www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1991-1997

IMPLEMENTATION OF REPUTATION INDEX PROTOCOL (RIP) FOR SECURE COMMUNICATION IN MANET

Kirti Patil[1,] Atish Mishra[2], and Praveen Bhanodia[3]
[1]Research Scholar of Computer Science dept. PCST, Indore (M.P.)
patilkirti52@gmail.com
[2]Faculty of Computer Science dept. PCST, Indore (M.P.)
atish_mishra2404@yahoo.co.in
[3]HOD of Computer Science dept. PCST, Indore (M.P.)
pcst.praveen@gmail.com

ABSTRACT

In an ad hoc network, the transmission range of nodes is limited; hence nodes mutually cooperate with its neighboring nodes in order to extend the overall communication. However, along with the combination of nodes, there may be some reluctant nodes like selfish nodes and malicious nodes present in the environment. These types of nodes degrade the performance of the network. This paper, gives a solution using reputation based mechanism and credit based mechanism. Moreover it includes different strategies by which non cooperative nodes are detect, isolated and/or prevented their advantages and limitations. Also, a global reputation based scheme is proposed in this paper for the detection and isolation of malicious nodes. A cluster head is used which is responsible for reputation management of each node in the environment. Detection of selfish nodes is accomplished which are created due to nodes conserving their energy using NS2. After their detection, performance analysis of network with selfish node and the network after isolation of selfish node is carried out.

Keywords: Manet, ns2, RIP, tcp, wireless, AODV.

I Introduction: A Mobile ad-hoc network is a set of self-directed nodes that communicate with each other in dynamic topology environment. There is no centralized management for the nodes. In order for a node to communicate to other node that is out of its radio range, [4] then the cooperation of intermediate nodes is most important in the network. This type of communication is called multi hop communication [1]. MANET provides anytime and anywhere services to user for collaboration among nodes. The main concentration is on packet forwarding because some nodes only cooperate for their own communication, such nodes known as selfish nodes. A selfish node damage or interrupt the network. Our goal is to construct a victorious atmosphere. The next section entails a discussion of some related efforts which is followed by RIP system design in section III. Section IV describes protocol and simulation results. In the last Section V concludes and direction for future work.

II Literature survey:

2.1 Isolating selfish nodes by Reputation based mechanism M. Refaei [2] introduces a reputation mechanism for building trust among nodes. Here, a distributed Tamer reputation evaluation scheme is implemented by neighboring nodes based on completion of the requested services. For each successful delivery of packets, node increases the reputation index of its next neighbor that forwarded the packet and packet delivery failures result in penalty applied to such node by decreasing their reputation index. There is no need of exchanging of reputation information among nodes, Thus involves less overhead.

2.2 CORE Pietro Michiardi and Refik Molva et al [3] schematized a Collaborative Reputation mechanism which is use to calculate reputation value of node to make decision about isolated and cooperative nodes. Core uses a watchdog component for monitoring nodes reputation with the help of past behavior. It awarded nodes for their good behavior and punish for their bad behavior.

2.3 Reputation based system for encouraging the cooperation of nodes. Tiranuch Anantvalee and Jie Wu[5] proposed a new category of a node known as Suspicious node beside between cooperative and selfish node. In this paper, they describe a state model for deciding what to do with node in each state and state is controlled by timing period.

2.4 Reputation based dynamic source routing protocol Sangheetaa Sukumran[7] present a reputation mechanism using watchdog monitoring for construction of trustable network. In this packet route determine by reputation value. Nodes can maintain high reputation value only by successful packet delivery. If a node reputation is lower than threshold value than nodes are put in the gray list and if a node reputation is decrease continuously than node puts into black list and denote as a selfish node. But this protocol does not deal with selfish nodes.

III RIP Protocol:

3.1 Description: Reputation Index Protocol proposes a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a secure route. According to RIP solution the requesting node does not send the DATA packets to the reply node without further ado, it has to wait till other replies with next hop details from the other neighboring nodes. Later than receiving the first request it sets timer in the 'Timer ExpiredTable', for gathering the further requests from different nodes that having equal hop count. Each replying node will store the 'sequence number', and the time at which the packet reached. The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. According to reputation Based AODV the requesting node transmit request to the node having hop count 2, then calculate the ratio of their total reply and time taken by all reply and generate reputation value flanked by 0 to 10, for those neighboring nodes who reply for the request will have reputation value greater than 5, the neighboring node that are reply for some of the request will have reply ratio less than those neighbor who are good to reply, and these neighbor have reputation value less than 5, based on these reputation values we find neighbors who have reputation value minimum and remove its entry from the routing table, and based on reputation values a safe route to the destination to reduce the probability of Black Hole Attack is generated. After the reputation value calculation, it first checks in Routing Table whether there is any entry for the node and its reputation value for hop node. If any entry to next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited.

3.2 Operation: In the above figure 3, S wants to communicate with D. So it first sends the route request to all the neighboring nodes. Here node 1, node M and node 2 receive request from S. The malicious node M has no intention to send out the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node. So it immediately replies to the request as (M – 4). Instead of send out the DATA packets immediately through M, S has to wait till the reply does not come from the other nodes. After receiving all reply from neighbor node 1 as (1 – 3), and node 2 as (2 – 3). According to this RIP solution [8] it first checks the path in the routing table that contains reputation value acceptable for next hop node to the destination. If there is a path node having trust than select that path and send the data through the trusted path.

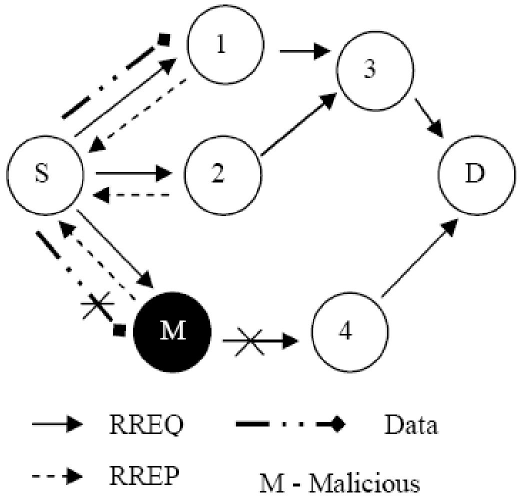

Figure 1. Operation of RIP Protocol

3.3 Design Consideration

S. NO.	Parameter	Value
1	No of Simulating Nodes	30
2	Area size of topography x(m)	800
3	Area size of topography y(m)	600
4	Routing protocol	AODV
5	Simulation Time	100 second
6	Traffic Type	CBR/FTP
7	Data Type	TCP/UDP
8	Packet Size	1500 Byte
9	Node Placement	Dynamic
10	Wireless Range	250 m

Table1

IV Evaluation of RIP Protocol:

4.1 Background: The evaluation of RIP performed upon network simulator ns2 for configuring mobile ad-hoc network with different simulator parameter which is defined in table 1.

4.2 Performance Matrix:

4.2.1 Packet Delivery Fraction: It is the ratio of data packets delivered from source to destination. It is evaluated by dividing the number of packet received by destination through the number packet originated from source.

PDF = (Prcv/Psent)*100

Where Prcv is total Packet received & Psent is the total Packet sent.

4.2.2 End to End Delay: This includes all possible delay caused by buffering for the duration of route discovery latency, queuing at the interface queue, retransmission delay at the MAC, propagation and transmission time. It is defined as the time taken by source for transferring a data packet to the destination through the MANET.

E2E = Trcv-Tsent

Where Trcv is receive Time and Tsent is sent Time.

4.2.3 Throughput: It is the average rate of successful message delivery over a communication channel.

V RIP Result and discussion:

To evaluate the performance of network we implemented RIP using NS2 simulator [9]. We integrate RIP as extension of AODV protocol. The results are comparing against the AODV protocol.

5.1 Here describe comparison on Packet Delivery Fraction of simple AODV network, Malicious AODV network, and RIP Network shows in figure 2 result shows that RIP protocol improves PDF percentage than others. Our protocol gain 97% with presence of Black hole attack in the network, while in AODV protocol without attack gives 89% and last is AODV in malicious network it gives 82%, this because of RIP send data packets only through the reputed node. Figure 3 present the no of drop packets in the network through communication among nodes.

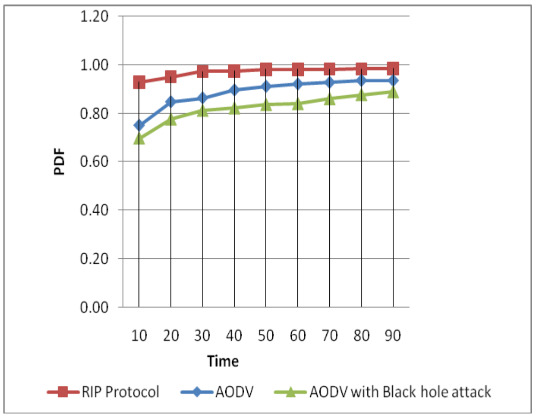

Figure2. Comparision on Packet Delivery Fraction of AODV, AODV with attack and RIP Protocol

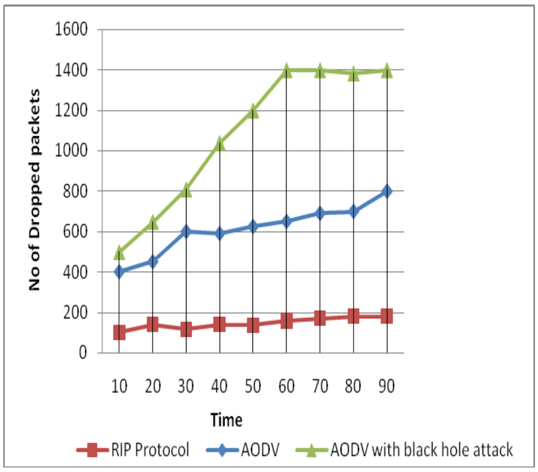

Figure3. Comparision on No of Drop packets vs time among AODV, AODV with attack, and RIP protocol

5.2 Figure 4 and 5 shows the end to end delay of sent packets. End to end delay of RIP protocol in figure 6. Here we can easily compare AODV with RIP, thus the RIP offer enhanced network efficiency than AODV.

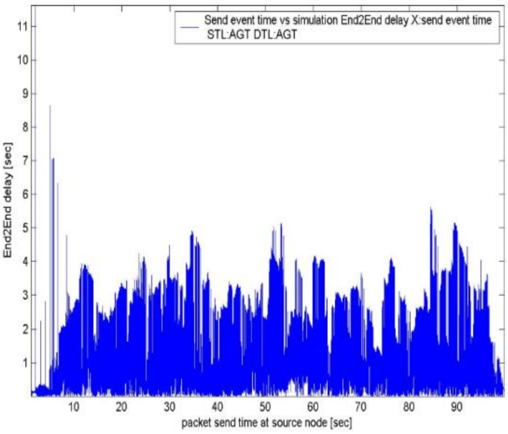

Figure 4. End to End delay of AODV protocol

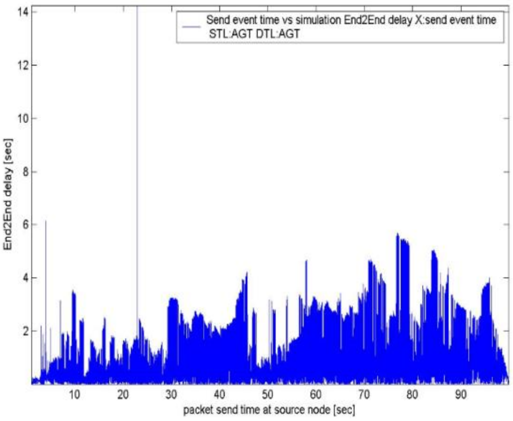

Figure5. End to End delay of AODV with wormhole attack

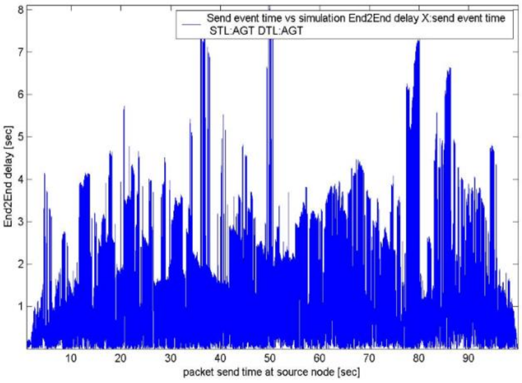

Figure6. End to End delay of RIP Protocol

5.3 Figure 7 gives you an idea about the throughput of sent, receive and drop packets in RIP Protocol and figure 8 and 9 also express the comparison with other protocol like AODV. Moreover it show that RIP protocol provide reliable communication and better throughput than AODV also in Malicious network.

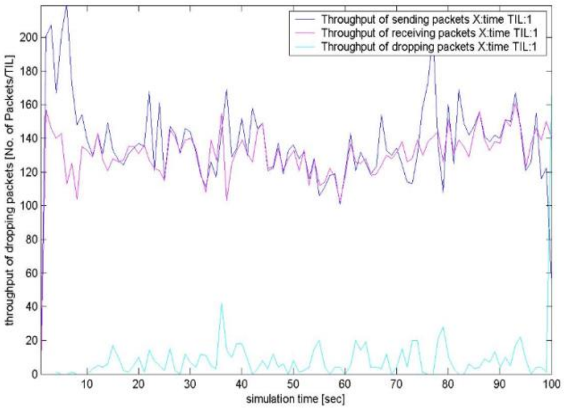

Figure7. Throughput of AODV protocol

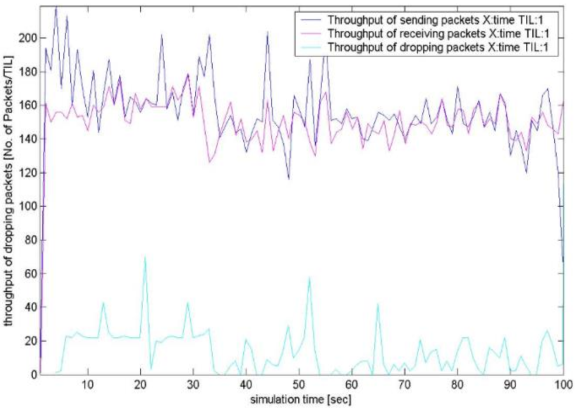

Figure8. Throughput of AODV with Wormhole attack

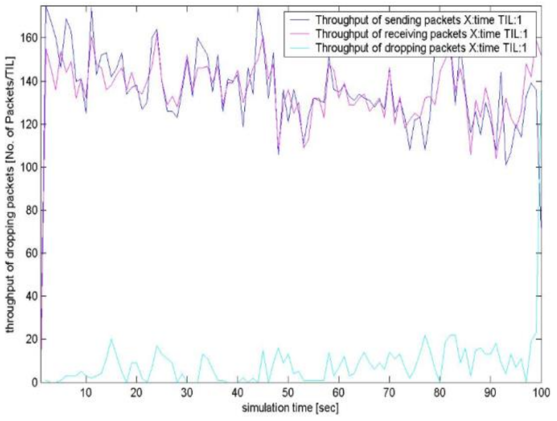

Figure9. Throughput of RIP protocol

VI Conclusion:

In this paper, we proposed an efficient and scalable routing protocol for MANET. This has been achieved by creating a new Reputation Index Protocol. To greatly increase the performance and security among mobile ad-hoc network we have proposed a trust based or reputation index mechanism for attack prevention with implementation. The performance of proposed scheme is better because as we can point out from results that Packet Delivery Fraction in case of Prevention is better than that of simple scenario and attacked scenario. Also if we consider throughput we can conclude that the overall throughput is of RIP is better than other two protocols.

VII Future Scope:

Our Future work will focus on studying the impact of centrality and configuration parameters on the protocol performance in relation to network throughput, network delay, network jitter and the protocol detection ratio. We will investigate the response of the reputation protocol under the same high-mobility conditions and subject to collaborative black hole and gray hole attacks.

References

[1] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, “Mobile ad hoc networking: imperatives and challenges” . Chlamtac et al. / Ad Hoc Networks 1 (2003) 13–64.
.

[2]. M. Tamer Refaei, Vivek Srivastava, Luiz De Silva, Mohamed Eltoweissy, "A Reputation based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks", Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05) , 2005

[3]. Pietro Michiardi and Refik Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia, 2002.

[4]. Buchegger, Sonja; Le Boudec, Jean-Yves, "Performance Analysis of CONFIDANT Protocol: Cooperation of Nodes - Fairness in Dynamic Ad-Hoc Networks," Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June 2002.

[5]. Tiranuch Anantvalee, Jie Wu: Reputation-Based System for Encouraging the Cooperation of Nodes in Mobile Ad Hoc Networks”, Proceedings of International conference of Communications, pp 3383-3388, 2007.

[6]. Fei Wang. Furong Wang, Benxiong Huang, Laurence T. Yang, ”COSR: a reputation-based secure route protocol in MANET “in Journal EURASIP Journal on Wireless Communications and Networking - Special issue on multimedia communications over next generation wireless networks archive Volume 2010, pp. 1-11, January 2010.

[7] Sangheetaa Sukumarn Venkatesh Jaganathan and Arun Korath,“Reputation based Dynamic Source

Routing Protocol for MANET", International *Journal of Computer Applications (0975 – 888) Volume 47– No.4, June 2012.*

[8] Kirti Patil and Praveen Bhanodia, "A Novel Paradigm: RIP (Reputation Index Protocol) For MANET" in International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 2, February- 2013 ISSN: 2278-0181

[9] Simulation Tools for Wireless Sensor Networks E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, P. Pavón-Mariño, J. García-Haro, Summer Simulation Multiconference - SPECTS 2005