

A Comprehensive Framework for Packet Injection Avoidance in MANET without Authorization

¹G. SaiRani, ²P. Nikhitha, ³D. Chandrika, ⁴Dr. G. Manjunath

^{1,2,3}Dept. of CSE, JNIT, Hyderabad, India

⁴Dept. of CSE and IT, JNIT, Hyderabad, India

Abstract

Mobile Adhoc network is an on the fly network with a dynamic topology where the node association changes frequently. Such a network is vulnerable to different types of attacks as there is no centralized mechanism for providing the security and due to the fact that the network uses 802.11 based MAC layer which is considered to be a very weak in terms of security and data integrity. Packet injection is one of the most severe attack types in such a network. A Packet injection is type of attack where by any unauthenticated node injects malicious packets along with the valid data or control packet. Detection of such injections are difficult and requires huge processing which drains limited battery resources of MANET. Therefore in this paper we propose a unique technique for minimizing packet injection attack with the help of traffic splitting and fair resource reservation policy for the neighbors. The method is compared with conventional cryptosystem based transmission and it is shown that the performance of the proposed system is way better in preserving network lifetime while ensuring better protection against packet injection attacks.

Keywords

MANET, Packet Injection, 802.11 Session Hijack, Wireless Session Attack, Traffic Splitting, Resource Reservation.

I. Introduction

A. Mobile Ad-Hoc Network

A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of such network conflict with the challenges, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load). The ad hoc routing protocols should address location awareness, cooperation fairness and power of the nodes in order to provide QoS. In this paper we propose a Position based routing collaborated with cross layer information exchange of MAC and network layer about the received power of the packets.

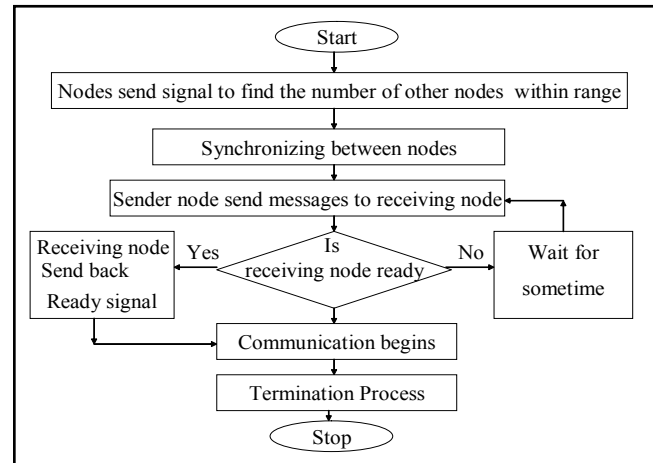


Fig. 1: Typical Functioning of MANET

B. Packet Injection

As wireless packets are broadcasted in the open air, it is impossible to secure the transmission with certainty and confidence equivalent to that of wired network. Consider fig. 2, that demonstrate a simple transmission of packets from node 1 to node 4 through an intermediate node 3. The transmission is also propagated to node 2. The attack can come in different form. Node 2 may find out that node 3 is routing the packets from 1 to 4 and can flood node 3's interface with subsequent control packets blocking the bandwidth and network interface of 3 which raises a route error and 2 takes control of the next route and injects malicious packets along with the packets that are coming from source node i.e. node 1.

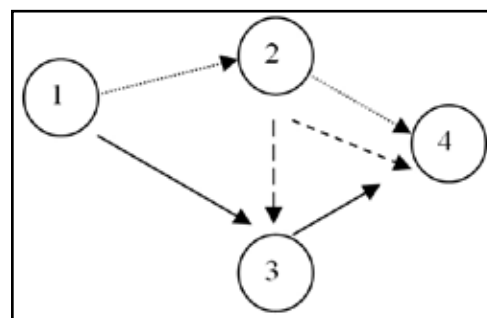


Fig. 2: A Sanapshot of Network Topology with Node 2 Injecting Probe Packets to 3 and 4

On the other hand node 3 might also decide to inject malicious packets (for example a raw ICMP packet) along with the transmitted packet from the source. Injected packets may also be probe packets which are responded with network information like MAC address, bandwidth, frame control version etc. A simple format of injected packet is presented in fig. 3.

Hence the effect of injected packets can be minimized substantially if a adopts following precautions:

- Limit the flow from a particular node
- Limit Response to probe packets
- Periodically switch to Listen Only mode to obtain the

- neighbor's activity
 - Maintain a history of type of packets (data, audio, video, files) generated from particular nodes and compare with the type of packets being received.
 - Blacklist the nodes with huge volume of probe packets.
- The solution must also take into account that the preventive measure must not affect the performance of the network.

```

oid * CreatePacket(
    DOT11_MGMT_SUBTYPE subtype,
    PCHAR Source,
    PCHAR Dest,
    PCHAR Bssid,
    ULONG packetsize
)
{
    PDOT11_MGMT_HEADER pMgmtHeader = NULL;
    PDOT11_PROBE_REQUEST pProbeRequest = NULL;
    PDOT11_INFO_ELEMENT pInfoElement = NULL;
    PDOT11_BASIC_RATE pBasicRate = NULL;
    PDOT11_EXT_RATE pExtRate = NULL;
    PVOID DataBuffer = NULL;

    if(Source == NULL || Dest == NULL || Bssid == NULL){
        printf("CreatePacket ==> null mac address \n");
        return DataBuffer;
    }

    DataBuffer = malloc(packetsize);

    pMgmtHeader = (PDOT11_MGMT_HEADER)(PCHAR)DataBuffer;
    pMgmtHeader->FrameControl.Version = 0;
    pMgmtHeader->FrameControl.Type = DOT11_FRAME_TYPE_MANAGEMENT;
    pMgmtHeader->FrameControl.Subtype = subtype;

    //firmware can handle rest of framecontrol
    pMgmtHeader->FrameControl.ToDS = 0;
    pMgmtHeader->FrameControl.FromDS = 0;
    pMgmtHeader->FrameControl.MoreFrag = 0;
    pMgmtHeader->FrameControl.Retry = 0;
    pMgmtHeader->FrameControl.PwrMgt = 0;
    pMgmtHeader->FrameControl.MoreData = 0;
    pMgmtHeader->FrameControl.WEP = 0;
    pMgmtHeader->FrameControl.Order = 0;

    //no specific duration was required to send
    pMgmtHeader->DurationID = 314;

    memcpy(pMgmtHeader->DA, Dest, MAC_ADDR_LEN);
    memcpy(pMgmtHeader->SA, Source, MAC_ADDR_LEN);
    memcpy(pMgmtHeader->BSSID, Bssid, MAC_ADDR_LEN);

    pMgmtHeader->SequenceControl.FragmentNumber = 0;
    pMgmtHeader->SequenceControl.SequenceNumber = 0;

    switch (subtype)
    {
        case DOT11_MGMT_SUBTYPE_PROBE_REQUEST: //0
            packetsize = sizeof(DOT11_MGMT_HEADER) +
                sizeof(DOT11_MGMT_SUBTYPE_PROBE_REQUEST) + 1;
            pProbeRequest = (PDOT11_PROBE_REQUEST)
                ((PCHAR)pMgmtHeader + sizeof(DOT11_MGMT_HEADER));

            pProbeRequest->ssid.ElementID = 0; //ssid frame
            pProbeRequest->ssid.Length = 0;

            //the number of rates is up to the user
            pProbeRequest->rateframe.ieheader.ElementID = 1; //rate frame
            pProbeRequest->rateframe.ieheader.Length = 1; //1 rate object
            pProbeRequest->rateframe.rate[0] =
                (USHORT)0x82; //mandatory, // 1mbps

            break;

        default:
            break;
    }

    return pMgmtHeader;
}

```

Fig. 3: Injected Packet Format (Using Windows 7 Drivers for Generating and Injecting Probe Packet in the Interface)

If any Node is Aware of Neighbor Devices (or Device Interfaces) than the Packets can be Injected with a Simple Format as Presented in fig. 4.

II. Related Work

[1] present the analysis of current WLAN fingerprinting techniques. [2] proposes an approach based on Gaussian mixture models, building RSS profiles for spoofing detection and shown that the proposed approach is robust against antenna diversity and significantly outperforms existing approaches. [3] propose an attack detector for wireless spoofing that utilizes K-means cluster analysis. Integrated attack detector into a realtime indoor localization system, which is also capable of localizing the positions of the attackers. Also shown that the positions of the attackers can be localized using either area-based or point-based localization algorithms. [4] proposed an algorithm to enhance the performance of the correlation of two WIDTs in detecting MAC spoofing Denial of Service (DoS) attacks. The two techniques are the Received Signal Strength Detection Technique (RSSDT) and Round Trip Time Detection Technique (RTTDT) [4-5], investigates the current security issues in MANET and examined different routing attacks, such as flooding, blackhole, link spoofing, wormhole, and colluding misrelay attacks, as well as existing solutions to protect MANET protocols. Wide variety of methods exists for detecting spoofed packets which include both active and passive host-based methods as well as routing based methods[6]. The exploitation of Internet elements and protocols of the purpose of covertly communicating identity information, armed with simple cryptography is proposed as a solution for preventing spoofing attack [7].

A method of spoof detection using signal strength analysis where currently no fielded method exists today is proposed [8]. [9] proposes a new framework of intrusion detection systems exclusively for wireless mesh networks which will serve as a baseline guide for investigating intrusion detection systems for large scale multi-hop wireless broadband networks.

```
DeviceHandle = OpenHandle(pPacketuiDevice);
IORequest(DeviceHandle, IOCTL_PACKET11_GET_MAC, NULL, 0, Source, MAC_ADDR_LEN);

PacketLength = sizeof(DOT11_MGMT_HEADER) + sizeof(DOT11_PROBE_REQUEST) + 1;

pMgmtFrame = CreatePacket(DOT11_MGMT_SUBTYPE_PROBE_REQUEST, Source,
                          Broadcast, Broadcast, PacketLength);

IORequest(DeviceHandle, IOCTL_PACKET11_INSERT_PACKET,
          (PUCHAR)pMgmtFrame, PacketLength, NULL, 0);

CloseHandle(DeviceHandle);
```

Fig. 4: Sample Code Snippet for Injecting the Packets to Particular Device

[10] proposes an algorithm to detect spoofing by leveraging the sequence number held in the link-layer header of IEEE 802.11 frames, and demonstrates how it can detect various spoofing without modifying the APs or wireless stations. An overview of attacks according to the protocols stacks, and to security attributes, mechanisms, preventive approaches following the order of the layered protocol stacks is presented [11] and also an overview of MANET Intrusion Detection Systems (IDS), which are reactive approaches to thwart attacks and used as a second line of defense [11].

III. Problem Formation

Packet Injection is a means by which an unauthenticated or malicious node injects packets in the network. For example a malicious node broadcast RREQ packet and keep broadcasting them which keeps the other nodes responding to RREQ and thus

causing denial of service. In another form of packet injection, a malicious node upon receiving RREQ packets may falsely generate RREP packet which causes all the data packets being routed through this node rather than the legitimate path. Another form of packet injection includes false generation of RERR packets which causes the source node to drop the current route and start a new route request. As there is no centralized authorization protocol in MANET, such attacks are easy to device and can be used effectively for denial of service. Adopting an authorization scheme effectively means changing the firmware at the link layer which is neither cost effective nor can guarantee a flowless integration with legacy deployment. Therefore we propose a network layer based approach for avoiding packet injection attack. The aim here is to avoid and minimize the effect of such an attack rather than detect and prevent. There are no core protection in the protocol stack of MANET to prevent the nodes from packet injection attacks such as packet flooding or probe packets. One of the most preferred technique for preventing such attack is access control technique which is described in short here.

Each node uses this network access control key to authenticate every outgoing packet, i.e., to insert a Packet Authentication Header (PAH).

Each node also uses this key to verify the PAH of an incoming packet, either intended for this node or transiting through it. They will immediately drop any packet not properly authenticated.

As a result, a non-authorized node that is either unknown to or revoked by the key manager is prevented from injecting packets into the MANET.

Clearly, the network access control key may have to be updated due to the revocation of compromised nodes. Since each key update (rekeying) event defines a key session, the access control keys are also referred to as session keys. In this paper, we use network access control key and session key interchangeably, and we assume a legitimate node only uses the most recent session key it has received.

The system requires all legitimate nodes agree on the same key at the time they communicate. However, no existing group key distribution scheme can guarantee that all nodes receive the latest session key after a key update. Maintaining a synchronized session key therefore becomes a non-trivial task, given the dynamic nature of MANETs and the possibility of intermittent communication failures.

Two legitimate nodes cannot communicate in the system, if a more recent key update message only reaches one of them, unless they can agree on one specific session key. Thus, another challenging problem is how a node handles the received packets authenticated with different session keys, to ensure secure establishment continuation of communication with corresponding senders[12]. Therefore it can be safely said that even a node access control cannot guarantee a secured network, as loss of any packets carrying the key immensely increases the network overhead. The keys also increases an overhead in key update phase, encryption and decryption phase. Beside control packets are not encrypted so security is extended to probe packets generated by MAC or Network layer.

IV. Proposed System

1. Firstly we generate N-Node disjoint path from source to destination and adopt traffic splitting with equal split factor to balance the traffic across different routes so that even if a node is attacked, the effect is minimum over the overall session.

2. Each node adopts a fair share based queue model where queue length is preserved for each of the neighbors equally. When a node consistently request for resource or bandwidth, that node is blacklisted for current session. As the protocol adopts load balancing mechanism, network congestion will never cause a node to continuously keep requesting for packets.
3. The technique adopts a rate limiter where any node trying to utilize more than 30% of the free bandwidth of the other node triggers a blacklisting of the node requesting for excess bandwidth.
4. Any packets arriving with more than 30% delay deviation than the normal average par hope delay would cause a trigger and the source of the packet is marked as blacklisted.
5. Node categorizes the type of packets and maintains a history of packet types. If the current packet from a node is deviated entirely from the past record, than the subsequent packets from that node is kept in MAC buffer for further validation
6. Each node goes to listen only mode periodically and monitors the packets from the neighbors. If any node is found to generate too many ICMP/Probe packet, the node is blacklisted.
7. If the packet rate from a node is more than the acceptable packet rate, which is 30% of the allowed bandwidth per node, than the nodes are marked as blacklisted and packets from those nodes are dropped. This may lead to drop of packets in valid applications like video frame transmission where the bandwidth requirement is higher. Therefore packet type based resource allocation is suggested for future improvement.

The system is tested with real time testbed comprising of 4 Laptops powered by windows 7 OS, exactly setup as fig. 2. An adhoc network is created and deployed and packet injection attack is generated at a node. Now for obtaining multiple paths, a 5th node is incorporated and traffic from 1 to 4 is splitted in equal volume and transmitted through 3 and 5.

V. Results

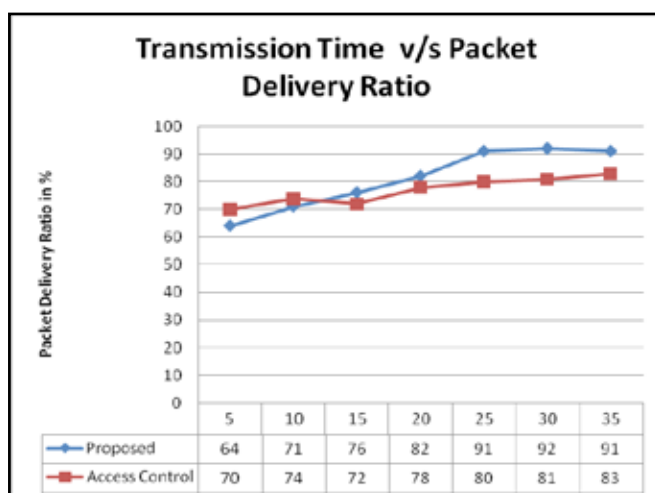


Fig. 5: Transmission Time v/s Packet Delivery Ratio

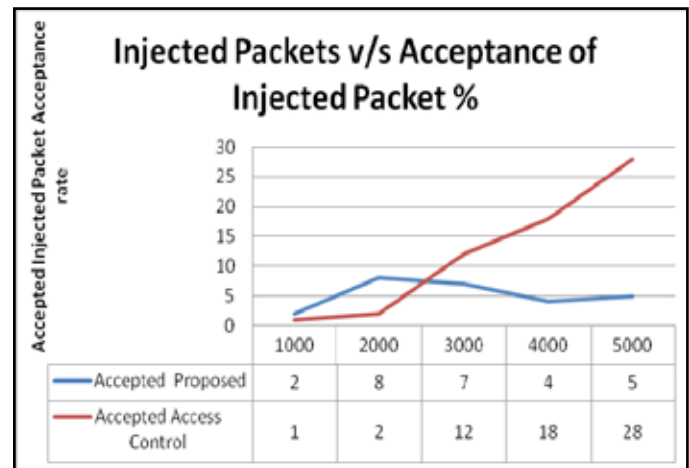


Figure 6: Accepted Injected packet Acceptance rate

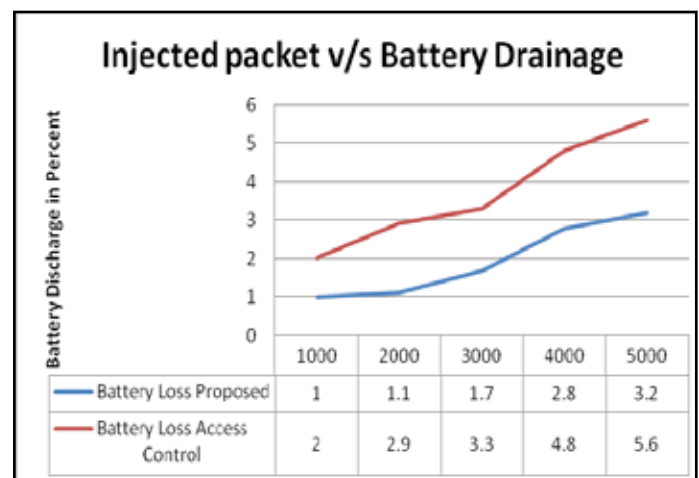


Fig. 7: Battery Discharge Percent

VI. Conclusion

Figure 5 clearly shows that packet delivery ratio of the proposed system improves with time due to more multiple path acquiring and splitting the traffic. But Node access control based mechanism can not guarantee an improvement in the packet delivery ratio as it is not meant for ensuring faster transmission. Figure 6 is a proof of the presented concept. The performance clearly explains that the proposed system is way better in rejecting the injected packets due to it's ability to minimize the rate of injected packets as well as the ability of minimizing the effect of probe packets. Node access control does respond to both MAC as well as network layer probes.

Fig. 7, proves the battery efficiency of the proposed technique. When the Testbed laptops are configured with the proposed system, the battery drainage is found to be less. Such a loss also incorporates the ideal time battery loss due to processing. But Access control techniques drains up the battery life by frequent key exchange and excessive encryption and decryption.

Therefore it can be safely said that proposed technique is better suitable for practical Adhoc networks for preventing the nodes from packet injection attacks.

The technique can also be validated with Fuzzy base state check and optimization technique for better inference of the transmission pattern of the nodes.

References

- [1] Lackner, G., Payer, U., Teufl, P., "Combating Wireless LAN MAC-Layer Address Spoofing with Fingerprinting Methods", International Journal of Network Security 9 (2), 164–172, 2009.
- [2] Y. Sheng et al., "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength", Proc. IEEE INFOCOM, Apr. 2008, pp. 1768–76.
- [3] Y. Chen, W. Trappe, R. Martin, "Detecting and localizing wireless spoofing attacks", in Proc. Sensor, Mesh and Ad-Hoc Communications and Networks, 2007, pp. 193–202.
- [4] Aiman Abu Samra, Ramzi Abed, "Enhancement of Passive MAC Spoofing Detection Techniques", International Journal of Advanced Computer Science and Applications, Vol. 1, No. 5, November 2010.
- [5] Rashid Hafeez Khokhar, Md Asri Ngadi, Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad-Hoc Networks", International Journal of Computer Science and Security, volume (2) issue (3), pp. 18-29, 2008.
- [6] S. Templeton, K. Levitt, "Detecting spoofed packets", Proceedings of The Third DARPA Information Survivability Conference and Exposition (DISCEX III) '2003, Washington, D.C., April 2003.
- [7] Wesam S. Bhaya, Suad A. Alasadi, "Security against Spoofing Attack in Mobile Ad-Hoc Networks", European Journal of Scientific Research, Vol. 64, No. 4, pp. 634-643, 2011.
- [8] Douglas Madory, "New Methods of Spoof Detection in 802.11b Wireless Networking", A Thesis Submitted to the Faculty in partial fulfillment of the requirements for the degree of Master of Science, Thayer School of Engineering, Dartmouth College, Hanover, New Hampshire, JUNE 2006.
- [9] Shafiullah Khan, Kok-Keong Loo, Zia Ud Din, "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks", The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
- [10] F. Guo, T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection", Recent Advances in Intrusion Detection: 8th International Symposium, RAID 2005, 2006.
- [11] B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer, Vol. 17, 2006.



G. SaiRani pursuing her B.Tech Computer Science and Engineering in Jawaharlal Nehru Institute of Technology, Ibrahimpatnam, RangaReddy dist., Andhra pradesh, India. Her areas of interest are Network security, software engineering and Image processing.



P. Nikhitha pursuing her B.Tech Computer Science and Engineering in Jawaharlal Nehru Institute of Technology, Ibrahimpatnam, RangaReddy dist., Andhra pradesh, India. Her areas of interest are Network security and Data mining.



D. Chandrika pursuing her B.Tech Computer Science and Engineering in Jawaharlal Nehru Institute of Technology, Ibrahimpatnam, RangaReddy dist., Andhra pradesh, India. Her areas of interest are Network security and software engineering.



Dr. Manjunath Gadiparthi is working as an Associate Professor and Head Department of CSE & IT in JAWAHARLAL NEHRU INSTITUTE OF TECHNOLOGY (JNIT). His areas of interest are Image Processing, Data Mining & Network security. He published several journal articles and Conference papers, in the areas of Image Processing, Data Mining & Network security.