Middle-East Journal of Scientific Research 23 (8): 1720-1726, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.08.22467

Performance Enhanced Reverse AODV Routing Protocol for MANETs

[1]A. Vinodh Kumar, [2]S. Kaja Mohideen and [3]A. Kathirvel

[1]B.S. Abdur Rahman University, Chennai, India
[2]School of Electrical Communication and Sciences, B.S. Abdur Rahman University, Chennai, India
[3]Department of Information Technology, Anand Institute of Higher Technology, Chennai, India

Abstract: In latest era, a number of techniques and applications have been used generally for transmitting information over heterogeneous wireless networks. In common, a wireless network may fit to one of the two types: infrastructure network and ad hoc network. Ad hoc networks be situated frequently defined as an autonomous system of nodes connected by wireless links for communicating in a multi-hop fashion. The ad hoc network deals numerous advantages, including low cost, simple network maintenance and convenient service coverage. Depends upon available resources, nodes can be controlled, therefore each nodes are limited to carry out its own needs are being eliminated to coordinate that the Reputation system is one of the main results to the non-cooperation node problems. A reputation system categorizes safe node and unsafe nodes by calculating node position by reputation values and uses a reputation origin. Then this system has been broadly used, very small experimentation has been dedicated to inspecting the capability of the node aid inducement afford by the concept. We propose Performance Enhanced Reverse Ad Hoc On Demand Vector Routing Protocol (PERAODV), which usages Hybrid Reputation System (HRS). A Hybrid Reputation system is an enhanced version of Classical Reputation System (CRS). Contrasting the CRS it takes into account all the reputation values from the node to determine whether it is reliable or not. Extensive simulation studies using NS2 establish the soundness of the proposal.

Key words: MANET · RAODV · PERAODV · Routing

INTRODUCTION

A computer with a network is created to afford a means of carrying data, sometimes crucial data, from one computer to another. There are two types of networks, based on the connections made. They are wired and wireless networks.

A wired network is one in which all the components are connected with network cables. For mobility, Wireless LAN technology is a key permissive technology that allows computers to elongate their expensive network into areas where hardwiring would be excessive or difficult. It allows users to achieve total PC anticipation and location independence.

Ad hoc wireless network (Fig. 1) have been increased transformation in a collection of methods because they can be setup with simple framework and basically no fundamental administration, so the decision of which nodes forward data is made dynamically on the basis of network connectivity. There are two types of routing protocols used in MANETs are: Proactive and Reactive protocols [1].

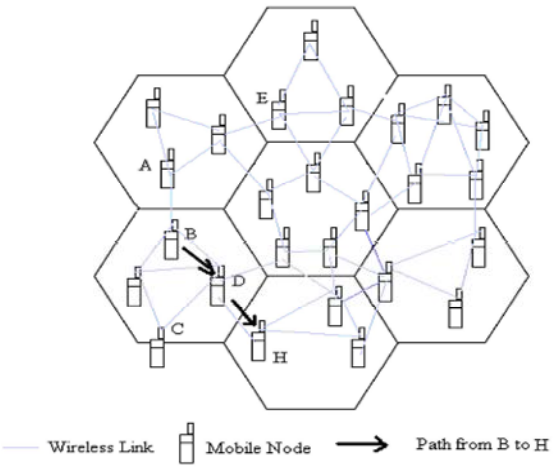

Fig. 1: Ad hoc wireless network

Corresponding Author: Mr.A. Vinodh Kumar, B.S. Abdur Rahman University, Chennai, India.

However, Delay control methods not apply directly to ad hoc networks, which contain special challenges like inadequate wireless bandwidth, power constraints and route failures owing to node mobility and limited buffer size. This means that as added number of packets is being showed complete a network, network congestion would result in high packet loss rate, re-routing variability, loss of energy and bandwidth and retransmission of absent packets. Though, delays and packet losses need not necessarily be caused by network congestion, however these can be misconstrued as congestion losses.

Ad hoc On-Demand Distance Vector (AODV) is a packet routing protocol designed for use in mobile ad hoc network [2]. Once the packet is received in hand and if the packet is needed to transmit then only a route is establish by AODV. By routing path information this protocol select its own routing path independently. Our aim is to design a new protocol based on Reverse Ad hoc On Demand Vector (RAODV) called as Performance Enhanced Reverse Ad hoc On Demand Vector (PERAODV), which provides better security, compared to AODV and RAODV.

Unlike fixed networks such as the Internet, a dynamic network like a MANET is classy in terms of delay and throughput and it is possible only to remove a delay but not prevent it altogether [8] to eradicate network congestions, many investigators have proposed the use of active queue PERAODV strategies

The main goal of this research work is to detect the malicious nodes (Non co-operative nodes) in the network and avoid them to conserve computational resources such as power consumptions etc. And choose a trustworthy node in order to forward a packet in the network. We face problems while forwarding the packets in a single best path chosen, as they are chance that the node in the path may drop the packets in order to retain its CPU resources. So our main goal is to efficiently increase the QOS factors like: Throughput, Delay and Security by using hybrid reputation system [3].

Secondly we provide essential security by using PERAODV that forwards the packet in a multi path manner, which provides security against the sniffing attacks on the network. So, by integrating both the hybrid system and the PERAODV [4], high throughput with security is achieved.

In this paper we will explain, some of the attacks is solved by our proposed PERAODV. The respite of the paper is organized as follows: Section 2 delivers models and assumptions; Section 3 Overview of proposed model; Simulations and experimental Results are given in section 4. Section 5 we explore related work on different attacks and Section 7 draws up conclusions [5].

Models and Assumptions: In this part, we articulate the wireless mobile ad hoc network model and security model and then designate the security attacks [6, 7].

Network Model: We study a wireless mobile ad hoc network involving of an unconstrained number of networking nodes. For differentiation drive, we need each node to have a distinctive non-zero ID [2]. Conventions made in the design of PERAODV system are as follows:

- A wireless mobile ad hoc network where nodes are allowed to move about or endure at stand still, at their will is presumed. Each node may seam to the network, or node may leave from the network at any time.
- The source and the destination node are not cruel.
- Nodes may fail by any time.
- Each node in the network have neighbors list.
- There exists a bi-directional communication link between any couple of nodes, which is a requirement for most wireless MAC layer protocols including IEEE 802.11 intended for unfailing transmission.
- Wireless interfaces support loose mode of operation. Most of the existing IEEE 802.11 constructed wireless cards support such promiscuous mode of operations, to expand routing protocol performance.

The promiscuous mode may also find additional communication overhead and energy utilization in order to process the transit packets. We do not address the energy efficiency in this work [1-2].

Security Model: Mobile Ad hoc Networks are vulnerable to security attacks due to its features of shared radio channel, insecure open medium, dynamic changing topology, lack of cooperative algorithms, lack of centralized monitoring, limited resource availability and physical vulnerability. Attacks on MANET can be classified into two categories, namely, passive attacks and active attacks. A passive attack does not disrupt the operation of the network. The passive attackers are less vulnerable to the network security. We do not address passive attackers who eavesdrop and record the wireless transmissions [1]. An active attack attempts to destroy or alter the data packets and routing messages being exchanged in the network. The active attackers are more vulnerability to security attacks. In this paper we address only active attackers.

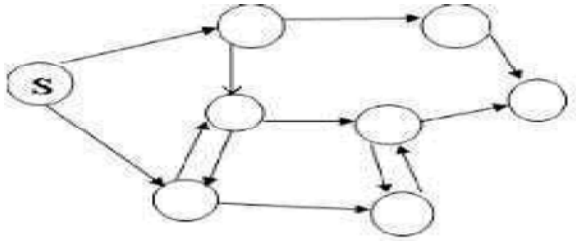

Fig. 2: RREQ Broadcast

Proposed System: The proposed system explains how the node creates, route request and route reply and route error message.

Peraodv Route Discovery: When the source node initiate the communication with the destination then route discovery is generated and if path is not available to destination, then source floods or broadcasts RREQ as shown in the Fig 1. *i.e.* request packet to all its neighbors in the network [3]. This RREQ message contains source and destination node's IP address, sequence number of destination, its current sequence number, hop count and RREQ ID. RREQ ID is regularly increasing number. It gets incremented after each node initiates RREQ. Fig. 2 illustrates this flooding procedure [8].

When intermediate node receives RREQ, they create reverse link to previous node. They first of all check whether, valid route to destination is present or not. If, valid route is present then another condition must hold. i.e intermediate node's sequence number must be greater than the destination sequence number in RREQ packet. If both conditions hold, then that node generates RREP *i.e.* reply packet. If valid route is not present then RREQ is further forwarded [4]. As RREQ is forwarded, hop count is incremented. While sending RREQ, intermediate nodes start a timer. If reply doesn't come within that time means, there is no more active route or link failure has occurred. RREP has source and destination IP address as well as destination sequence number. When the node generates the forward route entry, the RREP is forwarded to the destination node. Now the source node gets the RREP through various hops and it uses the path for transmission of packets [5].

Algorithm I: Route Discovery Process

```
When the src node S need a route to a dst node D
Begin
Construct PQR set for all mobile Adhoc hosts
* PQR – congestion free PQR –set nodes *
For each node pair (I, J) i. where i=1 to (N-1)
/*Z= 6, 7,8.. . N*/
X = 2; Router = Null;

/* Src: source node; Dst: destination node; Route: output
path set created for node pair (S, D), set to be Null */

If (Dst is in two hop list of PQ) Then
    Path generated for pair (PQ, RS)
    Set Routei =TRUE
    X= 6

Else
    PQR=PQ;

Call Procedure PATH (input:PQR, Di; output: Routei)
End

Procedure PATH (input:PQR, Di; output: Routei)
Begin

If (EFG is in PQR) Then
    Path generated for pair (PQ, RS)
    Set Routei = TRUE
    Increment X by 2
    Return

Else If (PQR-SET is not in Routei) and (PQR-SET's two-
hop list does not hold Di) Then

/* X: number of X */
Begin
    Increment X by 1
    Add PQR-SET to Router

For each neighboring node Neib of node PQR-SET Do
/* Neib: the neighbor PQR-set node of PQR-set */
    PATH (Neib,RS, Router)
End
End
```

Peraodv Route Maintenance: As MANET is dynamic *i.e.* mobility and topology of nodes always change, link break occurs. When path breaks, both the nodes inform their end nodes about link failure, who were using that path by sending RERR *i.e.* error message as illustrated in Fig. 2. End nodes delete their entries from route table, as path is no longer useful. RREQ broadcasting or path finding or repair broken link is again reinitialized by source node, if it still needs communication with the destination node.

Algorithm II: Route Maintenance Process

```
Begin

//initilize

Avgerage_new=2
Avgerage_old=3;
Instance_queue= 4
MinVal= 1.25 * Queue_Count
Marvel=6*Manvel
Queue_utilizationization[] ={1.27,1.324,2.7}
Xy=1.270;
v_line=Queue_Count / 2

//For every arriving packet in the queue

Instance_queue++

//Calculate average queue count

If the queue is not empty then
Avgerage_new= (1-Xy) Avgerage_old+ Instance_queue * Xy
If (Avgerage_new<MinVal and and Instance_queue<v_line) then

Queue_stat= ‘‘Secure’’;

Else if (Avgerage_new> MinVal and and Avgerage_new< MaxVal) then


Queue_stat= ’’True’’;

// Initiate Alternate Route Discovery Process

If (Instance_queue> MaxVal and and alter_path= FALSE) then

MaxVal=Queue_utilization[i++]*buff_count;

Else
    Queue_status= ‘‘False’’;
    Avgerage_old=Avg;
    Xy =Xy*S*T
End
End

For each desertion packet in the queue
Instance_queue
```

Implementation of Peraodv Algorithm: Performance Enhanced RAODV is our proposed protocol, which extends the Reverse AODV protocol implementation step are given below. In this protocol the selfish node interrupt the network activity by entering in to radio transmission range and also affect the performance of the whole network. Therefore, data security places a major role in Mobile Ad hoc networks [6]. PERAODV provides a path hopping method based on reverse AODV (R-AODV). In reverse ADOV, the source node generates the multiple paths to destination as well as all available paths.

By hopping these paths can prevent data from the intrusion of interrupting nodes. For this we introduce a multipath routing mechanism to simulate module NS-2 (Network Simulator 2). Also it integrates the Hybrid Reputation System, which identifies and thereby avoids the non-cooperative and malicious nodes in the network.

Begin

Step 1: Initialize source and destination.
Step 2: Find neighbors of source node.
Step 3: Select the node which has the maximum reputation value.
Step 4: Find the Reputation value using the formula Reputation value = Last five reputations / 5;
Step 5: Compare that value with the threshold value as Reputation value >= threshold value.
Step 6: If that returns true, declare that node as co-operative and send RREQ request to that neighbor.
Step 7: Otherwise, do declare that node as non-cooperative and repeat steps 2-7 until the request is reached at the destination.
Step 8: Reply via same path on which request is reached.

End

Simulations: The existing RAODV is compared with the proposed PERAODV using Network Simulator 2 (NS2). The topology we have used is shown. Considered 2 Mbps of bandwidth and actually for every nodes transmission range varies randomly. At first communication takes place between two nodes namely node S and node D [1-2]. A new communication has been set up so that using the HRS and Multipath routing systems can connect node 0 and node 29. The results are shown in figure 3(b). At first the node chooses single path routing without having any cooperation incentive strategy, when RAODV original routing protocol is used.

Table 1: Parameters setting

Simulation time	300 Seconds
Number of nodes	30
Topology area	1000 x 1000 m
Mobility Model	Random way point
Traffic type	CBR (UDP)
Maximum Speed	1 0 - 20 m/s
Payload size	512 bytes
Propagation	Two Ray Ground
Channel type	Wireless channel

In comparison with PERAODV, different results have been received.

Network Simulator 2 (NS2) is used to evaluate the performance of PERAODV. To compare PERAODV with prior work in routing RAODV, this uses flooding. CBR traffic flows were selected, originating from randomly selected sending nodes.

Each CBR flow uses 512-byte packets [2]. The following aspects of PERAODV are emphasized:

- Increased Throughput
- Increased Security
- Low latency/delay

Simulation Parameters: Before the simulation we randomly selected a 20 % of the network population as generic malicious performance nodes [1]. For each flow did not change its source and destination for the lifetime of a simulation run. We ensured the simulation time as 300s, so as to allow us to equate our results with that of PERAODV. Simulation parameters are given in Table 1.

Network Topology: Network topology defines how the node of network is connected with each other. The topology is defined by physical and logical topology. Physical topology defines physically connected nodes on network and logical topology defines connection establishment between selected source and destination pairs. A collision occurred when two nodes send the packet simultaneously. Bad connection in the cable also brings down the entire network [2].

In the following Fig. 3, we have shown the network topology we used, while consider to design the PERAODV routing protocol. It shows a Mobile Ad Hoc Network, which consist total of 30 nodes and they communicate each other over wireless channel using two ray ground propagation channels with 20 m/s maximum speed of transmission.

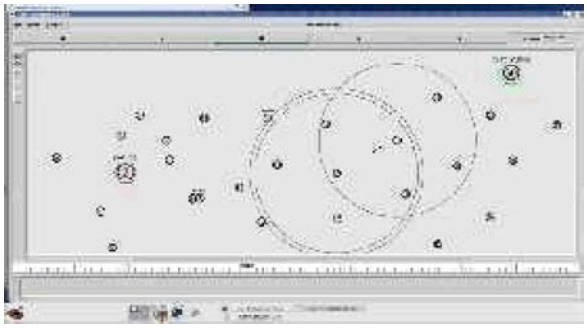

Fig. 3: Network Topology

Through put: In the world of MANET, packet delivery ratio has been accepted by way of a standard measure of throughput. Packet delivery ratio is nobody but a ratio between the numbers of packets received by the destinations to the number of packets showed by the sources [2]. The following conclusion we have got from the results (Fig. 3).

- In general packet delivery ratio falls as mobility and percentage of malicious nodes increase.
- As compared to RAODV and PERAODV, generic PERAODV results are superior.

Communication Overhead: Communication overhead can be estimated based on the number of communications of control messages like RREQ, RREP and RERR in the case of PERAODV [2] and in addition M_ERROR, M-Flag. As compared to plain RAODV and PERAODV, PERAODV results incur additional control packets.

Performance Analysis: Performance analysis deals with the comparison of the results over RAODV and ERAODV protocols using x-graph tool with the parameters, throughput and delay. The analysis result is found by comparing the trace files generated by the protocol in discussion. Trace graph is a tool, which is used to extract the values needed to perform a comparative analysis of the parameters considered throughput and delay. The result generated by the trace graph is given in Figure 3 to the x-graph tool of NS2 to plot the comparative graph.

Packets Delivery Ratio: The ratio of the data packets delivered to the destinations to those generated by the CBR sources; also, a related metric, received throughput (in kilobits per second) at the destination has been evaluated in some cases. The number of packets originated by the source at application layer to number of packets received by the destination node, which also known as the packet delivery ratio or throughput.

Table 2: Throughputs for RAODV and PERAODV.

	Throughput	
Mobility (m/s)	RAODV	PERAODV
0	74.92	76.83
5	72.32	74.45
10	70.52	72.69
15	66.85	68.88
20	62.78	64.98

Table 3: Communication overhead for RAODV and PERAODV.

	Communication overhead	
Mobility (m/s)	RAODV	PERAODV
0	19234	19125
5	19366	19436
10	20345	20234
15	20553	20433
20	20984	20584

Following Table 2 shows that the delivery ratio in which result is shown between packet ratio and mobility.

Communication Overhead: Communication overhead is the number of control packets generated by each routing protocol.

Analysis of Results: We find that PERAODV yields much higher packet delivery ratio compared to RAODV in the presence of 30% selfish nodes in Table 2. It is found that with PERAODV throughput is a 3.38 % increased in 20 m/s mobility. As Compared with RAODV and PERAODV, our proposed PERAODV have less communication overhead. We find that our proposed PERAODV yield much higher output as compared to all other system.

Related Work: The Key Distribution Center (KDC) architecture is the main stream in wired network because KDC has so many merits: efficient key management, including key generation, storage and distribution and updating. The lack of Trusted Third Party (TTPs) key management scheme is a big problem in ad hoc network [1-2].

Sudha Rani *et al.* [3] expose a finding and prevention of wormhole attack in stateless multicasting. Their scheme has no central administrator. They have exposed that their schemes can wormhole attacks.

Leonidas Georgiadia *et al.* [4] make a review of threats and possible solutions for resource allocation and cross layer control in wireless networks. Raj *et al*. [5] intend a solution for black hole attacks. It was employed in projecting AODV protocol based MANET. Tsou [6], developing a novel scheme BDSR to Avoid Black Hole Attack Based on Proactive and Reactive Architecture.

All the upstairs schemes only try to keep the system from the attacker, but not difficulty about quarantining attackers. The ETUS systems [1-2] not only detect the mischievous nodes but also prevent their further participation in the network.

CONCLUSION

A mobile Ad-hoc network provides the mobility of nodes, which is so helpful in any emergency situations. However, if security accidents and packet loss occurs, ruinous economic damages are inevitable. Our proposed work has been design a new hybrid reputation system that focuses on detection on malicious node and avoids them to increase the Qos parameters. Proposed method provides how we decrease the traffic and rate of vulnerability in the system using PERAODV protocol. Implementing the same concept in wireless sensor networks which may be helpful in real-time.

In future we propose to improve the Hybrid Reputation System for achieving null packet loss and simultaneous multi path packet forwarding may be done to reduce the transmission time. Cryptographic systems can also be included to encrypt the packets that we sent during transmission for security. Considering the energy resources of each node will do packet forwarding, so that energy efficient transmission can be achieved.

REFERENCES

1. Kathirvel, Ayyaswamy and Rengaramanujam Srinivasan, 2011. ETUS: Enhanced Triple Umpiring System for Security and Robustness of Wireless Mobile Ad Hoc Networks. International Journal of Communication Networks and Distributed Systems, 7(1/2): 153-187.
2. Kathirvel Ayyaswamy and Rengaramanujam Srinivasan, 2011. ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc Networks. International Journal of Network Management, 21(5): 341-359.
3. Georgiadia, Leonidas, Michael J. Neely and Leandros Tassiulas, 2006. Resource Allocation and Cross-Layer control in Wireless Networks. Foundations and Trends in Networking, 1(1): 1-444.

4. Raj, P.N and P.B Swadas, 2009. DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science, 2: 54-59.
5. Tsou, P.C., J.M. Chang, Y.H. Lin, H.C. Chao and J.L. Chen, 2011. Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Proc. of 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea.
6. Li Ze and Haiying Shen, 2012. Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, 11(8): 1287-1303.
7. Lochert, C., B. Scheuermann and M. Mauve, 2007. A survey on congestion control for mobile ad-hoc networks. Wiley Wireless Communications and Mobile Computing, 7(5): 655-676.
8. Perkins, C.E., E.M. Belding-Royer and I. Chakeres, 2003. Ad hoc on demand distance vector (AODV) routing. IETF Internet Draft.