International Journal of Mathematics and Computational Science
Vol. 1, No. 4, 2015, pp. 206-213
http://www.aiscience.org/journal/ijmcs

Kuder Richardson Reputation Coefficient Based Reputation Mechanism for Isolating Root Node Attack in MANETs

S. Parthiban[*], **Paul Rodrigues**

Faculty of Engineering, Department of Computer Science and Engineering, DMI College of Engineering, Affiliated to Anna University, Chennai, India

Abstract

In multi-hop networks like MANETs, the mobile nodes relies upon the intermediate nodes for routing the packets. But, the existence of root node attack in an ad hoc environment may degrade the network performance. Hence, the critical issues that could arise due to the existence of root node attack are considered as one of the important research issues to be solved. In this paper, we propose a Kuder – Richardson Reputation Co-efficient based Cooperation Enforcement Mechanism (KRRCM) for mitigating Root node attack based on Kuder – Richardson Reputation Co-efficient (KRRC) that quantifies the reputation level of mobile node. This Kuder – Richardson Reputation Co-efficient is calculated based on second hard reputation. The coefficient value obtained through KRRCM approach reflects an individual root node's behaviour in relation to cooperation, so that the particular node can be selected as core point for group communication. The performance analysis of KRRCM carried out based on ns-2 simulator and the proposed KRRCM approach outperforms the existing mechanisms by increasing the packet delivery ratio and throughput by 23% and 28%, while decreasing the control overhead and total overhead in an average by 18% and 29% respectively. Further, KRRCM ideally mitigates the root node attack at a faster rate of 32% than the considered benchmark mechanism considered for investigation.

Keywords

Root Node Attack, MAODV, Kuder – Richardson Reputation Co-efficient, Threshold Detection Point, Group Communication, Packet Drop Variance

Received: April 6, 2015 / Accepted: May 8, 2015 / Published online: June 8, 2015

1. Introduction

Mobile ad hoc network is a composition of active mobile nodes which communicate each other without relying on a centralized infrastructure. In this network, nodes are free to move in an arbitrary fashion and hence the topology of the network is highly dynamic in nature [1]. In the dynamic topology, the mobile nodes present in a particular range can communicate directly, whereas the nodes present outside the communication range make use of intermediate nodes to transfer a data packet to its destiny and this type of transmission may be called as multi-hop routing [2]. In this multi-hop routing, the probability of a node participating in a routing activity is highly dependent on the reputation factor of the node. The reputation factor of a mobile node reflects the reliability and cooperativity of the particular mobile node to participate in a routing activity. But, there are some classes of mobile nodes which do not actively participate in the routing activity and drops many packets without transmitting to the next intermediate or to the destiny node [3]. In general, such classes of nodes are known as malicious nodes, which by its activity drastically reduce the network performance.

Although, researchers have put forward large number of

[*] Corresponding author
Email address: parthi_ns@yahoo.com (S. Parthiban), drpaulprof@gmail.com (P. Rodrigues)

techniques, to detect and mitigate various types of malicious attacks in MANETs, most of the proposed approaches were mainly framed for unicast routing activity [4]. The influence of malicious attacks on the multicast application has not been explored in the literature. This paper focuses on detecting and mitigating malicious nodes in a multicast routing activity by making use of MAODV protocol. The MAODV protocol is a tree based protocol, in which the data dissemination from source group to destination group is done through the rendezvous point present in each multicast group. This meeting point may be called as root node, which is chosen from the group of mobile nodes according its reputation factor. Hence, in this paper, we propose a Kuder Richardson Reputation Coefficient Based Reputation Mechanism (KRRCM) for mitigating root node attack in MANETs. The proposed KRRCM approach manipulates Kuder Richardson Reputation Coefficient for each and every mobile node. The coefficient values obtained through KRRCM approach reflects the nodes behaviour, either cooperative or non-cooperative, according to which the particular node can be selected as rendezvous point for group communication.

2. Related Work

In the literature, researchers have proposed a variety of mitigation mechanism for detecting root node attack. Some of them are enumerated below:

In [5], a novel mitigation framework was proposed for integrating a routing protocol known as reactive multicast protocol that performs reliable data transmission by grouping nodes in the form of shared meshes. This framework mainly investigates reliable packet delivery in a shortest routing distance. A trust management framework has been proposed in [6] which enable the cooperation among the mobile nodes. In this, authors have incorporated a hardware module named as tamper resistant module to detect and mitigate malicious behaviour of the mobile node.

A novel mechanism [7] mitigates various types of attacks that are possible with multicast tree routing protocol. various issues related to route discovery and route establishment by designing new control messages such as RREP-INV, MACT (J) –MTF and RREP-INV, MACT (P) –PART. A collaborative mechanism [8] was investigated a based on Watch Dog, Path-rater and IDS which does the monitoring of reliable data transfer among the mobile nodes and also the key manipulation operations performed by each and every mobile node. These mechanisms provide reactive solution to predict the existence of any type of attack by determining the reputation factor of the mobile node.

Furthermore, a reliable mitigation mechanism was proposed in [9] that could provide a solution to the recovery of root node in case of shared tree network. Authors have implemented a bootstrap router which could able to perform efficient routing based on rendezvous point mechanism. A novel routing mechanism [10] based on the auction concept was proposed that selects the routing path according to the minimum cost calculated from the individual node bids. This mechanism also manipulates the payment that should be given for the winning routing path which is equivalent to that of the second smallest biding route.

In addition to this, A one-way hash function mechanism [11] was proposed to estimate the genuinenity factor of a mobile node. This hash function was computed based on both the information obtained from the mobile nodes and its neighbour nodes. This paper also investigates on fault tolerance and fault recovery technique for the network through explicit acknowledgement scheme.

Yet another, a novel trust based mitigation mechanism have been proposed in [12] which detects the malicious nodes based on Dempster-Shafer Theory. This mechanism manipulates a reputation factor for each and every mobile node based on second hand information using posterior probability.

3. Kuder – Richardson Reputation Co-efficient Based Cooperation Enforcement Mechanism (KRRCM)

KRRCM is presented for mitigating Root node attack in an ad hoc environment. In this mechanism, the detection of Root node attack is based upon a factor called Kuder – Richardson Reputation Co-efficient (KRRC), which aids in estimating the reputation level of each and every mobile node and enables effective and efficient mitigation of root node attack from the routing path established between the multicast groups.

Let us consider the number of packets received by a mobile node shall be $P_1, P_2, P_3, \dots, P_r$ and the number of packets forwarded by mobile node as $P_{1,}P_2, P_3, \dots, P_f$ for‘s’ sessions.

The number of packets dropped by a mobile node in any particular session says in session $'s'$, can be given in (1),

$$P_d = P_{r(s)} - P_{f(i)} \tag{1}$$

Then, the average packet drop in ‘s’ sessions is computed by (2),

$$P_{avg} = \sum_{i=1}^{k} \frac{P_{d(i)}}{s} \tag{2}$$

Based on the values of P_{avg} for 's' sessions and $P_{r(i)}$ the number of packets received by a mobile node in a session, the total variance in packet delivery of mobile node in each session is given in (3),

$$\sigma_{pd}{}^{2} = \sum_{i=1}^{s} \frac{(P_{r(i)} - P_{avg})}{s} \quad (3)$$

Based on (3), Kuder – Richardson Reputation Co-efficient is manipulated through (4),

$$KRRC = \frac{s}{s-1}\left[\frac{1-\sum_{i=1}^{s} P_d P_r}{\sigma_{pd}{}^{2}}\right] \quad (4)$$

Here, the values of KRRC is analyzed, if it is found to be less than 0.40 (as obtained through simulations) then the node is said to be malicious node affected by means of root node attack and isolated from the routing path. At the same time, if the value is equal to or greater than 0.40, then the mobile node is said to be cooperative node.

4. Algorithm for the Computation of Kuder – Richardson Reputation Co-efficient

Algorithm1: Computation_KRRC( )

Notations:

N - Number of mobile nodes in the network

s - Number of sessions

P_r- Number of packets received by a mobile node

P_f - Number of packets received by a mobile node

```
1. Begin
2. For each mobile node in the network, $j = 1\ to\ N\ do$
3. For each session of packet transmission, $i = 1\ to\ k\ do$
4. Find the packet dropped, $P_d = P_{r(ij)} - P_{f(ij)}$
5. Find the average drop rate as, $P_{avg} = \sum_{i=1}^{k} \frac{P_{d(i)}}{s}$
6. Total Variance in packet delivery as $\sigma_{pd}{}^{2} = \sum_{i=1}^{s} \frac{(P_{r(i)} - P_{avg})}{s}$
7. Compute the KRRC using $KRRC = \frac{s}{s-1}\left[\frac{1-\sum_{i=1}^{s} P_d P_r}{\sigma_{pd}{}^{2}}\right]$;
8. End for
9. For each mobile node in the network, $j = 1\ to\ N\ do$
10. If $|KRRC| < 0.4$, then
11. The mobile node $N_j$ is said to malicious node
12. Else $N_j$ is the cooperative node.
13. End if
14. End
```

In MAODV protocol, if the source needs to establish the route to the destination then it is carried by broadcasting RREQ packets through the forward route and determines an optimal route to the destination through RREP packets. When the source node sends the multicast packet to the destination nodes, the group leader of each multicast group may be compromised. This is estimated through the neighbor information obtained from each and every node .In the first step, the mechanism identifies the average drop rate. In the second step they calculate the total variance in packet delivery .In the third step KRRC is calculated by using Eq., (4). In the last step, If the KRRC value is below a threshold value of 0.4, then the root node is mitigated or else the normal routing of packets are done.

In this section, we present the Kuder Richardson based mechanism for isolating root node attack that comprises the rendezvous point of the multicast tree with the aid of AODV, in an ad hoc network. This is accomplished through the computation of the Kuder – Richardson Reputation Co-efficient (KRRC). In this mechanism , each and every mobile nodes are monitored through the help of their neighbor to detect whether they exhibit root node attack or not The node is identified as root node attack compromised when the KRRC value is below 0.3 or else the node(RN) is confirmed as co-operative as presented in Figure 1. Experimental analyses for evaluating the performance of RFBMM based on the different packet drop rate are as follows:

5. Simulations and Experimental Analysis

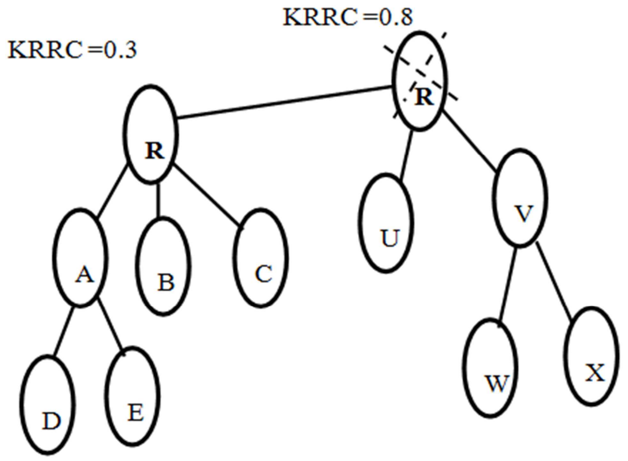

Figure 1. The multicast tree with a Root Node Attack.

The performance of KRRCM is thoroughly investigated through simulation using network simulator ns-2.26. The proposed simulation environment consists of 50 mobile nodes that randomly move in the terrain size of 1000x1000. Further, the channel capacity, refresh interval time and simulation time for the implemented algorithms is considered as 2 Mbps, 20 seconds and 150 seconds respectively. Furthermore, each source is considered to transmit packets with a constant bit rate of 30 packets/sec.

5.1. Performance Metrics

In group communication, the dissemination of data between the source and destination depends upon the group leader of the multicast tree. Further, the reliability in packet transfer gets affected when a node gets compromised through root node attacked. Furthermore, root node attack in an ad hoc scenario decreases the packet delivery ratio and throughput, while at the same instant increases the number of retransmissions. Finally, the performance of this mitigation algorithm is evaluated based on:

Packet Delivery Ratio: Packet delivery ratio is defined as the ratio of data packets received by the mobile node in the destinations to those generated by the sources.

Throughput: It is defined as the total number of packets delivered over the total simulation time.

Total Overhead: It is the ratio of total number of packets necessary for connection establishment and data delivery to the number of data packets that reaches the destination.

Control overhead: It is the maximum number of bytes of packets that are used for establishing communication between the source nodes and the destination nodes.

Table 1 illustrates the simulation parameters that are set for our study.

Table 1. Simulation Parameters.

Parameter	Value	Description
No.of mobile nodes	50	Simulation Node
Type of Protocol	MAODV	Multicast ad hoc On-demand Distance Vector Protocol
Type of Traffic	40 packets per Second	Constant bit rate
Type of Propagation	Two Ray Ground	Radio propagation model
Simulation Time	50m	Maximum simulation time.
Number of packets used	1000	Maximum number of packets used in simulation.
Channel capacity	2 Mbps	Capacity of the wireless channel

5.2. Performance Analysis for KRRCM

The performance of KRRCM is investigated through three experiments viz.,

a) Experiment 1: Based on varying number of mobile nodes with root node attackers as 10.

b) Experiment 2: Based on varying number of mobile nodes with root node attackers as 20.

c) Experiment 3: Based on varying number of root node attackers.

In all the three experiments, the network related parameters are considered to be the same for simulation.

5.2.1. Experiment 1: Based on Varying Number of Mobile Nodes with Root Node Attackers as 10

Figure. 2 demonstrates the superior performance of KRRCM compared to mechanisms like CONFIDANT, MAODV WITH ATTACK and MAODV WITHOUT ATTACK with regard to packet delivery ratio. Our proposed mechanism, KRRCM shows a phenomenal increase in packet delivery ratio when compared to MAODV WITH CONFIDANT from 10% to 17% and from 23% to 31% over MAODV WITH ATTACK. This increase in packet delivery ratio is due to the rapid isolation rate of 34% in mitigating root node attackers.

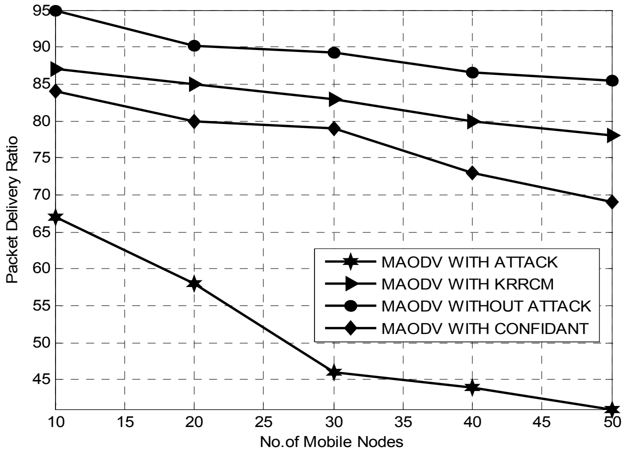

Figure 2. Experiment 1-Comparison Chart for KRRCM based on Packet Delivery Ratio.

Hence, it is evident that KRRCM effectively isolates root node attacker nodes that hinders reliable communication and increases the packet delivery rate in an average of 16%.

Figure. 3 demonstrates the superior performance of KRRCM compared to mechanisms like CONFIDANT, MAODV WITH ATTACK and MAODV WITHOUT ATTACK with respect to throughput. Our proposed mechanism, KRRCM shows a phenomenal increase in throughput when compared to MAODV WITH CONFIDANT from 10% to 19% and from 20% to 28% over MAODV WITH ATTACK. This increase in throughput is mainly due to the efficient and effective isolation of root node attackers that drops packets.

Hence, it is evident that KRRCM effectively isolates root node attacker nodes that hinders reliable communication and increases the throughput in an average of 12%.

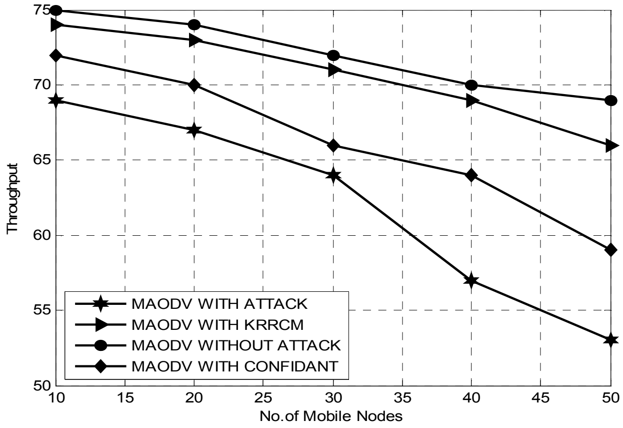

Figure 3. Experiment 1-Comparison Chart for KRRCM based on Throughput.

Figure. 4 presents the comparative analysis of KRRCM with CONFIDANT, MAODV WITH ATTACK and MAODV WITHOUT ATTACK with respect to total overhead. Our proposed mechanism, KRRCM shows an optimal decrease of total overhead than CONFIDANT from 21% to 29% and from 26% to 33% over MAODV WITHATTACK.

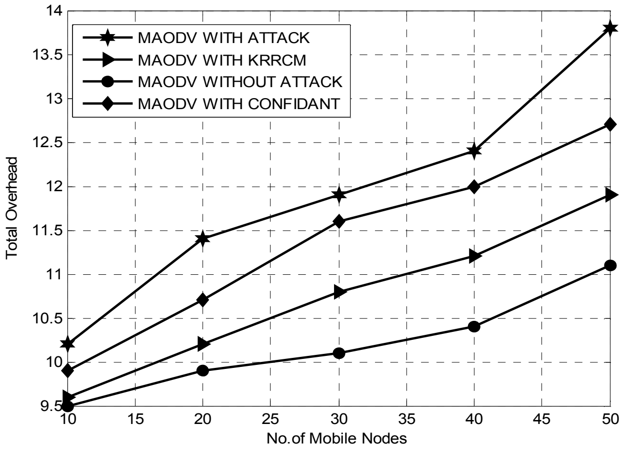

Figure 4. Experiment1-Comparison Chart for KRRCM based on Total Overhead.

Hence, it is obvious that KRRCM is an effective approach greatly reduces the number of retransmissions in an average of 21%.

Figure. 5 presents performance of KRRCM with CONFIDANT, MAODV WITH ATTACK and MAODV WITHOUT ATTACK based on control overhead. The proposed KRRCM shows a phenomenal decrease of control overhead than CONFIDANT from 13% to 23% and from 16% to 27% over MAODV WITHATTACK.

Hence, it is obvious that KRRCM is an effective approach for mitigating the root node attack by reducing control overhead by an average of 14%.

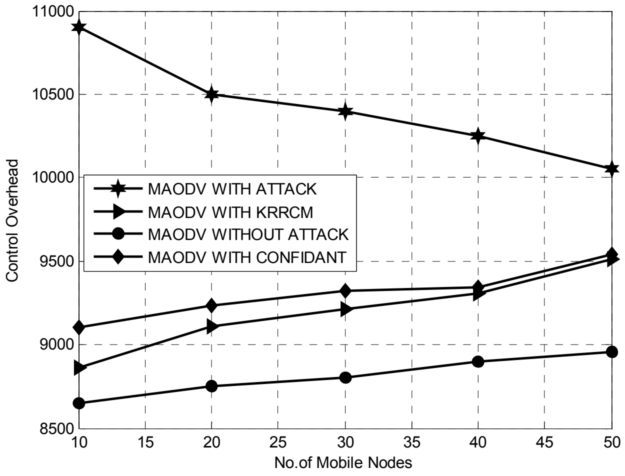

Figure 5. Experiment 1- Comparison Chart for KRRCM based on Control Overhead.

5.2.2. Experiment 1: Based on Varying Number of Mobile Nodes with Root Node Attackers as 20

Figure. 6 demonstrates the superior performance of KRRCM compared to mechanisms like CONFIDANT, MAODV WITH ATTACK and MAODV WITHOUT ATTACK with regard to packet delivery ratio. Our proposed mechanism, KRRCM shows a phenomenal increase in packet delivery ratio when compared to MAODV WITH CONFIDANT from 15% to 21% and from 25% to 29% over MAODV WITH ATTACK. This increase in packet delivery ratio is due to the rapid isolation rate of 34% in mitigating root node attackers.

Hence, it is evident that KRRCM effectively isolates root node attacker nodes that hinders reliable communication and increases the packet delivery rate in an average of 14%.

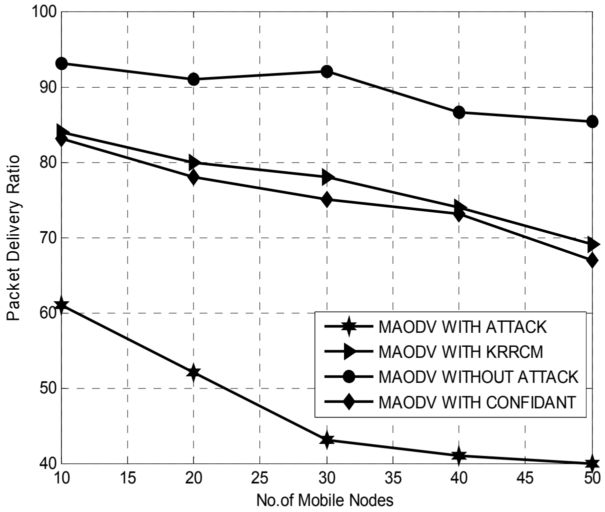

Figure 6. Experiment 2-Comparison Chart for KRRCM based on Packet Delivery Ratio.

Figure. 7 demonstrates the superior performance of KRRCM compared to mechanisms like CONFIDANT, MAODV

WITH ATTACK and MAODV WITHOUT ATTACK with respect to throughput. Our proposed mechanism, KRRCM shows a phenomenal increase in throughput when compared to MAODV WITH CONFIDANT from 12% to 17% and from 17% to 23% over MAODV WITH ATTACK. This increase in throughput is mainly due to the efficient and effective isolation of root node attackers that drops packets.

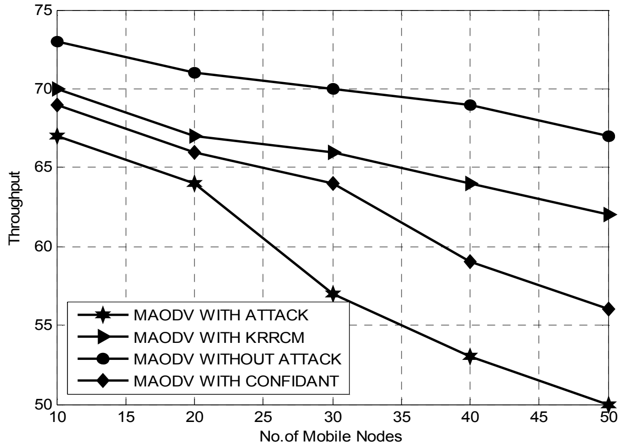

Figure 7. Experiment 2-Comparison Chart for KRRCM based on Throughput.

Hence, it is evident that KRRCM effectively isolates root node attacker nodes that hinders reliable communication and increases the throughput in an average of 10%.

Figure. 8 presents the comparative analysis of KRRCM with CONFIDANT,MAODV WITH ATTACK and MAODV WITHOUT ATTACK with respect to total overhead. Our proposed mechanism, KRRCM shows an optimal decrease of total overhead than CONFIDANT from 16% to 24% and from 23% to 29% over MAODV WITH ATTACK.

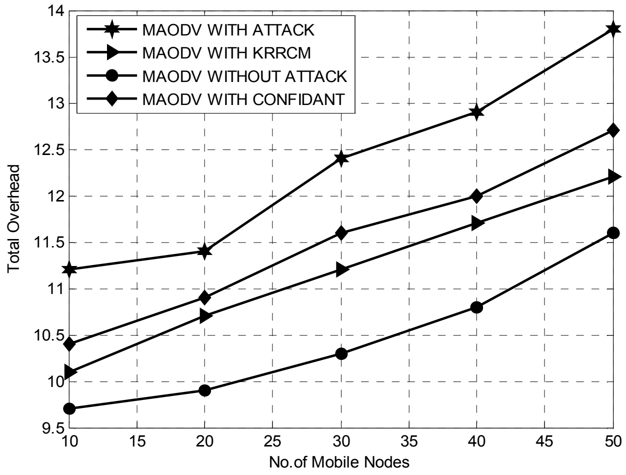

Figure 8. Experiment 2-Comparison Chart for KRRCM based on Total Overhead.

Hence, it is obvious that KRRCM is an effective approach greatly reduces the number of retransmissions in an average of 18%.

Figure. 9 presents performance of KRRCM with CONFIDANT, MAODV WITH ATTACK and MAODV WITHOUT ATTACK based on control overhead. The proposed KRRCM shows a phenomenal decrease of control overhead than CONFIDANT from 11% to 20% and from 18% to 25% over MAODV WITHATTACK.

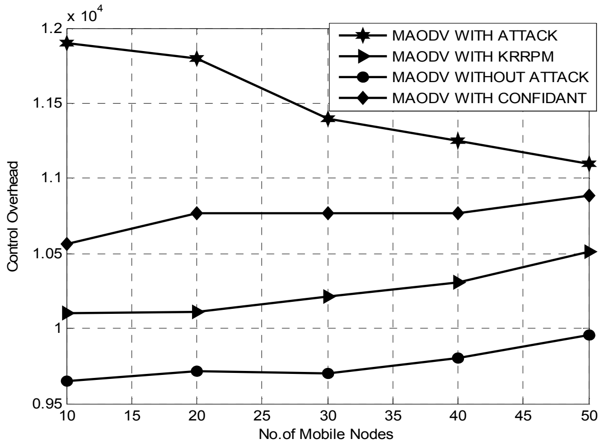

Figure 9. Experiment 2- Comparison Chart for KRRCM based on Control Overhead.

Hence, it is obvious that KRRCM is an effective approach for mitigating the root node attack by reducing control overhead by an average of 12%.

5.2.3. Experiment 3: Based on Varying Number of Root Node Attackers

Figure. 10 demonstrate the superior performance of KRRCM compared to the mechanism CONFIDANT with regard to packet delivery ratio. Our proposed mechanism, KRRCM shows a phenomenal increase in packet delivery ratio when compared to CONFIDANT from 14% to 19%.

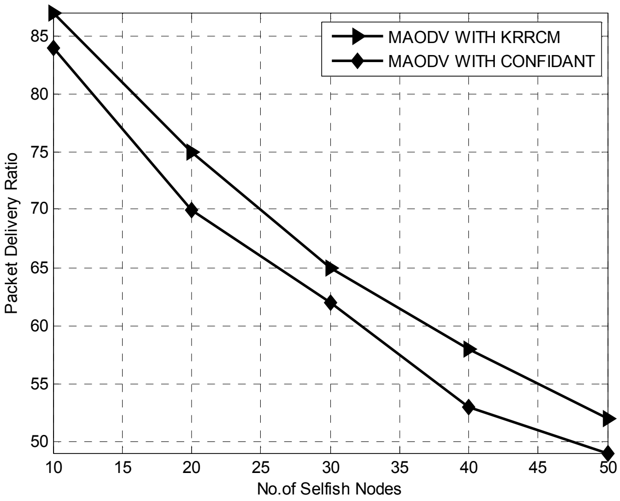

Figure 10. Experiment 3-Comparison Chart for KRRCM based on Packet Delivery Ratio.

Hence, it is evident that KRRCM effectively isolates root node attacker nodes that hinders reliable communication and increases the packet delivery rate in an average of 13%.

Figure. 11 demonstrates the superior performance of KRRCM compared to the mechanism CONFIDANT with respect to throughput. Our proposed mechanism, KRRCM shows a phenomenal increase in throughput when compared to CONFIDANT from 16% to 22%.This increase in throughput is mainly due to the efficient and effective isolation of root node attackers that drops packets.

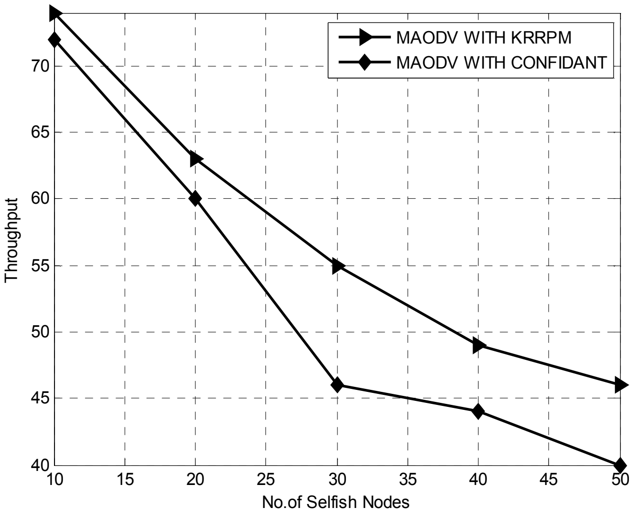

Figure 11. Experiment 3-Comparison Chart for KRRCM based on Throughput.

Hence, it is evident that KRRCM effectively isolates root node attacker nodes that hinders reliable communication and increases the throughput in an average of 17%.

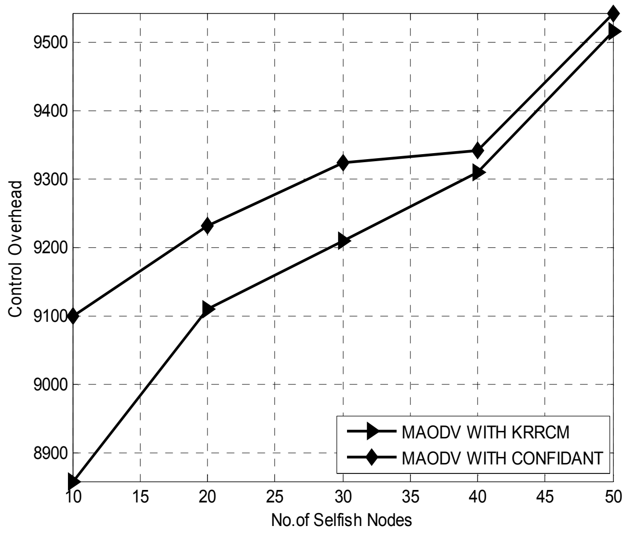

Figure 12. Experiment 3-Comparison Chart for KRRCM based on Total Overhead.

Figure.12 presents the comparative analysis of KRRCM with CONFIDANT with respect to total overhead. Our proposed mechanism, KRRCM shows an optimal decrease of total overhead than CONFIDANT from 26% to 33%.

Hence, it is obvious that KRRCM is an effective approach greatly reduces the number of retransmissions in an average of 16%.

Figure. 13 presents performance of KRRCM with CONFIDANT, based on control overhead. The proposed KRRCM shows a phenomenal decrease of control overhead than CONFIDANT from 6% to 27% over MAODV WITHATTACK.

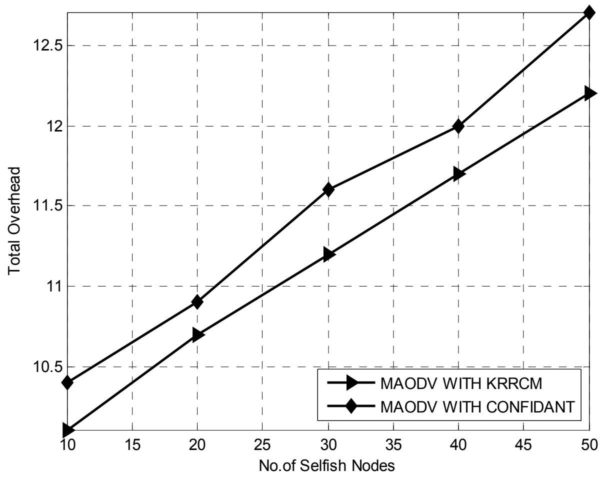

Figure 13. Experiment 3- Comparison Chart for KRRCM based on Control Overhead.

Hence, it is obvious that KRRCM is an effective approach for mitigating the root node attack by reducing control overhead by an average of 19%.

6. Conclusion

This paper has presented a Kuder – Richardson Reputation Co-efficient based Cooperation Enforcement Mechanism (KRRCM) for isolating Root node attack through the identification of the reputation level of mobile node based on Kuder Richardson Reputation Coefficient. The simulation results of KRRCM isolates root node attackers with a successful rate of 34% and further improves the performance of the network with respect tot Packet delivery ratio, Throughput, Control overhead and Total overhead than the existing CONFIDANT mechanism. As the part of our future work, there is a innovative plan to elect a group leader based on average length metric for choose the core leader.

References

[1] Rizvi, S and Elleithy, M, (2009) ‘A new scheme for minimizing malicious behavior of mobile nodes in Mobile Ad Hoc Networks’, IJCSIS Internation Journal of computer Science and Information Security. Vol.3, No.1, pp. 45-54.

[2] Fahad Tarag, Askwith Robert, (2006), A node misbehaviour detection mechanism for mobile ad hoc networks. In: Proc, seventh annual post graduate symposium on the convergence of telecommunications, networking and broadcasting (PGNet), Vol. 1, No. 1; pp. 78–84.

[3] Zouridaki,C, Mark,B.L, Hejmo,M and Thomas,R.K (2005). ‘A quantitative trust establishment framework for reliable data packet delivery in MANETs’, Proceedings of the 3rd ACM Workshop on security of ad hoc and sensor networks, vol 1, pp.1-10.

[4] Roy, S, Addada, V.G, Setia, S and Jajodia, S (2005), Securing MAODV: Attacks and countermeasures, in Proceedings of. SECON’05, IEEE, Vol. 1, No. 1, pp. 521-532.

[5] Subir Kumar Das, B.S. Manoj, and C. Siva Ram Murthy, (2002), Dynamic Core-Based Multicast Routing Protocol for Ad Hoc Wireless Networks. In Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, Vol. 1, No. 1, pp 33-46.

[6] Buttyan, L and Hubaux, J-P (2003), Stimulating Coperation in Self –organizing Mobile Ad hoc Networks”, Mobile Computing and Networking, Vol.1, No.1, pp 255-265.

[7] Sengathir, J Manoharan, R A Split Half Reliability Coefficient based Mathematical Model for Mitigating Selfish Nodes in MANETs, in Proc., 3rd IEEE International Advance Computing Conference (IACC-2013), Ghaziabad, India, Feb 22-23, 2013, IEEE pp.267-272.

[8] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, (2006) A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks. WIRELESS/MOBILE, NETWORK SECURITY Springer, Vol. 1, No. 1, pp. 1-38.

[9] Chi-Yuan Chang, Yun-Sheng Yen. Chang-Wei Hsiesh Han-Chieh Chao, (1998) an Efficient Rendezvous Point Recovery Mechanism in Multicasting Network, International Conference on Communications and Mobile Computing, Vol. 1, No.2, pp.187-196.

[10] Demir, C and Comaniciu C, (2007), An Auction based AODV Protocol for Mobile Ad Hoc Networks with Selfish Node. Communications ICC'07. IEEE International Conference, Vol. 1, No. 1, pp. 3351-3356.

[11] Yang, H, Luo, Y, Ye, F, Lu,W, S and Zhang, L, (2004) Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications, Vol. 1, No. 1, pp. 38-47.

[12] Chen, T.M, Varatharajan,V (2005) Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks. IEEE Internet Computing, Vol. 3, No. 1, pp 233-245.