Detection of misbehavior of routing layer in wireless mess network

Hina Wadhawan

Department of Computer Science and engineering
RIET, Ropar, Punjab, India

Abstract- Wireless mesh networks (WMNs) 802.11s has emerged as key technology for the next-generation wireless networking due to independency of backbone network. Because of their advantages over other wireless networks, WMNs are undergoing rapid progress and inspiring numerous applications. However, many technical issues still exist in this field. This article presents detection of packet dropping attacks in routing layer. Packet dropping attacks are one category of Denial of Service attacks and can deplete network performance hence decrease throughput. Solutions are needed to detect such attacks. In this paper, we propose a solution called Watchdog monitoring mechanism which will detect malicious nodes that drops packet. It is basically a intrusion detection scheme.

Keywords: Wireless mesh networks, Packet Dropping Attack, Watchdog monitoring mechanism, Securing WMNs

I. Introduction

Wireless Mesh networks (WMNs) 802.11s [1] [3] as shown in Figure 1 comprise of “mesh routers” which are mostly static and “mesh clients” which are generally mobile. WMNs offer numerous advantages. They can be deployed very rapidly without needing any wiring and major infrastructure support. WMNs can be self organize and self-configure in continuously changing dynamic topology and connectivity of the network. WMN also exhibit self-healing characteristic. By using alternate path, WMN can overcome route failures due to mobility, interference, congestion etc. Using multi-hop routing the range of wireless devices can be extended in WMN. Lastly, with the use of multi- hop routing the transmission power can be significantly reduced thereby reducing the interference in the network and increasing battery longevity of the mobile nodes. Due to these and many other advantages, WMN has been used in various applications such as disaster relief and metropolitan area networks etc.

OUTLINES

T his paper bases on the detection of packet dropping attack i.e black hole attack at routing layer in wireless mesh networks. In Section II we describe an overview of network architecture of wireless mesh networks. Also, briefly describes applications. Section III tells about Packet Dropping Attack. Section IV explores standard protocol for wireless mesh networks. In Section V, we explore the Watchdog monitoring mechanism to detect packet dropping attack. Section VI reveals two ways to secure WMNs. Section VII finally gives the conclusion of this review paper.

II. NETWORK ARCHITECTURE

WMNs [5] consist of two types of nodes: Mesh Routers and Mesh Clients:

Mesh router

Multiple wireless interfaces with same or different wireless access technologies can be used. Thegateway/bridge functionality enable the integration of WMN’s with existing wireless networks. (cellular, sensor net,WI-FI, WIMAX).

Mesh clients

Conventional nodes (e.g PDA’s,desktops,laptops.) equipped with wireless network interface cards(NICs) and can directly connect to wireless mesh routers. Customers without wireless NICs can access WMNs by connecting to wireless mesh routers through e.g Ethernet[2].

2.1 Application Scenario

1) Broadband Home Networking
2) Community and neighbourhood Networking
3) Enterprising Networking
4) Metropolitan Area Networking
5) Transportation Systems
6) Building Automation
7) Health and Medical Systems
8) Security and Surveillance Systems[6]
Infrastructure/backbone WMNs

III. PACKET DROPPING ATTACK

Packet dropping attack is basically a category of Denial of Service (DoS) attack. It occurs when one node or mesh router does not forwards requests to destination that is it drops all of the packets or some of the packets. Packet dropping attack consists of two types:
1) *Black Hole Attack[4]*: The malicious node always replies positively to a Route Request although it may not have a valid route to the destination. Almost all the traffic within the neighborhood will be directed towards the malicious node, which may drop all the packets. This is one of the categories of control plane attack.
2) Grey Hole Attack: In Black Hole Attack, the malicious node drops all the packets but in Grey Hole Attack, malicious node drops some of the packets [2].

IV. STANDARD PROTOCOL

Wireless Mesh Networks suffers from these attacks and to detect it an IEEE 802.11s standard protocol is defined that is HWMP (Hybrid Wireless Mesh Protocol).
1) It is based on Radio-Metric AODV (Ad-Hoc ondemand distance vector routing)(RF-3561) and Treebased Routing.
2) It support both broadcast/multicast and unicast delivery using “radio-aware metrics” over self configuring multi-hop topologies.
3). It helps in congestion control and power save [9].

V. WATCHDOG MONITORING MECHANISM

The watchdog [7] detects misbehaving nodes. Suppose there exists a path from node S to D through intermediate nodes A,B,C. Node A cannot transmit all the way to node C, but it can listen it on B’s traffic. Thus, when A transmits a packet for B to forward to C, A can often tell when B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header. When B forwards the packet from S to towards D through C, A can overhear B’s transmission and can verify that B has attempted to pass the packet to C. The solid line shows the intended direction of the packet sent from B to C, while the dashed line indicates that A is in transmission range of B and can overhear the packet transfer. We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overhead packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotton by the watchdog, since it has been forwarded on. If a packet in the buffer is remained for so longer than a certain timeout, the watchdog increments the failure tally for the node responsible for forwarding on the packet. If the tally exceeds the certain threshold bandwidth, it determines that the node is misbehaving node sends the packet to the source notifying it of the misbehaving node. The watchdog technique has advantages and weaknesses. The watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. It has certain limitations[8] in ad-hoc networks that is it might not detect the misbehaving node in the presence of 1) Ambiguous collisions 2) Receiver collisions 3) Limited transmission power 4) False misbehavior 5) Collusion 6) Partial dropping

VI. SECURING WMNs

We can secure our network by using the appropriate measures like using IDS in our system.

A. Intrusion Prevention

We can secure our network by running the security services that stop the attacker from intruding into the network and launching the attack on the network these including authentication, access control, data confidentiality, data integrity and non-repudiation.

B. Intrusion Detection

In this we have to identify the illegitimate activities, which may be the consequence of an attack or may lead to an attack. Most of the security mechanisms and protocols follow the prevention approach. But Watchdog monitoring mechanism is an intrusion detection mechanism [4].

VII. CONCLUSION

The backbone of WMNs provides a viable solution for users to access the Internet everywhere anytime. It can also enhance the reliability of the mobile and the ad-hoc network of mesh clients. WMNs enable the integration of multiple wireless networks. WMN suffers from black hole attack and to detect this attack watchdog monitoring mechanism has been proposed.

VIII. REFERENCES

[1] Akyildiz, I.F.;Xudong Wang "A survey on wireless mesh networks" in communications Magazine,IEEE Volume 43, Issue 9, Sept.2005 Page(s): S-23 - S30.
[2] Sahil Seth, Anil Gankotiya, Amandeep Jindal, "Current State of Art Research Issues and Challenges in Wireless Mesh Networks", 2010.
[3] Sahil Seth, Anil Gankotiya, Amandeep Jindal,"A Comparitive Study between Wireless Local Area Networks and Wireless Mesh Networks",2010.
[4] Anil Kumar Gankotiya, Sahil Seth, Gurdit Singh,"Attacks and their Counter Measures in Wireless Mesh Networks", 2010
[5] I.F Akyildiz,X.Wang and W. Wang,"Wireless Mesh Network:A survey" in computer Networks and ISDN Systems, Volume 47,Issue 4,March 2005
[6] http://www2.cs.uh.edu/~rzheng/course/C0SC7397 sp07/cunqing.ppt.
[7] Sergio Marti, T.J. Giuli,Kevin Lai and Marin Baker,"Mitigating Routing Misbehaviour in mobile ad-hoc networks", 2000
[8] J. Jubin and J. Tornow. The DARPA Packet Radio Network Protocols,In Proceedings of the IEEE, 75(1):21-32,1987.
[9] http://en.wikipedia.org/wiki/IEEE_802.11s