International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 9 (September '2016)

A STUDY ON PACKET ROUTING AND DROPPING IN MANET MALICIOUS NODES

T.Jayanthi,
M.Phil Scholar,
Department of Computer Science,
Siri PSG College of Arts and Science for women,
Sankari, Tamilnadu, India.

K.Sumathi,
Head cum Assistant Professor,
Department of Computer Science,
Siri PSG College of Arts and Science for women,
Sankari, 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. In this paper discussed packet routing and dropping, malicious node detection techniques and an experiment in random way test.

Keywords: Mobile ad hoc network, packet routing, malicious node, security

1. 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. As wireless nodes proliferate and as applications using the Internet become familiar to a wider class of customers, those customers will expect to use networking applications even in situations where the Internet infrastructure itself is not available. For instance, people using laptop computers at a conference in a hotel might wish to communicate in a variety of ways, without the mediation of routing across the global Internet. These user expectations lead to what is called an "ad-hoc network", a short-lived network just for the communication needs of the moment. In other words, an ad-hoc network is one that comes together as needed, not necessarily with any assistance from the existing Internet infrastructure [1].

II.LITERATURE REVIEW

Kennedy Edemacu1, *et al.* [2] Wireless ad hoc networks have gained lots of attention due to their ease and low cost of deployment. This has made ad hoc networks of great importance in numerous military and civilian applications. But, the lack of centralized management of these networks makes them vulnerable to a number of security attacks. One of the attacks is packet drop attack, where a compromised node drops packets maliciously. Several techniques have been proposed to detect the packet drop attack in wireless ad hoc networks. Therefore, in this paper review some of the packet drop attack detection techniques and comparatively analyze them basing on; their ability to detect the attack under different attack strategies (partial and or cooperate attacks), environments and the computational and communication overheads caused in the process of detection.

A.Janani, *et al.* [3] Mobile Ad-hoc Network (MANET) is an application of wireless network with self-configuring mobile nodes. MANET does not require any fixed infrastructure. Its development never has any threshold range. Nodes in MANET can communicate with each other if and only if all the nodes are in the same range. This wide distribution of nodes makes MANET vulnerable to various attacks, packet dropping attack or black hole attack is one of the possible attacks. It is very hard to detect and prevent. To prevent from packet dropping attack, detection of misbehavior links and selfish nodes plays a vital role in MANETs. In this paper, a comprehensive investigation on detection of misbehavior links and malicious nodes is carried out.

Thaier Hayajneh, *et al.* [4] Detecting malicious packet dropping is important in ad hoc networks to combat a variety of security attacks such as black hole, greyhole, and wormhole attacks. We consider the detection of malicious packet drops in the presence of collisions and channel errors

and describe a method to distinguish between these types. We present a simple analytical model for packet loss that helps a monitoring node to detect malicious packet dropping attacks. The model is analyzed and evaluated using simulations. The results show that it is possible to detect malicious packet drops in the presence of collisions and channel errors.

Oscar F. Gonzalez, *et al.* [5] 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.

Ignacy Gawedzki, *et al.* [6] Proactive routing protocols for mobile ad hoc networks currently offer few mechanisms to detect and/or counter malevolent nodes. Stability and performance of most, if not all, emerging standard proactive protocols rely on cooperation between nodes. While cryptographic methods may be a solution to secure control messages, nodes not willing to cooperate may still decide not to forward data packets. In this paper, a method to enable resilience to such malevolent nodes is presented. It is non-intrusive with respect to the packet forwarding mechanisms (e.g. TCP/IP kernel stack) and particularly well suited for integration with proactive routing protocols.

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 [7]. 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 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.

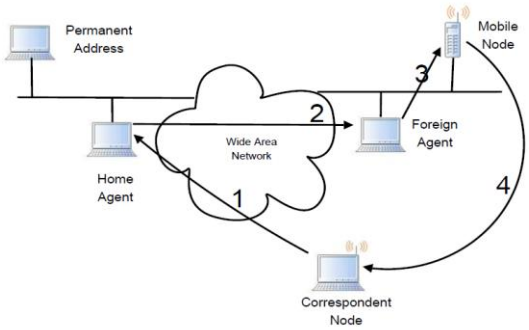

Figure.1: Indirect Routing in Mobile IP

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. In an ad-hoc network, nodes are able to move relative to each other; as this happens, existing links may

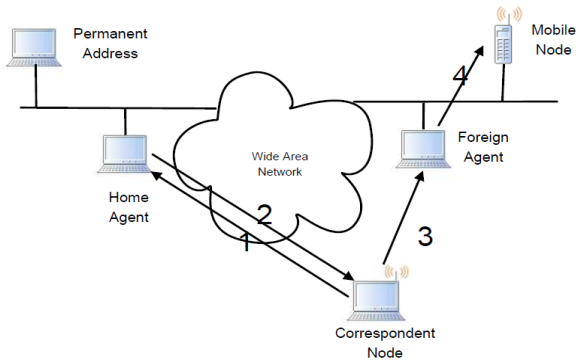

Figure 2: Direct Routing in Mobile IP

IV. PACKET DROPPING IN AD HOC NETWORKS

Packet dropping can be experienced in wireless ad hoc networks where no compromised nodes are present. This packet loss is mainly associated with the following events;

- **Network Congestion:** Network congestion in wireless ad hoc networks is something unavoidable. These networks are mainly scalable due to in and out

movements of nodes. As a result, congestion is more likely to happen which can lead to loss of packets.

- **Channel Conditions:** In wireless networking the channel condition cannot be neglected since it changes drastically. Free path loss, interference, presence of noise on the channel and fading of the transmitted wireless signals are among the channel conditions that can lead to packet loss or bit errors in the transmitted signal. In the presence of these factors, some packets can get dropped.
- **Resource Constraints:** Nodes in wireless ad hoc networks have limited energy resource [8]. Intermediate nodes in these networks may behave selfishly and fail to forward the received packets in order to conserve their limited resources battery power. These packets in turn get dropped.

V. MALICIOUS BEHAVIOR DETECTION

Watchdog and Path rater: Watchdog is used to detect and identify a malicious node, while the path rater performs the job of isolating that node. Every node in the network includes both a watchdog and a path rater. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions, which requires the presence of bi-directional links. If the next node does not forward the packet, it is misbehaving. The watchdog detects misbehaving nodes. Every time a node fails to forward the packet, the watchdog increments the failure tallies. If the tally exceeds a certain threshold, it determines that the node is misbehaving; this node is then avoided using the path rater. The path rater combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. For example, if node 1 forwards a packet to node 2 and node 2 forwards the packet to node 3, node 1 can snoop node 2's retransmission and compare it with a copy of the packet, as shown in Figure 4.1. If the packets differ, which is the case when the packet is corrupted or misrouted or node never transmits the packet, and then the packet source is notified.

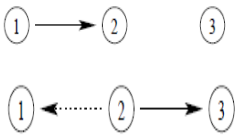

Figure 3: "Watchdog" operation.

Each node starts with a rating of 0.5, which increases by 0.1 every 200ms to a maximum of 0.8. The node gives itself a rating of 1.0. Every time a node reports a broken link, its rating decreases by 0.05 to a minimum of 0.0. When there are multiple paths to a destination, a node will choose the path with the highest rating. If all nodes in all paths are ranked equally, then the node will pick the shortest path to the destination, which is the same as standard DSR. When a node receives a notice about a malicious node, it reduces the rating for that node to -100.0. Over time the rating for that node will increase, and, unless it continues to misbehave, after 200 seconds its rating will be up to 0.0. This prevents falsely identified nodes from being permanently excluded from the network.

Nodes Bearing Grudges: This protocol is composed of four components that are closely coupled together, as shown in Figure 4. Nodes start out trusting all other nodes in the network, but build grudges against nodes that exhibit malicious behavior. The monitor component monitors neighboring nodes to detect malicious behavior in a similar manner as the watchdog. If it detects any malicious behavior, it alerts the reputation system. The reputation system evaluates the alarm and determines if the event is significant. If the event is significant, the event count is incremented. Once the count reaches some threshold, the reputation for the misbehaving node is reduced. When the reputation for the node gets low enough, the path manager is alerted.

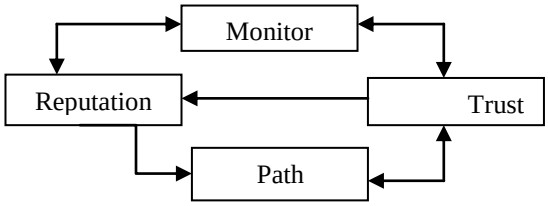

Figure 4: "Nodes Bearing Grudges" components.

The path manager is similar to the path rater. It adjusts the ranks of paths based on information about nodes in the path. If a path has a malicious node, that path is deleted to prevent routing through the malicious node. The path manager also ensures that the node does not forward data for malicious nodes. This prevents the problem of rewarding bad behavior. Finally, the trust manager handles interaction with other nodes through the use of special alarm messages. The trust manager has a trust table and a friends table. The trust table is used when processing incoming alarm messages and the friends table is used when sending alarm messages. If a malicious node is detected, the trust manager sends an alarm message to other nodes in the friends table so that they will avoid the malicious node. When the node receives an alarm message, it looks up the source node in the trust table to see how much it trusts the sender. The trust level controls how much weight the event in the alarm message is given. The event is weighted and passed on to the reputation system [4].

Route-based Packet Filtering: This technique was developed for wired networks but may be adapted to ad-hoc wireless networks. Packet filtering works by placing filters at key points in the network, which perform rout ability checks on incoming packets. The rout ability checks determine if the packet is traversing a legitimate path between the source and destination addresses. In an ad-hoc wireless network, this can catch some malicious behavior, including misrouting of packets, impersonation attacks where the malicious node is not next to the impersonated node, and possibly some black hole routing protocols attacks. Figure 5 shows how route-based packet filtering can catch misrouted packets. In this example, node 7 knows the packet is not routed correctly because destination node 9 is not reachable from node 7. Node 6 knows that the packet it received is not routed correctly since source node 1 is not reachable from node 4.

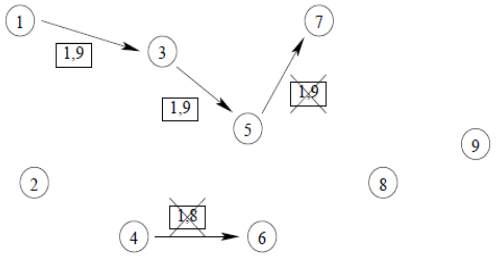

Figure 5: Packet filter operation.

The routability checks require knowledge of valid routes in the network, which is difficult to determine due to the dynamic nature of the network. In some routing protocols, such as DSDV and CGSR, each node has a table with all valid routes in the network. With other source-routed ad-hoc routing protocols, such as DSR, the packet carries the full route between the source and destination, and this information can be used to check for valid routing.

Perfect Ingress Filtering: A variant of route-based distributed packet filtering that places filters on all nodes in the network. It may catch more packets sooner than route-based distributed packet filtering and is effective in preventing some types of attacks, such as DDoS. Since the filters are placed on all nodes, every packet will be examined. Perfect ingress filtering has similar drawbacks to route-based distributed packet filtering. Because the filters are placed on all nodes, it is even more difficult to deploy. It may not even be possible to deploy on some nodes that are very limited in processing capability.

VI.UNOBTRUSIVE MONITORING

Unobtrusive monitoring technique is proposed to overcome some of the problems associated with the existing techniques. This technique can be used to detect Byzantyne faults such as dropping or misrouting packets. The main focus of this research is *malicious packet-dropping*, where a node intentionally drops packets that are destined for other nodes. The methodology and the algorithm used for detecting malicious packet dropping is discussed with an example scenario in the following. The unobtrusive monitoring technique relies on readily available information at different network levels to detect the presence of malicious nodes and does not require modification or cooperation of all the nodes in the network. This technique mainly involves collecting and analyzing locally available data. Local data such as DSR route request and route error messages, and TCP timeouts is used to detect malicious behavior in the network. Some of the salient features of this technique include:

- ***Single node operation*:** Unobtrusive monitoring requires modification only to the node that it runs on.
- ***Portable*:** This technique does not require any new protocols. It works with existing protocols, such as DSR, mobile IP, and ICMP which allows the technique to be easily ported to many different systems.
- ***No additional battery wastage*:** This technique uses data that is readily available in the network. So, it does not dissipate or waste battery power for exchanging control information with the neighboring nodes.
- ***No node cooperation*:** This approach does not rely on the cooperation of other nodes in the network.
- ***No security associations*:** Since this technique does not need the cooperation of other nodes in the network, there is no requirement to have security associations between the nodes. Other security mechanisms such as "Nodes Bearing Grudges" and "Intrusion Detection in Wireless Ad-Hoc Networks" require security associations between neighboring nodes to authenticate the messages passed among themselves.
- ***No infrastructure*:** It does not require support of any type of infrastructure, such as network controllers or certificate authorities.
- ***Highly scalable*:** Since this technique is not tied down by the cooperation or security associations between neighboring nodes, it can be incorporated into as many nodes as needed making it highly scalable. Currently, unobtrusive monitoring has been tested to work with DSR, and it is expected to work with other routing protocols as well.

The unobtrusive monitoring technique uses data that is readily available from different network levels. The data collection and analyzer components lie at the core of the detection technique. The data collection component collects useful control information such as DSR Route Error messages and TCP timeout and retransmission times. The data collection component gathers this information received within a certain interval of time called the *detection interval*. Any information older than the detection interval is discarded which guarantees the freshness and relevance of the collected information and also suits the requirements of a memory constrained node. This collected data is passed on to the data analyzer component which extracts useful information from these control messages and checks for any deviation from normal behavior. The information extracted by the analyzer may include the following:

- The TCP flow on which the DSR route error message is received.
- The TCP flow id on which a packet timed out and the sequence number of that packet.
- The time that each message was received or each event occurred.

The data analyzer uses this information to determine if any malicious activity is taking place. If any such behavior is detected, the corresponding node is alerted so that it can take appropriate action.

VII. SIMULATION

In our simulations, the following mobility models were used to evaluate our unobtrusive monitoring technique.

Random Way-Point Model: In this model, a node moves from its current location to a new location by randomly choosing a direction and speed in which to travel and pauses between changes in direction and/or speed. This is a memory less mobility pattern because it retains no knowledge concerning its past locations and speed values. The current speed and direction of a node is independent of its past speed and direction. This characteristic can generate unrealistic movements such as sudden stops and sharp turns [9]. In these kinds of networks a node chooses a random destination, speed and starts moving towards that destination. Between movements it pauses for some amount of time referred to as

"pause time". To simulate medium mobility networks a maximum node speed of 5 meters/second and a pause time of 30 seconds were chosen and a maximum speed of 20 meters/second and a pause time of 5 seconds were chosen for high mobility networks. For high mobility networks, we present the results for detection intervals of 20, 30, 35, 40, and 50 seconds. For medium mobility networks, we present the results for detection intervals of 30, 35, and 40 seconds. Also, for the metrics considered, the number of malicious nodes is increases from 5% to 40% in 5% increments. The results for the metrics used for these simulations are as given below:

Detection Efficiency:

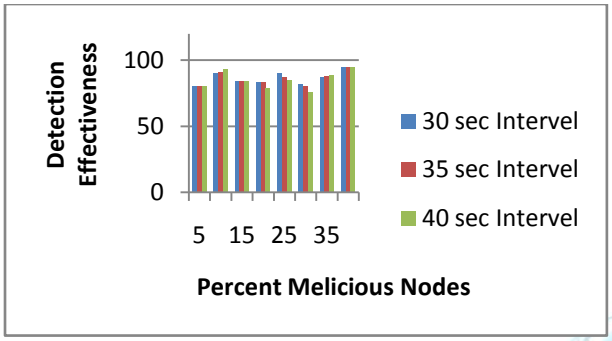

Figure 6: Detection Efficiency – Random Way Point (Medium Mobility)

The detection effectiveness for medium and high mobility networks is as shown in figures 6 and 7 respectively. From these figures we can see that for both medium and high mobility networks, increasing the detection interval lowers the detection effectiveness. This is because when using a bigger detection interval, there is a much higher probability of getting unrelated route error messages within this interval. Also, we can see that the detection effectiveness is better in the case of medium mobility networks when compared to high mobility ones. Due to higher mobility, the links get broken quite frequently and there are many route error messages sent out by the nodes in the network. This also increases the probability of receiving unrelated route error messages within the detection interval at a source node and the source node correlates any TCP timeouts with the received route error message and thus leads to a decrease in detection effectiveness.

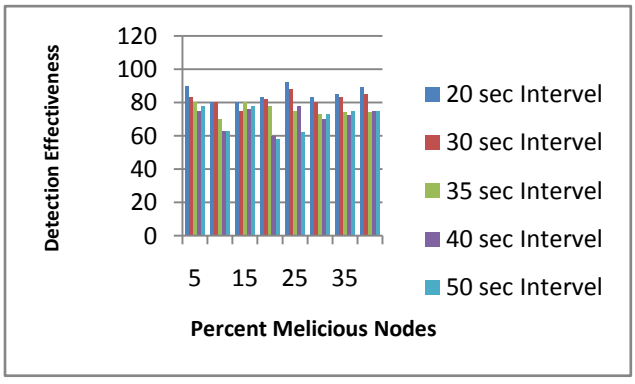

Figure 7: Detection Efficiency – Random Way Point (High Mobility)

VIII.CONCLUSIONS

Mobile ad-hoc networks 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. 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.

REFERENCES

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

[2]. "Packet Drop Attack Detection Techniques In Wireless Ad Hoc Networks: A Review" , Kennedy Edemacu1, Martin Euku2and Richard Ssekibuule3 International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014

[3]. "Survey Of Packet Dropping Attack In MANET", A.Janani, A.Sivasubramanian A.Janani et.al / Indian Journal of Computer Science and Engineering (IJCSE) ISSN : 0976-5166 Vol. 5 No.1 Feb-Mar 2014

[4]. "Detecting Malicious Packet Dropping in the Presence of Collisions and Channel Errors in Wireless Ad hoc Networks", Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, and Taehoon Kim

[5]. 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.

[6]. Proactive Resilience to Dropping Nodes in Mobile Ad Hoc Networks Ignacy Gawedzki and Khaldoun Al Agha Laboratoire de Recherche en Informatique, CNRS Université Paris-Sud 11, F-91405 Orsay, France

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

[8]. H. Bakht. Understanding mobile ad-hoc networks. Online. http://www.computingunplugged.com.

[9]. K. Park and H. Lee. On the effectiveness of probabilistic packet marking for ip traceback under denial of service attack. In *Proceedings of the INFOCOM*, volume 1, pages 338–347, April 2001.