Intrusion Detection Systems for Trust based Routing in Ad-Hoc Networks

Dharmesh Patel
Department of Information & Technology,
Parul Institute of Engineering & Technology,
Vadodara, Gujarat, India
dharmeshgpatel1985@gmail.com

Yask Patel
Department of Computer Science & Engineering,
Parul Institute of Engineering & Technology,
Vadodara, Gujarat, India
yaskpatel@gmail.com

Abstract : Ad Hoc Networks are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures, and vulnerability of nodes, vulnerability of channels and open medium of communication. To address these concerns this work discusses a Trust based mechanism coupled with Ad Hoc Network based intrusion detection system (IDS) which can ensure the security services required by users. The idea is to implement Network based intrusion detection system (NIDS) for trust based routing in Ad Hoc Networks. There are many attacks in Ad Hoc Networks like availability, integrity, authentication, confidentiality and no repudiation. This paper discusses detect selfishness attack and define the Trust based mechanism coupled with Ad Hoc Networks based Intrusion Detection System (IDS) .

Keywords: Ad hoc Network; Insrusion Detection System(IDS); Routing Protocol; Selfishness Attack.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) have a set of mobile hosts to carry out various networking functions like packet of forwarding, routing and service discovery without the help of any pre deployed infrastructure. It is an infrastructure-less network. The interconnections between nodes are capable of changing on a continual and arbitrary basis. MANET is dynamic in nature and they constantly move in and out of their network vicinity. Due to dynamic nature of ad hoc network securing the network is a big challenge. Many routing protocols have been proposed like AODV, DSR to handle the network with large number of hosts with limited resources like energy and bandwidth but no security consideration have been made, and then many secure routing protocols are developed to secure the network.

In this, individual network is constructed and nodes of this network forward packets to and from each other. Due to node mobility, network topology changes frequently So it is important to manage routing information efficiently. To make cooperation between nodes procedure feasible, Trust between nodes is necessary. This network is flexible so it introduces new security risks. Intrusion detection System (IDS), which is an essential part of a security system, also presents challenges due to the dynamic nature of Ad hoc networks. This paper discusses Availability Attacks like Black hole and Selfishness. This paper presents the survey of different IDS schemes, their advantages and disadvantages. This paper will be useful for deciding the best IDS scheme for particular attack. The presented IDS scheme is tested for AODV protocol. The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. BASIC ROUTING

A. Routing in Ad-Hoc Networks

Using limited recourses, routing helps to find and maintain routes between nodes in dynamic topology with preferably unidirectional links. There are two types of Routing Protocol.

1) Pro-active (table-driven) Routing Protocols

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

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

Table-driven protocols are Destination-Sequenced Distance Vector Routing Protocol (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Hierarchical State Routing (HSR), Zone-based Hierarchical Link State Routing Protocol (ZHLS) and Cluster head Gateway Switch Routing Protocol (CGSR).

2) Reactive (on-demand) Routing Protocols

This type of protocol creates on demand routes because this type of protocols finds a route on demand by overflowing the network with route request packets. The main disadvantages of such algorithms are:

- High lead time in route finding.
- Excessive overflowing can lead to network jam.

Ad-Hoc On-Demand Distance Vector Routing Protocol (AODV)

The Ad-hoc On-demand Distance Vector (AODV) routing protocol is a routing protocol used for dynamic wireless networks where nodes can enter and leave the network. The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for dynamic wireless networks. As the name suggest AODV builds routes between nodes as per the wish of source code. AODV is capable of both unicast and multicast routing. These routes are maintained by the time it is required by source node. Additionally, AODV is capable of forming trees to connect multicast group member with nodes. The source node transmits a Route Request (RREQ) to its immediate neighbors to find route to a particular destination node. The neighbor replies back with Route Reply (RREP) if the neighbor has a route to the destination. Otherwise the neighbors in turn rebroadcast the request. This continues until the RREQ hits the final destination or a node with a route to the destination. At that point a chain of RREP messages is sent back and the original source node finally has a route to the destination.

Advantages:

- Here routes are established on demand and the latest route to the destination is found based on sequence number So the connection setup delay is lower.

Disadvantages:

- Here, if source code sequence number is very old, the intermediate nodes may follow inconsistent route and the intermediate nodes have higher but not the latest sequence number leads to stale entries.
- Multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead.
- Periodic beaconing leads to unnecessary bandwidth consumption.

B. Vulnerabilities of Ad-Hoc Networks

- Nodes of mobile ad hoc networks have limited ranges and because of that it requires multi hop communication. Ad hoc network runs on an assumption that once the node has promised to transmit the packet, it will not cheat but this does not holds true when nodes in the networks have contradictory goals. Due to this, neighbors of intermediate nodes can use the reputation of intermediate nodes to transmission.
- Node mobility leads to frequent change in network topology
- Use of wireless links into network increases the risk of link attacks.
- Relatively poor protection.
- Long life of network requires distributed architecture.
- Risk of Denial of Service (DoS) attacks due to lack of infrastructure and chances of link breakage and channel errors due to mobility.
- Need of scalability.
- Nodes in Ad Hoc Networks have limited services and security provision due to limited memory and computational power
- Dynamic topology.

C. Types Of Attacks

Attacks on networks come in many varieties and they can be grouped based on different characteristics.

a) Availability Attacks

Availability is the most basic requirement of any network. If the networks connection ports are Unreachable, or the data routing and forwarding mechanisms are out of order, the network would cease to exist[3].

b) Packet Dropping or Black-hole Attack

In mobile ad hoc networks(MANETs), nodes usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as packet dropping attack or black hole attack[4].

c) Fabricated route Attack

Fabrication attacks generate false routing messages. Such attacks can be difficult to confirm as invalid constructs, especially in the case of fabricated false messages that claim a neighbor cannot be contacted[5].

d) Resource Consumption Attack

In this attack, a malicious node intentionally tries to consume the resources (e.g. battery power, bandwidth etc) of other nodes in the network. The attack can be of various types like unnecessary route requests, route discovery, control messages, or by sending stale information[6].

e) Selfishness Attack

Selfishness and malicious nodes participate in route discovery stage properly to update their routing table, but as soon as data forwarding stage begins, they discard data packets[7].

D. Intrusion Detection System(IDS)

Intrusion Detection System (IDS) continually monitors activities like packet traffic. It can automatically recognize malicious, doubtful or inappropriate activities and then activates alarms to system admin. Each mobile node runs an IDS independently to observe behavior of neighboring nodes, looking signs of intrusion locally, making decision to overcome attack, and it can request data or actions from neighboring nodes if needed.

Classification of Intrusion Detection System (IDS)
Intrusion Detection Approach:

Anomaly Detection: The anomaly detector checks network parts and compares their state to the normal baseline and observes for irregularities. Signature Detection: In signature detection, the IDS checks the information it collects and compares with the large databases of attack signatures. Basically, the IDS looks for a specific attack that has already been known.

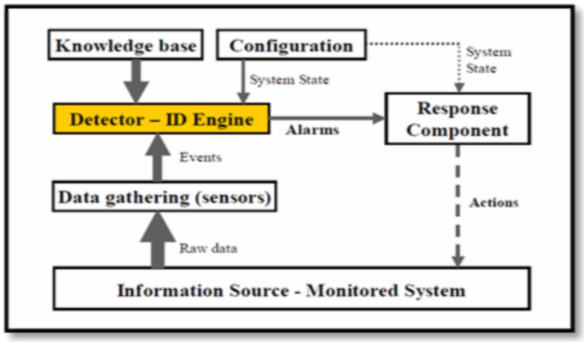

Figure 1. Intrusion Detection System

a) Protected System

*Host-based Intrusion Detection System (HIDS)***:** In a host-based system, the IDS checks activity on each individual computer or host. *Network-based Intrusion Detection System (NIDS):* In a network-based system, the individual packets owing through a network are evaluated. *Hybrids:* It combines the advantages of low false-positive rate of signature based intrusion detection system (IDS) and the ability of anomaly detection system (ADS) to detect new novel unknown attacks.

b) Structure Based

Centralized System: In Centralized System, collection of data is done from single or multiple hosts and the entire data is shifted to a central location for analysis. *Distributed System:* In Distributed System, Data at each host is collected and Distributed analysis of the data is done.

c) *Data Source Based*

Audit Trail: Audit trail analysis is the common method used by periodically operated systems. It includes detection of attack manifestations for post-mortem analysis, detection of recurring intrusion activity, identification of successful intruders, identification of own system weaknesses, development of access and user signatures and definition of network traffic rules that are important for anomaly detection-based Intrusion Detection Systems[8].

III. IDS SCHEMES FOR AVALIBILITY ATTACK

A. Black-Hole Attack

In this, there are two types.

1) Single Black hole attack:

In this, one malicious node uses routing protocol to claim itself of being shortest path to destination node but drops routing packets but doesn't forward packets to its neighbors. In this, Packet Delivery Ratio (PDR) is reduced.

2) Cooperative Black hole attack:

Black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all receiving packets. The damage will be serious if malicious nodes work together as a group.

This is called cooperative black hole attack.

1) Neighborhood-based and Routing Recovery [9]:

This scheme uses neighborhood-based method to recognize the black hole attack, and a routing recovery protocol to build the correct path. This method is employed to identify the unconfirmed nodes, and the source node sends a modified route entry control packet to destination node to renew routing path in the recovery protocol.

Advantages:

- Lower Detection time
- Higher throughput
- Accurate detection probability is achieved.

Disadvantages:

- There must be a public key infrastructure or detection is still vulnerable.
- Failed when attackers cooperate to forge fake reply packets.

2) Aggregate Signature Algorithm [10]:

This detection scheme solves packet dropping problem of Single Black Hole attack.

Advantages:

- Reliability is satisfied as evidence on forward packet is used.
- Application scope is broad, as bi-directional communication links are not necessary.
- Security is satisfying, as it is hard for malicious nodes to escape detection.

3) DPRAODV (A Dynamic Learning System Against Black hole Attack in AODV Based MANET)[11]:

In this scheme, if RREP sequence no. is greater than threshold, sender is regarded as an attacker and updated to black list. ALARM is sent to its neighbors which includes black list, thus RREP from malicious node is blocked but is not processed. On the other hand, dynamic threshold value is changed by calculating average of destination sequence number between sequence number and RREP packet in each time slot. In this, black hole is not only detected but also prevented by updating threshold which responses the realistic network environment.

Advantages:

- PDR is improved.
- Detects multiple black holes.

Disadvantages:

- Higher Routing overhead
- Can't detect cooperative black holes.

4) SIDSR (Source Intrusion Detection Security Routing Method) [12]:

When black hole node sends fake RREP, this scheme is used. This scheme is performed on source node.

Identify applicable sponsor/s here. *(sponsors)*

Disadvantages:

- Increase routing overhead packets between source and next hop node especially when this mechanism is applied on a large-scale MANET and distance between source node and attacker node is long.
- If distance between source node and attacker node is long, delay in the discovery period of route will be high, which causes an overall network performance degradation.

5) LIDSR (Local Intrusion Detection Security Routing Method)[12]:

This scheme performs locally.

Advantages:

- Reduce routing information overhead that results in a less congested network.
- Less utilized bandwidth which decreases dropping of data packets.
- Increase in net*work throughput with decrease in both-end-to-end delay and routing overhead.

6) IDAD (Intrusion Detection using Anomaly Detection)[13]:

This scheme introduces new packets. This scheme doesn't modify AODV routing table.

Disadvantages:

- Neighbor nodes may give false information.

B. Selfishness Attack

This IDS Schemes deal with problem of Selfishness on packet forwarding in MANET.

1) End-to-end Acknowledgements[7]:

This mechanism consists of monitoring the reliability of routes by acknowledging packets in an end-to-end manner, to render the routing protocol reliable. In this, the destination node gives acknowledgement of receipt of packets by sending a feedback to the source.

Advantages:

- Helps to avoid sending packets through unreliable routes and it can be combined with other technique.

Disadvantages:

- Lack of misbehaving node detection.
- This technique may detect routes containing misbehaving or malicious nodes and those which are broken, but without any further information regarding node causing packet loss.

2) Watchdog[7]:

It aims to detect misbehaving nodes that don't forward packets, by monitoring neighbors in the promiscuous mode. The solution also includes path-rater component, that selects route based on the link reliability knowledge.

Advantages:

- It is able to detect misbehaving nodes in many cases, and requires no overhead when no node misbehaves.

Disadvantages:

- It fails to detect misbehavior in cases of collisions, partial collusion and power control employment.
- It fails when two successive nodes collude to conceal the misbehavior of each other.
- It doesn't control detected misbehaving nodes.

3) ABO (activity-based overhearing)[7]:

It is a generalization of Watchdog.

Advantages:

- Node constantly monitors in promiscuous mode the traffic activity of all its neighbors and oversees the forwarding of each packet whose next forwarder is also in its neighborhood. This can increase the number of observations and improve watchdog efficiency.
- It mitigates collusion problem.

4) Two-hop Acknowledgements[7]:

This scheme uses asymmetric cryptography.

Advantages:

- Mitigate Watchdog's problem related to power control technique usage.

5) Probing[7]:

It is a combination of route and node monitoring. This approach consists of simply incorporating into data packets commands to acknowledge their receipt. These commands are called probes and intended for selected nodes. Probes are launched when a route that contains a misbehaving node is detected.

Disadvantages:

- A selfish node could analyze each packet it receives before deciding either to forward this packet or not. When it gets a probe packet, it would notice that a probing is under way and would consequently choose to cooperate and forward packets for a limited time, until the probe is over.

6) Signed Token[7]:

This scheme uses asymmetric cryptography. It aims at protecting both-the routing and data forwarding. Threshold cryptography based signature and Watch-dog technique are at core of this technique. The solution is structured around 4 components.

1. Neighbor verification-that describes how to verify whether each node in net- work is Selfish.
2. Security enhanced routing protocol-which enhances AODV and extends to the termed AODV-S that explicitly incorporates security information in routing.
3. Neighbor monitoring-that is based on Watchdog to describe how to monitor the behavior of each node in network and how to detect packet droppers.

4. Intrusion reaction-which describes how to alert network and separate the misbehaving and serve as a bridge between neighbor verification and neighbor monitoring.

Disadvantages:

- All the Watchdog's problems remain untreated, since the neighbor monitoring component completely relies on it.
- It prevents a node which has less than k(number of parts of secret key) neighbors to communicate and poses a critical issue on choice of parameter (threshold) k(number of parts of secret key) for sharing of secret key.
- The choice of low k (number of parts of secret key)weaken the key whereas choice of high values requires high connectivity which is not always ensured in MANET.

7) *CORE (Collaborative Reputation)[7]:*

It can be easily integrated with any network functions. It can be applied to packet forwarding function, both on data and request packets. It defines 3 types of reputations.

1. Subjective reputation-that is calculated directly from a node observations and gives more relevance to the past observations in order to minimize influence of random misbehavior in recent observations.
2. Indirect reputation-which is calculated basing on the information provided by other nodes.
3. Functional reputation-that combines subjective and indirect reputation.

Advantages:

- It uses Watchdog for monitoring and collecting direct observations, thus both directed and broadcasted packets would be monitored.
- Signed Token problem of k (number of parts of secret key) is solved.

Disadvantages:

- All the Watchdog's drawbacks related to detections are present.
- Can't detect malicious node behaviors.

8) *CONFIDANT(Cooperation Of Nodes and Fairness In Dynamic Ad-hoc Network)[7]:*

It consists of four components present in each node.

1. Monitor-Similar to Watchdog.
2. Trust manager-deals with incoming and outgoing alarm messages.
3. Reputation system-that manages nodes view on reputations of the others.
4. Path manager-is responsible for controlling the misbehaving nodes by not relaying any packet to them, as well as deleting paths containing misbe-having nodes and re-ranking paths according to nodes trustworthiness.

Disadvantages:

- Watchdog's problems remain same.
- Reputations are periodically exchanged with each other, which causes an overhead.

9) *Friends and foes[7]:*

In this, nodes are permitted to publicly claim that they are unwilling to forward packets to some nodes. Each node maintains basically three sets.

1. Set of friends-to which it is willing to provide services.
2. Set of foes-to which it is unwilling to provide services.
3. Set of nodes-known to act as if it is their foe(they don't provide service packets for it)named set of Selfish.

Advantages:

- It is used to secure control packet from dropping.

Disadvantages:

- Watchdog's problems remain same.
- More overhead
- Each node only keeps information about its current neighbors and information of nodes leaving its neighborhood are begun, a mobile selfish can easily avoid and would never be detected.

10) *OCEAN (Observation based Co-operation enforcement in Ad hoc Networks)[14]:*

It avoids direct reputation information and uses only direct observation of other nodes behavior. A node makes routing decisions only on the basis of direct observation. In this, rating is given to each node; initially each node is given Null(0)-Neutral. With every positive action, its value is incremented by 1 and with every negative action, its value is decremented by 2. If the rating of node falls below certain faulty threshold(-40), it is added to list of faulty nodes.

11) *SORI(Secure and Objective Reputation based Incentive)[1]:*

It targets non-forwarding misbehavior type and uses a Watchdog like mechanism for monitoring. The reputation system keeps count of packets forwarded both by and for neighboring nodes. In this, there are three components-Neighbor monitoring, Reputation propagation and Control.

Advantages:

- The propagation of reputation is secured by 1-way hash function, which makes it difficult for a selfish node with bad reputation to send packets or fake broadcast information.

12) *Ex-Watchdog[1]:*

It is implemented with encryption mechanism and maintaining a table that stores entry of source, destination, sum(Total number of packets+ the current node sends+ forwards or receives) and path. It's main feature is ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving.

Advantages:

- Solves problem of Watchdog.

Disadvantages:

- Fails when malicious node is on all paths from specific source and destination.

IV. OUR PROPOSAL SYSTEM TO DETECT SELFISHNESS ATTACK

Since AODV does not operate in promiscuous mode by default, some modifications had to be performed in the internal files. The fact that promiscuous mode was enabled in AODV had no impact in the overall performance of AODV and the tap method that handles the overheard packets is only utilized in the detection of the selfishness attack. Detection of this attack is triggered whenever a node forwards routing traffic to its neighboring nodes. A structure called SELFISH Node was developed to hold information necessary to monitor the neighboring nodes that are suspected for malicious behavior.

The SELFISH Node data structure holds the following information:

Node Id: the IP address of the node to which the routing traffic was forwarded.

Send Reply: a Boolean value that becomes true whenever the offending node replies to a RREQ packet that was forwarded to it.

Pre Alarm: a Boolean value that becomes true if the node does not respond as expected to the forwarded traffic.

Alarm: a Boolean value that becomes true whenever we decide that the offending node performs the dropping routing packets attack.

Time: a double variable that keeps the time where the offending node was added in the data structure.

Hence, whenever a node forwards routing traffic for which a neighboring node is not the destination it adds each neighboring node to the data structure and waits to observe their behavior. Then in the tap method if it overhears that a neighboring node has replied to the forwarded RREQ, it means that it has acted appropriately and it can be removed from the monitoring list. If this is not the case and the packet was a RREP then the offending node has to forward the packet. If it fails to do so within the pre alarm time threshold time period, which was determined by experiments to be seconds, the pre alarm state becomes true. This remains in the pre alarm state for, seconds which is the alarm threshold time period. If the offending node fails to forward the routing packet within this time limit, it moves to the Alarm state. In case of an alarm the legitimate node marks this node as malicious and stops forwarding traffic to it for seconds and it also sends a RERR message to all its upstream neighbors to inform them that all the routes that include this node are not valid.

V. CONCLUSION

Ad-hoc networks are vulnerable due to absence of infrastructure, limited physical security, restricted power supply, dynamically changing network topology, lack of centralized monitoring and mobility. In this paper, we first analyze the pros and cons of various IDS schemes for black hole and selfishness attack using AODV protocol in Ad Hoc networks. Then, the various IDS schemes are discussed. The proposals are presented in a chronological order. However, we also discover that some of the IDS like Neighborhood based and routing recovery schemes are useless when the attackers cooperate to forge the fake reply packets. For this purpose, AODV protocol is implemented and then selfish node is appended in that to analyze its effectiveness. If presence of selfish node in routing, calculate PDR and end-to end delay. For detection of the selfishness attack we have proposed IDS. After implementing the IDS, again calculate PDR and end-to-end delay. If to make system more reliable we have added trust factor in routing and after comparing both ratio.

REFERENCES

[1] S.Tamilarasan and Dr.Aramudan,” A Performane and Analysis of Misbehaving node in MANET using Intrusion Detection System”. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011.

[2] Niyati Shah,Sharada Valiveti “Intrusion Detection Systems for the Availability Attack in Ad-hoc Networks ,” International Journal of Electronics and Computer Science Engineering , ISSN- 2227-1956/V1N3-1850-1857.

[3] Adam Burg, “Ad hoc network specific attacks”, Seminar Ad hoc Net working: concepts, applications, and security Technische Universitt Mnchen, 2003.-

[4] Pinki Tanwar, Shweta, “A Survey On Behaviour Of Blackhole In Manets”, IJRIM Volume 1 Issue 4, August 2011.

[5] Ioanna Stamouli, “Real-time Intrusion Detection for Ad hoc Networks”, 2003.

[6] http://sites.google.com/site/securezrp/routingattacks

[7] Djamel Djenouri,Nadjib Badache, “MANET: Selfish Behavior on Packet Forwarding”

[8] K. Kumar, "Intrusion Detection in Mobile Adhoc Networks," Master's Thesis, University of Toledo, December 2009.

[9] Sun B, Guan Y, Chen J, “Detecting Black-hole Attack in Mobile Ad Hoc Networks”, Paper presented at the 5th European PersonalMobile Communications Conference, Glasgow, United Kingdom, 22-25, April 2003

[10] Rajiv Ranjan, Naresh Trivedi and Anoop Srivastava, “Mitigating of Blackhole Attack in Manets”, VSRD, International Journal of Computer Science and Information Tech., Vol.1, 53-57, 2011.

[11] Raj PN, “DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET”, International Journal of ComputerScience 2: 54-59, 2009.

[12] Maha Abdelhaq, Sami Serhan,Raed Alsaqour and Anton Satria, “Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol”,Australian Journal of Basic and Applied Sciences,5:1137-1145, 2011.

[13] Ekta Kamboj,Harshil Rohil, ”Detection of Black Hole Attack on AODV in MANET using Fuzzy Logic”, Journal of Current Computer Science and Technology,Vol.1 Issue 6:316-318, 2011

[14] Preeti Nagrath,Ashish Kumar,Shikha Bhardwaj, “Authenticated Routing Protocol based on Reputation System For Adhoc Networks”, International Journal on Computer Science and Engineering(IJCSE), Vol.2: 3095-3099, 2010.