A cache based Defence Mechanism for Eliminating DoS Attack in Wireless Mesh Network (WMN)

Anju Singh [1], Ms. Nisha Pandey[2],

M-Tech Student[1], Assit. Prof. [2] & Department of CSE & Shri Ram College of Engg. & Mgmt
Palwal, Haryana, India

Abstract:

Wireless Mesh Networks (WMNs) are developing to be an attractive substitute for offering high bandwidth broadband facilities to a large community of subscribers, they arise several security issues. The current attraction of research in WMNs is mainly concentrated on evolving Load balancing mechanism and multi-path routing protocols; and security is very much in its early stage. The Mesh Routers (MRs) cooperatively send the traffic towards the Internet gateway (IGW). The MRs self-configurable architecture paves way for dangerous attackers to carry out a Denial-of-Service attack (DoS) on the MRs by broadcasting the network with a huge amount of traffic; hence building the system inaccessible to the actual subscribers. In this research paper, we introduce a cache based defense at the MRs to detect broadcasting type DoS attacks. We utilize a *most frequently employed* cache technique to identify these flows and arise an early alert to control them. We efficiently avoid any performance reduction by discarding the detected attack flows with the forwarding routers. Simulation results show that our mechanism provides an active line of defense against DoS attacks.

***Index Terms*—DoS Attack, MFU, Internet Gateway, Spoofing**

I. INTRODUCTION

Wireless Mesh Network (WMN) is developing to be a novel substitute for wireless Internet connectivity as it eliminates the requirement for wired infrastructure at each Access Point (AP) and Mesh Router (MR) [1]. A typical WMN contains a hierarchical architecture is composed of three layers as depicted in Figure 1. Internet Gateways (IGWs) are on the top of hierarchy which is linked to the wired internet. They make the backbone infrastructure for offering internet facility to the second level entities. The second level of hierarchy contains wireless mesh routers (MRs) that eliminate the requirement for wired infrastructure at each MR (a.k.a Access Point) and broadcast their traffic in a multi-hop manner towards the IGW. The underlying paradigm of WMNs is same as multi-hop ad hoc networks [2]. The security concerns in WMNs are multi-dimensional owing to its hierarchical architecture. The MRs build the skeletal backbone of WMNs and high security is needed to secure them. As the WMNs perform in the unlicensed 2.4 GHz band, a dangerous intruder can easily conduct a Denial of Service (DoS) attack. Unlike a responsive flow i.e. TCP that follows its rate with respect to the end-to-end congestion; a DoS attack flow constantly pumps traffic into the network to lead congestion. It also causes to the starvation of another ingenious flows. A DoS attack raise critical threat to WMNs as it can be easily established by an intruder by creating spoofed source traffic.

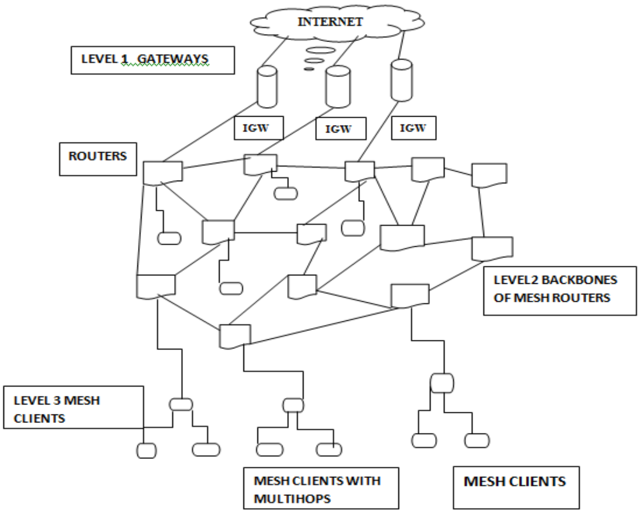

Figure 1: Hierarchical architecture of WMN

A DoS attack raise critical threat to WMNs as it can be easily established by an intruder by creating spoofed source traffic. A flooding type DoS attack is complicated to stop by the victim node. The IP layer architecture is such that any node can create traffic towards any other destination node and the destination node is helpless in ending the traffic before it arrive the network. The basic features of WMNs also provide an easy ground for carrying out DoS attack. As the large amount of traffic in a WMN is predominantly go towards the IGW, the routes leading to IGW are highly congested. Hence, it is easy to carrying out a DoS attack on these over-loaded MRs which would further reduce the network performance.

The closeness of an intruder to the IGW, measures the effect of DoS attack on the network. A DoS attack from a closest mesh clients introduce a critical threat to longer hop flows which already obtain poor service because of the IEEE 802.11 poor performance in a multi-hop network. .Unlike WLANs or cellular network where the backbone infrastructure is maintained by a single authorized entity, a WMN can be maintained either by a set of independent subscribers or can be partially maintained by a single ISP. Hence, the type of management style used in established WMNs, selects the robustness of the network to an antagonist. A WMN automatically arranges to assimilate a newly connected node [3]. Hence, it is easy to present a rogue MR and begin interrupting the network facilities. Using even a sophisticated authentication technique is an insufficient defense to stop attackers in a public network i.e. WMN. As MRs are generally deployed in public place i.e. buildings, rooftops, towers, poles, traffic signals, even an trusted node can be easily tampered by an antagonist. There are many types of DoS attacks i.e. SYN, Smurf and Teardrop attack that change in their sophistication degree [4]. A DoS attack is a more bitter model of DoS attack; where an attack is established synchronously from various compromised innocent hosts operated by a remotely hidden intruder. In a SYN attack, the attacker feats the TCP’s 3- way handshake technique by opening several fraud links with the server. The intruder then refuses to forward the TCP ACK, thus withholding the resources at the server indefinitely. In a Teardrop attack, the intruder feats the fragmentation mechanism at a router, by introducing a wrong offset, thus leading unsuitable re-assembly. A Smurf attack is a more sophisticated attack, in which an intruder forwards devised ICMP echo request to large number of innocent nodes on the network; which in return forward the victim unknowingly by forwarding ICMP response packets.

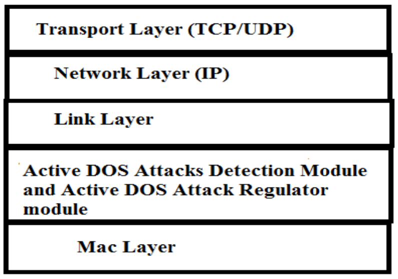
Transport Layer (TCP/UDP)
Network Layer (IP)
Link Layer
Active DOS Attacks Detection Module and Active DOS Attack Regulator module
Mac Layer

Figure 2: Location of our proposed module

In this research paper, we introduce a new mechanism that introduces the problem of combating DoS attacks by arising an early alert. We use a simple mechanism that manages minimal state information at every router and functions independent of the fundamental queuing technique at the routers. We use two components at every router: *Active DoS attack detection module* and *DoS attack regulator module*. The active DoS attack detection module detects the high bandwidth attack flow depending on *Most Frequently Used* (MFU) cache discipline. The DoS attack regulator module uses a trace notifier that employs rate limit along the upstream routers by which the attack flow travels. Thus, it efficiently prevents the starvation of other innocent flows. We implement the introduced mechanism just above the MAC layer and do not need any modification in the MAC firmware of the routers. Fig. 2 shows the physical positioning of our introduced mechanism.

II. RELATED WORK

In this section, we discuss the related work in the field of combating DoS attacks and examine its applicability for protecting WMNs from DoS attacks. Various mechanisms have been introduced in the literature to prevent DoS attacks. The main line of defense against DoS attacks can be widely categorized into few wide fields i.e. traceback scheme, filtering schemes, and rate limiting schemes. The first two mechanisms defend the victim of an attack and a rate based mechanism protects the network itself from observing a DoS attack. Ferguson et al. [5] introduce to utilize ingress filtering as a preventive phase against spoofing of IP address. Park et al. [6] introduce a distributed packet filtering technique to identify source IP address spoofing utilizing BGP routing information. Yaar et al. [7] introduce Pi marking mechanism to enable the victim to identify spoofed source IP address. Firstly, these mechanisms are inefficient against bandwidth flooding attacks which impress routers upstream from the victim. Secondly, they do not stop compromised machines with right source address in carrying out DoS attack and achieve considerable overhead on the ISP. A different kind of combating DoS attack includes identifying an attack in progress and establishing the route of attack causing to the real attacker called as traceback [8]. The trace data can be probabilistically conducted in-band within the 16-bit identification field of the packets IP header as introduced by Savage et al. [9].

Watchdog monitoring technique was proposed by Marti *et al.* [10] to detect misbehaving nodes in wireless ad hoc networks. This technique can be employed in WMN and it was the former trust technique which is the basis of several defense mechanisms. In their mechanism, every sensor node has its own watchdog that maintains and stores the behaviors of its one neighboring hop. The watchdog method of every node saves the routing table which is about the performance bad or good of the neighboring nodes. When the node M forwards a packet to its neighboring node N, the watchdog of M detects whether N send the packet to the BS or not by utilizing the sensor’s overhearing capability. The benefit of this type of security technique is that the principle is simple, complication is low and it adjusts to the WMN totally. But this mechanism can only solve restricted situations of harmful nodes packet discarding.

Depending on Watchdog mechanism, Yu *et al.* [11] explain various representative methods to make a trust model. In their research paper, Bayesian mechanism, Entropy mechanism, Game-theoretic mechanism, and Fuzzy approach are introduced. By the various algorithms, we change the information which comes from the watchdog mechanism to statistical data for weighing the behaviour of maintained node whether bad or good. The design of trust measurement is proposed at examining the situation of detecting a forwarding node. We expect to select the node whose all types of attributes are comprehensively correct as the adjacent-hop node.

Employing various trust models, the reputation value of a node will be distinct. When the trust model is evaluated, we should adjust a fair threshold. If a node’s reputation value is less than the threshold, it will be stored as a harmful node. Furthermore, based on the WMN's trust technique, the detection of these harmful node will or will not be forward to the remaining nodes and base station in the WMN.

Harmful node may be the intersection of various routes, that is to say this type of node may broadcast more than one source node's data. It can discard the data package of one or many node between those source nodes so that the determination to this harmful node from every source node is different. Hence, this type of harmful node cannot be rejected in time. Hence, a detection technique depending on neighbor nodes managing was introduced. By hearing to each other, every node considers statistics of the no. of broadcasted packets by neighboring nodes. Then, every node computes the reputation values of its neighboring nodes. All reputation values information will be set up for computing every node's weighted credibility. Various works [16] [17] that utilized neighbor-based mechanism have been presented for mitigating selective forwarding attacks. Lu *et al*. [17] have introduced a neighbor-based monitoring technique. In their design, every node calculates the trust value of its 1-hop neighbors depending on their various behavior measurement and creates a trust management so that it can ensure whether a node is a harmful node or not. The advantage of this mechanism is that we can detect the caught node more quickly and accurately by various nodes

No matter how analyzing the detection technique is, it always demonstrates on the condition that harmful nodes have already dropped a mass of data packets. Hence, if we wish to make confirm that the packets are broadcasted to the base station completely, we should let the packets avoid the harmful node.

B.Yu [18] introduces a mechanism to determine selective forwarding attacks depending on checkpoints. If any checkpoints node doesn't obtain enough acknowledgments, it will create warning messages to the source node, so that the determination of the selective forwarding attacks can be observed. But an apparent issue is available in this mechanism is that the nodes have to forward acknowledgments in a continuous way, which will highly increase the network cost. By the way, this mechanism can't decide whether there malicious tamper action available.

Sophia Kaplantzis et al [11] introduced a centralized intrusion detection technique that utilizes only two characteristics to determine selective forwarding and black hole depending on Support Vector Machines (SVMs) and sliding windows. This intrusion detection is operated in the BS and thus the sensor nodes utilize no energy to support this extra security characteristic. From this they conclude that the system can determine selective forwarding attacks and black hole attacks with high accuracy without exhausting the nodes of their energy.

Brown and Xiaojiang [12] have introduced a technique to determine selective forwarding utilizing a Heterogeneous Sensor Network (HSN) model. The HSN contains powerful high-end sensors (H-sensors) and large no. of low-end sensors (L sensors). After deploying sensors, a cluster formation occurs with H-sensor as cluster head.

Xin, etal. introduced [13] a light weight defence technique against selective forwarding attack which utilizes neighbour nodes as monitor nodes. The neighbouring nodes (monitoring nodes) monitor the transmission of packet loss and re-forward the lost packets. They employed a hexagonal WSN mesh configuration.

Zurina Mohd Hanapi et al [14] introduced the dynamic window stateless routing protocol DWSIGF that is resilience to selective forwarding and black hole attack caused by the CTS rushing attack. Even without embedding any security technique inside the routing protocol, the dynamic window protected implicit geographic forwarding (DWSIGF) however promise a good defense against black hole attack with good performance of network.

Riaz Ahmed Shaikh et al [15] introduced two new identity, location privacy and route algorithms and data privacy method that addresses the challenging issues because of the constraints imposed by the sensor networks, sensor nodes and QoS problems.

Jiang [19] introduces a mechanism to determine selective forwarding attacks, which depend on the trust level and packet loss. After networking configuration being demonstrated, when sensing data is transmitted on the route, the intermediary nodes determine and count the no. of the packets they obtain and forward, and inform the statistical results to the Base station; with respect to these data, the BS computes the trust level of nodes and measure the packet drop, so that it can detect whether this node is an active attacking node

Yu and Xiao in [20], introduced a technique which utilizes a multi-hop acknowledgment mechanism to launch alarms by receiving replies from intermediary nodes. Every node in the forwarding path is in charge of determining harmful nodes. If an intermediary node determines a node as harmful in its upstream/downstream, then it will forward an alarm packet to the base station/source node via multi-hops

III. OVERVIEW OF THE SCHEME

In this section, we first describe the design objectives and then proceed to the overview of our introduced mechanism. Our primary objective is to deploy a detection mechanism that would unambiguous identify attack flows that continuously have an unfair buffer space at the MRs. It is necessary to punish these flows, as admitting these flows would result in no buffer space for other innocent flows when they finally reach. We continue the traffic rate of these continuous flows utilizing our cache based defence technique. We preempt such misbehaving flows from the IFQ (Interface Queue) of the MRs by discarding them. In a WMN, a distant flow obtains low throughput owing to the multi-hop communication. Thus, an intruder can lead total violence to the far away flows by introducing an attack on the MRs from a closest source. The innocent flows in our network comprehends HTTP transfer requests emerged from the mesh clients, TCP flows that reply to congestion, and low data rate UDP flows.

Our algorithm is composed of two main sub-parts: *Active DoS attack detection module* based on most frequently viewed cache discipline and *DoS attack regulator module*. Before we continue to explain our mechanism in detail, we first present the data structures and the variables utilized at every mesh router for managing the per-active-flow state information.

IV. ACTIVE DOS ATTACK DETECTION MODULE

Before a rate controller can be employed on the attack traffic it is significant to find potential attack flows. This module provides help in the identification of these high-bandwidth flows that are risky to the network.

We introduce an active cache based technique to detect high-bandwidth flows. The cache table manages a record of *most frequently seen* flows. When, a packet reaches at a node, its packet signature is compared with the available packet signature in the cache. If not detected, an entry is produced for this novel flow; else if the flow is already available in the cache, its frequency counter is increased. When the cache becomes full, the cache entry with the minimum count is preempted to create space for the new flow. In this manner, the cache manages a list of potential high-bandwidth flows. The attack packets reach in large amount to broadcast the victim MR and are ensured to be available in the cache with a large frequency count.

We can differentiate between a link congestion using application level information and DoS attack and [19]. It is possible that our mechanism can arrange burst flows as an attack flow. For avoiding these false positives, the comparison between the frequency counts of this flow with the frequency counts of the other flows in the cache is performed. If the frequency count of this flow is higher than half of the maximum frequency count in the cache, the burst flow is arranged as an attack flow. But, this labeling is local as in another time frame the burst flow would act normally and would no longer be act as an attack flow. Since, an intruder slowly pumping traffic into the network would be constantly categorized as an attack flow for the whole duration of the attack.

A. DoS attack regulator module:

After the attack traffic is detected, an alert is forwarded to the DoS attack regulator module to limit it. The module controls the entry of an attack flow depending on a particular dynamically tuned drop probability.

Each MR is related with an initial drop probability of 0. In the existence of attack flows, a packet related to the innocent flows always discovers a full buffer because of which it is forcefully discarded at the IFQ. Hence, whenever a packet related to an innocent flow is discarded, we increase the drop probability at this MR. finally when a packet related to the attack traffic reaches it is discarded even if there is place in IFQ based on this drop probability. Unlike attack flows, an innocent flow has a greater inter-arrival time and thus is not affected highly by this drop probability. As more and more innocent packets are discarded during the attack, the drop probability is correspondingly incremented which in turn behaves to control the attack flow. Once the drop probability arrives maximum value DPmax and lies so for Tmonitor_drop, we utilize a trace notified that forwards a Quench request to its upstream neighbor pumping the attack packets.

V. SIMULATION

In this section, we measure the performance of our mechanism utilizing NS-3. We first show the reduction in the network performance because of the DoS attack traffic and prove the efficiency of our mechanism in enhancing the aggregate throughput of innocent flows. We then describe how our mechanism helps in a fair distribution of bandwidth for all the network flows. We eventually measure the optimal selection of starting value for the *drop probability* through simulations. We take a simple IEEE 802.11s based mesh network with 9 MRs established randomly as illustrated in Fig. 3 (with every MR serving on average 4-5 mesh clients). One of the MR is designed as IGW that offers internet connectivity to other MRs. All mesh clients and mesh nodes communicate utilizing IEEE 802.11 DCF running at 11 Mbps with RTS/CTS enabled. The two-ray ground model was utilized with a transmission range of 350 m as the radio propagation model and carrier sensing range of 650 m. All the traffic begins from the clients under the MRs, and is then integrated at the corresponding MR and sent to the IGW. The duration of simulation is adjusted to 150 seconds. Without loss of generality, we consider a constant packet size of 512 bytes for all the UDP flows.

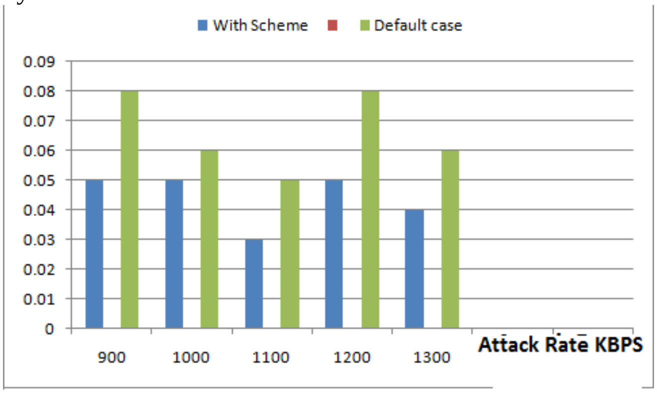

Figure 3. Normalized Throughput of attack flow under varying rate of attack traffic

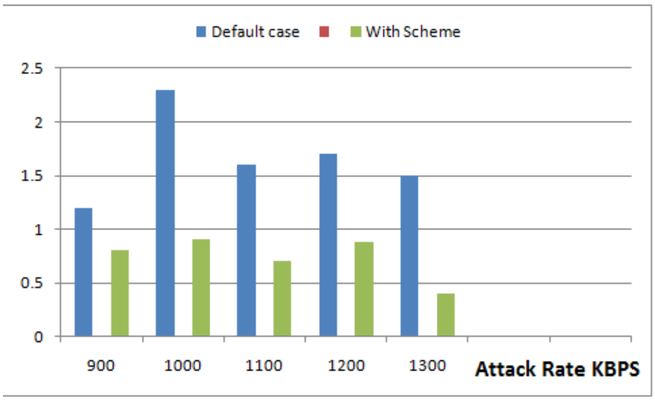

Figure 4. Normalized Aggregate Load of innocent flows under Varying rate of attack traffic

As UDP has no intrinsic congestion control technique, the attack flow can easily overload the network, thus stripping internet services for other legitimate subscribers.

VI. RESULTS AND ANALYSIS

We also measure the efficiency of our technique by evaluating the flows normalized throughput, which is the ratio of the throughput achieved to the provided load. We do the comparison of the normalized throughput of flows in the default mechanism and when utilizing our mechanism for the attack flow as well as the innocent flows.

We view from Fig. 3 that in the default situation, the attack traffic enjoys highest throughput. But, when our mechanism is employed, it is efficiently limited by the controller module. It is significant to observe that our cache based mechanism rigorously continues only those flows that are creating high UDP traffic. From Fig. 4, we view that as the rate of attack traffic is incremented from 800 Kbps to 1300 Kbps, the attack traffic network load slowly reduces. In our mechanism, while attack traffic of 800 Kbps is hardly limited, attack traffic of 1.5 Mbps is drastically reduced by 70%. We next analyze how our mechanism secures the network innocent flows. We begin one attack flow from MR4 (at 1500 Kbps) and about 6 innocent flows (at rates- 50 Kbps to 300 Kbps) from the several MRs. The sources are taken randomly from the mesh topology. We take the integrated throughput of all innocent flows and normalize them according to the total provided load. From Fig. 8, we view that our cache based defense offers a maintained throughput close to 1 regardless of the attack rate; while in the default mechanism the normalized integrated throughput slowly decreases (from 0.86 to 0.46) as the attack rate increments.

VII. CONCLUSION AND FUTURE WORK

A DoS attack makes a large umbrella of potential security attacks against WMNs preventing their widespread deployment. We introduce a cache based technique fitted with a trace notifier that provides help in protecting the network against DoS attacks. We use a simple mechanism that manages minimal state information at every router and functions independent of the fundamental queuing method at the routers. Simulation results tell that our technique efficiently mitigates the impact of DoS attacks by efficiently filtering the attack traffic at each intermediary router.

REFERENCES

[1]H. Lee, V. Mashhad, and D. Cox, “Time-driven simulation of large wireless networks with parallel processing," IEEE Communications Maga- zine, vol. 47, no. 3, pp. 158-165, Mar. 2009.

[2] H. Lee and Zu Li, “Simulation of mobile cellular systems with integrated resource allocation and adaptive antennas," Proc. of IEEE Wireless Communications and Networking Conference (WCNC), pp. 3210-3215, Mar. 2007

[3] A. Goldsmith and L. Greenstein, “A measurement-based model for predicting coverage areas of urban microcells," IEEE Journal on Selected Areas in Communications, vol. 11, no. 7, pp. 1013-1023, Sep. 1993.

[4] D. Cox, R. Murray, and A. Norris, “800 MHz attenuation measured in and around suburban houses," AT & T Bell Laboratories Technical Journal, vol. 63, no. 6, pp. 921-954, Jul./Aug. 1984.

[5] Z. Tang and J. Garcia-Luna-Aceves, “A protocol for topology-dependent transmission scheduling in wireless networks," Proc. of IEEE Wireless Communications and Networking Conference (WCNC), pp. 1333-1337, Sep. 1999

[6] C. Zhu and M. Corson,” Reservation protocol for mobile ad hoc networks," Wireless Networks, vol. 7, no. 4, pp. 371-384, Jul. 2001.

[7] W. Smith, “Urban propagation modeling for wireless systems," Ph.D. dissertation, Stanford University, Stanford, CA, USA, Feb. 2004

[8] M. Feuerstein et al., “Path loss, delay spread, and outage models as functions of antenna height for microcellular system design," IEEE Transactions on Vehicular Technology, vol. 43, no. 3, pp. 487-498, Aug. 1994.

[9] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. “Lightweight defense scheme against selective forwarding attacks in wireless sensor networks” pages 226 –232, Oct. 2009

[10] C. Intanagonwirat, R. Govindan and D. Estrin, “Directed diffusion: a scalable and robust communication paradigm for sensor networks,” in 6th Annual Conf. on Mobile Computing and Networking, pp. 56-67. Aug. 2000.

[11] B. Karp and H. Kung, “GPSR: greedy perimeter stateless routing for wireless networks,” in 6th Annual Conf. on Mobile Computing and Networking, pp. 243-254, Aug. 2000.

[12] Wazir Zada Khan et.al “Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks” in I.J. Computer Network and Information Security, pp.1-10, Aug-2012

[13] Anthony Wood, John A. Stankovic, “Denial of Service in Sensor Networks,” IEEE Computer, 35(10):54-62, October 2002.

[14] B Yu, B Xiao. “Detecting selective forwarding attacks in wireless sensor networks”. In: Proe. of the 20th International Parallel and Distributed Processing Symposium, RhodesIsland, Greeee,pp.1218- 1230, 2000