Research Paper

Engineering

KEYWORDS : Ad-Hoc, AODV, Reputation

Reputation based Route Computation for Wireless Ad-Hoc Network Using AODV

Ashiq Irphan K Department of Computer Science and Engineering, SRM University, Chennai.

Srisusindhran K Department of Computer Science and Engineering, SRM University, Chennai.

ABSTRACT

Routing in an ad-hoc network is different from that of an infrastructure based network. Ad-Hoc on Demand Distance Vector (AODV) routing protocol is a protocol that is used in an Ad-Hoc environment to find a route to the destination. Though AODV is effective in determining routes, it does not provide any security. In order to provide security, a reputation value (RV) is assigned to the next hop neighbors by the sender this is considered as a factor in computing the route in addition to the factors considered by AODV. To achieve this new component named Reputation Table (RT) is added to AODV protocol. This system aims at increasing the reliability of route selection of AODV protocol by adding additional information in the control messages while keeping the overhead of the system at a minimum.

Introduction

A wireless ad hoc network is a decentralized type of wireless network. The network is called ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity [3].

To set up an ad hoc wireless network, each wireless adapter must be configured to work in ad hoc mode. In addition, all wireless adapters on the ad hoc network must use the same SSID and the same channel number [3]. An ad hoc network tends to feature a small group of devices, all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad hoc network quickly becomes difficult to manage.

Ad hoc networks make sense when needing to build a small, all-wireless LAN quickly and spend the minimum amount of money on equipment [6] Ad hoc networks also work well as a temporary fallback mechanism if normally-available infrastructure mode gear (access points or routers) stop functioning.

Routing in Ad Hoc Networks

A node in an ad hoc network does not need a route to a destination until that destination is to be the recipient of packet sent by the node, either as the actual source of the packet or as an intermediate node along a path from the source to the destination. Routing in an ad hoc network is of two major types, Proactive and Reactive, based on the when the route computation is initiated [3].

Routing protocols in ad hoc networks may work on a proactive basis, which is to keep track of routes to all destinations in the network. Proactive routing is also known as table driven routing. When an application starts, a route can immediately be selected from the routing table. By doing so the initial delay experienced by the application is avoided because routes are available as part of a well maintained table. One of the major disadvantages of using a proactive routing protocol is the need for additional control traffic, continually in order to keep the routes updated.

Unlike proactive routing protocols, reactive protocols work in an On-Demand basis. An ad hoc network usually experiences frequent link state changes. On-Demand routing, also called reactive routing protocols are designed in a way to acquire route information only when an application need to communicate with a specific node in the network. Reactive routing protocols use less bandwidth for maintaining routes at each node. It is also to be noted that the initial delay experienced by the applications might be very high.

Attacks on Ad Hoc Networks

Most attacks against the routing protocol of ad hoc network may have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. An attack may also aim at impeding the formation of the network, making legitimate nodes store incorrect routes, and more generally at perturbing the network topology [2]. Attacks at the routing level can be classified into two main categories: incorrect traffic generation and incorrect traffic relaying. Sometimes these coincide with node misbehavior that are not due to malice, e.g. node malfunction, battery exhaustion, or radio interference.

Incorrect Traffic Generation

This category includes attacks which consist in sending false control messages: i.e. control messages sent on behalf of another node (identity spoofing), or control messages which contain incorrect or outdated routing information. The network may exhibit Byzantine behavior, i.e. conflicting information in different parts of the network. The consequences of this attack are degradation in network communications, unreachable nodes, and possible routing loops [7] [8]. The following are some of the types of incorrect traffic generation attacks

- Cache Poisoning
- Message Bombing
- DOS and DDOS attacks

Incorrect Traffic Relaying

Network communications coming from legitimate, protocol-compliant nodes may be polluted by misbehaving nodes. Making the legitimate nodes to relay incorrect information to other nodes, eventually making the all the nodes on the network to use wrong routing table [13]. This would lead to a state in which no part of the network functions as expected. The following are few attacks that fall under the category of Incorrect Traffic Relaying [15].

- Blackhole attack
- Message tampering
- Replay attack
- Wormhole attack
- Rushing Attack

Ad Hoc On-Demand Distance Vector Protocol

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol provides quick and effective route establishment between nodes between nodes desiring communication [1] [4]. Unlike most other protocols that are used in an Ad Hoc environment AODV is not a modification of routing protocols used in infrastructure based network, it has been specifically designed for the use in ad hoc environment [9] [7]. AODV achieves its efficiency from minimizing the route acquisition latency and the use of minimal control overhead.

Security Considerations

As on date AODV does not provide any explicit security measures against impersonation attacks. In an ad hoc network nodes work under the assumption, that all the relaying nodes are part of the network, and any node which comes into the communication range can be used to relay traffic. This imposes a threat if the relaying node has intentions to breach the security of the network [9]. So there is a need to establish a mechanism that would tell AODV to consider a more reliable route rather than just selecting the shortest route.

Modified AODV

A Reputation Value (RV) is created based on the number of transmissions vs. number of successful transmissions. This is accomplished by adding a control field to the Route Reply (RREP) packet, which is the Reputation Value. This value can be computed as shown in the Equation 1.

$$RV=1-(FT/TT) \qquad (1)$$

Where RV is Reputation Value,

TT is Total number of transmissions and

FT is Number of Failed Transmissions.

The system uses a new table that stores the reputation value against its neighbors, when a route has to be selected in cases where a node receives more than one route; AODV always selects the shortest path. But the purpose of this work is to select the most reliable route, in order to do this the proposed system checks the reputation table before selecting a route in case a RREQ message receives more than one RREP messages [14]. Fig. 1 shows the logical components that exist in the existing AODV routing protocol and the component that are added to perform the proposed modification.

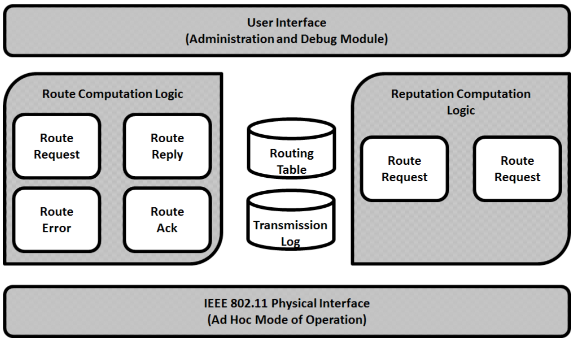

Figure 1 Logical Components

Route Selection

The route request process is similar to that of the existing system as usual the node sends a RREQ message to its neighbors with the same control information. For which any node is free to respond by sending a RREP message, but the choice of accepting the route is the choice of the original requestor [15].

When a node receives the RREP packet, it first checks it routing table to see if it already has a route to that particular destination node, if it does not have any, an entry is added to the routing table, and the structure of the routing table is unaltered in the proposed system. If there is a route available, then it compares the sequence number in the RREP message with that of the sequence number in the routing table entry, if both the sequence number are the same the RREP is discarded, if the sequence number in the RREP message is greater than the one in the routing table entry, the next hop is checked, if the next hop node is same in both the RREP message and the routing table entry, the sequence number in the routing table entry is updated. If the next hop node is not same or if the sequence number in the RREP message is lower than that in the routing table entry, then the reputation value of that node is checked, if the Reputation Value (RV) of the next hope node is low then the RREP is ignored. If the Reputation Value of the next hop is higher than the existing route then the routing table is update.

Modified RREP Packet

In order to propagate the reputation value of the neighbor to the route requesting node, an additional field is added to the RREP Packet. This field carries a numeric value computed by the responder node, as per the equation 1. The proposed field is a 32 bit field. The need for 32 bits is in order to maintain higher values because in an ad hoc network even when the node is not actually transmitting, the number of transmissions may go high because all the nodes maybe involved in routing process. Fig. 2 shows the proposed modification to the RREP packet format.

<table>
<tr><td colspan="10">0</td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type</td><td>R</td><td>A</td><td colspan="9">Reserved</td><td colspan="5">Prefix Sz</td><td colspan="8">Hop Count</td></tr>
<tr><td colspan="32">Destination IP Address</td></tr>
<tr><td colspan="32">Destination Sequence Number</td></tr>
<tr><td colspan="32">Originator IP Address</td></tr>
<tr><td colspan="32">Lifetime</td></tr>
<tr><td colspan="32">Reputation Value (RV)</td></tr>
</table>

Figure 2 Modified RREP Packet

Comparison with AODV

As a requirement to compare the modified AODV with the conventional AODV, a few metrics have been taken under consideration. Those are as follows:

- Delay in Route Discovery.
- Packet Loss Percentage.

Delay in Route Discovery

Delay in route discovery is the delay that a node experiences while establishing the route to a specific destination when establishing the route for the first time [10] [11]. Because of the additional computation of the Reputation Value (RV) the modified version of AODV experiences a slight delay than the conventional AODV [5].

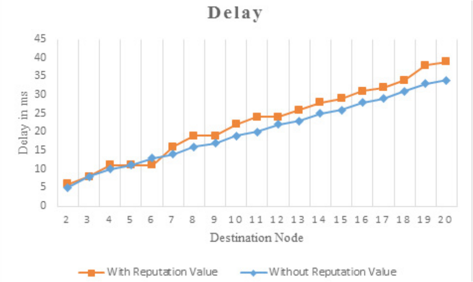

Figure 3 Delay Comparison

Packet Loss Percentage

For the purpose of estimating packet loss, simple ICMP Ping is used and different nodes respond to the ping request, it is noted from the figure that packet loss percentage is consistent along with the AODV network implemented without the additional reputation value [10] [11]. This proves the effective implementation of the reputation value does not affect the delivery ratio of AODV based ad-hoc networks [12].

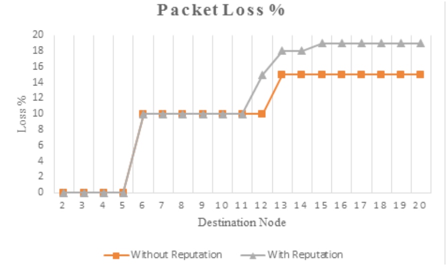

Figure 4 Packet Loss Comparison

Conclusion

The proposed modification in comparison with AODV shows the performance of both the systems to be close to one another, while providing an additional reliability in route selection process.

REFERENCE

[1] Amit N.Thakare, Mrs. M Y Joshi, "Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks". IJCA transaction on Issues on MANET, vol. 4, no. 9, pp 211-218, January 2000. | [2] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, "Byzantine robust trust establishment for mobile ad hoc networks", Springer transaction on Telecommunication Systems, vol.35, no.3-4, pp 189-206, August 2007. | [3] Charles E. Perkins, "Ad Hoc Networking", Chapter No: 6, pp 173-220, Addison-Wesley Professional, 1st Edition, 2001. | [4] Ehsan, H.; Uzmi, Z.A., "Performance comparison of ad hoc wireless network routing protocols", Proceedings of the Eight International Multitopic Conference, pp. 24-26, December 2004. | [5] Gamal, A.El.; Mammen, J.; Prabhakar, B.; Shah, D., "Throughput-delay trade-off in wireless networks," Proceedings of the Twenty-third AnnualJoint INFOCOM Conference, pp. 7-11, March 2004. | [6] Gupta, P.; Kumar, P.R., "The capacity of wireless networks", IEEE Transactions on Information Theory, vol.46, no.2, pp.388-404, March 2000. | [7] http://help.metasploit.com/ accessed on 17.10.2013. | [8] http://nmap.org/book/man.html accessed on 14.10.2013. | [9] http://tools.ietf.org/html/rfc3561 accessed 08.11.2013. | [10] http://www.oracle.com/us/technologies/virtualization/virtualbox/overview/index.html accessed on 10.10.2013. | [11] http://www.wireshark.org/docs/wsug_html_chunked/ accessed on 15.10.2013. | [12] Julian Hsu; Bhatia, S.; Ken Tang; Bagrodia, R.; Acriche, M.J., "Performance of mobile ad hoc networking routing protocols in large scale scenarios," Proceeedings of the Military Communications Conference, IEEE MILCOM 2004, pp.21-27 November 2004. | [13] Nait-Abdesselam, F., "Detecting and avoiding wormhole attacks in wireless ad hoc networks," IEEE Transaction on Communications, vol.46, no.4, pp.127-133, April 2008. | [14] Shafiullah Khan, Nabil Ali Alrajeh, Kok-Keong Loo, "Secure route selection in wireless mesh networks", Springer transaction on Computer Networks, vol. 56, no. 2, pp 491-503, February 2012. | [15] Xiaojuan Liao; Dong Hao; Sakurai, K., "Classification on attacks in wireless ad hoc networks: A game theoretic view," Proceedings of the Seventh International Conference on Networked Computing and Advanced Information Management, pp. 21-23, June 2011. |