A New Intrusion Detection System for AODV (IDAODV)

Prasanna Lakshmi G S, Dr.Shanta Kumar B Patil, Mamatha C.M, John.J.P, Dr.Prema Jyoti Patil

ABSTRACT:

Mobile Ad hoc Networks (MANET) is one of the most vital and exclusive applications. On the contrary to traditional network architecture, MANET does not need a stable network infrastructure; the self-configuring ability of nodes in MANET made it popular among critical mission application like military use or emergency retrieval.

AODV is an important on demand routing protocol. Security is a central requirement for mobile Ad Hoc networks. Intrusion Detection System aimed at securing the AODV protocol has been studied by Stamouli et al [1] using specification based technique.

In this paper, the work of Stamouli et al [1] has been extended and the proposed protocol is called IDAODV (Intrusion Detection AODV).In our work, we make use of Knowledge-based intrusion detection. Our Intrusion Detection and Response Protocol for MANETs have been demonstrated to perform better than that proposed in [1] in terms of false positives and percentage of packets delivered. IDAODV performs real time detection of attacks in MANETs running AODV routing protocol.

----------------------▼-------------------

KEYWORDS: Ad-Hoc Networks IDAODV, Network Monitor**,** Finite State Machine**.**

INTRODUCTION:

Since the appearance in 1970 in the form of ALOHANET, wireless packet radio networks have come a long way in terms of numbers, applications, and the feature set, among other things. The two largest attractions of wireless communication have been mobility and ease of deployment – laying cables is not only laborious and time consuming, but their maintenance is equally bothersome.

In any but the most trivial networks (point-to-point links), some mechanism is required for routing the packets from the source to the final destinations. This includes discovery and maintenance of routes along with associated costs. In what is called an ‘infrastructure based’ Wireless network, the job of routing is assigned to dedicated nodes called access points (AP).

Configurations of the APs are much less dynamic than there, possibly mobile, end-point nodes. APs are like base stations which keep track of nodes ‘associations/disassociations, authentication etc. and control the traffic flow between their clients as well as between fellow APs.

The term wireless network implies a computer network in which the communication links are wireless. The term Ad Hoc comes from the fact that there is no fixed infrastructure for forwarding/ routing the packets. Figure 1.1 shows an infrastructure-based and an AdHoc wireless network. In AdHoc networks, each node is willing to forward data to other nodes, and so the Determination of which nodes forward data is made dynamically based on the network connectivity.

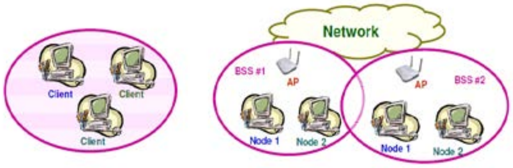

Figure 1.1 - Ad Hoc and Infrastructure Network Topologies

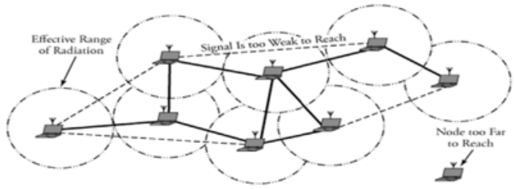

Figure 1.2 – A Typical MANET

RELATED WORK:

AODV [15] can be thought of as a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence

- *Prasanna Lakshmi G S is currently pursuing Ph.D program in Computer Science & Engineering inV.T. University, Belgaum,Karnataka PH-9035827037 E-mail:prasannalakhsmigs@gmail.com*
- *Shanta Kumar B Patil, is working a sHOD in CSE Dept,Nagarjuna College Of Engineering & Technolgy.*

numbers, and periodic beacons from DSDV. AODV is an on-demand routing protocol, which initiates a route discovery process only when desired by a source node. When a source node S wants to send data packets to a destination node D but cannot find a route in its routing table, it broadcasts a Route Request(RREQ) message to its neighbors, including the last known sequence number for that destination. Its neighbors then rebroadcast the RREQ message to their neighbors if they do not have a fresh enough route to the destination node enough route is a valid route entry for the destination node whose associated sequence number is equal to or greater than that contained in the RREQ message.)

This process continues until the RREQ message reaches the destination node or an intermediate node that has a fresh enough route. Every node has its own sequence number and RREQ ID1. AODV uses sequence numbers to guarantee that all routes are loop-free and contain the most recent routing information. RREQ ID in conjunction with source IP address uniquely identifies a particular RREQ message.

The destination node or an intermediate node only accepts the first copy of a RREQ message, and drops the duplicated copies of the same RREQ message. Each node that forwards the ROUTE REQUEST creates a *reverse route* for itself back to node S; after accepting a RREQ message, the destination or intermediate node updates its reverse route to the source node using the neighbor from which it receives the RREQ message.

The reverse route will be used to send the corresponding Route Reply (RREP)message to the source node – when the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPLY that contains the number of hops necessary to In order to maintain routes, AODV normally requires that each node periodically transmit a forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPLY containing an infinite metric for that destination.

Upon receipt of such a ROUTE REPLY, a node must acquire a new route to the destination using Route Discovery as described above. HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbor is taken as an indication that the link to the neighbor in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbors.

When a link goes down, any upstream node that has recently reach D and the sequence number for D most recently seen by the node generating the REPLY. Meanwhile, it updates the sequence number of the source node in its routing table to the maximum of the one in its routing table and the one in the RREQ message. When the source or an intermediate node receives a RREP message, it updates its *forward route* to the destination node using the neighbor from which it receives the RREP message. It also updates the sequence number of the destination node in its routing table to the maximum of the one in its routing table and the one in the RREP message. A Route Reply Acknowledgement (RREP-ACK) message is used to acknowledge receipt of a RREP message. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing.

MOTIVATION:

Mobile Ad Hoc networks (MANETs) are vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed operation and constrained capability. AODV is an important on demand routing protocol. Security is a central requirement for mobile Ad Hoc networks. Security and robustness will impact the design of the standard for Ad Hoc networks is the main motivation in this paper.

PROBLEM STATEMENT:

Intrusion Detection System aimed at securing the AODV protocol has been studied by Stamouli et al [1] using specification based technique. They conclude that AODV performs well at all mobility rates and movement speeds. However, we argue that their definition of mobility (pause time) does not truly represent the dynamic topology of MANETs. In this paper, the work of Stamouli et al [1] has been extended and the proposed protocol is called IDAODV (Intrusion Detection AODV).

In our work, we make use of Knowledge-based intrusion detection. Our Intrusion Detection and Response Protocol for MANETs have been demonstrated to perform better than that proposed in [1] in terms of false positives and percentage of packets delivered.

Since the earlier work by Stamouli et al [1] do not report true positive i.e. the detection rate, we could not compare our results against that parameter with their method, IDAODV performs real time detection of attacks in MANETs running AODV routing protocol. The prototype has also given some insight into the problems that arise when trying to run real applications on an Ad

Hoc network. The algorithm also imposes a very small factor for the resource constrained nodes.

INTRUSION DETECTION AODV (IDAODV)

In this paper we propose and discuss IDAODV, an Intrusion Detection mechanism for Wireless Mobile Ad Hoc Networks. IDAODV is based on State Transition Analysis Technique, which was initially developed to model host-based and network-based intrusions in a wired network environment. Of all the routing protocols proposed for MANETs, AODV has been very popular and has become an Internet standard. This also has been the reason for AODV becoming more and more vulnerable to attacks.

Problem Statement/ AODV Routing Attacks

AODV presents many opportunities to attackers. We first identify a number of misuse goals that an inside attacker may want to achieve [8].

1) Route Disruption: Route Disruption means either breaking down an existing route or preventing a new route from being established.

2) **Route Invasion:** Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.

3) **Node Isolation:** Node isolation refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.

4) **Resource Consumption:** Resource consumption refers to consuming the communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.

5) **Denial of Service**
To achieve goals, the following misuse actions or attacks may be performed

Packet Dropping Attack

In a packet dropping attack, the attacker simply drops the received routing message. Packet dropping is detected by checking whether a neighbor forwards packets towards the final destination. To be able to do this, it is necessary to maintain a neighbor table. This attack can be divided into various subcategories as follows:
If an attacker applies such attacks to all the RREQ messages it receives, this kind of misuses equivalent to not having the attacking node in the network. An inside attacker may also selectively drop RREQ messages. Attackers that launch such misuses are in nature similar to the selfish nodes.
If the attacker applies this attack to RREP message, it can in some cases lead to route disruption.

The attack can also be applied to data packets, where an inside attacker prevents a victim node from receiving data packets from other nodes for a short period of time. The attacker may make the following modifications after it receives a RREQ message from the victim node:
(1) Increase the RREQ ID by a small number; (2) Replace the destination IP address with a non-existent IP address;
(3) Increase the source sequence number by at least one;
(4)Set the source IP address in IP header to a non-existent IP address.

The attacker then broadcasts the forged message. When the neighbors of the attacker receive the faked RREQ message, they update the next hop to the source node to the non-existent node, since the faked RREQ message will have a greater source sequence number. Due to the non-existent destination IP address, the faked message can be broadcast to the farthest nodes in the adhoc network. When other nodes want to send data packets to the source node, they will use the routes established by the faked RREQ message, and the data packets will be dropped due to the non-existent node. This attack, however, cannot fully isolate the victim node due to local repair mechanisms in the AODV protocol.

The other nodes will initiate another round of route discovery if they note that the data packets cannot be delivered successfully. In addition, the victim node may still be able to send data packets to other nodes. Several of the atomic misuses of RREQ messages use RREQ messages to add entries the routing table of other nodes.
These entries are different from those established through normal exchange of RREQ and RREP messages. In particular, the lifetime of these entries is set to a default .Thus, to make such entries effective, an attacker needs to launch the atomic misuses periodically.

Details of IDAODV

We now describe the details of the design and implementation of the proposed IDAODV. IDAODV detects attacks against the AODV routing protocol in

Wireless Mobile Ad Hoc Networks. The components of IDAODV are discussed in the following sections.

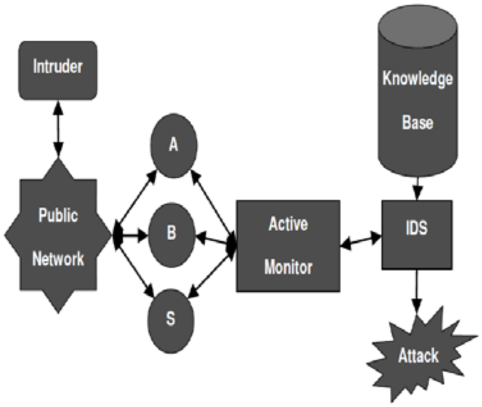

Figure 4.3: Architecture of IDAODV

Network Monitor

The nature of Ad Hoc networks prohibits any single IDS node to observe all messages in a request-reply flow. Therefore, tracing of RREQ and RREP messages in a request-reply flow has to be performed by distributed network monitors (NM). Figure 4.3 depicts the architecture of a network monitor. Network monitors passively listen to IDAODV routing message and detect incorrect RREQ and RREP messages. Messages are grouped based on the request-reply flow to which they belong. A request reply flow can be uniquely identified by the RREQ ID, the source and destination IP addresses.

Finite State Machine

Specification-based approach provides a model to analyze attacks based on protocol specifications. A network monitor employs a finite state machine (FSM) [4] for detecting incorrect RREQ and RREP messages [3, 5, 6, and 7].

It maintains an FSM for each branch of a request-reply flow. A request flow starts at the 'Source' state. It transits to the 'RREQ Forwarding' state when a source node broadcasts the first RREQ message (with a new REQID).
When a forwarded broadcasting RREQ is detected, it stays in 'RREQ Forwarding' state unless a corresponding RREP is detected. Then if a uncast RREP is detected, it goes to 'RREP Forwarding' state and stays there until it reaches the source node and the route is set up. If any suspicious activity or an anomaly is detected, it goes to the 'Suspicious or Alarm' states. When an NM compares a new packet with the old corresponding packet, the primary goal of the constraints is to make sure that the AODV header of the forwarded control packets is not modified in an undesired manner.

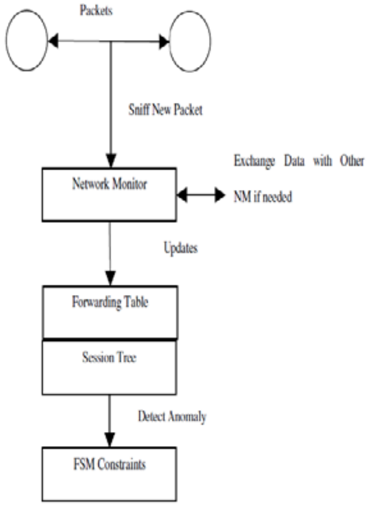

Figure 4.4: Network Monitor

If an intermediate node responds to the request, the NM will verify this response from its forwarding table as well as with the constraints in order to make sure that the intermediate node is not lying. In addition, the constraints are used to detect packet drop and spoofing. The finite state machine is depicted in Figure 4.4. Stamouli [1] has not used network monitor to trace RREQ and RREP message in a request reply flow for distributed network. Whereas in the proposed FSM, we used the above flows Figure 4.4.

PROPOSED ALGORITHM

For the intrusion detection to identify the sequence number attack, we analyzed two algorithms.

Notations

The following notations have been used for the description of the algorithms.

For a set of paths denoted by **P**, where, path P is an ordered set of nodes,

The length of P is defined in terms of number of hops and denoted by $|P|$

For $0 \le i \le |P|$, $P[i]$ is the i^{th} node in the path

Assumptions

The following assumptions have been made for the algorithms.

1. **$\forall$ Pi, Pj $\in$ P, Pi $\not\subset$ Pj**
   e.g. if P1 = {A, B, C} and P2 = {A, B, C, D}, remove P1

2. **$\forall$ Pi, Pj $\in$ P, Pi[|Pi| - 1] $\notin$ Pj, |Pj|**
   e.g. if P1 = {A, B, C} and P2 = {A, B, D, E}, remove C from P1

3. **$\forall$ Pi $\in$ P, |Pi| > 1**

Algorithm 1: Detection of Routing Packets Dropped

- Check a path from the farthest node to the nearest
- $\forall$ p $\in$ P, check p[|p|]
- If an ACK is received $\forall$ v $\in$ p and v ≠p[|p|], v is *Good*
- Otherwise, check p[|p| - 1]
- If an ACK is not received from p[i+1] but received from p[i], 0≤i<|p|, select p[i]

Algorithm 2: Node Selection

If p[i] is responsive but p [i+1] is not, there are three possibilities:

- p[i] is *Bad*
- p[i+1] is *Lost*
- The link p[i+1] → p[i] is broken

CONCLUSION & FUTURE ENHANCEMENT

An Intrusion Detection System aiming at securing the AODV protocol has been developed using specification-based technique. It is based on a previous work done by Stamouli et al [1]. The IDS performance in detecting misuse of the AODV protocol has been discussed. In all the cases, the attack was detected as a violation to one of the AODV protocol specifications. Our Intrusion Detection and Response Protocol for MANETs have been demonstrated to perform better than the ones proposed by Stamouli et al in terms of false positives and percentage of packets delivered. Since Stamouli et al do not report true positive i.e. the detection rate, we could not compare our results against that parameter with their method.

The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols. A study can be conducted on the relationship between the average detection delay and the mobility of the nodes. More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained. A complete system can be designed to implement intruder identification.

REFERENCES

[1] I. STAMOULI. Real-time intrusion detection for ad hoc networks. Master's thesis, University of Dublin, September, 2003.

[2] PERKINS, C. E., AND BHAGWAT, P. DSDV Routing over a Multihop Wireless Network of Mobile Computers. In Perkins [20], 2001, ch. 3, pp. 53–74.

[3] TSENG, CHIN-YANG, ET AL. A Specification-based Intrusion Detection System for AODV, In Proceedings of the 1st ACWorkshop on Security of Ad hoc and Sensor Networks (SASN’03). Fairfax, VA. 2003.

[4] K. ILGUN, R. A. KEMMERER, AND P. A. PORRAS. State Transition Analysis: A Rule-Based Intrusion Detection Approach. IEEE Transactions on Software Engineering, 21(3):181–199, 1995.

[5] C. KO, M. RUSCHITZKA, AND K. LEVITT, “Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-based Approach,” In Proceedings of the 1997 IEEE Symposium on Security and Privacy, May 1997, pp. 134-144.

[6] D. DREEF ET AL, “Utilizing the Uncertainty of Intrusion Detection to Strengthen Security for Ad Hoc

Networks”, Third International Conference, ADHOCNOW2004, Vancouver, Canada, July 22-24, 2004, pp.82-95.

[7] R. RAO AND G. KESIDIS, “Detection of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited”, Brazilian Journal of Telecommunications, 2003.

[8] CHARLES E. PERKINS, “Ad Hoc on Demand Distance Vector (AODV) Routing”. Internet draft, draft-ietf-manet-aodv-01.txt.