World Research Journal of Telecommunications Systems
Volume 1, Issue 1, 2012, pp.-08-12.
Available online at http://www.bioinfo.in/contents.php?id=357

A MECHANISM TO DETECT BLACKHOLE ATTACK ON ROUTING PROTOCOL AODV IN MANET

THOSAR T.P.*, SURANA K.A., RATHI S.B. AND SNEHAL MEHATRE

Department of Computer Science and Engineering JDIET, Yavatmal -445001, MS, India.
*Corresponding Author: Email- thosar_tushar@yahoo.com

Received: April 03, 2012; Accepted: May 15, 2012

Abstract- The Mobile Ad-hoc Networks (MANET) is collection of mobile nodes which are connected dynamically forming temporary network without using any existing infrastructure or centralized access point. The black hole attack is one of the security attacks that occur in mobile ad hoc networks in which malicious node impersonate destination node by sending forged route reply packet to source node that initiate the route discovery. Anomaly detection in conventional schemes is achieved by defining the normal state from fixed training data. However, in mobile ad hoc networks where the network topology changes dynamically, such fixed training method could not be used efficiently. In this paper, an anomaly detection scheme using dynamic training method is proposed in which the learning data is updated at regular time intervals and we also proposes watchdog mechanism to detect the blackhole nodes in a MANET.

Key words- MANET, anomaly detection, blackhole attack, AODV

Citation: Thosar T.P., et al. (2012) A Mechanism to Detect Blackhole Attack on Routing Protocol Aodv in Manet. World Research Journal of Telecommunications Systems, Volume 1, Issue 1, pp.-08-12.

Introduction

An ad-hoc network is a collection of wireless mobile nodes forming a temporary network without required assistance of any pre-existing infrastructure or centralized administration [4]. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the liability of managing the network. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. . Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [5].

Security Challenges in MANET

Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [8][10]. Challenges to MANET are discussed as follows:

Confidentiality

It ensures that classified information in the network is never disclosed to unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

Availability

Availability is the most basic requirement of any network. It assures that the services of the system are available at all times and are not denied to authorize users. If the networks connection ports are unreachable, or the data routing and forwarding mechanisms are out of order, the network would cease to exist.

Integrity

It guarantees that a message being transferred between nodes is never altered or corrupted and the message must be genuine.

Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

Authenticity

Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes.

Non-Repudiation

It ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

Routing Approaches in MANET

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. Following are the categories of routing protocols in MANET,

Table-driven or Proactive Protocols

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative proactive protocols include: Destination-Sequenced Distance- Vector (DSDV) routing, Wireless Routing Protocol (WRP).

On-demand or Reactive Protocols

A different approach from table-driven routing is reactive or on-demand routing. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired. Reactive routing protocols include: Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing, and Associativity Based Routing (ABR).

Hybrid Routing Protocol

Purely proactive or purely reactive protocols perform well in a limited region of network setting. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP.

In this paper, we use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing [7]. Then, we select attributes in order to define the normal state from the characteristic of blackhole attack. Lastly, we present a new training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment. Also watchdog mechanism is proposed for detecting misbehaving nodes in network.

Related Works

Secure Routing

Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET. In [9], Hu proposed common key encryption system for Dynamic Source Routing (DSR) [4]. In [11], Authenticated Routing for Ad hoc Networks (ARAN), an AODV-based secure routing protocol using public key encryption system is proposed. Hu and Perrig [9] survey the weakness and strength of various secure routing protocols. The above mentioned secure protocols can only guard against external attacks. However, for the internal attacks coming from compromised hosts could still have severe impacts on network performance and its connectivity. Therefore, detecting the internal attack launching from these compromised hosts is indispensable.

IDS Approaches for MANET

To protect against the blackhole attack, five methods have been proposed. In [8], the method requires the intermediate node to send a RREP packet with next hop information. When a source node receives the RREP packet from an intermediate node, it sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the RREP packet, and that it has a route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route. In [12], the method requires the intermediate node to send Route Confirmation Request (CREQ) to next hop node toward the destination. Then, next hop node receives CREQ, and look up its cache for a route the destination. If it has one, it sends Route Confirmation Reply (CREP) to source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP. In these methods, the operation is added to routing protocol. This operation can increase the routing overhead resulting in performance degradation of MANET which is bandwidth-constrained. In [13], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes. Therefore, a method that can prevent the attack without increasing the routing overhead and the routing delay is required.

Huang et al. [5] propose a method in which the packet flow is observed at each node. In this method, they define a total of 141 features with traffic related and topology- related, and suggest anomaly detection means with interrelation between features. In [6], Huang et al. construct an Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol; modelize normal state; and detect attacks with both specification based detection and anomaly detection. In specification based detection, they simply detect attacks as deviant packet from condition defined by EFSA. Also, in anomaly detection, they define normal state and compare it with condition of EFSA and amount of statistic of transition, and then detect attacks as a deviation from those states.

From the characteristics of the blackhole attack, we need to take a destination sequence number into account. In [11], feature related to the destination sequence number has not been taken into account as the feature to define the normal state. In [6], the threshold is used and the feature is defined as the number of time that the destination sequence number is greater than the threshold. However, since a destination sequence number changed depending on the network environment, up to a threshold it may be difficult to successfully discriminate between the normal state and the state where blackhole attack took place. And hence cause degradation in detection accuracy. Excluding the destination sequence number issue, the above mentioned approaches use fixed training data to define the normal state. But, the MANET topology can be changed easily, and the difference in network state becomes larger by time. Moreover, these methods cannot be applied to a network while the training has been done in another network. As a result, these methods are considered very difficult in a MANET environment. To solve this problem, normal state needs to be defined using the data reflecting the trend of current situation which leads to the idea of updating the training process within a time interval. By so doing, attack detection can be adaptively conducted even in a changing network environment.

AODV Routing Protocol

AODV is ad hoc on demand distance vector routing protocol [7]. In this route is created only when it is needed (on demand). Every node in an Ad-hoc network maintains a routing table. This AODV protocol operates in two phases: route discovery and route maintenance. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If route is not available then route discovery process is initiated. It broadcasts a RREQ message into the network. A node that receives a fresh RREQ message will check its routing table to see whether it is a destination for that packet and if so it sends back an RREP message. 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, the RREQ is broadcasted to its neighbors. If routing table contain route to destination then next step is comparison of destination sequence number in its routing table to that present in RREQ message. If the number in the routing table is higher than the number in the RREQ, it denotes that the route is a 'fresh route' and packets can be sent through this route. The intermediate node then sends a RREP packet to the node through which it received the RREQ message.

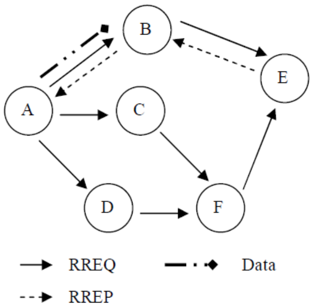

Fig. 1- Propagation of RREQ & RREP from A to E

The RREP message gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR message to all other nodes that uses this link for their communication to other nodes. This is illustrated in fig 1 [2].

Blackhole Attack

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad-hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A Blackhole attack [8][9] is a sort of denial of service attack where a malicious node can deprives all packets by spuriously claiming a fresh route to the destination and then consumes the intercepted packets without forwarding them to the destination.

A source node wants to send data packets to destination node, and initiates the path finding process. In the following illustrated figure 2, imagine a malicious node 'M'. When node 'A' broadcasts a RREQ message, nodes 'B' 'D' and 'M' get it. As Node 'M' is a malicious node, it does not test up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP message, declaring a route to the destination. Node 'A' gets the RREP from 'M' to the front of the RREP message from 'B' and 'D'.

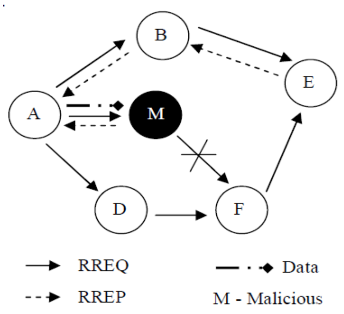

Fig. 2- Black hole Attack in AODV

Node 'A' thinks that the route through 'M' is the shortest route to the destination and sends any packet through it. When the node 'A' sends data to 'M', it attracts and absorbs all the data without forwarding to destination and thus acts like a 'Black hole'[2].

Blackhole Attack Detection

In this paper, we proposed two methods for detecting blackhole attack which are dynamic learning method and watchdog mechanism.

Dynamic Learning Method

In dynamic learning method we use dynamic training data for learning purpose. This method contains following two steps:

Attribute Selection

Multidimensional attribute vector is defined for expressing state of network. At every time slot each dimension of attribute vector is counted. The destination sequence number is taken into consideration for detecting blackhole attack. In normal state, each node's sequence number changes depending on its traffic conditions. When there are few connection in network destination sequence number increases monotonically. When number of connection increases then destination sequence number is also increases. However the sequence number is increased largely when the attack took place regardless of the environment. Generally the number of sent out RREQ and the number of received RREP is almost the same. From these reasons we use the following attribute to express the state of the network.

- Number of sent out RREQ messages
- Number of received RREP messages
- The average of difference of Dest Seq in each time slot between the sequence number of RREP message and the one held in the list [1].

Now, the average of the difference between the Dest Seq in RREQ message and the one held in the list are calculated as follows. Each node records the destination IP address and the Dest Seq in its list during sending or forwarding a RREQ message. When a RREP message is received, the node looks over the list to see if there is a same destination IP address. If it does exist, the difference of Dest Seq is calculated, and this operation is executed for every received RREP message. The average of this difference is finally calculated for each time slot as the attribute [1].

Discrimination Module of Anomaly Detection

The network state in time slot i for the traffic that flow across each node is expressed by three-dimension vector xi = (xi1, xi2, xi3). Here, the groups of normal states are considered to be gathered close in feature space. On the other hand, the abnormal state is considered to be the scattering data that deviates from the cluster of normal state. According to this, the distribution of network state is shown in fig 3.

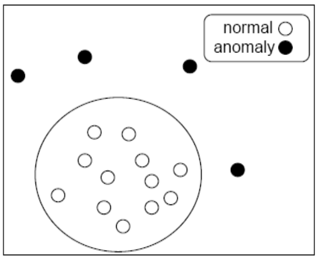

Fig. 3- The distribution of network state

From now, the Mean vector $\bar{x}^D$ is calculated using training data set D of N time slots from Equation (1).

$$\bar{x}^D = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (1)$$

After that, the distance from input data sample x to the mean vector $\bar{x}^D$ is calculated from Equation (2).

$$d(x) = ||x - \bar{x}^D||^2 \qquad (2)$$

When the distance is larger than the threshold T_h (which means it is out of range as normal traffic), it will be judged as an attack (Equation (3)).

$$\begin{aligned} d(x) &> T_h \quad &: \text{attack} \\ d(x) &\le T_h \quad &: \text{normal} \end{aligned} \qquad (3)$$

Here, the projection distance with maximum value is extracted as T_h from the learning data set (Equation (4))

$$T_h = d(x_I), \qquad \text{where } I = \underset{xi \in D}{\operatorname{argmax}}\, d(xi) \qquad (4)$$

Let ΔT_0 be the first time interval for a node participating in MANET. The initial mean vector is calculated using data collected in this time interval, then the calculated mean vector will be used to detect the attack in the next period time interval ΔT. If the state in ΔT is judged as normal, then the corresponding data set will be used as learning data set. Otherwise, it will be treated as data including attack and it will be accordingly discarded. In this way, we keep on learning the normal state of network. The procedure is shown in Fig 4.

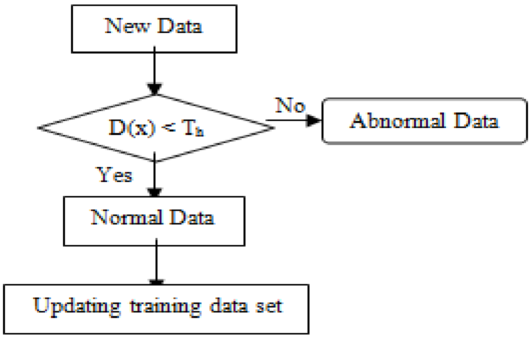

Fig. 4- Learning flow chart of proposed method

By doing this, we update the training data set to be used for the next detection. Then, the mean vector which is calculated from this training data set is used for detection of the next data. By repeating this for every time interval ΔT, we can perform anomaly detection which can adapt to MANET environments [1].

A Path-Based Detecting Method

This method is based on a path based scheme. In this a source node does not watch every node in the neighbor, but only consider the next hop in current route path. For example, in Figure 5, S is the source node; D is the destination node; and A is a black hole. Node S is sending data packets to node D through the path S, A, B, D. In our scheme, Node S only watches Node A, which is the next hop; but does not care Node 1 and Node 2.

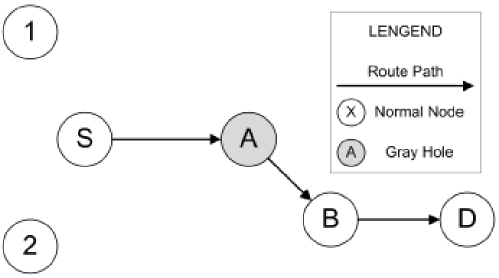

Fig. 5- A path based detection scheme

To implement the algorithm, every node should keep a FwdPktBuffer, which is a packet digest buffer. The algorithm is divided into three steps:

- When a packet is forwarded out, its digest is added into the FwdPktBuffer and the detecting node overhears.
- Once the action that the next hop forwards the packet is overheard, the digest will be released from the FwdPktBuffer.
- In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. We define overhear rate in the Nth period of time as OR (N).

$$OR(N) = \frac{total\ overheard\ packet number}{total\ forwared packet\ number}$$

If the forwarding rate is lower than the threshold, the detecting node will consider the next hop as a black or gray hole. Latter, the detecting node would avoid forwarding packets through this suspect node.

Conclusion

MANET is vulnerable to various kind of attack due to dynamic topology and lack of centralized access point. Blackhole attack is one type of security attack in which malicious node impersonates destination node by sending spoofed route reply to source node which initiates route discovery process. This malicious node deprives traffic from source node.

In this paper, attributes are introduced for defining the normal state of the network and also presented two blackhole detection methods which are dynamically updated training data and path based detection method.

References

[1] Kurosawa S., Nakayama H. and Kato N. and Jamalipour A. (2007) *International Journal of Network Security*, 338-346.

[2] Latha Tamilselvan and Sankaranarayanan V., (2007) *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications* (AusWireless).

[3] Kanika Lakhani, Himani bathla, Rajesh and Yadav (2010) *International Journal of Computer Science and Network Security*, 10(5).

[4] David B. Johnson and Dravid A. Maltz (1996) *Technical report, Carneigie Mellon University*.

[5] Huang Y.A., Fan W., Lee W. and Yu P.S. (2003) *The 23rd International Conference on Distributed Computing Systems* (*ICDCS*), 478487.

[6] Huang Y.A. and Lee W. *The 7th International Symposium on Recent Advances in Intrusion Detection*, 125-145.

[7] Perkins C.E., Royer E.M.B. and Das S.R. (2003) *Ad hoc On-Demand Distance Vector routing,* RFC 3561.

[8] Jiwen C.A.I., Ping Y.I., Jialin Chen, Zhiyang A.N.G. and Ning Liu (2010) *24th IEEE International Conference on Advanced Information Networking and Applications*.

[9] Routing Security in Wireless Ad Hoc Networks (2002) *IEEE Communications magazine*.

[10] Yi-Chun Hu and Adrian Perrig (2004) *IEEE Security and Privacy*.

[11] Lidong zhou, Zygmunt J. Haas (1999) *IEEE network*, special issue.

[12] Sanzgiri K., LaFlamme D., Dahill B., Levine B.N., Shields C. and Royer E.M.B. (2005) *IEEE Journal on Selected Areas in Communications*, 23(3), 598-610.

[13] Lee S., Han B. and Shin M. (2002) *Robust routing in wireless ad hoc networks*, in ICPP Workshops, 73.

[14] Shurman M.A., Yoo S.M. and Park S. (2004) *ACM 42nd Southeast Conference* (*ACMSE*), 96-97.