are the high MANET infrastructure susceptibility and the existence of large volume of pseudo-legitimate traffic generated towards the destination nodes.

IDS is defined as a device or application that supervises network for malicious activities or policy violations and generates reports (based on gathered information) to the network management systems. Although some systems may implement procedures for blocking, denouncing and/or excluding of certain threats from the network, this is non required but optional feature of a monitoring system.

The categorization and comprehensive survey of existing IDS systems for MANET can be found in the literature [14]. The presented IDS comparison is based on a group of critical evaluation parameters related to performance and security issues, targeting mostly the operational strengths and weaknesses. The final touch is on proposal of a set of design principles and features important when designing and implementing future IDS architectures. It is of great importance to include this aspect into the evaluation, and further compare the latest and most prominent IDS for MANET architectures against this limitation as well.

Another approach, based on analyzing the performance of six different algorithm classifiers applied in the process of intrusion detection, has been exhaustively explored in [15]. With an aim to occupy less resources consumption and obtain best performance results, the study proposes a model of generating universal classifier for different attack detection in MANET. Still, one of the indispensable topic concerning proper IDS settings is provisioning of proper security measures, such as the threshold cryptography, certification authorities, repudiation schemes, and authentication [16].

IDS performance is typically estimated through two particular metrics: false positives and detection scheme coverage. **False positive** represents the ratio of the number of regular network nodes or events that are incorrectly reported as malicious and the overall number of reported attacks. **Coverage** is calculated as a percentage of actual attacks that can be detected. In fact, it is a degree of IDS detection effectiveness. In the case of DoS attacks this is rather easy to measure, because of obvious degradation of target's services (e.g. high packet drop rate). Therefore, they can be easily detected. Though, the ideal IDS will have the *coverage* of 100% and 0% *false positives*. Besides these two metrics, the **intrusion detection time** might be also measured; certainly the system is more efficient when detection time is shorter.

The intrinsic mobility of MANET generates an additional problem of distinguishing between normal and anomalous node/network activities. The issue of differentiating false alarms from real intrusions becomes even more serious as it is hard to generate normal behavior profiles, due to various and unpredictable mobility patterns.

One solution for reduction of false positives produced by cooperative IDS has been proposed in [17]. The solution is based on the cooperative game theory combined with a series of applicable security mechanisms. The model presumes that each node runs the IDS, by local data gathering and anomaly detection. The study is related to two frequent intrusions, cache poisoning and malicious flooding, but it can be extended to the other types of MANET attacks. Further, a problem of considering the impact of mobility factor and energy/memory resource consumption to the detection system accuracy, represents one of the research challenges.

In [18] a mobility and energy-aware hierarchical IDS for MANET has been proposed, providing an idea of specific cluster based detection load and energy consumption balancing. The key idea of this approach is that mobile nodes belonging to the same cluster appear more static to each other, gaining less detection accuracy dependability on node mobility. The model includes energy resources balancing in reasonable, fair and efficient manner providing more IDS responsibilities to the nodes with more energy resources.

3 Network forensic analysis

Network forensic analysis refers to a set of procedures for identifying, preserving, analyzing, and presenting digital evidence for revealing information on malicious activities. Forensic analysis might represent a backbone of IDS proper functioning, and a valuable phase in the process of gaining knowledge of system weaknesses. As it is based on the assembled network/system behavior evidence it: (1) provides the identification of threats profiles, (2) indicates the necessary steps that should be applied by security solution to avoid further compromise of the network or system, (3) detects any significant deviation from the normal activity profiles or abnormal change in communication behavior and (4) recognizes specific attack symptoms, thus enhancing the process of future attack prevention [19].

A typical cycle of forensic analysis includes: network evidence capture, preservation, examination, analysis, visualization and presentation of the results (Fig. 1).

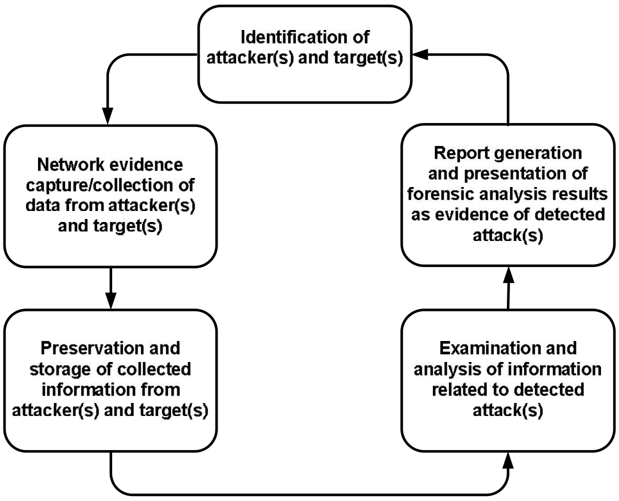

Identification of attacker(s) and target(s)
Network evidence capture/collection of data from attacker(s) and target(s)
Preservation and storage of collected information from attacker(s) and target(s)
Examination and analysis of information related to detected attack(s)
Report generation and presentation of forensic analysis results as evidence of detected attack(s)

Fig. 1. Typical cycle of forensic analysis.

Optimal analysis of results can provide a deep insight to the specific security issues such as: type of malicious activity, localization of malicious event, identification of attackers and victims, etc. The forensic analysis also considers the trend analysis, content clustering, pattern identification, data correlation, and detection of traffic abnormality. Data used in analysis come from multiple sources of evidence. The major one is the information maintained by network nodes, like log files, routing tables and configuration settings. Another source might be capture of the live traffic, which might be the only available source of evidence if the attacker erases all log files on a victim node.

In spite of existing literature concerning general principles of network forensic, only a few studies concern formal digital evidence investigation of security attacks in the context of wireless networks. Only a few of them have pointed out typical problems of MANET environment [19], [20].

A study introduced in [19] has indicated the need to further explore the basis of attack occurrences and potential countermeasures associated to DoS attacks, with respect to statistical analysis of IDS log files and flow information. The flooding attack model is based on the following parameters: number of attackers, each attack node’s rate, address spoofing frequency, and attack duration time. If these parameters are carefully chosen, the attack can be detected even if the difference between the attack traffic and legitimate traffic is rather insignificant. For example, frequency parameter represents the number of attack packets having the same spoofed address. By means of this parameter it is further possible to identify precise form of attack, i.e., the non-address-spoofing flooding attack (NASF).

The analysis relies on source and destination addresses and the time period that is needed to receive the traffic. Presented analytical model involves two detection features. The first detection feature (DF-1) considers this characteristic of NASF traffic, by calculating and analyzing entries in the IDS log files. This information mainly relies on network density, node number, node mobility, number of connections in the network and packet rate of every connection. When higher the number of malicious nodes that take part in the NASF attack, it is more likely that they will be discovered by DF-1 feature. In the case of only a small number of attackers with particularly high packet rate, second detection feature (DF-2) is implemented. DF-2 assumes that flow rate is the receiving rate of packets that are forming part of the same flow. Finally, NASF attackers will be identified by the combination of DF-1 and DF-2, regardless of how they set the parameters values.

In [21] a mobile ad hoc network composed of two types of nodes, mobile nodes and observer nodes, has been considered. The proposed model assumes the existence of specific inference system that integrates network and system evidence, collects aggregated network evidence from the observers and generates potential attack scenarios. This model drawback is the lack of the support for the cooperative attacks such as DDoS. Forensic analysis relies on a proper log file examination.

In [22], the mobile agent for TCP attacker identification, which uses the traffic history, has been proposed. The model is based on specific trace-back mechanism robust to mobile, untrustworthy environment and takes into consideration the issues of energy and memory resources consumption. It relies on a special log file (attack history database), which contains the information related to previous attacks that had occurred in a particular network segment. The shortcoming of this model is its suitability only for the needs of TCP attack type identification.

4 FMIDS – A Flexible MANET IDS

4.1. Functional model

The Flexible MANET IDS (FMIDS) model represents a modular system that provides security functions based on passive monitoring. FMIDS assumes two categories of network nodes: regular mobile nodes and IDS nodes. The model is based on the following assumptions:

a. IDS nodes are completely trustworthy;
b. The model is independent of network size, applied routing protocol, mobility model and mobile nodes speed.

The architectural framework is built upon a set of security mechanisms distributed across three logical planes: the control, data, and management planes.

Data plane: implies a set of activities performed on user data packets directly.

Control plane: includes a set of mechanisms that are performed over control traffic (e.g., routing messages).

Management plane: provides a set of security management functions.

FMIDS model relies on the overlay network approach. IDS nodes constitute the management network, which is built on the top of the existing MANET infrastructure.

Communication layers in the overlay network include: (1) communication between IDS nodes and (2) communication between regular and IDS nodes.

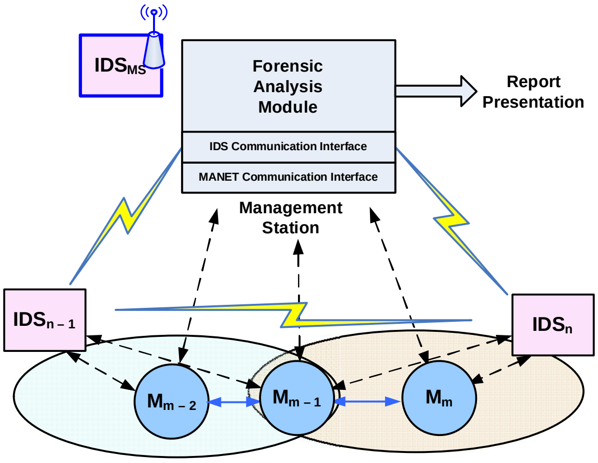


Fig. 2. FMIDS functionality block structure.

Fig. 2 provides an overview of the main FMIDS functionality block structure.

IDS_i $(1 \le i \le n)$ represents a node belonging to the management network, while ***M_j*** $(1 \le j \le m)$ represents a regular mobile node in MANET. The main building block of the security management application is **Forensic Analysis Module**, which performs the following tasks: (1) detection of attackers and victim; (2) detection of attack type and (3) report generation and presentation, including detailed analysis of attack as well as attacker's profile. Based on the collected evidence on different attacker behavior attributes, it is further possible to generate a particular "attack type" and "attacker profile" data base. Thus generated data base represents a foundation for applying specific IDS learning and training methodology, and further accelerating the future process of intruder detection.

IDS Communication Interface block is responsible for providing the management network communication, while **MANET Communication Interface** assures communication between regular network nodes.

At defined time intervals all IDS agents proceed with sending collected information related to the neighboring mobile nodes and the degree of their malice to neighboring IDS.

If the system determines that some neighbor node has the attacker's profile, it sends this information to all neighboring IDS nodes. IDS agents can detect malicious nodes even out of the determined time intervals.

The goal of IDS application is to provide information related to suspected nodes, and forward it to a prevention module of an applied network security system. Although the preventive and reactive parts of security system are out of the scope of this paper, it is clear that proper detection of malicious nodes is highly required for achieving the overall network security. The proposed IDS model relies on permanent testing of the existing evidence data according to pre-defined criteria set and further comparison of the test results with the pre-defined thresholds, in order to estimate whether the node corresponds to attacker's profile. Having a complete database related to potential attackers' profiles, would help predictability and avoidance of the future attacks.

IDS can be implemented either as a centralized or distributed process. Nodes have to be cooperative with an aim to align with the non-centralized MANET nature. Each node has unique identifier, the name by which it can be identified by IDS agents. Every IDS agent has two neighbor tables, one including only the information related to neighboring IDS nodes, and other containing information concerning the non-IDS neighboring nodes. Each IDS agent will periodically poll nodes from both neighbor tables and collects information on the perceived potential malicious behavior in the network. On the basis of gathered data, the intruder detection procedure can take effect and provide most accurate information on attacker nodes. Once detected, the list of discovered intruders IDs is being generated and presented in form of specific report to an attack prevention module for further security protection procedures.

4.2. A Forensic Analysis Algorithm

In the process of intrusion detection the FMIDS relies on the log file, which contains packet level data information, including event type, corresponding timestamp, source and destination node ID, tracing level (agent, routing or MAC), packet type, packet size, and specific ad hoc routing protocol information.

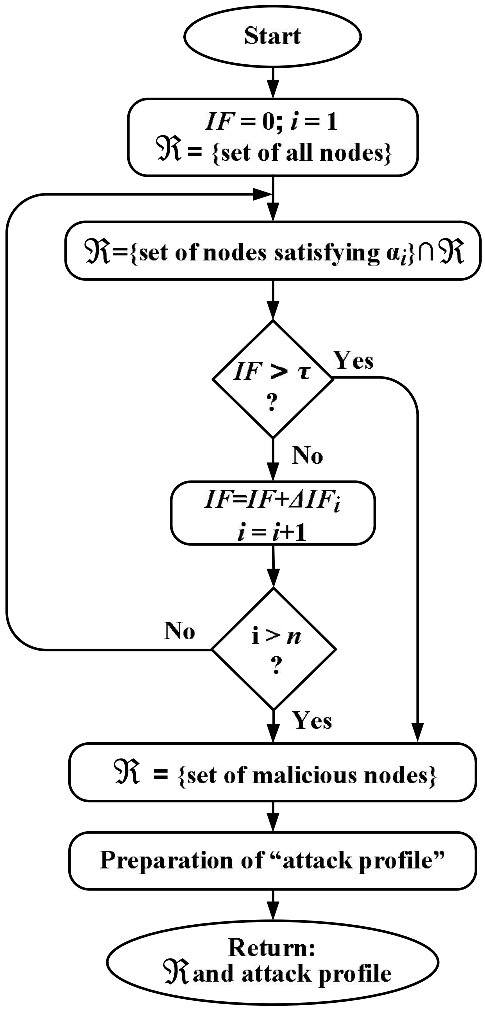

Start
$IF = 0$; $i = 1$
$\Re$ = {set of all nodes}
$\Re$={set of nodes satisfying α_i}∩$\Re$
$IF > \tau$?
Yes
No
$IF=IF+\Delta IF_i$
$i = i+1$
$i > n$?
No
Yes
$\Re$ = {set of malicious nodes}
Preparation of "attack profile"
Return:
$\Re$ and attack profile

Fig. 3. The proposed forensic analysis algorithm.

The algorithm proposed for forensic analysis is based on the elimination method and depicted in Fig. 3. We define a set of successive log file search criteria $\{\alpha_1, \alpha_2, ..., \alpha_n\}$. The log file is then retrieved in maximum n iterations. After retrieving iteration i (which corresponds to adding criterion α_i) the set $\Re$ represents a group of potentially malicious nodes, which satisfy set of successive criteria $\{\alpha_1, \alpha_2, ..., \alpha_i\}$.

We introduce the ***intrusion factor*** IF, which is incremented by some predefined value ΔIF_i after each retrieving iteration. If IF reaches the value of the administratively defined threshold τ, searching process is finished and $\Re$ represents the set of malicious nodes. Otherwise, searching process continues until the whole set of search criteria is exhausted.

After analysis of common properties of detected attackers (size of generated packets, type of transport protocol, periods of activity, etc.) the attack profile is generated. Therefore, the set $\Re$ and the attack profile represent the result of forensic analysis.

5 Simulation and results

Simulations have been carried out by the network simulator ns-2 (version 2.34) [23] in Linux Fedora 10 OS environment. The obtained results are evaluated using the Trace Graph analyzer (version 2.02) [24].

The specified network consists of 100 mobile nodes and one IDS station. The simulation area is set to be 500m x 500m, on which all nodes with transmission range of 250m are initially distributed uniformly and randomly. IEEE 802.11 and Ad hoc On-demand Distance Vector (AODV) protocols have been used for medium access control and routing, respectively. The propagation model is two ray ground.

The Manhattan Grid (MG) mobility model has been applied. It assumes that the simulation area is defined as a block of city streets, usually built through a set of intersecting lines. Each mobile node starts its movement from a randomly selected position in the grid (Fig. 4), and then moves towards the next position over the shortest path. After reaching the desired position, the node pauses for a certain time and than continues moving over the grid, in a randomly chosen direction. The MG mobility scenario has been generated by the software application BonnMotion (version 1.4) [25].

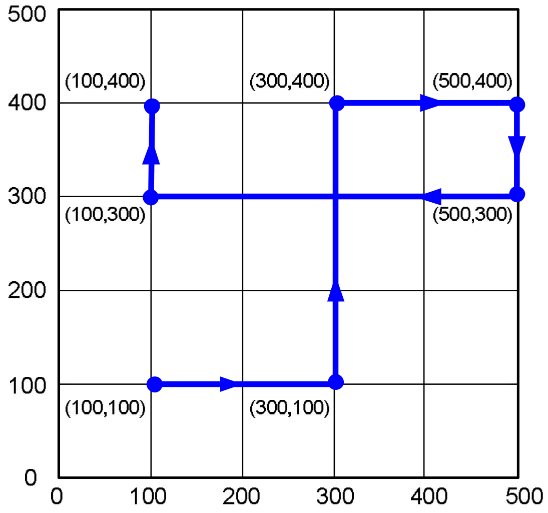


Fig. 4. *Manhattan Grid* mobility model pattern (adapted from [26]).

Realistic aspect of the MG model is accomplished by setting minimum street length to 50m, as well as by building a grid of minimum 10x10 blocks.

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. The background traffic is being simulated by 10 constant bit rate (CBR) sources with different packet sizes, inter-arrival time of 0.005s, and different and unsynchronized period of sources activity.

Blasting of the attack traffic is simulated by CBR sources, with packet size 512 bytes, inter-arrival time 0.005s and a synchronized, cooperative activity towards the same target node. Simulations have been performed for the cases of networks with 5 and 10 attackers (zombies). Initial positions of attackers are selected in such a manner that there is at least one hop between each zombie and the target.

For simulation experiments a set of six consecutive criteria $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ has been defined as follows:

- Criterion α_1 identifies node activity.
- Criterion α_2 refers to generating traffic from different sources towards the same destination node.
- Criterion α_3 denotes the use of the same type of transport layer protocol.
- Criterion α_4 denotes packets of the same or very similar size.

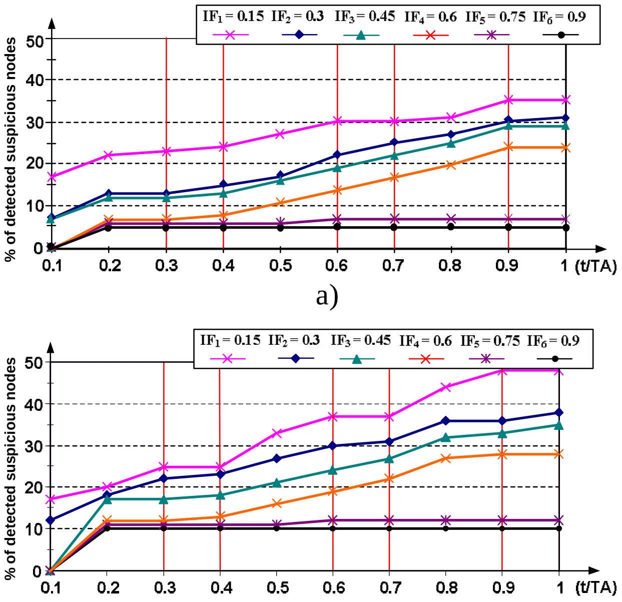
- Criterion α_5 refers to eliminating all routing messages and MAC (medium access control) packets.
- Criterion α_6 denotes concurrent and same intervals of traffic generation.

Intrusion factor IF, which is initially set to zero, is calculated by adding at each next step value of ΔIF_i. For the needs of our experiments, ΔIF_i for all iterations i is set to $\Delta IF_i = 0.15$.

The simulated experiments imply periodical and synchronized group activity of 5 and 10 attackers during three time intervals: $[0.1T_A,\ 0.3T_A]$, $[0.4T_A,\ 0.6T_A]$ and $[0.7T_A,\ 0.9T_A]$; where T_A represents the duration of network activity. Period of IDS activity is represented by variable t_S, which takes values from the interval $[0,\ T_A]$. The attackers do not perform malicious activity out of these predefined intervals; however there is noticeable activity related to legitimate and background traffic processing during the whole interval $[0,\ T_A]$.

Fig. 5 depicts cumulative function of number of network nodes detected as possibly malicious, for different values of IF, considering cases when the real percentage of attackers is 5% and 10%. These diagrams provide information related to process of gradual discovering of potentially malicious nodes, depending on portion of system activity time which is taken into consideration.

With each step in forensic analysis the number of detected suspicious nodes is closer to the real number of zombie nodes. Thus, taking into account the set of criteria $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ it is possible to detect the presence of intruders, but impossible to determine attackers' profile. In other words, it is still not apparent whether the number of zombies has been increased or the IDS detects their repetitive activity. Further, application of the criteria set $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ eliminates a considerable percentage of potentially malicious nodes, thus significantly decreasing the number of examined nodes in the next iteration. With adding criterion α_6, the number of remaining monitored nodes has been decreased only slightly. Since adding criteria α_5 and α_6 provides similar results, we can terminate the forensic analysis procedure.



a)

b)

Fig. 5. Percentage of detected attackers for different IDS sampling intervals with: a) 5% of malicious nodes; b) 10% of malicious nodes.

Fig. 6 depicts obtained results related to the number of detected percentage of potentially suspicious nodes at each IDS activity segment intervals (10 equal time intervals). When comparing Fig. 6 to Fig. 5, the specific intervals of IDS activity do match, but Fig. 6 provides the precise information related to potential synchronous node group activity. The extremely high activity of a group of nodes can be noticed in three isolated intervals. Out of these periods the number of potentially malicious nodes is constant. Again, adding of criterion α_6 provides the most noticeable differentiation of these periods. It is evident the difference between selectivity of each higher criterion applied, where furthermore, the segments of group activity are recognizable from the very start of the forensic analysis.

These results also provide information related to *coverage* metric. During the activity of forensic analysis algorithm, three separate attacks were successfully discovered. This information is available only by analysis of the IDS activity segment intervals (Fig. 6). Although this information is most precise after applying final two criteria, it can be also obtained from other algorithm phases, with rather high probability. Thus, the very similar symptoms to the DDoS attack activity eliminates from the set of previously suspicious nodes all these that might have similar packet, destination and transport protocol characteristics, but are not active in the same periods as the detected "malicious group".

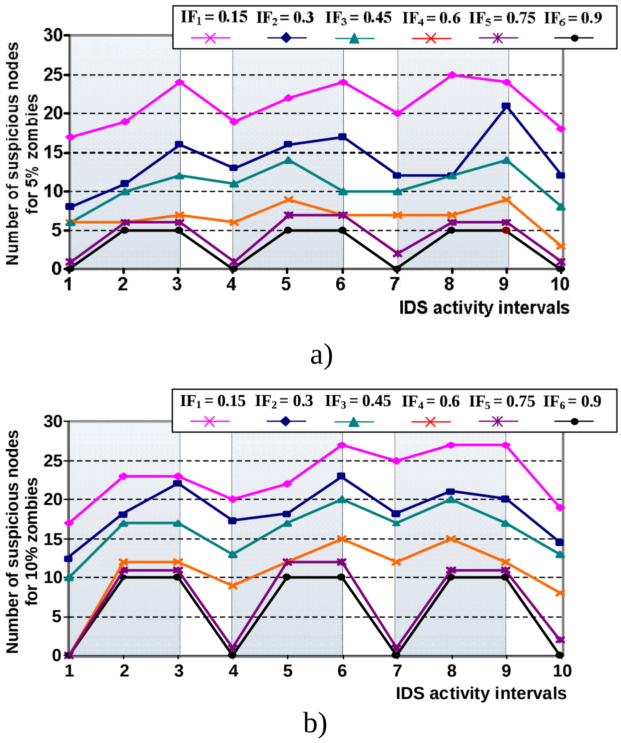


Fig. 6. Number of detected suspicious nodes for MANET with: a) 5% of malicious nodes; b) 10% of malicious nodes.

For defined experiment, it was necessary to successively apply a set of defined interdependent eliminatory criteria, thus finishing the proposed forensic analysis algorithm with obtaining the final set $\mathfrak{R}$.

By varying the value of t_S (Fig. 5) in the interval $[0,\ T_A]$, the *detection time* period can be obtained for the particular type of attack, taking also into account the percentage of malicious nodes that system reports (i.e., obtaining at the end of the forensic analysis the set of true malicious nodes $\mathfrak{R}$).

Considering results, it is clear that for either case (5% or 10% malicious network) when expanding the analyzed segment of IDS activity time (e.g. $[0,\ 0.3T_A]$, and than $[0,\ 0.4T_A]$, etc), the number of newly discovered potentially malicious nodes increases. This tendency is noticeable till the end of the penultimate decade of IDS activity time, $[0.8T_A,\ 0.9T_A]$, after which, in most cases, this number becomes constant.

These experiments have demonstrated that by applying forensic analysis it is possible to isolate malicious nodes. The results have indicated the need for additional considering of the dependence on network size, traffic type, packet characteristics, different criteria definitions and their order to the efficiency of providing final set $\mathfrak{R}$.

Fig. 7 depicts results of evaluating *false positive* metric depending on threshold τ.

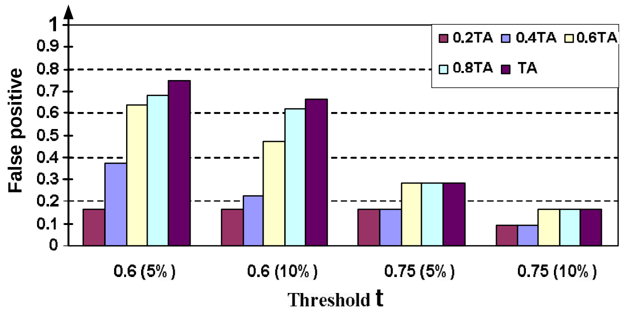


Fig. 7. False positives versus threshold τ for 5% and 10% of malicious nodes.

The value of threshold τ has been set to 0.60 and 0.75, respectively. As mentioned earlier, this value depends on security level requirements defined by the network administrator.

Fig. 7 actually provides information related to *false positives* versus two specific sets of criteria $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ and $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5\}$, in course of IDS activity and depending on the moment of rating. In the case of 5% zombie network, the values of *false positives* are slightly higher for all criterion set iterations, mainly because there is a larger number of regular nodes in network, thus resulting with greater probability to erroneously mark these nodes as malicious. Regardless the examined network case, the measured values of *false positives* for the set $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$ are unacceptably high, while in the case of second, stricter set these values are considerably lower, gaining a saturation trend starting from $0.6T_A$. This result indicates that the value of *false positives* under set $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5\}$ can be obtained without inspection of the whole IDS activity time period. This information can be also considered when estimating *detection time* value.

The dynamics and efficiency of the examined IDS can differ depending on defined set of criteria and its order of application. These IDS features can be estimated according to system security requirements. Generally, the efficiency of the applied forensic analysis algorithm relies on as smallest as possible number of criteria steps with an aim to get non further selective set of nodes $\mathfrak{R}$, that will be declared malicious.

6 Conclusions and future work

With an aim to explore the problem of intrusion detection against DDoS attacks in MANET, we have proposed flexible IDS for MANETs – FMIDS, with accompanying forensic analysis algorithm. We have developed a set of simulation scripts for ns-2 simulation environment merged with the BonnMotion scenario generation tools. The particular focus of the study is on the impact of number of attackers to the performance of proposed forensic analysis algorithm.

For both investigated cases, 5% and 10% zombie network, the $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ set of criteria is not eliminatory enough to identify the intruders, but only to detect their presence. The more precise attacker profiles are obtained after proceeding with additional criteria, finalizing the forensic analysis algorithm with set of six successive, mutually dependent criteria, $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$, and obtaining the set of true malicious nodes $\Re$.

Results of our study clearly indicate that the precise information related to potential synchronous node group activity is highly important for identification of malicious nodes as this behavior indicates the presence of DDoS attacks.

The values of *false positives* are higher for less “polluted” network, as there is a larger number of regular nodes, thus providing greater chance to mistakenly mark these nodes as malicious. Additionally, *false positive* and *detection time* metric values can be obtained without inspection of the whole IDS activity time period, and with more sophisticated set of mutually dependent criteria these values can further decrease. When coming to *coverage* features, our algorithm has successfully detected all the attack intervals and their duration.

This paper introduces the network forensic analysis algorithm for flexible MANET IDS (FMIDS) and provides guidelines for further investigation related to different network parameters: network size, node number, node speed, attack duration, and the influence of applied mobility model patterns.

Since DDoS zombies can follow different mobile patterns and speeds, our future work will encompass particular attention to specific mobility models impact to the forensic analysis algorithm efficiency.

Besides, it is required to additionally explore alternative forensic analysis criteria sets in order to assure network survivability in the different attack occurrences, guarantee node anonymity, efficient energy/memory resources consumption, privacy protection of mobility patterns and more efficiently discourage all future attacks.

Acknowledgement. The work presented in this article has partially been funded by the Serbian Ministry of Education and Science (projects TR 32025 and TR36002).

References:

[1] A. Vindašius, Security State of Wireless Networks, *Elektronika Ir Elektrotechnika*, No. 3(71), 2006, pp.19-22.

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

[3] P. Goyal et al., A Literature Review of Security Attack in Mobile Ad-hoc Networks, *Int. Journal of Computer Applications*, Vol. 9, No. 12, 2010, pp.11-15.

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

[5] M. Stojanović, V. Aćimović-Raspopović, V. Timčenko, The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks, *Elektronika Ir Elektrotechnika*, No. 3 (119), March 2012, pp. 29-34.

[6] P. Jain et al., Mitigation of Denial of Service (DoS) Attack, *IJCEM Int. Journal of Computational Engineering & Management,* Vol. 11, No. 4, 2011, pp. 38-44.

[7] P. M. Jawandhiya et al., A Survey of Mobile Ad Hoc Network Attacks, *Int. Journal of Engineering Science and Technology*, Vol. 2, No. 9, 2010, pp. 4063-4071.

[8] P. Yi et al., Effects of Denial of Service Attack in Mobile Ad Hoc Networks, *Journal of Shanghai Jiaotong University*, Vol. 14, No. 5, 2009, pp. 580-583.

[9] B. Sun et al., Integration of Mobility and Intrusion Detection for Wireless Ad Hoc Networks, *Int. Journal of Communication Systems*, Vol. 20, No. 6, 2007, pp. 695-721.

[10] G. Jayakumar, G. Gopinath, Performance Comparison of MANET Protocols Based on Manhattan Grid Model, *Journal of Mobile Communication*, Vol. 2, No. 1, 2008, pp. 18-26.

[11] V. Timčenko, M. Stojanović, S. Boštjančič Rakas, MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison, *in Proc. of the 9th WSEAS Int. Conf. on Applied Informatics and Communications (AIC '09)*, 2009, pp. 271-276.

[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), WSEAS Press*, 2010, pp. 186-196. [Online] www.wseas.com/wseas/volume3.pdf

[13] V. Timčenko, M. Stojanović, S. Boštjančič Rakas, Intrusion Detection Against Denial of Service Attacks in MANET Environment, invited paper, *in Proc.of XXIX Symposium on New Technologies in the Postal and Telecommunications Traffic – POSTEL 2011*, Serbia, 2011, pp. 201-212.

[14] C. Xenakis et al, A Comparative Evaluation of Intrusion Detection Architectures for Mobile Ad Hoc Networks, *Computers & Security*, Vol. 30, No. 1, 2011, pp. 63-80.

[15] S. Pastrana et al, Evaluation of Classification Algorithms for Intrusion Detection in MANETs, *Knowledge Based Systems*, 2012, doi: http://dx.doi.org/ 10.1016/j.knosys.2012.06.016

[16] M. Azer et al., Security in Ad Hoc Networks: From Vulnerability to Risk Management, *in Proc. of 3rd Int. Conf. on Emerging Security Information, Systems and Technologies*, 2009, pp. 203-209.

[17] H. Otrok et al., A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks, *Int. Conf. on Distributed Computing Systems Workshops*, Toronto, 2007, p.86.

[18] E. Darra et al., A Mobility and Energy-Aware Hierarchical Intrusion Detection System for Mobile Ad Hoc Network, *in Proc. of TrustBus*, 2011, pp. 138-149.

[19] Y. Guo, I. Lee, Forensic Analysis of DoS Attack Traffic in MANET, *4th Int. Conf. on Network and System Security*, Melbourne, 2010, pp. 293-298.

[20] Al-Sakib Khan Pathan, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, *Auerbach Publications, CRC Press*, USA, 2010.

[21] S. Rekhis, N. Boudriga, Formal Reconstruction of Attack Scenarios in Mobile Ad Hoc and Sensor Networks, *EURASIP Journal on Wireless Communications and Networking*, (39) 2011.

[22] N. Nishanth, P. Venkataraman, Mobile agent based TCP attacker identification in MANET using the Traffic History (MAITH), *13th IEEE Int. Conf. on Communication Technology (ICCT)*, 2011, pp. 1130-1134.

[23] The Network Simulator ns-2 and Network Animator Nam. [Online]. http://www.isi.edu/nsnam.

[24] Trace graph – NS Trace Files Analyzer [Online]. http://nsnam.isi.edu/nsnam/index.php /Contributed_Code.

[25] BonnMotion – A Mobility Scenario Generation and Analysis Tool. [Online]. http://net.cs.uni-bonn.de/wg/cs/applications/bonnmotion/.

[26] T. Camp, et al., A Survey of Mobility Models for Ad Hoc Network Research, *Wireless Communications & Mobile Computing*, Vol. 2, No. 5, 2002, pp. 483–502.