In Mobile Ad Hoc Networks, a Collaborative Security Architecture for Black Hole Attack Prevention

Monalisa Hati, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id- monalisa.hati@arkajainuniversity.ac.in

ABSTRACT: ***An ad hoc network is a collection of wireless mobile computers (or nodes) that collaborate by forwarding packets to one another, allowing nodes to interact beyond the range of direct wireless transmission. The black hole attack is a serious issue that may easily occur in ad hoc networks, particularly with popular on-demand protocols such as Adhoc On-demand Distance Vector Rooting (AODV). Prior ad hoc networking research has mostly focused on the routing issue in a now-adversarial network context, assuring a sufficiently secure environment. This article offers a collaborative architecture for detecting and excluding malicioos nodes that operate alone or in groups. The A&hoc On-demand Distance Vector Rooting (AODV) protocol is used as an example to concentrate on the network layer. This article explains how to extend the watchdog technique to include a collaborative architecture to combat node collusion.***

KEYWORDS: ***Collaboration, Intelligent networks, Mobile ad hoc networks, Ad hoc networks, Routing protocols, Communication system security.***

1. INTRODUCTION:

Mobile Ad Hoc networks are infrastructure-free networks in which nodes work together to relay packets so that they may interact beyond the range of direct wireless transmission. Because each node is free to move around, the network architecture has a lot of room to alter over time. Because of the dynamic nature of such networks, designing routing protocols, particularly secure routing protocols, is a difficult job. Malicious and selfish nodes may have a negative impact on a dynamic network like this. Our and others' simulation findings demonstrate that even a small number of rogue nodes may significantly reduce network throughput[1].Many research efforts have been made to address security issues in on-demand routing protocols in mobile ad hoc networks, such as authentication, intrusion detection, data encryption, and so on. This article focuses on the Ad-hoc On demand Distance Vector Routing (AODV) protocol, which allows a node to start the route discovery process only when it has data to send and includes routing security and resilience features.

The Black Hole Attack is a serious issue that may arise in Ad Hoc Networks, particularly with popular on-demand protocols like AODV. Any intermediate node in an ad hoc network may reply to a route request packet if it had a fresh enough route to the destination, according to the original AODV protocol. This was done in the hopes of reducing network routing delays. The original protocol, on the other hand, assumed that all nodes in a particular ad hoc network are trustworthy. Because this is not the case, any rogue node may easily crash the network in part or in whole by responding to the route request. Because the malicious node does not have to examine its routing database to respond to the route request, the malicious node's response will be quicker than a regular node's. When the malicious node responds, the node that initiated the route discovery concludes that the route discovery procedure is complete and begins transmitting data. As a consequence, the rogue node's routes are all gone[2].

The most apparent solution to the issue stated above is to deactivate intermediate node responses. There are two significant disadvantages to this approach. For starters, routing delays in big networks would skyrocket, and hostile nodes might easily masquerade and respond to the source node as the destination node, with the destination node not knowing the difference. As a result, this approach would be completely ineffective. In, Marti, Giuli, and colleagues proposed two methods for increasing throughput in an ad hoc network where nodes promise to forward data packets but do not. The concepts of a wutchdog, which identifies malicious nodes, and a pothunter, which aids routing protocols in avoiding harmful routes, are presented. However, the method used fails to identify node collusion, receiver collision, and other issues. a different approach, in

which they utilize additional request and reply messages to verify the authenticity of the node providing the route reply before transmitting the data packets. This approach implies that malicious nodes do not form groups, which is not always the case in real-world scenarios. The rest of the paper is laid out as follows. The watchdog idea is briefly explained in Section . Our extensions are described in Section.

THE WATCHDOG THEORY

The watchdog technique, as implemented by Marti, Giuli, and others in , identifies rogue nodes operating on their own by keeping a buffer of recently transmitted packets. When a node transmits a packet, its mtchdog guarantees that the packet is sent to the next node in the route. The watchdog does this by repeatedly listening to the next node. It is referred to as misbehaving if the following node does not send the packet.

To put it another way, every packet that the watchdog overhears is compared to the packet in the buffer to determine whether there is a match. The packet is deleted from the buffer when a match indicates that it was successfully delivered. A failure tally for the node responsible for forwarding the packet is increased if a packet remains in the buffer beyond the timeout interval. If the total exceeds a specified level, the node is classified as malicious, and the network is notified[3].

However, in a few of situations, this version of the watchdog fails to identify rogue nodes. Nodes with malicious intent, for example, may fraudulently report other nodes as misbehaving, even splitting the network by reporting that certain nodes in that route are misbehaving. Multiple nodes collaborating to knock the network down are a more sophisticated assault that our model cannot identify. This is one of the paper's main points of emphasis.

. Conceptual Extensions of the Watchdog

The categorization of network nodes into trustworthy, watchdog and regular nodes is one of the contributions offered in this article. Every node was a watchdog for every other node under the earlier application of the watchdog concept. Though simple to implement, this idea would lead to the aforementioned issue of nodes erroneously identifying other nodes as hostile.

Nodes are categorized into trustworthy and ordinary nodes using this method. When a network is established, it is presumed.

Trusted nodes make up the initial few nodes of a network.

Following that, any node that enters the network must demonstrate its trustworthiness in order to be promoted to the trusted group of nodes.

Another assumption is that trustworthy nodes are neither malevolent nor self-interested. This categorization of nodes into trusted and ordinary nodes, as well as the selection of watchdogs from only trustworthy nodes for a certain period of time, guarantees that false reporting issues are avoided.

For a particular period of time, the watchdog nodes are chosen from among the list of trustworthy nodes based on the following criteria. 1) node energy, 2) available node storage capacity, and 3) node computing power The watchdog nodes are then given the additional task of monitoring the nodes in the network for malicious activity for a certain period of time. At the conclusion of the specified period of time, a new set of nodes is chosen from the trusted nodes set based on the node's new energy and available storage capacity levels.

Every chosen watchdog maintains two thresholds for all of its neighbors who are not trusted nodes. The first threshold is known as the SUSPECT-THRESHOLD, and it is maintained for each of the watchdog's surrounding nodes. The watchdog deems a node malevolent if it crosses its SUSPECT-THRESHOL. The ACCEPTANCE-THRESHOLD is a measure of an adjacent node's excellent conduct, and when surpassed as a consequence of continuous acceptable packet forwarding behavior over a defined length of time, that surrounding node qualifies as a trusted node. As can be seen, the first threshold is determined based on the

network's sensitivity to malicious activity. The second threshold, known as the ACCEPTANCE-THRESHOLD, is set high enough that nodes are only deemed trustworthy after demonstrating excellent behavior over a long period of time[4].

It has been observed that certain network nodes may suffer significant traffic and network congestion at any given time, particularly if the node is the sole accessible connection between two network partitions. The SUSPECT-THRESHOLD for such nodes is expected to rise quite rapidly. To take into account such occurrences. The network's threshold level, which was set at the time of its creation, is maintained at a reasonable high level.

Four additional packet types are added over the existing ones to apply the security enhancements to the current AODV routing system.

The packet kinds are as follows:

Transmit-DATA: Every node in the network uses this packet type to notify the watchdogs that they are going to send a data packet. The packet contains the source ID, destination ID, and next hop ID[5].

NODESNEIGHBORS: Every time a node transmits a data packet to another node, the neighborhood's watchdog node records that node's neighbor. In this way, the watchdog node obtains a good understanding of who the neighbors of a particular node are over a period of time. The watchdogs on the network share and update the network structure amongst them by sending out this NODESmIGHBORS packet. This is useful for preventing a rogue node from delivering a data packet to a node that does not exist.

TRUSTED-ENC-REQUEST: Trusted nodes send out a request to all other trusted nodes at the start or end of each watchdog timeout, requesting them to broadcast their energy and storage capacity levels.

2. DISCUSSION:

IS-WATCHDOG: This packet type notifies all trustworthy nodes which nodes have been designated as watchdogs. We presume that the aforementioned three packet types are encrypted and can only be decrypted by trustworthy nodes. IS-MALICIOUS: When an ordinary node passes the SUSPECT-THRESHOLD, it is classified as malicious, and the watchdogs broadcast this packet type to the network in order to isolate such nodes[6].

When a malicious node acts alone , when a source node S wishes to transmit a data packet to a destination node D, it initiates the route discovery process by sending a Route Request packet. If malicious node M responds with a Route Reply packet, the source node will first give out its network ID and the network ID of the node that provided it the initial RREP on the secure watchdog channel. The watchdog nodes W in the suspect node's neighbors list would then begin listening to and monitoring the suspect node's activities. The watchdog nodes increase the SUSPECT-NODE counter for that node n if the suspect node loses the data packets sent out by the source.

If the SUSPECT-NODE counter reaches the SUSPECT-THRESHOLD level in a certain amount of time, the suspect node is labeled malicious and disconnected from the network.

Similarly, when nodes operate in groups , the results are similar. When a malicious node MI receives a route request from a source S, it responds with a route reply. On the secure watchdog channel, Source S would issue a SEND-DATA signal and subsequently transfer data to node MI. If MI loses data, the watchdog nodes monitoring M1 will instantly report it. If M1 does not dump data but instead sends it to a second malicious node M2, but fails to deliver the SEND-DATA signal on the watchdog channel, the SUSPECT-NODE counter will be incremented again by the watchdog nodes monitoring MI. When M1 sends data to M2, M2 loses data packets, and MI does not retransmit the data or broadcast a 77 message to the prior node or source to retransmit, the watchdog nodes will increase the SUSPECT-NODE counter again, and the new value of the SUSPECT-NODE will be broadcast[7].

The Network Simulator NS2 is used for computer simulation. For 900 seconds, the simulation simulates 50 wireless nodes creating an ad hoc network traveling across a rectangle 3000m x 1500m) flat area.

The network latency and speed of black hole attack detection are determined by simulating different load situations[8].

Links are considered to be commonly bidirectional and symmetric in this study. The wireless interface is also expected to enable promiscuous mode of operation, which means that if one node X is within hearing range of another node Y, node X may hear every communication made by node Y, regardless of whether node X is participating in that transmission. For the simulation, a static network with equally distributed trustworthy nodes is first examined[9].

The nodes interact via ten node-to-node links with a fixed hit rate. For a period of 100 seconds, the watchdog nodes are chosen among the trustworthy nodes. The energy and storage capacity levels of the watchdog nodes are decremented by an arbitrary amount using a random number generator, following which a new set of watchdog nodes is chosen.

The proportion of malicious nodes ranges from 0% to 45 percent, with 5% intervals. Though it's rare to come across a network in which 45 percent of the nodes are hostile,

Following the implementation of the extensions, the network performance is assessed using the following metrics.

- Throughput: The proportion of packets received by the intended destinations is known as throughput.

Overhead is defined as the ratio of control packets being routed to actual data packets being sent. Because the objective is to compare data transfer to routing-related transmissions, transmissions are tallied rather than packets.

In this part, we assess our suggested watchdog concept expansions. For our preliminary findings, we examined black hole attacks, in which the attacker would reject all data packets going through it apart from providing bogus routes.

The first findings of implementing the modifications are encouraging; it has been seen that the extensions are effective in identifying and isolating malicious nodes in the network after the initial data loss. The first findings obtained up to the time of this paper's submission indicate that the proposed modifications are fairly effective in identifying the existence of collaborating hostile nodes even in the lack of mobility. When the watchdogs are activated, preliminary findings indicate that the network throughput increases significantly.

The addition of additional packet types, on the other hand, substantially raises network overhead. The watchdog method adds little to the routing overhead. However, the low routing cost caused by the deployment of watchdogs may be further decreased by extending the time interval between two watchdog selection procedures, particularly in the case of watchdog selection from trustworthy nodes[10].

3. CONCLUSION:

The security of ad hoc network routing protocols is still a work in progress, and further study is needed. Secure and reliable data transmission, particularly audio and video data, is the main issue of the day, given the widespread use of the internet as a shopping destination and the rapid expansion of wireless mobile units in the combat field and search and rescue operations. As a result, in the wireless world, secure apps are more important than ever.

We propose some enhancements to the watchdog idea in this article for situations where no a priori test connection exists between the nodes. Our first findings are encouraging, pointing to a method for detecting and isolating rogue nodes in the network that are acting alone or in concert with other malicious nodes to

bring the network down. We want to follow up on these ideas and create an effective method that can be seamlessly incorporated into existing protocols to construct safe paths when incorrect routing information is found. We believe that the findings will aid in the development of a more secure ad hoc routing system.

This article presents some preliminary work on extending the watchdog idea to identify several cooperating nodes. The simulations utilize situations in which nodes move very little or at all. The next step would be to apply this idea to situations in which nodes move around quickly and the network composition changes. The performance of routing extensions using TCPflows, which are prevalent in most networks, is also of considerable interest.

REFERENCES:

[1] Y. F. Yuan, "Black hole binaries in the universe," *Scientia Sinica: Physica, Mechanica et Astronomica*. 2017.

[2] R. Emparan, P. Figueras, and M. Martínez, "Bumpy black holes," *J. High Energy Phys.*, 2014.

[3] G. Ruppeiner, "Thermodynamic black holes," *Entropy*, 2018.

[4] N. Dadhich, J. M. Pons, and K. Prabhu, "On the static Lovelock black holes," *Gen. Relativ. Gravit.*, 2013.

[5] Wang Ding-xiong, "Can black-hole entropy be quantized ?," *Chinese Astron. Astrophys.*, 1991.

[6] M. Fähnle and G. Schütz, "Comment on magnonic black holes," *Journal of Magnetism and Magnetic Materials*. 2017.

[7] I. D. Novikov, "Black holes," *Surveys in High Energy Physics*. 2003.

[8] P. Bueno and P. A. Cano, "Universally stable black holes," *Int. J. Mod. Phys. D*, 2017.

[9] I. D. Soares, "A boosted Kerr black hole solution and the structure of a general astrophysical black hole," *Gen. Relativ. Gravit.*, 2017.

[10] X. Calmet and R. Casadio, "What is the final state of a black hole merger?," *Mod. Phys. Lett. A*, 2018.