Packet Dropping Alleviation In Mobile Ad Hoc Networks By Power Saving AODV

R.Gunasekaran[1], V.P.Divya[2], S.Sharanya[3], V. Rhymend Uthariaraj[4]

Abstract

In a mobile ad hoc network every node acts as a router for its neighbor. The existing routing protocols assume that the all the nodes will fully participate in the transmission of packets. Though usually a waiting time is allotted for each participating node to send its data, some nodes, however, behave maliciously, by dropping the packets. This paper aims at developing an algorithm to detect misbehaving nodes and prevent such misbehavior by incorporating promiscuous properties in AODV. The new routing algorithm extensions presented in this paper make it possible to detect and isolate misbehaving nodes with energy saving mechanism, thus making it unattractive to deny cooperation. In the presented scheme, trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes.

Keywords : MANET, AODV, PSAODV, RIDAN, FSM, back off.

1. Introduction

A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network. It is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which forms an arbitrary topology. The IEEE 802.11 MAC protocol (or variants thereof) has been popularly considered for use in ad hoc networks. The decentralized random access nature of this protocol makes it especially vulnerable to attacks. A station deliberately misuses the MAC protocol to gain bandwidth at the expense of other nodes; this misuse is also hidden and independent from the upper layers and hence cannot be detected by any mechanism used in those layers.

This paper describes about the research made on incursion discovery for mobile Ad hoc networks. It mainly focuses on vulnerabilities of existing (Ad hoc on demand routing protocol) AODV protocol and attacks against AODV. The solution is proposed in terms of a new protocol called (Packet Saving AODV) PSAODV. The attack against AODV mainly concentrates on the nodes that fail to transfer the initial hand-shaking messages. Hand-shaking messages correspond to (Route Request messages) RREQ and (Route Reply messages) RREP.

In this paper, section 2 explains in detail about the works done in this field, section 3 discusses about the existing AODV protocol and its disadvantages. The incursion discovery mechanism is presented in sections 4 & the implementation of energy saving attack is described in section 5.The implementation of the proposed solution (Packet Saving AODV) is dealt in section 6 .The Experimentation results are presented in section 7 and finally conclusion is presented in section 8 .

2. Related Work

Several techniques have been proposed to detect back-off value violations (Selfish-misbehavior) at MAC layer in Mobile Adhoc Networks.

[1,2,3,4]Department of Information Technology, Anna University, Chennai-600044, India. e-mail : gunamit@annauniv.edu

The Real Time Intrusion Detection for Adhoc Networks (RIDAN) system can be characterized as an architecture model for intrusion detection in wireless adhoc networks, while its implementation targets specifically the AODV routing protocol [1]. It can be classified as an architecture model because it does not perform any changes in the underlying routing protocol but merely intercepts the routing and application traffic. Thus, the security component operates in a different layer without interfering with the normal operation of the routing protocol. Since the RIDAN system does not utilize any cryptographic mechanism to ensure protection from malicious activities, it does not introduce any additional computation overhead to the routing process. Furthermore, it does not require additional packets to be sent and does not increase the consumption of additional bandwidth.

Pradeep Kyasanur, Nitin H. Vaidya [2] proposes a solution in which receiver (the node to which the packets are destined) sets back-off timer for the sender. The number of idle slots of the sender monitored by the receiver anticipates the malicious sender. This scheme fails to detect the in intermediate nodes that are malicious. Alvaro A. Cardenas, Svetlana Radosavac and John S. Baras [4] proposed an algorithm to ensure honest backoffs when at least one, either the receiver or the sender is honest. Damon McCoy, Doug Sicker, Dirk Grunwald Misbehaving Node Detection (MIND) mechanism [5], which integrates policy, detection and remediation components for identifying and handling misconfigured, misbehaving, or malicious devices. This system relies on single trusted centralized node that monitors the entire wireless traffic. This approach has a disadvantage as it is based on centralized approach. Jing Deng, Richard Han, Shivakant Mishra [6], proposed a solution in which forwarding tables are constructed at each nodes to facilitate communication between sensor nodes and a base station.

3. Ad Hoc On Demand Routing Protocol

The Ad hoc On Demand Routing Protocol (AODV) routing protocol works on top of the Destination Sequenced Distance Vector Routing (DSDV) protocol. AODV is an improvement of DSDV as it minimizes the number of required broadcasts since it creates routes in an on-demand basis, in contrast to DSDV, which maintains a complete set of routes [6][7]. It utilizes destination sequence numbers to ensure loop-freedom at all times and to avoid the count-to-infinity problem associated with classical distance-vector protocols.

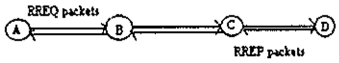


Figure 1 : An AODV Example

When a node needs a route to a destination it broadcasts a Route Request (RREQ) message. The RREQ message is spread throughout the network. As soon as the message reaches a node with fresh adequate routes to the specific destination or the destination node itself, a Route Reply (RREP) message is unicasted back to the requesting node. In Fig.1 the node A tries to find a route to the destination D by sending the RREQ. RREQ reaches the node B. when it decides that it is not destined for itself, it will send RREQ to the next node C. Node C acts in the same manner and sends to the Node D. On receiving the RREQ packets, it knows that it is destined for itself and hence sends RREP. Generally AODV offers low overhead, quick adaptation to dynamic link conditions and low processing and memory overhead. Thus the AODV routing protocol is used in this research, as it is the widely used one in the development of the Real-Time Intrusion Detection system. The disadvantage with this protocol is that it does not consider the vulnerabilities. The nodes that fail to transfer the routing packets are not identified in normal AODV. Thus a new routing protocol PSAODV is proposed as an extension of AODV protocol.

4. Incursion Discovery

A. Finite State Machine Constraints

The network monitor employs a finite state machine for detecting incorrect RREQ and RREP packets. A finite state machine is defined as an abstract machine consisting of a set of states (including the initial state), a set of input and output events and a state transition function. The function takes the current state and an input event and returns the new set of output events and the next state. The state machine can also be viewed as a function, which maps an ordered sequence of input events into a corresponding sequence of output events.

Timed finite state machines are an extension to normal finite state machines that are used when real-time behavior is required. Thus, timed finite state machines are state-transition graphs with timing constraints using finitely many real-valued clocks. Hence, a time related event might trigger the machine to move forward to a new state.

B. Assumptions

For the RIDAN [1] system to work, some factors have to be true. The assumptions that were made during the implementation of this system are not farfetched or unrealistic and can easily be realized in an ad hoc networking environment [3]. Our assumptions are:

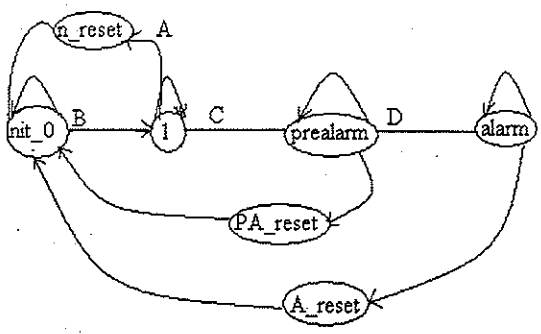
- Every link between the participating nodes is bi-directional.
- Nodes operate in a promiscuous mode, which means they can listen to their neighbor's transmissions.
- All the participating nodes have the RIDAN incursion discovery component activated.

C. Energy Saving Attack

Mobile nodes due to limited battery life and limited-processing capabilities may decide not to participate in the routing process in order to conserve energy. Thus, a malicious node upon receiving a routing packet that is not destined for it drops the packet deliberately. Though such nodes conserve energy, they may also cause network segmentation. If some of the participating nodes are connected only with the malicious node, they become unreachable and isolated from the rest of the network. This attack against AODV is realized as Energy saving attack and is not handled by the normal AODV.

D. Energy Saving Attack Detection

All the nodes participating in the network are set to be in promiscuous mode so that the neighboring nodes can detect whether a malicious node has forwarded a routing packet. However, some times a node may not forward the routing packet due to traffic overload also. Those nodes are not really malicious and are referred to as offending nodes. The incursion discovery component moves first to a pre-alarm state in order to prevent false alarms caused by traffic overload and in this state it unicasts the routing packet to the offending node again.



A-> If next node forwards the packet or replies with RREP
B->RREQ forwarded.
C->if next node does not forward a packet
D->If node does not forward second packet

Figure 2 : Finite State Machine

The presented Finite State Machine (FSM) is triggered whenever a node sends or forwards a RREQ or a RREP packet. It remains in state 1 for time t waiting for the node to forward/reply to the routing packet. If the node replies or forwards the packet, it normally resets the FSM with N_RESET as described in Fig.2 Finite state machine. If the node fails to appropriately respond to the forwarded routing traffic, the FSM moves to a Pre-Alarm state and remain there for time t. If the node manages to respond appropriately by forwarding the routing traffic or by replying to a RREQ, it is removed from the suspected nodes list and the FSM normally resets.

Otherwise, the FSM goes to an alarm state and the monitoring node marks this node as malicious. This is a distributed approach and hence overcomes the disadvantages of centralized approach [5] and as this system monitors all the intermediate nodes it overcomes the disadvantage of only monitoring sender or receiver [2].

Thus monitoring node does not forward any kind of traffic through the node that is marked malicious by the FSM and it also sends a RRER packet to the upstream neighbors in order to prevent them from sending traffic through the malicious node. Thus the mobile Ad hoc network is secured as the malicious nodes are detected and logically eliminated from the network.

5. Energy Saving Attack - Implementation

A new routing agent is proposed to detect the malicious behavior of the nodes in energy saving attack. The existing AODV protocol is extended as the new routing agent PSAODV (packet saving AODV).

In this attack, the malicious node acts selfishly and drops all routing traffic that it is not destined for itself. Thus, upon a RREQ packet the node checks the destination. Only if the destination is the same node, it further processes the packet and sends a RREP. Similarly, when the node receives a RREP packet, it will add the new route to its routing table only after checking if it had sent the original request for the route. In all the other cases the node just drops the received packet without processing. The Route Error (RERR) packets are processed normally in all cases, which help in detecting invalid routes.

A. Algorithm

Algorithm To Receive The Packet

- Extract the IP_header of the packet p
- Extract the routing information included in the packet p
- Drop if this node I the source of the packet if I have recently heard of this request.
- Check if this node is the destination of this RREQ packet, if yes then process it.
- If this node is not the destination drop it.

Algorithm To Reply For The Packet

- Extract the IP_header of the packet p
- Extract the routing information included in the packet p

- Check if this node is the destination of this RREP packet, if yes add the new route to the routing table and further process the packet normally
- If this node is not the destination then drop the packet.

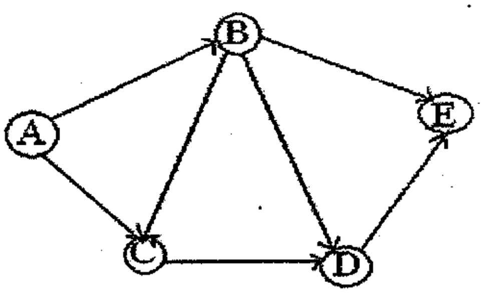


Figure 3 : Transform RREQ packets from A to E via B

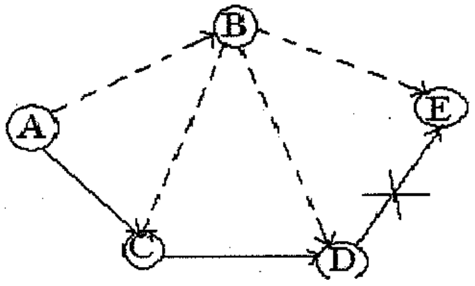


Figure 4 : Data sent from A to E via C. But D drops the packet

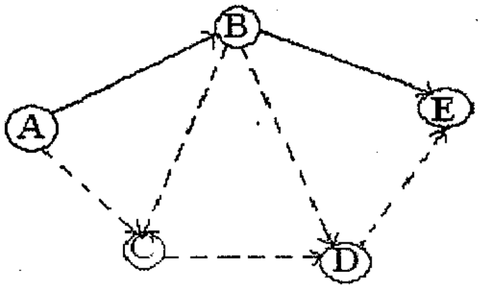


Figure 5. After the transmission discovery **route is changed & Data is sent Via B**

6. Packet Saving Aodv

The FSM developed to detect this attack was incorporated into the existing AODV routing agent. Since AODV does not operate in promiscuous mode by default, some modifications had to be performed in the existing files of ns-2[2]. The fact that promiscuous mode was enabled in AODV had no impact in the overall performance of AODV and the Enhanced tap module which is described below will make the nodes overhear the forwarded traffic.

The FSM developed to detect this attack is triggered whenever a node forwards routing traffic to its neighboring nodes. A structure called PS_Node is developed to hold information necessary to monitor the neighboring nodes that are suspected for malicious behavior. The PS_Node data structure holds the following information:

- node_id: The IP address of the node to which the routing traffic is 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 energy saving attack.
- Time: a double variable that keeps the time when 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 called monitoring list and waits to observe their behavior. The monitoring list (malicious node list) keeps track of the nodes which are participating in forwarding the packets. Once the packets have been forwarded by the node it will be removed from the list.

In the Enhanced tap module modification is done such that if it overhears that a neighboring node has replied to the forwarded RREQ, it means that the node 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 the offending node fails to forward the routing packet within a time limit, the FSM 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 2 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 any more.

The pseudo code of the Enhanced tap module that realizes the attack analysis and the countermeasure modules are illustrated below.

Algorithm For Enhanced Tap Module:

Steps to find the non-malicious node

If the node exists in the monitoring list and if the pre_alarm state is false

- Check the pre_alarm threshold against the time that this node was added in the list, if the time threshold has expired
    - Remove the node form the monitoring list.

If the node exists in the monitoring list and if the pre_alarm state is true

- Check the alarm threshold time against the time that this node was in the alarm state, if the time threshold has expired
    - Remove the node from the monitoring list.

Steps to find the malicious node

If the node exists in the monitoring list and if the pre_alarm state is false

- Check the pre_alarm threshold against the time that this node was added in the list, if the time threshold has not expired
    - Move the FSM to the pre_alarm state by setting the pre_alarm value to true.

If the node exists in the monitoring list and if the pre_alarm state is true

- Check the alarm threshold time against the time that this node was in the alarm state, if the time threshold has not expired
    - Set alarm value to true.
    - Send RERR packet to upstream neighbors.
    - Start timer for 2 seconds that the offending (malicious) node will be penalized.

7. Accuracy Of Ridan System

All incursion discovery systems suffer from false alarms that occur whenever the system incorrectly sounds an alarm when there is no malicious behavior present in the network.]. However, the traffic patterns that denote that an active attack is performed against the routing protocol can be realized when the AODV operates normally due to high application traffic and high node mobility. The advantages of PSAODV over AODV can be well seen from the graphs presented in Fig.6 and Fig.7.

The system was tested in terms of detection accuracy and it is found that it has greater accuracy in preventing the attack.

8. Implementation In Ns-2

The proposed solution is tested with ns-2 simulator. The testing was done with 25 nodes, in which 10 nodes are malicious nodes. At the initial phase there was high percentage of loss of packets as shown in Fig.7. According to the solution proposed, the malicious nodes that failed to transfer the packets were detected and finally the identified malicious nodes were re moved from the network of 25 nodes.

The metric delivery ratio is defined as the ratio between number of packets transmitted by the source and number of packets received by the destination.

The comparative study of the existing protocol AODV and the newly proposed protocol PSAODV is made with respect to the metric delivery ratio and the result is shown in the Fig.6.

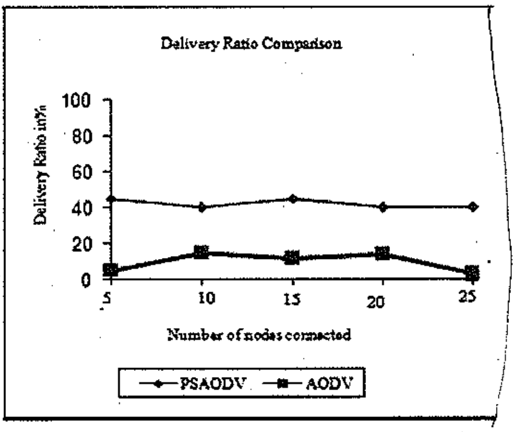


Figure : 6 Delivery Ratio Comparison

It can be seen from the graph that delivery ratio is high when PSAODV is used compared to the ratio when AODV is used.

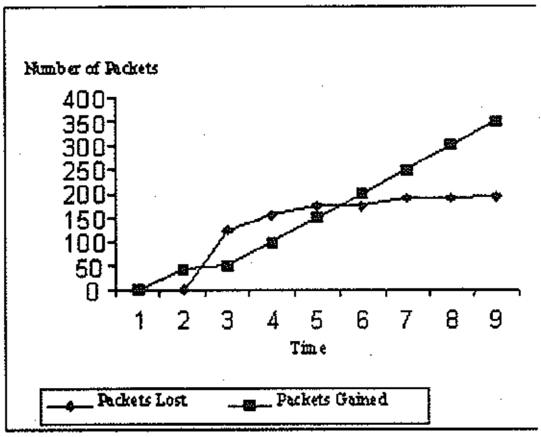


Figure 7 : Accuracy of the PSAODV In Reducing The Packet Loss

Fig.7. Depicts the accuracy of the new protocol PSAODV in reducing the packet loss. The malicious nodes that have been identified by the enhanced Tap module are being assisted by the PSAODV in reducing the packet loss by malicious node for saving its energy. Thus the graph shows that there is constant decrease in the packet loss against the packets gained in the network.

9. CONCLUSION

This paper identifies the special requirements of mobile ad hoc network security, robustness, and fairness, and it introduces a scheme to cope with them by retaliating for malicious behavior and warning affiliated nodes to avoid bad experiences. Nodes learn not only from their own experience, but also from observing the neighborhood and from the experience of their friends [9]. Observable attacks on forwarding and routing can be thwarted by the suggested scheme of detection, alerting and reaction. Thus a new routing algorithm Packet Saving Ad Hoc on Demand Distance Vector was proposed with energy saving mechanism from the MAC which improves the delivery ratio and reduces the packet loss.

References

[1] Ioanna Stamouli, *"Real-time Intrusion Detection for Ad hoc Networks",* A dissertation submitted to the University of Dublin, in partial fulfilment of the requirements for the degree of Master of Science in Computer Science.

[2] Pradeep Kyasanur, Nitin H. Vaidya, *"Detection and Handling of MAC Layer Misbehavior in Wireless Networks",* Technical report, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, August 2002.

[3] Frank Kargl, Andreas Klenk, Stefan Schlott and Michael Weber,*"Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks".*

[4] Alvaro A. Cardenas, Svetlana Radosavac and John S. Baras, *"Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks".*

[5] Damon McCoy, Doug Sicker, Dirk Grunwald, Department of Computer Science, *"A Mechanism for Detecting and Responding to Misbehaving Nodes in Wireless Networks".*

[6] S. Buchegger, *"Coping with Misbehavior in Mobile Ad-hoc Networks",* Ph.D. Thesis, EPFL, Switzerland 2004.

[7] Rebecca Bace, Macmillan Technical Publishing, 2000, *"Intrusion Detection".*

[8] G.L.F. Santos, Z. Abdelouahab, R.A. Dias, C.F.L. Lima, E. Nascimento (Brazil), E.M. Cochra, *"An Automated Response Approach for Intrusion Detection Security Enhancement".*

[9] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, karl Levitt, *"A Specification- based Intrusion Detection System for AODV",* Network Associate Laboratories, 2002.

[10] Pradeep Kyasanur and Nitin Vaidya, *"Selfish MAC Layer Misbehavior in Wireless Networks",* IEEE Transactions on Mobile Computing, September 2005.

[11] Koutsopoulos S. Radosavac, J. Baras, *"A Framework for MAC Protocol Misbehavior Detection in Wireless Networks",* WiSE, September 2005.

Authors Biography

R.Gunasekaran pursuing his Ph.D in the area of Mobile Ad hoc Networks in Anna University, received his ME degree in computer science and Engineering from Bharathiyar University and BE degree in Computer Science and Engineering from University of Madras. His area of interests includes Mobile Ad Hoc Networks, Mobile Communications, Pervasive Computing and Networking. He is presently working as a Lecturer in the Department of Information Technology, Anna University Chennai.

V.P.Divya is an undergraduate in Computer Science and Engineering in the Department of Information Technology from Anna University. Her area of interest includes Mobile Computing, Mobile Ad Hoc Networks and Database Management Systems

S.Sharanya is an undergraduate in Computer Science and Engineering in the Department of Information Technology from Anna University. Her area of interests includes Mobile Ad Hoc Networks, Mobile Computing and Pervasive Computing.

Dr. V.Rhymend Uthaiaraj received his PhD degree in Computer Science & Engineering from Anna university His area of interests includes Network security, Optimization of algorithms, Object oriented modeling, Pervasive Computing and Web design. He is presently the Professor and Director, Ramanujan Computing Center and Secretary, Tamilnadu Engineering Admissions in Anna University Chennai.