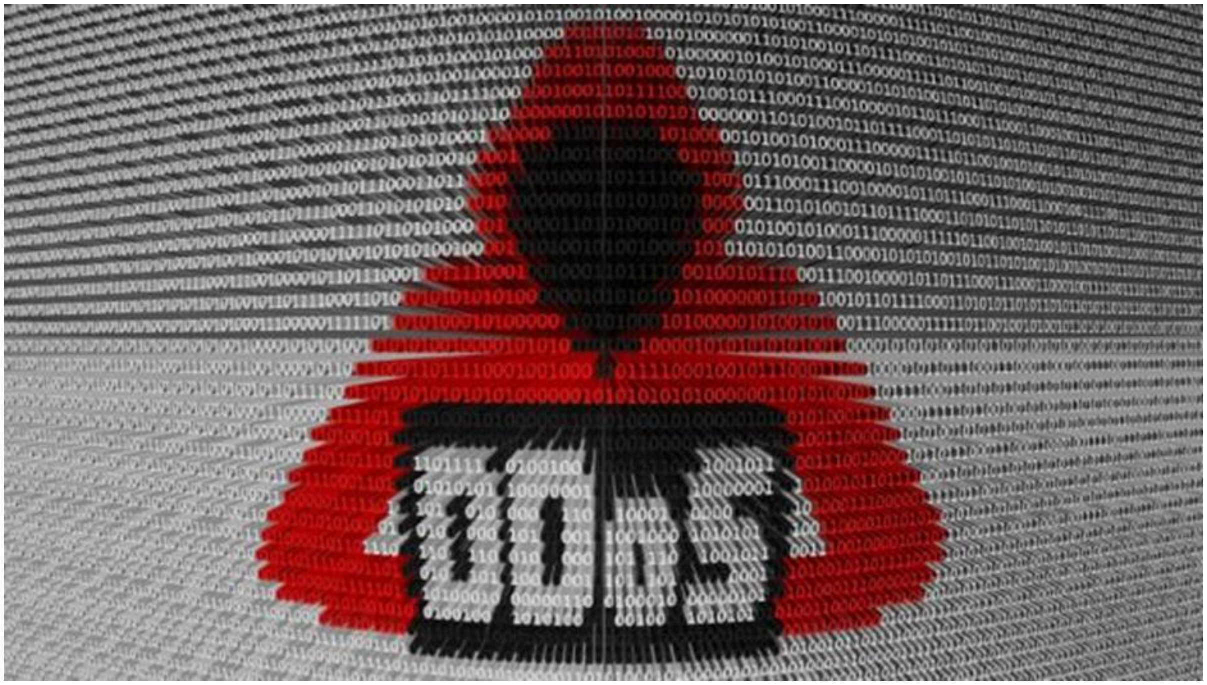

Mitigating DDoS Attacks in MANETs Using Protection Nodes

6G6Z1013 ASSIGNMENT PART 2

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

Abstract and Keywords

Mobile Ad Hoc Networks (MANET) allow mobile nodes to connect to one another dynamically and freely with no predetermined network topology. Although this provides a flexible network it also creates a large security risk and leaves the network vulnerable to Distributed Denial of Service (DDoS) attacks. In this paper, the author looks into the mitigation of such an attack using Protection Nodes placed within the network. The author then compares this form of mitigation against other forms of mitigation and evaluates them. Through research and critical analysis of the Protection Node system, the author found that this system is no better at protecting the network from DDoS attacks than any other currently implemented system or proposed system and actually fails to protect the network itself from this form of attack.

Keywords: MANET, DDoS, Mitigation, Protection Nodes

Contents

Table of Terms

Term	Description
MANET	Abbreviation of Mobile Ad-hoc Network
DDoS/DoS	'any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service' (Techopedia.com, 2017)
Botnet	A network of computers that work together to deploy a DDoS attack
Node	A single device connected to a network
IDS	Intrusion Detection System

Table 1: Table of Terms

List of Images

1) 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. As the topology of the network is almost constantly changing a new protocol needed to be devised that would allow the nodes of the MANET to communicate effectively. This protocol is known as the Ad Hoc On-Demand Distance Vector (AODV) protocol (see appendix 1). 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 2) and how to defend the MANET against them (Mitigation). In particular mitigating against these attacks using Protection Nodes (PN) as outlined in paper [2]. I will also be comparing this form of mitigation against other forms to see how it compares.

2) Literature review study

A. PROTECTION NODES

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.

B. REPUTATION SCORE

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.

C. FLOW MONITORING TABLE

In paper [5], the authors, S. A. Arunmozhi et al., propose a defence 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.

D. IDENTITY REPLACEMENT

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 [8] based on an Identity Replacement (IR) mechanism above the existing network layer in order to provide this stable topology.

E. TRAFFIC FLOW ALGORITHM

In paper [9], 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 preventing DoS attacks. Within this approach when a malicious node is discovered, rather than simply dropping all the packets from this node, the node itself is removed from the network.

3) 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 analyse each of the different approaches and will compare each of the other methods to the Protection Node method.

A. PROTECTION NODES

The Protection Node (PN) method has multiple benefits when attempting to mitigate DoS attacks. The nodes are divided into groups depending on their level of importance within the MANET. This system can successfully defend the higher importance nodes by using the lower importance nodes as their protection nodes. The impact of using this node as a protection node is minimal and the MANET will continue to function as normal. The malicious nodes, when identified, have a node assigned to them to monitor their traffic output and to determine if, in fact, this is the malicious node within the MANET and blocking all of its traffic if it is. A failure within this system is that only the high importance nodes can be successfully protected, thus leaving the rest of the nodes within the network vulnerable to attack and there is potential that the protection node itself could become compromised therefore causing the system to fail and the important node to be left open to attack.

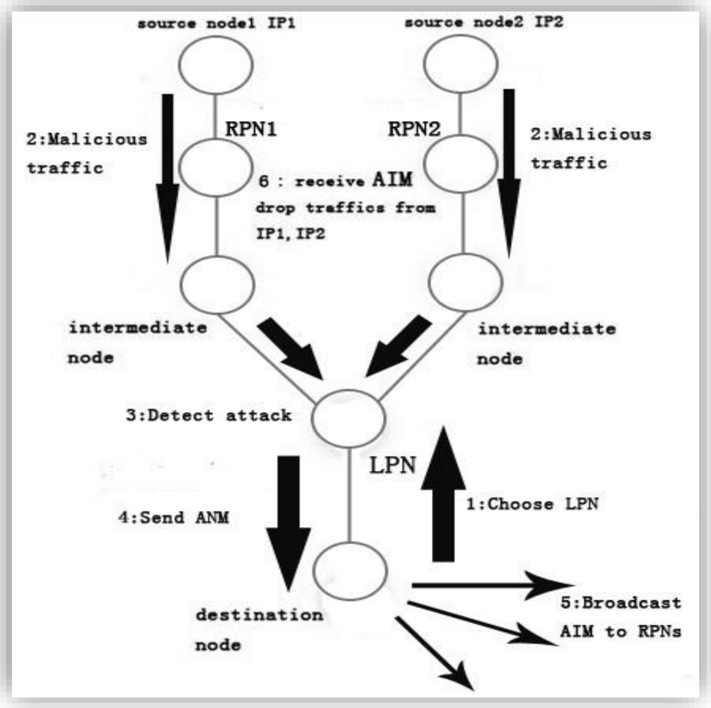

Figure ii: Process of defending DDoS attack

B. REPUTATION SCORE

The Reputation Score (RS) method uses a three step system for determining whether or not a node can participate in the forwarding of packets within the network. The network is split up into groups (Clusters). Calculations are then made to determine the most viable node to become the Cluster Head. A single node is then 'promoted' to become a Cluster Head. All of the traffic for this cluster of the network will pass through this single node. This system is a proposed algorithm, however, unlike the other proposed systems the author researched, there has been no testing within a simulation environment to determine how successful the algorithm may be. The proposed algorithms within the paper are not as efficient as they potentially could be and more research needs to be done into this. Furthermore, the mobility of the cluster head nodes has not been covered within the paper. What if that specific node was to move out of range of the rest of its cluster? Again, more research is needed into overcoming this potential issue.

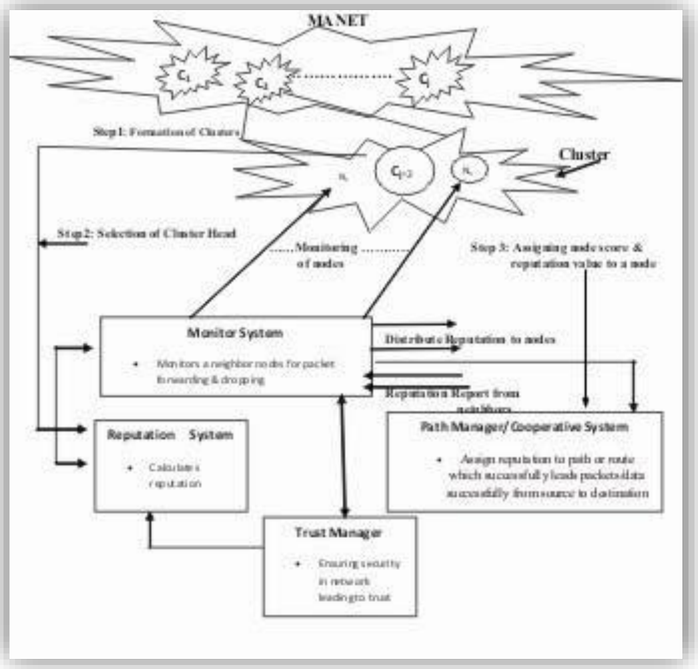
MANET
C1
C2
Cj
Step 1: Formation of Clusters
Cluster
Cj+2
Step 2: Selection of Cluster Head
Monitoring of nodes
Step 3: Assigning node score & reputation value to a node
Monitor System
Monitors a neighbor nodes for packet forwarding & dropping
Distribute Reputation to nodes
Reputation Report from neighbors
Reputation System
Calculates reputation
Path Manager/ Cooperative System
Assign reputation to path or route which successfully leads packets/data successfully from source to destination
Trust Manager
Ensuring security in network leading to trust

Figure iii: Cluster Formation and Cluster head election on basis of node Reputation and node score value

C. FLOW MONITORING TABLE

The Flow Monitoring Table (FMT) method makes use of an FMT deployed on each node of the network to monitor and maintain the traffic flow. The table consists of flow id, source id, packet sending rate and destination id. The updated FMT is sent along with each flow to the destination. If congestion is found within the network then an Explicit Congestion Notification bit is sent to notify the sender nodes about the congestion. Once the sender nodes receive this bit they will decrease their sending rates. If this congestion does not reduce then the updated FMT is checked and the reduced packet sending rates are compared to the old packet sending rates. If these rates are the same then the node is determined to be the attacker. Once the attacker has been identified then all of the packets from this sender are discarded and thus, the attack is thwarted. This method detects and discards traffic from malicious nodes very well in a simulated environment and decreases the amount of impact the attackers have on the network once they have been discovered. The proposed method seems simple to deploy within a network, however, with the FMT being deployed and updated at every node, could this increase the amount of computational overheads and decrease the timeliness of the packet distribution within the network?

D. IDENTITY REPLACEMENT

The Identity Replacement (IR) method attempts to increase the stability of the network topology to increase the support for Traceback. The stability comes from applying a virtual overlay of the network that contains logical ID's for the physical ID's of the nodes within the network. If any of the nodes disconnect from the network and are replaced with another node then the physical ID of the node will change however, the logical ID of this node will stay the same. This allows for the topology of the overlay to become much more stable and, as such, Traceback can then be performed to track attackers within the network. The experiments run by the authors of the paper simulate the effects of the IR-AODV protocol against the AODV protocol alone. The results of the simulations show a dramatic improvement in the stabilising of the network topology and thus improving the performance of Traceback within a MANET. However, there is no discussion on what the overhead of such a system would be and how this would affect the network itself.

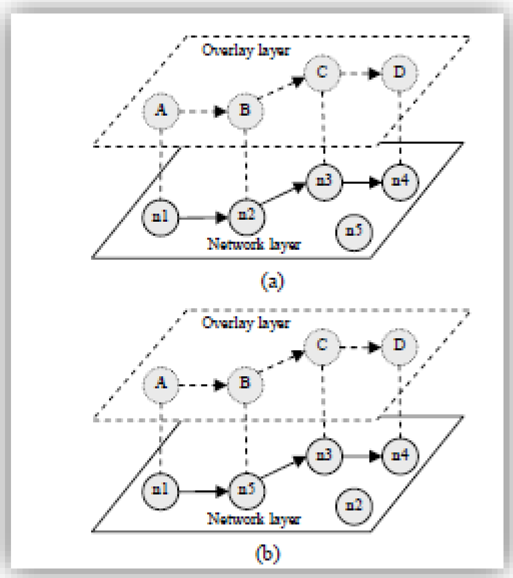

Figure iv: Migration of two layer topology

E. TRAFFIC FLOW ALGORITHM

The Traffic Flow Algorithm (TFA) method attempts to detect and manage malicious nodes in a MANET using AODV. This is proposed to be done using a five-step algorithm. Step one is to create a threshold for the number of packets dropped, step two is to monitor the sequence numbers of the packets, step three is to maintain a count of the packets dropped, step 4 is to compare the number of packets dropped to the threshold and if this number is greater than the threshold then raise the alarm and delete the routes of the nodes based on the amount of packets dropped by them, and finally, step five is to maintain a log file to determine whether or not the identified nodes are responsible for the packets being dropped and, if so, the node is dropped from the network. This proposed method seems simple and yet effective in a simulated environment when attempting to find and manage malicious nodes in a network. The method proposed needs research into the effectiveness of the algorithm in a larger network and with a larger DDoS attack being implemented. Also, research into the potential overhead of this algorithm needs to be completed.

F. COMPARISON TABLE

Design	Pros	Cons
PN	Small cost. No significant impact on the network.	LNP itself could be targeted by attackers. If the detector cannot determine the address of the attacker then the attack will continue. Cannot protect the network itself from attackers that just aim to congest the network itself rather than attacking a specific node.
RS	Cluster Heads form a virtual spine of the network and work to maintain routing states.	Could potentially degrade the Quality of Service (QoS) of the network and decrease performance when scaled up. The mobility of Cluster Heads not taken into account.
FMT	Accurate detection of DDoS attack flows. Simple to deploy within the network	Potential overheads could cause performance issues resulting in a degraded QoS of the network.
IR	Improves the ability to trace attackers within the network.	Potential overheads could cause performance issues resulting in a degraded QoS of the network.
TFA	Simple yet effective. Low cost.	Scaling the design up could create a low cost/benefit ratio, low throughput and large overheads.

G. EVALUATION

Each of the researched solutions has their own set of pros and deal with a form of DoS attack in their own way. However, each of them has 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 protection node system seems no better than any of the other currently implemented designs or proposed designs. It can successfully defend the important nodes of the network from attackers and does so with little cost and no adverse effects on the network itself. However, there has been several oversights during the design of the protection node system as the LPNs themselves can still be targeted by attackers and there has been no approach to mitigating an attack on the network itself rather than individual nodes.

4) Future Scope

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.

5) 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 is the main reason for their lack of security. Without a centralised administrative figure, there will always be security issues. This paper was aimed at looking at the Protection Node form of Mitigation of DDoS and as such the author can only conclude that the system is no better than any other system that is currently in place or that has been proposed. Even though the system can successfully mitigate DDoS attacks that are aimed at the important nodes of a network, the lesser nodes are still vulnerable to attacks as well as the LPNs themselves. Also, the network itself is vulnerable to attack as the protection nodes cannot protect the network against attackers that look to flood the network with congestion by simply sending a monolithic amount of broadcast packages that would potentially cripple the network.

Appendices

APPENDIX 1

AODV Protocol

The Ad Hoc On-Demand Distance Vector protocol is a mobile network routing protocol designed for use within a MANET. It offers quick adaptation to dynamic link conditions of the network, it has a low processing and memory overhead capability as well as a decreased network utilisation. When a node on the network needs to send a packet it requests a route to the destination node and is provided with it. The routes of the network are only considered active while data packets are travelling along them.

'When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination.' (Ietf.org, 2017)

APPENDIX 2

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.

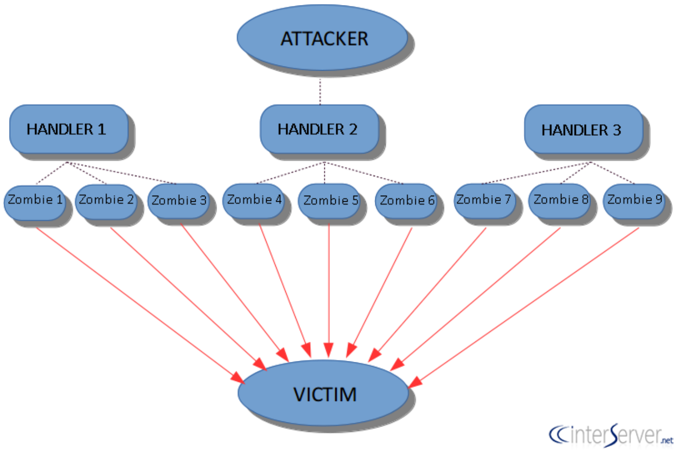

Figure v: How a DDoS attack works

Images Used

[i] Image Source: Adobe Stock

[ii] Image Source: 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.

[iii] Image Source: 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.

[iv] Image Source: 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.

[v] Image Source: Interserver.net, (2017). *How A DDoS attack works*. [image] Available at: https://www.interserver.net/tips/kb/troubleshoot-ddos-attack/ [Accessed 19 Mar. 2017].

References

Perkins, C., Belding-Royer, E. and Das, S., (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561).

[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.

[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] Savage, S., Wetherall, D., Karlin, A. and Anderson, T., (2000). "Practical network support for IP traceback." In ACM SIGCOMM Computer Communication Review (Vol. 30, No. 4, pp. 295-306). ACM.

[9] 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].

Ietf.org. (2017). "Request for Comments: 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing." [online] Available at: https://www.ietf.org/rfc/rfc3561.txt [Accessed 19 Mar. 2017].