Black Hole attack in Ad-hoc On Demand Distance Vector Protocol

Dhanashri Lamane, Swapna Patil, Ameya Naik

dhanashri.lamane@gmail.com
swapna80patil@gmail.com
ameyanaik@somaiya.edu

Abstract— Mobile ad hoc networks (MANETs) are multi-hop wireless networks of autonomous mobile nodes without any fixed infrastructure. In MANETs, it is difficult to detect malicious nodes because the network topology constantly changes due to node mobility. A malicious node can easily inject false routes into the network. A traditional method to detect such malicious nodes is to establish a base profile of normal network behavior and then identify a node's behavior to be anomalous if it deviates from the established profile. As the topology of a MANET constantly changes over time, the simple use of a static base profile is not efficient. In this presentation, we propose a clustering-based anomaly detection approach, called DCAD, which allows the profile to be dynamically updated. In the approach, we use the weighted fixed width clustering (WFWC) algorithm in order to establish a normal profile and to detect anomalies. We conduct MANET simulations using the NS2 simulator and consider scenarios for detecting several types of routing attacks on AODV protocol. The simulation results show that DCAD can be successfully used for detecting anomalies caused by malicious nodes in AODV-based MANETs.

Keywords*-anomaly detection; dynamic clustering; MANET; AODV; routing attack*

*****

1.1 Introduction

Mobile Ad-hoc Networks are collections of autonomous wireless mobile nodes constructed dynamically without the use of any existing network infrastructure or centralized administration [1]. These networks are suitable for applications in which no infrastructure exists, such as military battlefield, emergency rescue, and vehicular communications. In MANETs, due to mobility of nodes, the network topology may change quickly over time. Hence, MANETs can be described as networks with highly dynamic and constantly changing topology. These inherent features make MANETs more vulnerable to routing attacks than wired networks. Generally, there are two types of intrusion detection: misuse detection and anomaly detection [2]. A misuse detection approach compares current behavior with known attack signatures and generates an alert if there is a match. Although misuse detection approaches are effective and efficient in detecting known attacks, they cannot detect new attacks whose signatures are unknown. An anomaly detection appr`1oach establishes a profile of normal behavior and detects behaviours that deviate significantly from the established profile as anomalies. The advantage of anomaly detection approaches is that they do not require prior knowledge of attacks and can thus detect new or so called zero-day attacks.

The anomaly detection approaches can be classified into semi-supervised and unsupervised. Semi-supervised anomaly detection approaches require a set of purely normal training data from which they establish the profile of normal behavior. If the training data contains some attacks buried within it, the approach may not detect future instances of these attacks. On the other hand, unsupervised anomaly detection approaches establish the profile of normal behavior with unlabeled training data that consists of both normal as well as anomalous samples. These approaches make two assumptions about the data. The first assumption is that the number of normal samples greatly outnumbers the number of anomalous samples. The second assumption is that the anomalous samples themselves are qualitatively different from the normal samples [3]. As the topology of a MANET constantly changes over time, the simple use of a static base profile may not represent the current state of the network. In this paper, we propose a clustering-based anomaly detection approach, called DCAD, which allows the profile to be dynamically updated. The approach consists of two main phases: training and detection. In the training phase, we use the WFWC algorithm in order to establish a profile of normal network behavior. In detection phase, we use weighted coefficients and a forgetting equation to periodically update the normal profile

2.MOBILE AD-HOC NETWORKS

2.1 MOBILE AD-HOC NETWORKS

The network in which mobile nodes operates not only as host but also as a router is called as Mobile Ad-hoc Network (MANET) An Ad-hoc networks is a collection of mobile nodes that form temporary network and capable of communicating with each other without the use of network infrastructure or any centralized administration

2.2 Characteristics of Ad-hoc Network

i) Open medium
ii) Dynamic topology
iii) Distributed Co-operation

2.3 Introduction to routing

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network.In ad hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it: typically, a new node announces its presence and listens for announcements broadcast by its neighbors. Each node learns about others nearby and how to reach them, and may announce that it too can reach them.

Note that in a wider sense, ad hoc protocol can also be used literally, to mean an improvised and often impromptu protocol established for a specific purpose. The following is a list of some ad hoc network routing protocols

2.4Types of routing protocols in Ad-hoc Networks

Proactive (Table Driven Protocol)
Reactive(On Demand Protocol)
Hybrid

Proactive Protocol(Table Driven Protocol)

This type of protocols maintains fresh lists of destinations and their routes by periodicallydistributing routing tables throughout the network. The main disadvantages of such algorithms are:

i. Respective amount of data for maintenance.
ii. Slow reaction on restructuring and failures.

The routing tables are updated regularly in order to maintain up-to- date routing information

Reactive Protocol(On Demand Protocol)

This type of protocol finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

i.High latency time in route finding.
ii.Excessive flooding can lead to network clogging.
iii.Have a Lazy Approach
Creates routes only when desired by source node
iv.Source Initiated
Nodes does not initiate until route to the destination is required

3. AD-HOC ON-DEMAND DISTANCE VECTOR PROTOCOL

3.1 Ad-hoc On-demand Distance Vector(AODV)

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. AODV uses hop-by-hop routing. Every node forwards data packets towards a destination node according to its routing table. The routes in the AODV routing table are kept up to date as long as they are needed by the source. AODV maintains a single path per a destination. The routing is divided into two basic mechanisms. The first one is the route discovery. It is responsible for finding a route to the destination if none is currently available in the routing table of the node. The second one is the route maintenance which keeps the routes up-to-date, e.g. removes broken paths .AODV protocol only works in a network where the communication links are bidirectional because if an (intermediate) node receives either a Route REQuest (RREQ) packet or a Route REPly (RREP) packet, it caches the previous node in its routing table as a next hop to the end nodes. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the „Destination Sequence" number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors [4]. If the number in the routing table is higher than the number in the packet, it denotes that the route is a „fresh route" and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. This process goes on until the packet is received by destination node or an intermediate node tha has a fresh enough route entry for the destination.

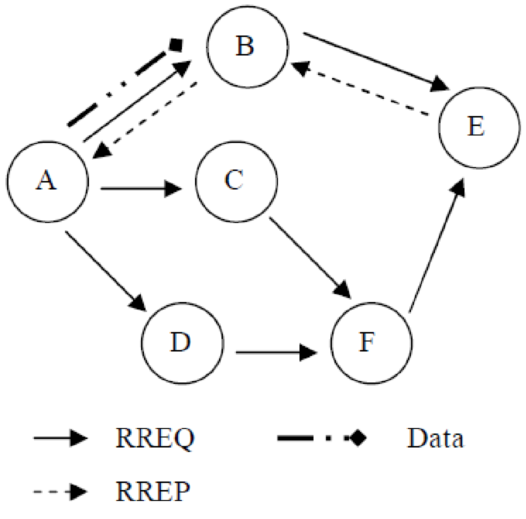


FIGURE : 1 Propagation of RREQ & RREP from A to E

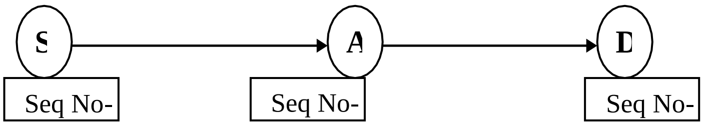


FIGURE: 2 Illustration of black hole attack

In the Fig.2 ‟S‟ is source, „D‟ is destination,‟ A‟ is intermediate node. If „A‟ node receives a RREQ packet, it checks if it is the destination node. If not, it checks if it has seen this RREQ before by checking the request ID and source node ID. If this is the case the node just drops the packet and does not forward the RREQ any further. This avoids loops in the route. If the RREQ packet is not dropped, the intermediate node searches in its route cache table. If there is an active route to the destination, it sends back a RREP with its route entity. Otherwise it just rebroadcasts the received RREQ. The freshness of a route is indicated by a destination sequence number that is attached to it. If the destination node has received the RREQ, it generates a RREP packet and sends it back in reverse way to the source. If an intermediate node receives either a RREQ or a RREP packet, it stores information about the previous node from which the packet was received in its routing table With this mechanism, hop-by-hop routing, a node can therefore decide which next hop it can use to reach a destination node..Then destination sends RREP to source through this reverse route. Then source starts sending actual data.

3.2 Attacks in Ad-hoc Network

1.Black Hole
2.Denial of Service
3.Routing table overflow
4.Impersonation
5.Energy Consumption
6.Information Disclosure

3.3 Black hole Attack

Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, In AODV, Destination Seq(Dst Seq) is used to determine the freshness of routing information contained in the message from originating node.[4] When generating a RREP message, a destination node compares its current sequence number, and Dst Seq in the RREQ packet plus one, and then selects the larger one as RREP‟s Dst Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst.Seq in order to construct a route. To succeed in the black hole attack the attacker must generate its RREP with Dst.Seq greater than the Dst Seq of the destination node. It is possible for the attacker to find out Dst. Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP‟s Dst Seq base on the received RREQ‟s Dst Seq. However, this RREQ‟s Dst Seq may not present the current Dst Seq of the destination node. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. In the above Fig.2 assume Node „B‟ is the malicious node. When Node „S‟ broadcasts the RREQ, Node „B‟ immediately responds to Node „S‟ with an RREP message that includes the highest sequence number of Node „D‟, as if it is coming from Node‟ D‟. indicates having fresh and shortest route. Node „S‟ assumes that Node ‟D‟ is behind Node

„B‟ with 1 hop and discards the newly received RREP packet come from other nodes. Afterwards Node 1 starts to send out its data packet to the node „B‟ trusting that these packets will reach to node „D‟ but Node „B‟ will drop all data packets. This is called as „black hole attack‟. Such many number of black hole nodes may be present is network which saviorly damages the network, called as „Co-operative Black hole Attack‟. Attacks to the wireless ad- hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses [5]. Cryptography or Authentication mechanisms protect the network against attacks that come from outside, malicious „insiders‟ which can also threaten the security. So to secure MANET it is important to know how an insider is able to attack. Wireless ad-hoc networks should be protected with intrusion detection system that can understand the possible actions of attackers and can produce a solution against these attacks. [5] Some time in AODV if in RREP the next hop information is also asked than malicious node provide next malicious node as next hop, so when confirmed with the next hop then next malicious node replies that i am having route to the destination node but actually they don't have any information of routes to destination. This case is shown in Fig. 4.

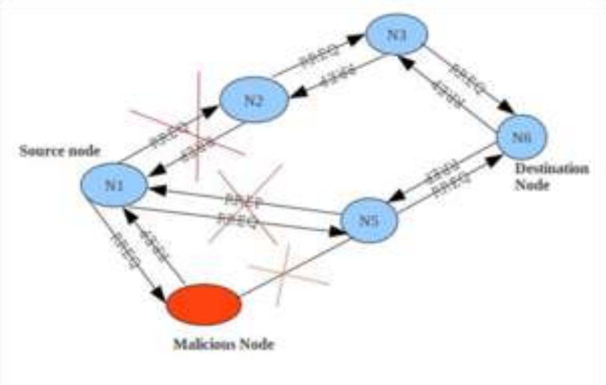


FIGURE. 3: Black Hole attack

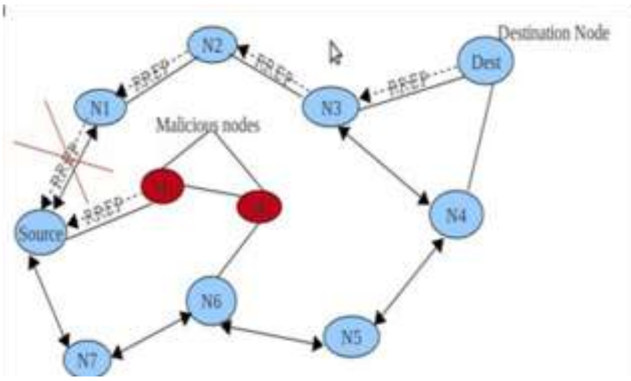


FIGURE.4: Cooperative black hole attack

4.1Black Hole Attack Detection

Many solutions are proposed for black hole attack detection or removal.

The approach that i am discussing is based on the backbone network discussed by Rubin et. Al.

We maintain a backbone network which operates at a level above the ad-hoc network. In this algorithm this idea is used to monitor the traffic flow.

In this Algorithm nodes are divided in three parts:

1. Regular Node (RN): low power and low transmission range, not trustworthy.
2. Back Bone Node (BN): Have high transmission range and form a core that monitors the nodes
3. Backbone core node (BCN) : Similar power as BN, these nodes can be elevated to BN nodes for increasing connectivity and coverage of the network

This algorithm is having mainly two parts.

i)Core Formation and maintenance

ii)Detection of Black/malicious nodes.

i) Core Formation and maintenance: Core formation progresses incrementally. During this BCN node perform some tasks those are detect RN in its neighborhood, if found broadcast "invitation" message.On receiving Join request from RN, check if it is reachable in specified number of hops, if yes add in associated node list else in unassociated list.Iif no other request go to next grid. If BCN detects any BN in its vicinity then this node sends a coordination message to BN and waits for reply.BCN on receiving reply to coordination message, it executes action which is specified in the reply.

Action of a Regular node:

Every Regular node first check if it is associated with some BCN or BN, if yes then terminate its actions. On receiving invitation message send a join request, and after getting reply for its join request from BN or BCN send "accept" to BN or BCN.

4.2Black Node Detection

The key idea is that source node, after every block of data packets, asks the backbone network to perform end-to-end check with the destination, whether the packets have reached it. If destination did not receive a block of data packets, then backbone network initiates the detection of the chain of malicious nodes.

Let Suppose here : S:Source node,

D: Destination node,

N1:Backbone node, to which S is associated N2:Backbone node, to which D is associated

V : Regular Node

Nr: is the node which send RREP to S (For the RREQ for S to D route)

Action of N1: (i) On receiving prelude from S, sends

monitor message to all neighbours of S asking them to monitor data sent by S.

on receiving "check" from S sends query to all neighbours of S and waits for result message.

on receiving result message set the the its max

counter value. If it receive "D malicious" then repeat the steps, and if not receive any message from D then sends message to D and terminate.

In same way N2 also send monitor message to neighbours of D to record the number of packets received by D and then set its counter accordingly.

Regular node on receiving monitor check if S is its

neighbour then start counting the number of packets S to D. And also on receiving query message send result message to the source of query message. Once the N1 finds that ack message not received until a predefined timeout. Then Black hole removal process get initiated by N1. The actions of different node are as follows:

Action by N1: Broadcast find_chain message on the backbone network. The message contains the id of node Nr(node sending RREP to S).

Action of a BN Nb:(i) On receiving the find_chain message, checks if node Nr belongs to its associated list. If not, no further action. Initialize a list (black_node_chain) to contain node Nr.

Instruct all neighbours of Nr to vote for the next node to which Nr is forwarding packets originating from S and Destined to D.

On receiving node ids from the neighbours of Nr, find the node to which Nr is sending the packet. If no node is getting packet from Nr in its neighbourhood, means Nr is dropping all the packets. Hence Nr is malicious node, black hole process terminates, then this node is black listed and a broadcast message is sent across the network to alert all other nodes about the node as malicious.Append the elected/found node to black_hole chain. If that node is in association list of this Nb the go to step (iii), replacing Nr with the elected node. Broadcast a find)chain message over backbone network containing id of the elected node as the malicious node. Also Broadcast the Black_hole_chain formed till now over the network so that other BN can append malicious nodes to the list

Intrusion Detection Using Anomaly Detection

Intrusion Detection Systems (IDS) are one of the main techniques utilized to prevent attacks against security threats . Intrusion detection is a process of detecting an adversary and preventing its subsequent actions. Anomaly Activities Vs Normal Activities

Fake RREP Parameters

i).Maximum destination sequence number to make the route up to date

ii).Single hop-count to make a route with the shortest path

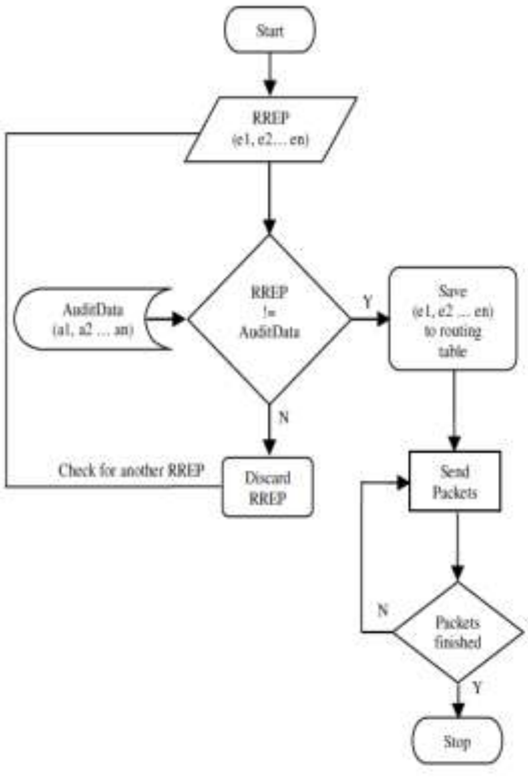
iii)Destination IP address

Address of the destination node copied from RREQ

iv).Time-stamp

The time the RREP was generated

Flowchart of Intrusion Detection by IDAD



About NS-2

- Is a discrete event simulator for networking research
- Is primarily Unix based.
- Use TCL as its scripting language.
- Compatible with C++
- Provide substantial support to simulate bunch of protocols like TCP, UDP,
- Work at packet level.

ns-2 is a standard experiment environment in research community

Conclusion

With development in computing environments, the services based on ad hoc networks have been increased. However, wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes.Using NS-2 we can study the protocol and analyse the network. We can perform any type of simulation on NS-2 before implementing it on to the actual network We can also secure our network with malicious attack using NS-2 by testing that network.

References

[1] Tamilselvan,L.;Sankaranarayanan V.,"Prevention of Blackhole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[2] H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad-hoc networks: simulation, implementation andevaluation," International Journal of Software Engineering and Its Applications, Vol. 2, No. 3 (2008) pp. 39-54.

[3] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineering and Electronic Commerce, 2009. IEEC '09. InternationalSymposium on, vol., no., pp.26-30, 16-17 May 2009

[4] Medadian, M.; Mebadi, A.; Shahri, E., "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.

[5] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009