An Approach for DDoS Attack Prevention in Mobile ad hoc Networks

V. V. Timcenko[1]
[1]*University of Belgrade, Institute Mihailo Pupin,*
Volgina 15, Belgrade, Serbia
valentina.timcenko@pupin.rs

***Abstract*—In this paper we propose a prevention mechanism for distributed denial of service (DDoS) attacks in Mobile Ad hoc Networks (MANET) environment. Since MANETs are wireless, self-configuring networks with highly unpredictable node movement, the security provisioning represents one of the most sensitive issues. The presented approach relies on the investigation of widespread bandwidth attacks, with focus on Distributed Denial of Service (DDoS) attacks, which are extremely dangerous, hard to detect and challenging to prevent. DDoS represents a coordinated activity of a group of attackers aiming to prevent legitimate users the access to network resources. Intrusion prevention systems (IPS) are mainly considered as extensions of intrusion detection systems (IDS) with a purpose to actively prevent and block intrusions that are detected by IDS. The presented IPS model is based on the analysis of the forensic analysis report generated by IDS incorporated into the network security monitoring system.**

***Index Terms*—Mobile ad hoc networks, attack prevention, forensic analysis, simulation.**

I. INTRODUCTION

Mobile ad hoc networks (MANET) are dynamic peer-to-peer, self-configuring networks. Their wireless nature, lack of central administration and inherent node mobility imply specific security requirements. The most important MANET advantage is its applicability to a wide range of services and applications, mostly suitable in situations when fixed network infrastructure and centralized administration are unavailable (disaster hitting places, emergency services, vehicular networks, campus networking, military communication, etc.). For proper implementation and use of these networks, the imperative is to ensure the security and minimize the probability of the attacks occurrence [1].

In this paper the focus is on efficient use of the IDS report and its application for the preventive and responsive activities in MANET security provisioning. We have first provided an overview of the DDoS attacks in MANET, and set the requirements for digital evidence analysis by means of proper IDS solution. Then, the Flexible MANET Prevention Algorithm (FMPA) has been proposed, and explained its interoperability with the used IDS solution. Next, we have described the use of the report generated by IDS, blacklist database updating and adequate statistical analysis procedure of reported data. Finally, we have indicated possible enhancements and provided concluding remarks.

Manuscript received October 24, 2013; accepted March 6, 2014.
This paper has been partially financed by Serbian Ministry of Education, Science and Technical Development (Development Projects TR 32025 and TR 32037).

II. SECURITY IN MANET

One of the most arguable questions related to the proper implementation and use of the MANET is the security provision. MANETs are far more vulnerable to the attacks that the conventional networks [2]. The external attacks are performed by the attackers that are active outside the monitored network, while usually more severe attacks are coming from the insiders. Actually, insiders are usually legal, but malicious nodes, well informed of applied security policies, and in most cases protected by them. From the aspect of the interaction type, the attacks are classified as passive or active. Passive attacks rely on capturing the traffic and procuring to obtain the information that the packets carry without any communication disruption. Conversely, active attacks can severely obstruct and even interrupt the network communication jeopardizing the network survivability, while node participants are considered malicious. Some of the most widespread active attacks in MANET are blackhole, wormhole and Denial of Service (DoS). MANET has become highly favourable environment for flooding attack. Flooding tends to insert a huge amount of junk packets into the network. DDoS is a typical representative of flooding attacks. The complete taxonomy of the most common MANET attacks can be found in [3].

For building a survivable MANET, a joint implementation of prevention, detection and reaction techniques is needed. Each of these security segments is highly correlated with two others, while there is a demand to strive on timely adjustment of the applied methodologies in order to preserve the strong coordination of prevention, detection, and response system cycles. Intrusion prevention is a first line of defence against the network attacks, but it is worthless without the presence of an active IDS. On the other side, the response phase findings will be processed and mapped appropriately to the prevention measures settings and intrusion detection configurations. The ultimate goal of the security system is to protect the confidentiality, integrity and provide availability. Although attack prevention is one of the most actual security issues, there is a lack of studies targeting the specific prevention solutions. Majority of

existing research studies have focused on providing routing protocol attacks preventive schemes. Most of them are based on encryption and key management techniques, thus preventing unauthorized nodes to join the network. Nevertheless, these models introduce heavy traffic loads during the key verification exchange procedures, this way exhausting the already limited node memory and processing resources. In [4] the proposed black hole attack prevention relies on routing protocol procedures modification in order to generate only top secure routes. The proposed algorithm is highly CPU, energy and memory demanding as it requires engagement of all network nodes and continuous exchange of Data Routing Information (DRI) tables and current routing tables. DRI should provide information to source and destination nodes of detected black hole nodes that might be on the selected route. Therefore, a method that can prevent the attack without increasing routing overhead and delay is required [5]. Our aim is to provide preventive technique independent of relying protocol characteristics, network size and number of attackers. In [6] different DDoS attacks have been examined in context of profile-based and specification-based detection techniques, while the focus is still on existing solutions for routing protocols protection. Generally, there are two types of preventive defence, global and local [7]. Global solutions rely on several nodes cooperation, while local solutions are intended to be implemented on the target node. Local techniques comprehend: *local filtering* – solution that will stop infiltrating specific packets on the node by applying a filter to detect them; *changing IDs* – change of the victim node's ID, thereby invalidating the old one; *zombie bottlenecks creation* - this approach creates bottleneck processes on the zombies, limiting their attacking ability. Global techniques improve security of the entire network by *impeding attackers from finding the most vulnerable nodes*, suitable for injecting the malicious code thus converting them to zombies. Other approach would apply *globally coordinated filters* thus preventing the accumulation of a critical mass of attacking packets in time. Global preventive techniques can rely on *tracing the source ID*: where the intruder's path is traced back to zombies this way impeding their attacks.

III. MANET SECURITY SYSTEM PROPOSAL

Recently, the intrusion detection and prevention techniques have gained a strong momentum. The intrusion detection system purpose is to indicate possible security holes and failures in the system. The survey on different intrusion detection systems can be found in [8], whereas only some of them base their functionality on forensic analysis [9].

The basic assumption for this study is that we already have a proper intrusion detection system, Flexible MANET Intrusion detection System (FMIDS) [10]. FMIDS is a modular MANET IDS that relies on the application of forensic analysis of log data and generation of adequate report. It assumes two categories of network nodes: regular mobile nodes and IDS nodes, where IDS nodes constitute the management network built on the top of the existing MANET infrastructure. In defined time intervals all IDS agents are sending collected information related to the activities in network to the main IDS station. This way merged log file data are processed by means of forensic analysis resulting with report generation. The log file contains packet level data information, such as event type, timestamps, node ID, packet type and size, and routing protocol information. The algorithm proposed for forensic analysis is based on the elimination method, where a set of successive log file search criteria is applied and results are retrieved in a number of IDS iterations. Based on such defined IDS model, we have made a step forward and generated a DDoS attack prevention scheme. In Fig. 1 the overall security system proposal is shown, providing the basic activities within each part of MANET security system.

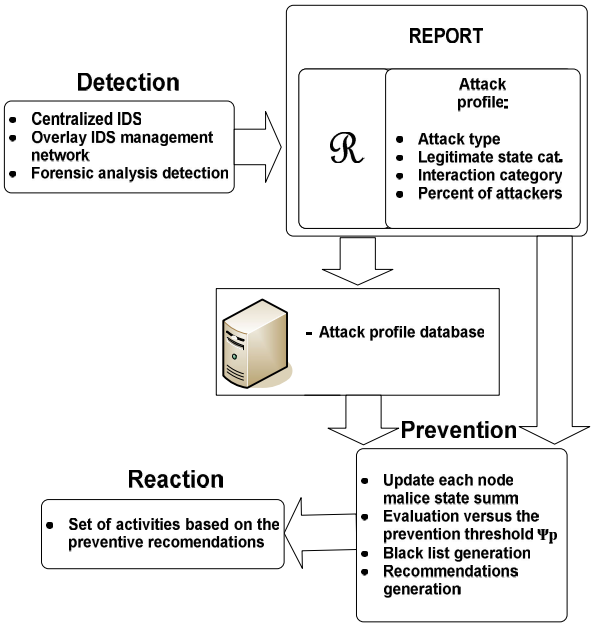

Fig. 1. An overview of the proposed MANET security system.

The report provides a situation at the moment of the IDS analysis, and these can be just segments of the further overall evaluation of the network security for a certain period of time. Having a set $\Re$, that represent the detected malicious nodes, and attack profile that provides information related to the characteristics of the attack (type, legitimate state category – external/internal, interaction category – passive/active) and number of detected attackers, it is further possible to proceed with statistical analysis of the attack occurrence and attacker behaviour during variable periods of activity in network and generation of adequate Attack Profile Database (APD). Thus, APD provides a long term statistical analysis for each node malice characteristics. The obtained results allow possibility to obtain valuable information for prevention of further similar attacks. The report generated at the IDS module is used as a base for giving iterative evaluation of each network node.

IV. INTRUSION PREVENTION SCHEME PROPOSAL

DDoS attacks are usually generated with an aim to disable some network functionality, mainly specific service and resource availability. Based on the APD it is possible to make systematic evidence of which nodes are malicious and what is their level of severity. Each IDS cycle will generate report. Every change in the reported number of detected malicious nodes will trigger the update of APD. Based on

that, the prevention algorithm FMPA will be initialized. The goal of our solution is to provide adaptive and iterative security system, instantly aware of any new circumstance. Thus, in prevention part of the system there is a blacklist file where nodes are listed in order related to their overall number of gained "malicious" states. The proposed prevention algorithm FMPA is represented in Fig. 2. Ψ_p is the value of preventive threshold, given as an integer number. It represents the highest allowed number of gained "malicious" states for a node, over which certain nodes will be treated as blacklisted. $\Re$ is the set of malicious nodes detected in previous IDS activity cycle. The members of set $\Re$ are identified by their node ID, thus their ID values will be used for the needs of further prevention analysis.

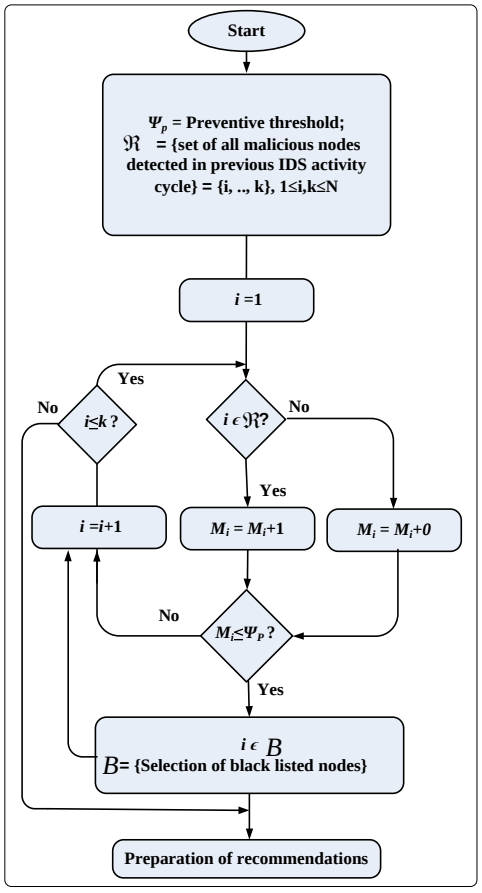

Fig. 2. The proposed attack prevention FMPA algorithm chart.

The assumed network consists of N nodes. The APD keeps track of each node malice state number, M. Whenever a certain node i has been detected as malicious in previous IDS startup, it's M_i value in APD table will be increased, otherwise its M_i value will remain the same. If the current M_i value is higher than the defined Ψ_p, the node i will be added as a new member to the set of blacklisted nodes, B. The assumed preventive measures will generate and send to a response module a periodical recommendation of what should be done to protect the security of the network. The nodes with positions in the list higher than administratively set Ψ_p are deemed as with high probability to be malicious. As a consequence, in a reactive part of the system the activity of these nodes will be minimized and they will be declared as unreliable and denied from forming part of network routes. In more severe circumstances they are marked as ineligible for further activities in network and ignored in the communication with other nodes. As the IDS report comprehends the possibility to obtain the information related to the group activity of certain nodes, these nodes are marked in the blacklist file and their activity is evaluated individually and as a group. The response module will have a set of activities which are exercised in the circumstances of the attack presence. It relies on the information and measures realized by the prevention module, and are mutually interdependent. The goal of the proposed system is to consequently improve the overall MANET performance in the presence of the attacks. In the case of blacklist change, prevention mechanisms will alarm the reaction module. The listed malicious nodes can be bypassed when generating routes, but the most severe prevention recommendation would be to deny them any form of activity.

V. Simulation and Results

Simulations have been carried out by the network simulator ns-2 (ver. 2.34) [11] in Linux Fedora 16. The obtained results are evaluated using the Trace Graph analyser (ver. 2.02) [12]. We assume that the intruders were detected based on FMIDS algorithm [10], which basically applies the forensic analysis methodology and retrieves the log file in maximum x iterations. Each of the iteration implies the addition of a new elimination criterion, thus narrowing the detected set of potentially malicious nodes. The final set $\Re$ is generated when the whole set of search criteria is exhausted and final IDS iteration is completed. IDS_{itx} represents the specific IDS activity iteration (cycle), where in the case of the experiments presented in this paper $x \in \{1,..,6\}$ stands for six consecutive FMIDS iterations that are used for generation of the report. Each IDS_{itx} iteration can be a base for initializing the execution of FMPA. The IDS report is used as input data for blacklist creation and prevention mechanism recommendations generation. The specified network consists of 100 mobile nodes. The simulation area is set to be 500 m × 500 m, on which all nodes with transmission range of 250 m 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 legitimate traffic is simulated by two File Transfer Protocol (FTP) sources, attached to the TCP agents, with packet size 1500 bytes, default window size 20 and each with ingress rate 0.5 Mb/s. The attack traffic is simulated by CBR sources, with packet size 512 bytes, inter-arrival time 0.005 s and a cooperative, synchronized activity towards the same target. Simulations have been performed for networks with 5 and 10 attackers. The background traffic is simulated by 10 Constant Bit Rate (CBR) sources with different packet sizes, inter-arrival time of 0.005 s, and different and unsynchronized period of sources activity. The experiments imply synchronized and periodical 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 simulated network activity (represented as 10 consecutive equal time intervals).

The applied IDS analysis is performed in 6 consecutive forensic analysis iterations, each providing more precise set of suspicious nodes, terminating with final set $\Re$. This procedure can be performed over the entire period of simulation or it can be applied on partial periods which can indicate a presence of the attackers.

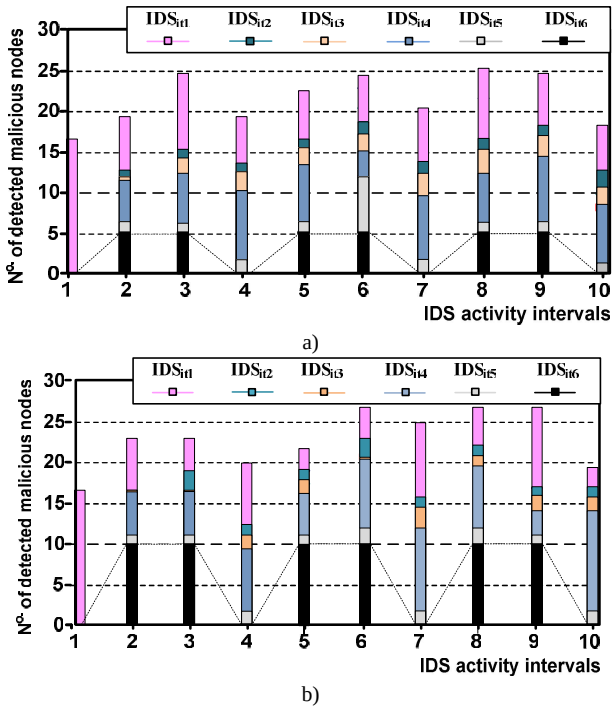

Fig. 3. Number of detected malicious nodes for MANET with: a) 5 % of intruders; b) 10 % of intruders.

Figure 3(a) and Fig. 3(b) provide a representation of the obtained results when considering ten equal IDS activity time intervals, for six IDS_{itx} iterations, covering the entire simulated network situation for the case of 5 % and 10 % intruders, respectively. It can be seen that, starting with IDS_{it1}, each consecutive iteration has further narrowed the set of suspicious nodes, terminating with final set $\Re$, obtained with IDS_{it6}. The analysis for 5 % and 10 % intruders has provided and identified a set of malicious nodes. It is indicative that the algorithm has isolated three periods of activity generated by a group of nodes. In the case of our simulations, the sets of detected nodes include IDs = {12, 45, 49, 63, 95} for 5 % intruders, and IDs = {3, 8 12, 26, 45, 49, 54, 60, 63, 95} for 10 % intruder network. FMPA will increase the M_i for detected node's IDs. Thus, three consecutive attacks, generated by a synchronous activity of a group of nodes, were detected. When allowing the FMIDS report generation after the first detected group attack (indicating the presence of DDoS attack), even before finishing the examination of entire simulation data, it is possible to update the APD and allow FMPA to proceed with updating the blacklist. If FMPA activity has generated any change to the blacklist, these changes are immediately sent to the reactive module which could react according to the recommendations. For the needs of this study we have assumed that each detected group attack updates the black list. For rigorous preventive settings, the blacklist will be formed by these sets of nodes, and reactive module will receive recommendation to exclude specified nodes from further communication. As results, two additional attacks which were detected in FMIDS can be prevented.

VI. CONCLUSIONS

The power of DDoS attacks is intensified with use of multiple attack sources, thus providing favourable conditions for jeopardizing network security. The factor of attack duration and repetition can additionally reinforce the attack effect, weaken network performances and prevent legal users the access to network services. In this paper we have pointed out the possible security measures and proposed prevention algorithm suitable to be applied in DDoS vulnerable MANETs. Based on the developed IDS system we have used the results in proposed prevention algorithm FMPA, in most time concerning manner. The FMPA is administrative adjustable for different security needs, but also adaptable according to the previously obtained information and continuously updatable malicious node's blacklist. This way it is possible to generate up to date recommendations for reactive module, thus tending to assure network survivability in the presence of the attack.

REFERENCES

[1] B. Wu, J. Chen, J. Wu, M. Cardei, *A survey on attacks and countermeasures in mobile Ad Hoc networks*. *Wireless network security, network theory and applications*. Springer, 2007, ch. 12.

[2] M. Stojanovic, V. Acimovic-Raspopovic, V. Timcenko, "The impact of mobility patterns on MANET vulnerability to DDoS attacks", *Elektronika ir Elektrotechnika*, no. 3, pp. 29–34, 2012.

[3] P. M. Jawandhiya, M. M. Ghonge, M. S. Ali, J. S. Deshpande, "A survey of mobile ad hoc network attacks", *Int. J. of Eng. Science and Technology*, vol. 2, no. 9, pp. 4063–4071, 2010.

[4] S. Ramaswamy, F. Huirong, S. Manohar, J. Dixon, K. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks", in *Proc. of Int. Conf. Wireless Networks (ICWN 2003)*, Las Vegas, Nevada, USA, 2003, pp. 570–575.

[5] P. N. Raj, P. B. Swadas, "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET", *Int. J. of Computer Science Issues (IJCSI)*, vol. 1, pp. 54–59, 2009.

[6] S. Kannan, T. Maragatham, S. Karthik, V. P. Arunachalam, "A study of attacks, attack detection and prevention methods in proactive and reactive routing protocols", *Int. Business Management*, vol. 5, no. 3, pp. 178–183, 2011. [Online]. Available: http://dx.doi.org/10.3923/ibm.2011.178.183

[7] N. Sharma, B. L. Raina, P. Rani, "Attack prevention methods for DDOS attacks in MANETs", *Asian Journal of Computer Science and Information Technology*, vol. 1, no. 1, 2011.

[8] C. Xenakis, C. Panosb, I. Stavrakakisb, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks", *Computers & Security*, vol. 30, no. 1, pp. 63–80, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2010.10.008

[9] 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.

[10] V. Timcenko, M. Stojanovic, "Application of forensic analysis for intrusion detection against DDoS attacks in mobile ad hoc networks", in *Proc. 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN 2012)*, Vienna, 2012, pp. 301–310.

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

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