Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detecting Packet-Dropping Faults in Mobile Ad-Hoc Wireless Networks

Priya Malhotra
Student of Master of Technology
Department Of Computer Science and Engineering
Shobhit University, Meerut, Uttar Pradesh, India

Abstract— Mobile Ad-hoc networks are inherently prone to security attacks, with node mobility being the primary cause in allowing security breaches. This makes the network susceptible to Byzantyne faults with packets getting misrouted, corrupted or dropped. In this paper we propose solutions using an unobtrusive monitoring technique using the "Detection Manager" to locate malicious or faulty nodes that misroute, corrupt or drop packets. The unobtrusive monitoring technique is similar to an intrusion detection system that monitors system activity logs to determine if the system is under attack. This technique uses information from different network layers to detect malicious nodes. The detection manager we are developing for Mobile Ad-hoc networks stores several rules for responding to different situations. Any single node in the network can use unobtrusive monitoring without relying on the cooperation of other nodes, which makes unob-trusive monitoring easy to implement and deploy.

Keyword— MANETS, Mobile Ad-Hoc Networks, Unobtrusive Monitoring, Domain Name Server, Detection Manager

I. INTRODUCTION

Mobile Ad-hoc networks are prone to security attacks, with node mobility being the primary cause in allowing security breaches. As the information regarding the mobile node needs to be updated continuously in Mobile Ad Hoc networks (MANETS), the network is more susceptible to Byzantyne faults such as misrouting, corrupting and dropping packets. This makes the network more vulnerable to attack or disruption due to faulty nodes and so solutions that are native and more relevant to ad-hoc networks are needed. The nature of these attacks is such that they consume resources associated with various network elements. This impedes the efficient functioning and provision of services in accordance with their intended purpose [3]. There must be means to provide reasonable protection for mobile nodes from malicious networks and for networks against malicious nodes. Unfortunately, current protocol architectures do not provide adequate support for such protection. Motivated by these needs, this paper takes a fresh look at security management from a real-time perspective and proposes solutions using an *Unobtrusive monitoring* technique which does not require modification of all the nodes in the network and relies on already existing network information to detect the presence of malicious nodes.

The proposed mechanism is similar to an intrusion detection system that monitors system logs and activity to determine if the system is under attack. This technique combines information available at different network levels and is designed with the following principles in mind:

- ***Single node operation:*** requires modification only to the node that it runs on.
- ***No modification to existing protocols:*** works with existing protocols, such as DSR (Dynamic Source Routing) and ICMP (Internet Control Message Protocol).
- ***Battery life:*** uses readily available network information such as route error and ICMP destination unreachable messages; hence does not dissipate too much battery life.
- ***No security associations:*** since it does not rely on the cooperation of other nodes in the network, security as-sociations and additional infrastructure are not required between the nodes.
- ***Adaptive:*** designed to work with DSR and can be ex-tended to work with other routing protocols, such as AODV (An On Demand Vector routing) and DSDV (Destination-Sequenced Distance Vector routing).
- ***Varied capability:*** designed to detect malicious behavior arising from dropping packets and misrouting packets. Also designed to distinguish between behavior such as link failure, and malicious behavior.

Existing approaches so far, [1],[2] either require expensive security associations or the modification of all the nodes in the network.

II. RELATED WORK

There are three steps in handling a malicious node. First it is important to identify that a node has mishandled packets intentionally. Second, the identity of the malicious node must be determined. The third step is to isolate the malicious node from the network or cope with the issue. Several solutions have been proposed to address these problems.

- ***Malicious Behavior Detection:*** In the route-based distributed packet filtering technique the algorithm performs routability checks on incoming packets. Filters are placed at key points in a network, unlike perfect ingress

filtering which places filters at every node. Implementing this would require modifying some or all of the nodes in the network. Watchdog is a technique where each node "snoops" the retransmission of every packet it forwards. If the watchdog detects that the node has not correctly retrans-mitted the packet, it can raise a warning. Again, this requires modification of some or all of the nodes in the network and is developed primarily for ad hoc networks operating with omni-directional transmissions. Another variation of this technique "nodes bearing grudges" proposed requires security associations between nodes to authenticate messages.

- ✓ ***Malicious Node Identification:*** The audit trail approach facilitates tracing via traffic logs at routers and gateways. This method is suitable for the off-line traceback of DoS (Denial of Service) attacks. It incurs significant storage and processing overhead at the routers. In behavioral monitoring, the likely behavior of a malicious node during a DoS attack is monitored to identify the source. For example, the malicious node may perform DNS (Domain Name Server) requests to resolve the name of the target host which may not be resident in its local name server's cache. During a DoS attack, the malicious node launching the attack may try to gauge the impact of the attack using various service requests including Web and ICMP echo requests. Thus maintaining a log of such events and activities may reveal information about the malicious node. IP traceback is similar to the mechanism used by the "trace route" command. In IP traceback, packets are sent out with ever-increasing time-to-live values, and listen for returning ICMP Time Exceeded packets. This may not work in all cases, especially if the malicious node chooses to judiciously handle the traceroute packet correctly.
- ✓ ***Isolation of Malicious Node:*** Whenever a node identifies a malicious node, it broadcasts a special blacklist message. When a node receives a blacklist message, it removes the blacklisted node from all of its routes, effectively isolating the node. A voting mechanism can also be used where each blacklist message counts as a vote, and a node is only blacklisted after receiving a minimum number of votes. A major disadvantage of blacklisting is that it makes the network vulnerable to DoS attacks and requires modification of all nodes on the network. With pathrating, each node maintains rating of all paths to all other nodes it knows about. The rating for each path increases with each good transmission and decreases each time a broken link is detected. The rating for each path containing a malicious node is identified along with the path. This can be seen as an extension to blacklisting.
- ✓ ***Research Challenges:*** The solutions proposed so far can either be not adapted to MANETS or they are sexpensive to implement and require the modification of all the nodes in the network. Moreover it is im-portant to develop solutions that are scalable, implementable, and capable of detecting malicious behavior while the com-munication is in progress. Techniques such as nodes bearing grudges rely on security associations between different nodes in the network. This can be accomplished through the use of a Certificate Authority which requires infrastructure support that MANETS lack. Another challenge to implementing the techniques is that they involve modification in most or all of the nodes in the network. In addition, they consume the battery life of the mobile devices to perform the overhead of cryptographic operations.

III. UNOBTRUSIVE MONITORING

The heart of the unobtrusive monitoring technique is the *detection manager* which is responsible for collecting and analyzing locally available data. The detection manager is implemented on the source nodes requesting service. Local data such as DSR route request and route error messages, ICMP time exceeded and destination unreachable messages, and TCP timeouts are fed into the detection manager. The data collection component takes these messages and events and extracts useful information from them.

ALGORITHM:

Algorithm 1 Data Collection (*detection interval)*

```
for :: do
  If DSR route error message received then
    fid := flow on which the route message received;
    Store the received route error in the store corresponding to fid
    Current time := get current time;
    if there are message older then "current time- detection interval" then
        Purge those message from the store
      end if
   end if
 end for
```

Algorithm 2 data analyser (detection interval)

```
For :: do
  if TCP timeout occurred then
    fid := flow on which the timeout occurred;
    Current time := get current time;
     if any route error  messages received for fid then
        if no route error  messages in[current time-detection interval, current time ] then
            raise a flag indicating malicious activity;
          end if
```



```
    else
        Raise a flag indicating malicious activity;
    end if
  end if
end for
```

This information includes the following:

- ✓ The location of broken links in DSR route error messages.
- ✓ The address of a node that was unable to deliver a packet in an ICMP destination unreachable message and the destination of that packet.
- ✓ The address of a node that dropped a packet whose time-to-live had expired from an ICMP time exceeded message and the destination of the original packet.
- ✓ The destination of a TCP packet that timed out.
- ✓ New routes from unsolicited route reply messages.
- ✓ The time that each message was received or each event occurred.

The data collection component extracts useful information and passes that data to the data storage component which in turn files the data for use by the data analysis component. Data is periodically purged to reduce the storage overhead, which is important for memory constrained nodes. This also ensures that the data analysis component is only working with recent and more relevant data. Finally, the data analysis component processes the stored data to determine if any malicious activity is taking place. If there is undesirable activity, the detection manager then alerts the node so that it can take appropriate action.

A. Example Scenario

We present a scenario to demonstrate how the unobtrusive monitoring technique uses information from route error mes-sage to detect malicious activity. In our example as shown in Figure 1, node S is source and node D is

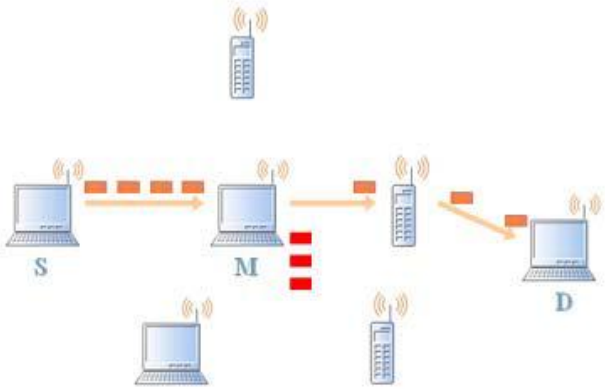

Fig. 1. Example Scenario for packet dropping

destination and the path S–M–D was found by the routing protocol during the discovery phase. Assume that M, the malicious node drops packets from node S which are destined for node D. There must be a distinction made between packet dropping arising due to broken links from malicious behavior.

First the detection manager checks if there are any route error messages indicating the broken links. In the absence of route error messages, the detection manager checks if any TCP packets have timed out and no TCP acknowledgement has been received. If this is the case, it raises a flag indicating malicious activity.

IV. CONCLUSION AND FURTHER RESEARCH

Mobile ad-hoc networks have several advantages over traditional wireless networks including ease of de-ployment, speed of deployment, and decreased dependence on a fixed infrastructure. Mobile ad-hoc net-works constitute an emerging wireless networking technology for future mobile communications. However, unless the networks can be secured against malicious activity, their usefulness may be stifled. The task of finding good solutions for these security challenges prevalent in ad-hoc wireless networks will play a critical role in achieving the eventual success and potential of mobile ad-hoc network technology.

To help protect ad-hoc wireless networks from malicious nodes, we developed an unobtrusive monitor-ing technique to detect malicious behavior in the network by gathering information from different network levels with out relying on node cooperation. Unlike some other proposed methods, this technique is easy to deploy, since it only requires modification to a single device, and it does not require any additional infras-tructure or security associations.

In the future, we would like to extend the unobtrusive monitoring technique to distinguish packet drops arising due to congestion and malicious behavior. We also plan to investigate the use of this technique with other ad-hoc routing protocols, such as AODV, TORA, and with other types of networks, such as hybrid wired-wireless networks and traditional wired networks. We would also like to extend this technique to handle partial packet dropping and also to detect any sophisticated attacks launched by colluding nodes.

REFERENCE

[1] C. E. Perkins. *Ad Hoc Networking*. Addison-Wesley Professional, first edition, 2000.

[2] D. B. Johnson, D. A. Maltz, Y. Hu, and J. G. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet draft, February 2002. draft-ietf-manet-dsr-08.txt.

[3] S. R. Medidi, M. Medidi, and S. Gavini. Detecting packet-dropping faults in mobile ad-hoc networks. In *Proceedings of The Thirty-Seventh Asilomar Conference on Signals, Systems & Computers*, pages 1708–1712, November 2003.

[4] S. Medidi, M. Medidi, S. Gavini, and R. Griswold. Detecting packet mishandling in manets. In *Security and Management*, pages 159–162, 2004.

[5] A. S. Tanenbaum. *Computer Networks*. Prentice Hall, third edition.

[6] J. F. Kurose and K. W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley, second edition, 2002.

[7] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM'94 Conference on Communications Architectures, Proto-cols and Applications*, pages 234–244, 1994.

[8] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. Internet draft, February 2003. draft-ietf-manet-aodv-13.txt.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, 11(1):38–47, March-April 2002.

[10] R. Griswold and S. Medidi. Malicious node detection in ad-hoc wireless networks. In *Proceedings of SPIE AeroSense, Digital Wireless Communications V*, April 2003.

