A Taxonomy of Defence Mechanisms to Mitigate DoS Attacks in MANETs

A.F.Alsumayt and J.Haggerty

School of Science and Technology, Nottingham Trent University, Clifton Campus, Clifton Lane, Nottingham, NG11 8NS, United Kingdom
e-mail: Albandari.Alsumayt2013@my.ntu.ac.uk; john.haggerty@ntu.ac.uk

Abstract

In recent years MANETs (Mobile ad hoc Network) have had a large prevalence in many sectors. Due to their nature, MANETs have faced some challenges, especially with regard to security;- dynamic topology, power and bandwidth constraints and the absence of central administration make MANETs vulnerable to many attacks. DoS (Denial of Service) attacks are a major problem for the network. These attacks deplete resources and greatly degrade network performance. In this paper, a taxonomy of the defence mechanisms is identified and their advantages and disadvantages are discussed. As posited in this paper, this taxonomy provides the basis for the development of an approach to detect DoS attacks in MANETs.

Keywords

MANET, Denial of Service, Intrusion detection

1. Introduction

It is notable that MANETs (Mobile *ad hoc* network) have received tremendous attention over the last few years with the rapid growth of the interconnected network technologies. When there is a pressing need to communicate between devices, MANETs help to set up a connection without any fixed infrastructure. It is a type of wireless network and includes the contents of a group or collection of nodes that communicate with each other without any central form of administration such as access points. Each node in MANET is considered to be a router and a host for forwarding and receiving packets. The use of MANETs have been proposed for emergency and disaster situations and may be utilised in other environments such as conferences, meeting rooms, the military arena and airports. There are other advantages of MANETs such as high level of convenience, small size, support for many different devices (laptops, smart phones, iPads, etc) as well as the low costs of setting the network up and high mobility. There are also some disadvantages such as power constraints, link failures and a lack of security. Indeed, as there is little or no central management in MANETs, security awareness is critical.

In the MANET environment there are many problems that need to be tackled such as quality of service (QoS), optimization, scalability and security issues. The main interest here is security; in particular, the mitigation of DoS (Denial of Service) attacks. As discussed above, the continuous changing topology of MANETs, its dynamic nature, and the fact that it has no central administration makes it vulnerable to many attacks. Applying security to MANETs is a complex task. Many security

parameters need to be applied for a MANET to be considered secure: confidentiality, integrity, availability, non-repudiation and authentication. As such, many challenges to security in MANETs remain. First, as mentioned above, the power and resource constraints on nodes limit cryptographic measures which are used to apply a secure connection in other environments. In addition, bandwidth constraints can prevent nodes from communicating with other nodes which are not in the network domain. Second, static configuration is not generally effective in a MANET environment. For example, any node can pretend to be a legitimate node and provide incorrect information. Third, nodes without a central management and with dynamic topologies may lead to compromise and the ability to launch some attacks, such as DoS.

A DoS attack paralyses and degrades the performance of the network resulting in the unavailability of key network nodes. This kind of disruptive attack affects and causes harm in many ways such as financial losses, time wasting, and wasting of resources. If one popular and successful website such as Amazon is affected by such an attack even for an hour, the financial losses can be huge. There is not always a clear reason for the attackers to perpetrate such an attack and range from personal reasons such as the desire for revenge against certain organisations, gain prestige or the respect of the hacker community or for political reasons. Thus MANET is vulnerable to DoS attack. This is due to a number of contributory factors; their open nature, lack of authentication, heterogeneity of devices, no central control beyond network tasks such as IP address configuration and allocation, and lack of computing resources for security countermeasures. There are many types of DoS attack and each attack has a different mechanism requiring a specific algorithm to detect it.

The novelty of this paper is that existing taxonomies have been posited for DoS attack in general but not specifically aimed at MANETs. The aim of this paper is to examine approaches to DoS attacks in other network environments to determine the requirements for a novel approach to detect such attacks in MANETs. This paper therefore posits a taxonomy of such approaches.

The rest of the paper is organized as follows. Section 2 illustrates related work. Section 3 presents the taxonomy of different approaches to handle DoS attacks on MANETs and a discussion of this taxonomy and its applicability to MANETs. Finally, section 4 concludes the paper and proposes future work.

2. Related work

This section outlines related work in MANET and DoS attack mitigation, beginning with the common or traditional methods such as firewalls. Different approaches are also illustrated with regard to preventing DoS attacks.

Madhurya et al. (2014) identify the advantages and limitations of MANETs. In addition, a novel cryptographic algorithm named Disturbance Detection System (DDS) has been proposed in order to detect attacks on MANET. Garg et al. (2009) also specify the challenges to MANET such as dynamic topology, bandwidth and power constraints. The MANET architecture is shown below in Figure 1.

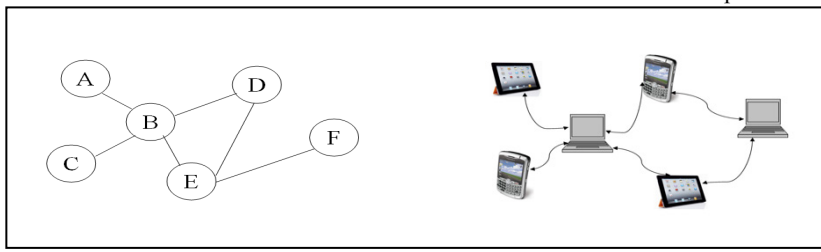

Figure 1: The MANET architecture

Khan and Vasta (2011) present a novel mechanism to detect DDoS (Distributed Denial of Service) attacks on MANETs based on reputation. The architecture of both DoS and DDoS attacks are shown below in Figure 2.

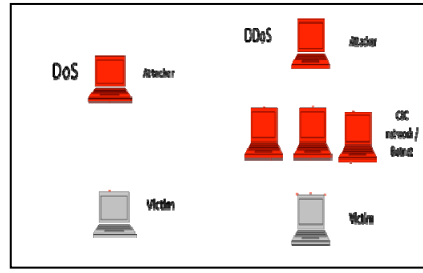

Figure 2: The architecture of DoS and DDoS attacks

Many defence mechanisms have been used to mitigate DoS attacks on MANET. Gupta et al. (2012) posits some common defence approaches against DoS attacks such as firewalls. A firewall is a system that is set up in order to monitor and control traffic between two networks. Unfortunately, the traditional firewall is considered to be unreliable because firewalls cannot distinguish between normal traffic and DoS attack traffic. Moreover, firewalls are susceptible to this type of attack as they act as a chokepoint between internal and external networks. Firewalls have simple and basic rules, such as allowing or denying some ports or IP addresses. In addition, most people do not keep their firewall up to date, which raises the level of vulnerability. Thus, distributed firewalls work efficiently in MANETs to prevent DoS attack. . In addition, many small devices do not have the computational power to employ such countermeasures or provide only limited security functions.

Akram et al. (2009) point out that distributed firewalls use a central policy framework which defines inbound and outbound movements, and seek to define what is permitted and appropriate connectivity. The distributed firewalls are designed to be reconfigurable so it can be considered that they are used in filtering in MANETs.

Filtering is another technique to mitigate DoS attacks. Filtering could be local or global. Local filtering means that filtering is implemented on the victim's side or the local network. This method is considered a short-time solution, and involves installing a filter on the local router to stop the infiltrating IP packets. DoS attack exploits the deficiencies of the internet and sometimes local filtering is unable to solve the problem. Global filtering is better to mitigate DoS attacks from the logical standpoint. In global or coordinated filtering, the idea is based on preventing any

accumulation of malicious packets in an appropriate time frame. Filters are installed throughout the internet, thereby helping victims to disseminate information about the detected attacks. As a result, the malicious packets will be stopped early. This method is effective, even though the intruder succeeds in seizing many botnets to launch the attack. Tyagi et al. (2013) assume that this technique cannot be considered reliable as sometimes the packets can overwhelm the router and cause a DoS attack.

Tan et al. (2005) propose the statistical filtering concept. This is considered to be a reactive method of detecting DDoS attacks in MANETs by using traffic profiling for the purpose of filtering and detection. The main advantage of using this mechanism is that the packet delivery ratio is raised, whereas the average end-to-end delay is clearly decreased. The major limitation of using this method is the cluster-based routing protocol filtering mechanism.

An IDS (Intrusion Detection System) is another common approach to mitigate DoS attack. Shrestha et al. (2010) propose a novel intrusion detection system to detect malicious nodes that perform DoS attacks. By exploiting the information which is available this protocol helps to improve the detection process drastically. Sahu et al. (2013) classify the different attacks and methods which are used for IDS and specify some challenges and limitations of IDS such as resource usage problem, reliability problems, and fidelity problems.

Another method of detecting DoS attacks is Watchdog, as proposed by Marti et al. (2000). This method shows how it is possible to increase the throughput of the network despite the presence of malicious nodes. The aim of this method is to detect nodes that are misbehaving. Watchdog is set in this node when forwarding a packet to ensure that the next node will also forward the packet in the same path. Watchdog performs this task by listening to all nodes within the transmission range in the network. The node will be tagged as a misbehaving node if it fails to forward the packet to the next node. The limitations of the Watchdog scheme fail to detect malicious nodes in some situations as posited by Buddha (2013). For instance, Watchdog cannot detect malicious nodes in the presence of receiver collisions, limited power for transmission or false misbehaviour reports. These limitations mean the Watchdog method is not an ideal method of detecting DoS attack. According to the easy implantation and the effectiveness of the Watchdog mechanism, many methods, such as Pathrater, use it as a base. With the Pathrater method, each node uses the information which is obtained from Watchdog to rate its neighbours. Neighbour nodes can be classified as members, fresh, unstable or malicious.

Jin et al. (2006) propose ZSBT traceback which is another method of detecting denial of service. Traceback is a useful method which helps identify the source of an attacker. Belenky et al. (2003) assume that manual traceback schemes have many disadvantages, such as management cost, inaccuracy of results and slow tracking speeds.

Ioannidis et al. (2002) posit a pushback approach to detect DDoS attacks. In a pushback mechanism, routers are enabled to identify the high bandwidth aggregates that contributes to the congestion rate and helps to limit it.

Khan and Vasta (2011) propose another scheme to detect DoS attacks in MANET based on using a reputation-based incentive mechanism. In order to perform reputation data management in distributed states, the authors suggest a clustering architecture. It might be possible to compromise a DoS attack via the information exchange and via collaborative monitoring.

A related method which is used to avoid DoS attack in MANET is trust between nodes. The first research into trust management for network security was carried out by Blaze et al.(1996).

DiDDeM (**Di**stributed **D**oS **De**tection **M**echanism) is another method for the early detection of DoS attack, which is described by Haggerty et al. (2005). The strength and effectiveness of this scheme stem from the early detection of DoS which enable a quick response in order to block the attack on the attack source side rather than on the intended victim's side.

This paper aims to find a new method of detecting DoS attacks on MANET, taking into consideration the existing methods of detecting DoS attacks. In the next section, a taxonomy is outlined which can help to develop a new approach to detecting DoS attacks in the MANET environment. The main contribution of this study is to: Determine the features and limitations of the existing defence approaches, and use these results to develop a novel approach to mitigate DoS attacks on MANETs.

3. A Taxonomy of DoS attack in MANET

The term 'taxonomy' refers to an order or classification of things according to specific conditions. In this paper, a taxonomy of defence approaches to detect DoS attacks on MANET is discussed. General detection methods to detect DoS attack, with their advantages and limitations are explained. As suggested in Section 1, there are many challenges to MANET security and it can become vulnerable to severe attacks, such as DoS attacks. There is a pressing need to mitigate such attacks in order to maintain security in the network. The victims of this attack could be a whole network, resources, or users. This Section presents taxonomy based on identifying the advantages and disadvantages of existing defences against DoS attack.

The taxonomy of common detection methods to detect DoS attack with their advantages and limitations are shown in Table 1.

Detection method	Advantages	Disadvantages
Firewalls and proxies	Has simple rules and easy to perform commands. (Gupta et al, 2012)	Firewalls cannot prevent DoS attack because it is hard to it to distinguish between legitimate and malicious traffic. (Gupta et al, 2012)
Ingress/ egress filtering	Success in thwarting DoS attacks before they are launched. (Jain et al,2011)	Unreliable in compromised machines – difficult to deploy this method universally. (Tupakula et al,2003)
Monitor process based on Bloom filter technique	Success in detecting attacks such as SYN flooding attack. (Geneiatakis et al, 2009)	Resource consumption such as CPU time, bandwidth, and memory during detection. (Geneiatakis et al, 2009)
Using statistical tests. Determining the threshold value of the normal traffic flow and checking it against incoming threshold. Comparing income traffic with normal traffic is the main method used here, in order to detect attacks.	This method gives an impression of the packet flow. (Chen ,2009)	It is difficult to model and even estimate the network traffic. (Chen ,2009)
Abnormal statistical method based on correlation analysis. The main idea of this method is based on extracting the anomalies from the network traffic	This method is intended to detect this attack compared with other methods by monitoring the derivation in co-relation analysis of the network traffic. (Li et al,2008)	The efficacy of this method could be unreliable if the attacker perpetrates a DoS attack using a low rate. (Li et al,2008)
An AIDS (Agent Intrusion Detection System) based on Chi-Square statistical method	It is necessary to analyse the variation and the amount of the packet which is sent by the sender. (Leo and Pai ,2009)	As this method is based on statistical analysis, it does not reflect the behaviour of AIDS. There are limitations of the communication performance (latency). (Leo and Pai ,2009)
Using detection method and a prevention algorithm based on a data mining concept	This technique can do a quick identification to determine if the traffic is normal or not. Moreover, this method can detect a DoS attack at an early stage. (Garg and Chawla ,2011)	Overhead in resource consumption such as CPU time and memory. (Garg and Chawla ,2011)
Hybrid IDS (Intrusion Detection System) based on an artificial neural network	Qualitative and quantative analysis has been applied in this method. This approach has a roughly 90% detection rate. (Jirapummin et al,2002)	This method fails to detect modern and current DoS and DDoS attacks. (Jirapummin et al,2002)
Uses fuzzy logic method	This method attains good results in detecting DoS attack. (Tuncer and Tatar ,2008)	It is difficult to model network traffic before and after an attack due to the packet flow characteristics. (Tuncer and Tatar ,2008)
Trust management / reputation	The effectiveness of trust management is that it is possible without any previous interactions so the nodes in the network can participate with an acceptable average of trust relationships of nodes. (Li et al,2012)	It is not based on an entirely decentralised concept, just localised trust management which is essential for policy information. (Li et al,2012)
Using machine learning algorithm	This method success to detect many types of DoS attacks such as ICMP flood and SYN flood attacks. (Suresh and Anitha ,2011)	This method increases the overhead of the network and cannot be integrated with the new types of attacks. Equally important is the redundant alert which is annoying as the attack. (Suresh and Anitha ,2011)

Table 1: the taxonomy of the existing detection methods against DoS attack

Related to Table 1, it can be seen that an optimal approach to mitigating DoS attacks without any flaws is rare. Common approaches such as firewalls, filtering, IDS,

Traceback, and Pushback which help to mitigate attacks are used on both the victim server and source server sides and even between them. Obviously, the nature of a MANET makes it hard to manage an attack. For example, filtering is unreliable for the detection of anomalies in MANET according to the continuous changing topology. Moreover, a firewall cannot prevent malicious nodes in when performing a DoS attack in a MANET according to its architecture. A distributed firewall is designed especially for MANET (Akram et al., 2009) which can protect network bandwidth and also end-host resources. The only problem with a distributed firewall is the need to use cryptographic operations which apply overhead to the network and cause latency.

There are some common disadvantages of the existing approaches such as latency in detection, resource consumption, difficulties in universal deployment, unreliability and difficulty in distinguishing between legitimate and malicious traffic. These flaws mean that the use of these approaches is not completely secure in the MANET environment. For example, monitor process is based on the Bloom filter technique, using a detection method and a prevention algorithm based on a data mining concept, and using a machine learning algorithm containing some of the common limitations.

Abnormal statistical method based on correlation analysis is another method to detect anomalies. The efficiency of this method is better than others to detect attacks like DoS attacks, but not if the attack rate is low. Therefore, identifying an attack in this situation is described as unreliable. In AIDS, there is a need to decrease the latency in detecting malicious nodes, which will be optimal for detecting DoS attacks in the early stages. Using a detection method and a prevention algorithm based on a data mining concept is efficient for the detection of DoS attacks in the early stages. The only drawback of this method is the resource consumption on the network and again that not capable with the energy constrained in MANET. Besides, the hybrid IDS, which is based on an artificial neural network, succeeds in detecting 90% of both DoS and DDoS attacks, respectively. However, this type of intrusion detection system is considered an old method and fails to detect new algorithms or types of DoS and DDoS attacks.

Using the fuzzy logic method gains excellent results for detecting DoS attacks, but it is difficult to deploy it in a MANET, as with a dynamic topology, it is hard to model the packet flow before and after the attack.

One of the modern methods to mitigate DoS attacks is based on trust management and reputation. Vasta (2011) posited the scheme to detect DoS attacks based on reputation between nodes by information exchange. In addition, trust management is considered a separate component of security services within the network. The effectiveness of trust management is that it is possible that the nodes in the network can participate, without any previous interaction, with an acceptable average of trust relationships. The main objectives of this framework are to support localised control and relationships by binding public keys to allow the access control process without complex security authentication procedures. The only limitation of this method is that it is not based on an entirely decentralised concept, just the localised trust management, which is not appropriate in MANET (Blaze et al., 1996).

Furthermore, considering a node as being always malicious or trusted can affect network communication. There is a pressing need to design a novel method to detect a DoS attack on MANET and to consider the limitations of the existing methods, along with the following four factors. First, any node should have an ID number, which establishes its identity. Second, each node should be subject to regular monitoring, so that its state as either normal or malicious can be established. Third, it is crucial to find a way to distinguish between legitimate and malicious traffic which will help in detecting this attack at an early stage and avoiding false alarms. Fourth, time and resource consumption should be considered in developing the new approach. The novel approach should try to correct the weaknesses of some approaches which help to mitigate DoS attacks as much as possible.

This section discusses the results of Section3 and also briefly analyses the elements of the taxonomy.

4. Conclusion and future work

MANETs have risen in prominence in recent years due to the requirement for heterogeneous devices to be networked together seamlessly. However, there are many challenges to this network environment such as power constraints and lack of computational resources available for security functions. This ensures that this environment is vulnerable to many attacks such as DoS. Such attacks can withstand some common defence mechanisms like firewalls. In this paper, a taxonomy of approaches to DoS in larger networks with more computational resources available has been conducted in order to identify the requirements of DoS attack mitigation in MANETs. This taxonomy takes into account the approaches to detection and response to DoS attacks. Future work aims to develop new and novel methods of detecting DoS attacks in MANETs. It will also be necessary to account for the results of these taxonomies, the location of the detectors and the flaws in the existing defence methods in order to mitigate the DoS attack in a better way.

5. References

Akram, S., Zubair, I. & Islam, M. H. (2009, July). Fully distributed dynamically configurable firewall to resist DOS attacks in MANET. In *Networked Digital Technologies, 2009. NDT'09. First International Conference on* (pp. 547-549). IEEE.

Belenky, A. & Ansari, N. (2003). IP traceback with deterministic packet marking. *Communications Letters, IEEE, 7*(4), pp. 162-164.

Blaze, M., Feigenbaum, J. & Lacy, J. (1996, May). Decentralized trust management. In Security and Privacy, 1996. *Proceedings., 1996 IEEE Symposium on* (*pp. 164-173). IEEE.*

Buddha, G. (2013). Improved watchdog intrusion detection systems In MANET. *International Journal of Engineering, 2* (3).

Chen, C. L. (2009). A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test. *J. UCS, 15*(2), 488-504.

Garg, K., & Chawla, R. (2011). Detection of DDOS attacks using data mining.*International Journal of Computing and Business Research (IJCBR), 2*(1).

Garg, N., & Mahapatra, R. P. (2009). MANET Security issues. *International Journal of Computer Science and Network Security, 9*(8), 241.

Geneiatakis, D., Vrakas, N., & Lambrinoudakis, C. (2009). Utilizing bloom filters for detecting flooding attacks against SIP based services. *computers & security, 28*(7), 578-591.

Gupta, B. B., Joshi, R. C. & Misra, M. (2012). Distributed Denial of Service Prevention Techniques. *arXiv preprint arXiv:1208.3557.*

Haggerty, J., Shi, Q., & Merabti, M. (2005). Early detection and prevention of denial-of-service attacks: a novel mechanism with propagated traced-back attack blocking. *Selected Areas in Communications, IEEE Journal on, 23(*10), 1994-2002.

Ioannidis, J. & Bellovin, S. M. (2002). Implementing pushback: Router-based defense against DDoS attacks.

Jain, P., Jain, J., & Gupta, Z. (2011). Mitigation of Denial of Service (DoS) Attack.*International Journal of Computational Engineering & Management IJCEM, 11.*

Jin, X., Zhang, Y., Pan, Y. & Zhou, Y. (2006). ZSBT: A novel algorithm for tracing DoS attackers in MANETs. *EURASIP Journal on Wireless Communications and Networking,* 2006(2), pp. 82-82.

Jirapummin, C., Wattanapongsakorn, N., & Kanthamanon, P. (2002). Hybrid neural networks for intrusion detection system. In *ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications* (pp. 929-932).

Khan, R., & Vatsa, A. K. (2011). Detection and control of DDOS attacks over reputation and score based MANET. *J Emerg Trends Comput Inf Sci, 2*(11), 646-655.

Leu, F. Y., & Pai, C. C. (2009, August). Detecting DoS and DDoS Attacks using Chi-Square. In *Information Assurance and Security, 2009. IAS'09. Fifth International Conference on* (Vol. 2, pp. 255-258). IEEE.

Li, W., Parker, J. & Joshi, A. (2012). Security through collaboration and trust in manets. *Mobile Networks and Applications, 17*(3), pp. 342-352.

Li, Z. L., Hu, G. M., & Yang, D. (2008, July). Global abnormal correlation analysis for DDoS attack detection. In *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on* (pp. 310-315). IEEE.

Madhurya, M., Krishna, B. A., & Subhashini, T. (2014). Implementation of Enhanced Security Algorithms in Mobile Ad hoc Networks. *International Journal of Computer Network & Information Security, 6* (2).

Marti, S., Giuli, T. J., Lai, K. & Baker, M. (2000, August). Mitigating routing misbehaviour in mobile ad hoc networks. In *International Conference on Mobile Computing and Networking: Proceedings of the 6th annual international conference on Mobile computing and networking* (Vol. 6, No. 11, pp. 255-265).

Sahu, L. & Sinha, C. (2013). A cooperative Approach to understanding the behaviour of intrusion detection systems in mobile ad hoc networks. *International Journal Of Computer Science, 1*(1)

Shrestha, R., Han, K. H., Choi, D. Y., & Han, S. J. (2010, April). A novel cross layer intrusion detection system in MANET. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on* (pp. 647-654). IEEE.

Suresh, M., & Anitha, R. (2011). Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. *In Advances in Network Security and Applications* (pp. 441-452). Springer Berlin Heidelberg.

Tan, H. X. & Seah, W. K. (2005, December). Framework for statistical filtering against DDoS attacks on MANETs. In *Embedded Software and Systems, 2005. Second International Conference on* (pp. 8-pp). IEEE.

Tuncer, T., & Tatar, Y. (2008, April). Detection SYN flooding attacks using fuzzy logic. In *Information Security and Assurance, 2008. ISA 2008. International Conference on* (pp. 321-325). IEEE.

Tupakula, U. K. & Varadharajan, V. (2003, February). A practical method to counteract denial of service attacks. In *Proceedings of the 26th Australasian computer science conference-Volume 16* (pp. 275-284). Australian Computer Society, Inc.

Tyagi, S. S. (2013). Analysis of techniques for mitigating DOS attacks on MANET. *International Journal of Engineering, 2* (4).