DETECTION OF MALICIOUS PACKET DROPPERS IN MOBILE AD HOC NETWORK

S.Sakthivel,
M.Phil Research Scholar,
P.G & Research Department of Computer Science,
Sengunthar Arts and Science College,
Tiruchengode,Tamilnadu,India.

P.Gayathiri Devi,
Assistant Professor,
P.G & Research Department of Computer Science,
Sengunthar Arts and Science College,
Tiruchengode,Tamilnadu,India.

Abstract: A mobile ad-hoc network is a collection of mobile nodes connected together over a wireless medium without any fixed infrastructure. Unique characteristics of mobile ad-hoc networks such as open peer-to peer network architecture, shared wireless medium and highly dynamic topology, pose various challenges to the security design. Mobile ad-hoc networks lack central administration or control, making them very vulnerable to attacks or disruption by faulty nodes in the absence of any security mechanisms. Also, the wireless channel in a mobile ad-hoc network is accessible to both legitimate network users and malicious attackers. So, the task of finding good solutions for these challenges plays a critical role in achieving the eventual success of mobile ad-hoc networks. Here we propose an "unobtrusive monitoring" technique, that uses readily available information from different layers of the protocol stack to detect "malicious packet-dropping", where a faulty node silently drops packets destined for some other node. A key source of information for this technique is the messages used by the special ad-hoc routing protocols. This technique can be deployed on any single node in the network without relying on the cooperation of other nodes, easing its deployment.

Keywords: Mobile Ad Hoc Network, Malicious Packet Droppers, Packet Routing, Security

I.INTRODUCTION

A Mobile ad hoc network is a collection of wireless nodes, all of which may be mobile, that dynamically create a wireless network amongst them without using any infrastructure. Ad hoc wireless networks come into being solely by peer-to-peer interactions among their constituent mobile nodes, and it is only such interactions that are used to provide the necessary control and administrative functions supporting such networks. Mobile hosts are no longer just end systems; each node must be able to function as a router as well to relay packets generated by other nodes. As the nodes move in and out of range with respect to other nodes, including those that are operating as routers, the resulting topology changes must somehow be communicated to all other nodes as appropriate. In accommodating the communication needs of the user applications, the limited bandwidth of wireless channels and their generally hostile transmission characteristics impose additional constraints on how much administrative and control information may be exchanged, and how often. Ensuring effective routing is one of the greatest challenges for ad hoc networking [1][2].

The current mobile ad-hoc networks allow for many different types of attacks. Although the analogous exploits also exits in wired networks but it is easy to fix by infrastructure in such a network. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this the attacks are classified as modification, impersonation, fabrication, wormhole and lack of cooperation[3].

Attacks using Modification: Modification is a type of attack when an authorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DOS attacks by modifying message fields or by forwarding routing message with false values.

Attacks using Impersonation: As there is no authentication of data packets in current ad-hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can either.

Attacks through Fabrication: Fabrication is an attack in which an authorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages

Gray hole attack: We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behaviour which is a combination of the above two, thereby making its detection even more difficult.

Wormhole Attacks: Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

Lack of Cooperation: Mobile ad-hoc networks rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources[4].

II. LITERATURE REVIEW

Soufiene Djahel, *et al.* [5] Nodes in mobile ad hoc networks (MANETs) usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments some nodes may refuse to do so for either saving their resources or intentionally disrupting regular communications. This type of misbehavior is generally referred as *packet dropping* attack or *black hole* attack, which is considered as one of the most destructive attacks that leads to the deterioration of network performance. The special network characteristics, such as limited battery power and mobility of nodes, make prevention techniques based on cryptographic primitives ineffective to cope with such attack. Rather, a more proactive alternative is required to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Once such scheme fails, some economic-based approaches can be adopted to alleviate the attack consequences by motivating the nodes cooperation. As backup, detection and reaction schemes remain as the final defense line to identify the misbehaving nodes and punish them. In this survey, we make a comprehensive investigation on state-of-the-art countermeasures to packet dropping attack. Furthermore, we examine the challenges that must be tackled for constructing an in-depth defense against such sophisticated attack.

K. Thirunadana Sikamani, *et al*. [6] Stream control transmission protocol (SCTP) is a transport level protocol providing end to end communication between two or more applications running in separate hosts. SCTP is operating on top of the connectionless packet network. It offers connection oriented, reliable transportation of independently sequenced message streams. It was originally designed to provide a general-purpose transport for message-oriented applications transporting signaling data. The biggest difference to TCP is multi-homing, the concept of several streams within a connection (multistreaming) and the transportation of sequence of messages instead of sequence of bytes. SCTP is designed to use multihoming. SCTP is capable to handle multiple IP-addresses on both endpoints. One of the possible address pairs is used as a primary path others are used for fault tolerance. Multi-homing and the heartbeat mechanism enable monitoring of the connection and detection of loss of a session in primary path. This gives the ability to change the transportation to a secondary path. SCTP includes appropriate congestion avoidance mechanisms and packet loss recovery functions as TCP and in addition it is resistant to flooding and masquerade attacks.

AikateriniMitrokotsa, et *al.* [7]The evolution of wireless network technologies and the recent advances in mobile computing hardware have made possible the introduction of various applications in mobile ad hoc networks. Not only is the infrastructure of these networks inherently vulnerable but they have increased requirements regarding their security as well. As intrusion prevention mechanisms, such as encryption and authentication, are not sufficient regarding security, we need a second line of defense, Intrusion Detection. The focus of this paper is on anomaly detection techniques in order to exploit their main advantage of being able to detect unknown attacks. First, we briefly describe intrusion detection systems and then we suggest a distributed schema applicable to mobile ad hoc networks.

Oscar F. Gonzalez, *et al.* [8] Mobile Ad Hoc networks (MANETs) are susceptible to having their effective operation compromised by a variety of security attacks. For example, misbehaving nodes can cause general network disruption by not forwarding packets on behalf of other nodes in the network. Nodes may misbehave either because they are malicious and deliberately wish to disrupt the network, or because they are selfish and wish to conserve their own limited resources such as power, or for other reasons. In this paper, we present a mechanism capable of detecting and accusing nodes that exhibit packet forwarding misbehavior. Our evaluation results demonstrate that our algorithm effectively detects and accuses nodes that drop a significant fraction of packets.

III. PACKET ROUTING IN MOBILE AD HOC NETWORKS

In wireless networking, a mobile node has a permanent "home" known as the home network. The entity within the home network that performs the mobility management functions is known as the home agent. The network in which the mobile node is currently residing in is known as foreign network, and the entity within the foreign network that helps the mobile node with mobility management functions is known as a foreign agent. A correspondent is the entity wishing to communicate with the mobile node [9]. When a mobile node is resident in a foreign network, all traffic addressed to the node's permanent address now needs to be routed to the foreign network. One way to handle this is for the foreign network to advertise to all other networks that the mobile node is resident in its network. But the problem with this approach is that of scalability. The routers may have to maintain forwarding table entries for potentially millions of mobile nodes. An alternative approach is to push mobility functionality to the network edge by having the home agent in the mobile node's home network track the foreign network in which the mobile node resides.

One of the roles of a foreign agent is to create a care-of address (COA) for the mobile node. Thus, there are two addresses associated with the mobile node one permanent address and one care-of address (COA). A second role of the foreign agent is to inform the home agent that the mobile node is resident in its network and has the given COA. This COA is used by the home agent to reroute datagram's to the mobile node via the foreign agent. There are two different approaches by which datagram's are addressed and forwarded to the mobile node:

- ***Indirect routing*** In indirect routing, the correspondent simply addresses the datagram to the mobile node's permanent address, and sends it into the network unaware of the mobile node's current location. The home agent intercepts and reroutes the datagram's addressed for nodes in the home network but are currently resident in a foreign network. Figure 3.1 depicts the process of indirect routing to a mobile node.
- ***Direct routing*** In direct routing, the correspondent node first learns the COA of the mobile node. Then it tunnels the datagram's directly to the mobile node's COA. When the mobile node moves from one foreign be broken and new links established.

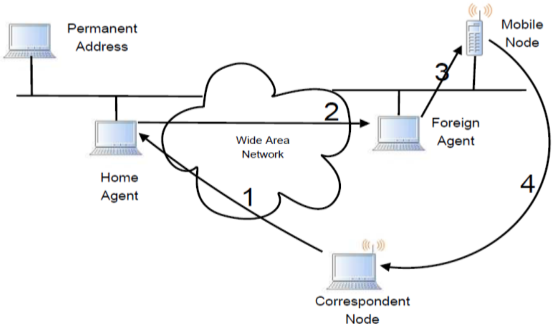

Figure 1: Indirect Routing in Mobile IP

network to another, either the correspondent node is to be notified or the new foreign agent inform the old one of the mobile node's current location and have the old agent forward the datagram's to the new COA. Figure 2 depicts the direct routing to a mobile node.

An ad-hoc network is one that comes together as needed to meet the communication needs of the moment without relying on the existence of any preinstalled infrastructure to deliver its services. Each node in an ad-hoc network, if it volunteers to carry traffic, participates in the formation of network topology. The nodes in an ad-hoc network may be mobile so that two nodes within communication range at one point of time may be out of range some time later. Also, the nodes assist each other in the process of delivering packets of data as not all of them are within the range of each other. An example ad-hoc network is shown in Figure 3.3. In an ad-hoc network, nodes are able to move relative to each other; as this happens, existing links may

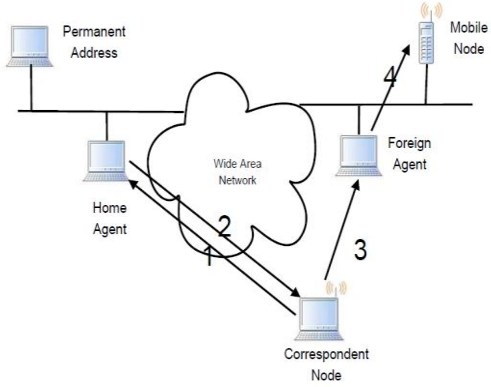

Figure 2: Direct Routing in Mobile IP

For example, as shown in Figures 3 and 4, node 4 moves away from node 1 and as a result the link between 1 and 4 gets broken and as it moves closer to 8, a new link is established between nodes 4 and 8.

ROUTING TECHNIQUES IN AD HOC

The network and routing protocols in the Internet were not designed with mobility in mind. So, the Internet cannot handle mobile computers very well. There are many kinds of protocols available today that are supported by network infrastructure. Some of these protocols need adaptation before they can be useful within a network no longer connected to the network infrastructure and some of them may not be appropriate for use when the infrastructure is not available (for example, credit card validation, network management protocols).

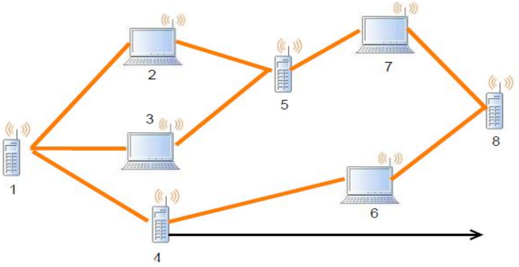

Figure 3: Ad-hoc network example (1)

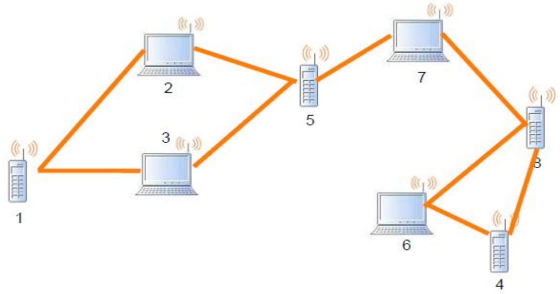

Figure 4: Ad-hoc network example (2)

Many efforts to support mobility and to repair the outdated assumptions in the Internet rely on additional infrastructure elements for managing data related to mobile computers (for example, Mobile IP and various proxy architectures). Ad Hoc routing protocols can be broadly classified based on whether nodes in an ad-hoc network keep track of routes to all possible destinations or instead keep track of only those destinations of immediate interest. All protocols that follow the former practice are called "proactive protocols" and the ones follow the latter one are called "reactive protocols". For any protocol to be useful in an ad-hoc network, it must provide for automatic topology establishment, to cater for the absence of any infrastructure, and dynamic topology maintenance, to enable user mobility.

IV.SIMULATION AND RESULTS

This chapter details the simulation model used for our experiments and provides an analysis of the simulation results obtained. For our experiments, we have used the Network Simulator 2 [10] to simulate an ad-hoc wireless network running the Dynamic Source Routing protocol. NS (version 2) is an object-oriented, discrete-event driven network simulator written in C++. NS is useful for simulating a variety of IP networks. It implements network protocols such as TCP and UPD, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as link-state, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations [11], [12].

- ***Gauss-Markov Model:*** This model was designed to adapt to different levels of randomness. Initially each node is assigned a current speed and direction. At fixed intervals of time, movement occurs by updating the speed and direction of each node. Specifically, the value of speed and direction at the n^{th} instance is calculated based upon the value of speed and direction at the $(n-1)^{th}$ instance. The main advantages of this model are that it eliminates the sudden stops, sharp turns present in Random way point mobility model and it is close to being realistic.

Gauss-Markov

In this model also, the nodes move about at a maximum speed of 20 m/s. So, this represents a high mobility Gauss-Markov model. We can observe a similar effect of the detection interval on the detection effectiveness and false positive rate as we have seen in the previous mobility models.

- ***Detection Efficiency*:**

Figure 5 shows the detection effectiveness of the technique for "Gauss Markov" mobility model. Here also, the detection effectiveness decreases with increase in the detection interval agreeing with the previous scenarios. As mentioned earlier, this is a more realistic mobility model when compared with the random way point model where nodes choose a random destination, speed and starting moving toward the destination. So, when we compare the detection effectiveness of this model with the high mobility random way point model, we can see that the Gauss-Markov model exhibits a slightly better detection effectiveness when compared to the random way point model. This could be due to the more realistic movement of the nodes in this model. Because of a more realistic mobility, the chances of getting an unrelated route error messages is lower in the case of Gauss-Markov model when compared to the Random Way Point mobility model which leads to a better detection effectiveness.

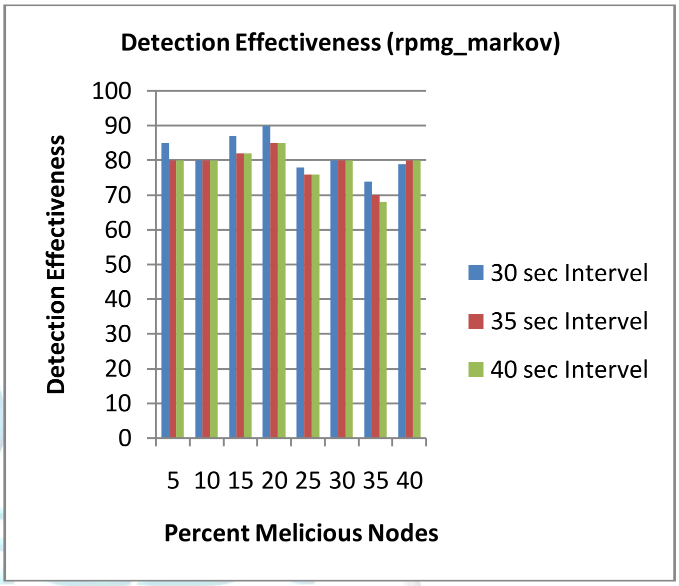

Figure 5: Detection Efficiency – Gauss Markov

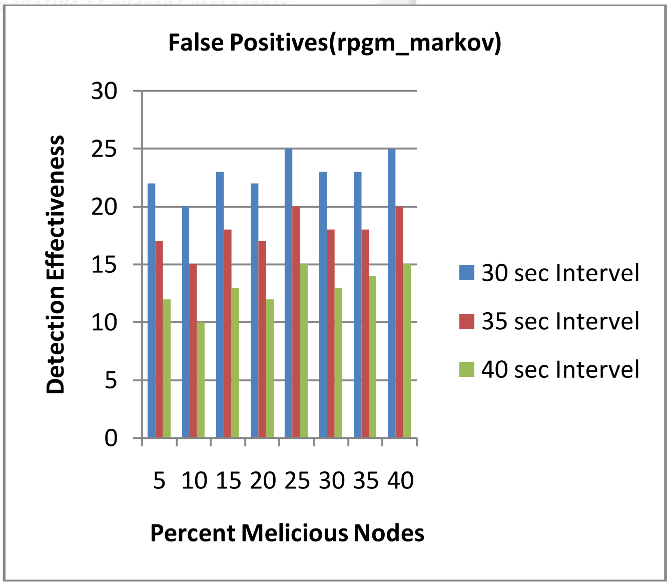

Figure 6: False Positive Rate – Gauss Markov

- ***False Positive Rate*:**

Figure 6 shows the false positive rate of the technique for "Gauss Markov" mobility model. The results agree with the previous scenarios as the false positive rate decreases with increase in detection interval. Also, when we compare this result with that of random way point mobility networks, we can observe that Gauss-Markov has a slightly lower false positive rate. This can again be attributed to the more realistic motion in the case of Gauss-Markov model. We speculate that the number of route error messages dropped is more in the case of random way point mobility when compared to Gauss-Markov mobility which leads to a lower false positive rate for Gauss-Markov mobility model.

V.CONCLUSIONS

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. Simulation results show that this technique has good detection effectiveness across a wide variety of network mobility models. The detection effectiveness tends to decrease when the network is highly loaded, when there is a long distance between neighboring nodes, or when the nodes are highly mobile. These situations are problematic for the network in general, since they cause increase in route maintenance and a decrease in packet transmission success. This technique also maintains low false positive rate in all the different scenarios considered.

VI.REFERENCE

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

[2] Ram Ramanathan and Jason Redi "A Brief Overview of Ad Hoc Networks: Challenges and Directions" IEEE Communications Magazine- 50th Anniversary Commemorative Issue/May 200.

[3] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[4] 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.

[5] Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges Soufiene Djahel, Farid Na¨ıt-abdesselam and Zonghua Zhang Manuscript received February 2010.

[6] "Packet loss recovery in mobile ad-hoc network by stream control congestion algorithm", K. Thirunadana sikamani, V. Rajamani and r. Madhusudhanan, International J. of Engg. Research & Indu. Appls. (IJERIA). ISSN 0974-1518, Vol.1, No. VII (2008), pp 129-140

[7] "Intrusion Detection of Packet Dropping Attacks inMobile Ad Hoc Networks AikateriniMitrokotsa, Rosa Mavropodi, Christos Douligeris Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str. Piraeus 18534, Greece Ayia Napa, Cyprus, July 6-7, 2006

[8] Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou Manuscript received September 25, 2007.

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

[10] S. Buchegger and J. Le Boudec. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In *Proceedings of the Parallel, Distributed and Network-based Processing*, pages 403–410, January 2002.

[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the Mobile Computing and Networking*, pages 255–265, 2000.

[12] R. Griswold. Malicious node detection in ad hoc wireless networks. Master's thesis, Washington State University, Pullman, 2003.