

Mitigating DDoS Attacks in MANETs Using Protection Nodes

6G6Z1013 Assignment Part 2

Dale Stubbs - 14024149 | Computer Forensics and Security | 11/03/2017

Contents

[Abstract and Keywords 2](#_Toc477293238)

[Table of Terms 3](#_Toc477293239)

[Introduction 4](#_Toc477293240)

[Literature review study 4](#_Toc477293241)

[Comparison, Critical Analysis and Evaluation 5](#_Toc477293242)

[Conclusion 6](#_Toc477293243)

[Appendices 7](#_Toc477293244)

[Appendix 1 7](#_Toc477293245)

[References 8](#_Toc477293246)

# Abstract and Keywords

# Table of Terms

|  |  |
| --- | --- |
| Term | Description |
| MANET | Abbreviation of Mobile Ad-hoc Network |
| DDoS/DoS |  |
| Botnet |  |
| Node |  |
| IDS |  |
|  |  |
|  |  |

Table 1: Table of Terms

# Introduction

Mobile Adhoc Networks (MANETs) are multi-node wireless networks that require no central administration and have no predetermined infrastructure as discussed in paper [1]. Since they contain no central administration they lack the basic security fundamentals and are at an elevated risk of attacks. MANETs are used in situations that require a quick set-up with little configuration such as during a war for military communications and data sharing, medical emergency situations and disaster areas following a natural disaster. The nature of the MANET is that it can be set-up quickly and efficiently whilst remaining dynamic and allowing the connected nodes to freely move around within the network area. This dynamic topology of the network is a double edged sword as, as previously mentioned, they are quick to set-up however, it leaves the MANET open to attacks. This paper will look at Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks (see appendix 1) and how to defend the MANET against them (Mitigation). In particular mitigating against these attacks using Protection Nodes as outlined in paper [2]. I will also be comparing this form of mitigation against other forms to see how it compares.

# Literature review study

In paper [2] the authors, Minda Xiang et al., provide a solution for the mitigation of dynamic Denial of Service (dDoS) attacks. They propose a hierarchical structure to protect the network against dDoS. Their structure combines a Remote Protection Node (RPN) that acts as a protection node from the first hop from a source node with a Local Protection Node (LPN) that acts as a protection node for the destination node. The higher level nodes within the system are protected by the lower level nodes. When a malicious packet/activity is detected an Attack Notification Message (ANM) is sent to the higher level nodes that then relay an Attack Information Message (AIM) to the RPN which will, in turn, drop all Route Request (RREQ) packets sent by the malicious node. This is how the structure protects the MANET against dDoS attacks.

In paper [3] the authors, Ramratan et al., discuss and present a method of intrusion detection determining or misbehavior within MANET using Intrusion Detection System (IDS) to protect the network from DDoS. They analysed their result on the basis of average end-to-end postponement during normal, DDoS attack and IDS time, TCP flow monitoring and routing distribution.

In paper [4] the authors, Rizwan Khan et al., suggest a new architecture of Detection and Control of DDoS in MANET that consists of a Path Manager, Monitor, Trust Manager/Co-operation system and a Reputation system.

In paper [5] the authors, S. A. Arunmozhi et al., propose a defense scheme to mitigate dDoS attacks in MANET. This scheme focuses on the use of a Flow Monitoring Table (FMT) distributed at each node within the network. This FMT is used to identify malicious nodes within the network and allows for all of the packets sent from these nodes to be discarded. When compared to the SWAN scheme proposed in paper [6] they found that their proposed scheme, when run inside a simulation, received higher bandwidth availability and higher packet delivery ratio while reducing the packets being dropped or lost for legitimate nodes on the network.

In paper [7] the authors, Yinan Jing et al., propose that a more stable topology is best when tracing attackers on a network when using a lightweight Probabilistic Packet Marking (PPM) scheme. It is proposed that if an overlay network is constructed for traceback based on an identity replacement mechanism above the existing network layer in order to provide this stable topology.

In paper [8] the author, Kanchan Sanjeev Rana, proposes a ‘novel’ approach to identifying malicious nodes within MANET using the Ad Hoc On-Demand Distance Vector (AODV) routing protocol and also preventing DoS attacks. Within this approach when a malicious node is discovered, rather than simply dropping all the packets from this node, it is removed from the network.

# Comparison, Critical Analysis and Evaluation

Each of the papers considered with the literature review study provide very different methodologies used for detecting and mitigating against DoS attacks in any form. This section will compare and contrast each of these methodologies.

|  |  |  |  |
| --- | --- | --- | --- |
| **Papers** | **Methodology** | **Pros** | **Cons** |
| Ahirwal, R. and Mahour, L. (2012) | IDS | Almost 100% data recovery. | IDS systems can provide a lot of False Positives for malicious behavior. |
| Xiang, M., Chen, Y., Ku, W.S. and Su, Z., (2011) | Protection Nodes | Effective for protecting critical nodes in MANET. | Can only protect the critical nodes of the network.  Cannot protect against packets broadcast to the entire network to cause congestion. |
| Khan, R. and Vatsa, A.K., (2011) | Reputation Based  Incentive Scheme | Effective and efficient algorithms. | Algorithms do not take into account the mobility of the nodes within the network. |
| Arunmozhi, S.A. and Venkataramani, Y., (2011) | FMT | Accurate identification of dDoS attack flows. | Possible network overhead due to each node containing a FMT. |
| Jing, Y., Wang, X., Zhang, L. and Zhang, G., (2011) | Stable Topology of MANET | Improved traceback performance. | Requires a network overlay above the existing network. A costly overhead. |
| Kanchan, S.R., (2011) | 5 Step Algorithm for Detection and Prevention of DoS | Simple and effective with minimal cost.  Malicious nodes are removed from the network. | Unknown scalability, cost/benefit ratio, throughput and overheads. |

Table 2: Pros and Cons of Each Methodology

Each of the proposed solutions have their own set of pros and deal with a form of DoS attack in their own way. However, each of them have their own set of cons too. Seemingly it is apparent that no one has come up with the ‘perfect’ solution to DoS attacks within a MANET. The author would like to suggest that rather than relying on one single methodology of detecting and mitigating against DoS attacks that research is done into combining one or more of the aforementioned methodologies and whether or not they provide a better solution to this problem.

# Conclusion

Upon completing this literature review the author concludes that security with a MANET environment has been and may always be a difficult thing to maintain. The basic infrastructure-less nature of MANETs are the main reason for their lack of security. Without a centralized administrative figure there will always be security issues. Some of the proposed methodologies for the detection and mitigation of DoS attacks seem promising however, without further testing and research they may never amount to anything. When proposing a new methodology or protocol for the pretection of a MANET there needs to be a thought to the potential for attackers to circumvent their methodology as, with the advancement of computers and applications, comes the advancement of the attackers’ arsenal. The author has suggested that a possible combination of the methodologies reviewed in this paper into a single form of detection and mitigation of DoS within MANET.

# Appendices

## Appendix 1

***DDoS/DoS Attacks***

A Denial of Service attack is defined as ‘*any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.’* (Techopedia.com, 2017)

This can be completed either by attacking the legitimate users’ computer (node) or by making the services provided by the network unavailable to the legitimate users. Although these types of attacks are considered different types of attack they are in fact the same. DDoS is the same type of attack as DoS, however, the only difference between the two is that during A DoS attack only one node is responsible for the attack whereas, during a DDoS attack multiple nodes such as a Botnet are responsible for the attack.

# References

[1] Das, K. and Taggu, A. (2014). A comprehensive analysis of DoS attacks in Mobile Adhoc Networks. 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[2] Xiang, M., Chen, Y., Ku, W.S. and Su, Z., (2011). “Mitigating DDoS Attacks Using Protection Nodes in Mobile Ad Hoc Networks.” In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE (pp. 1-6). IEEE.

[3] Ahirwal, R. and Mahour, L. (2012). “Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network.” International Journal on Computer Science and Engineering, 4(6), p.1164.

[4] Khan, R. and Vatsa, A.K., (2011). “Detection and control of DDOS attacks over reputation and score based MANET.” Journal of Emerging Trends in Computing and Information Sciences, 2(11), pp.646-655.

[5] Arunmozhi, S.A. and Venkataramani, Y., (2011). “DDoS Attack and Defence Scheme in Wireless Ad hoc Networks.” arXiv preprint arXiv: 1106.1287.

[6] Ahn, G.S., Campbell, A.T., Veres, A. and Sun, L.H., (2002). SWAN: Service differentiation in stateless wireless ad hoc networks. In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 2, pp. 457-466). IEEE.

[7] Jing, Y., Wang, X., Zhang, L. and Zhang, G., (2011). “Stable topology support for tracing DDoS attackers in MANET”. In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE (pp. 1-6). IEEE.

[8] Kanchan, S.R., (2011). “Methodology for detecting and thwarting dos in MANET”. In IJCA.

Techopedia.com. (2017). What is a Denial-of-Service Attack (DoS)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24841/denial-of-service-attack-dos [Accessed 14 Mar. 2017].