International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 23989-24001

http://www.ripublication.com

Cohen Kappa Reliability Coefficient Based Mitigation Mechanism For Byzantine Attack In Manets

[1]A.Geetha, [2]N.Sreenath
Department of Computer Science and Engineering
Pondicherry Engineering College, Puducherry,
INDIA
[1]gachuthansareeka@gmail.com, [2]nsreenath@pec.edu

Abstract

In mobile ad hoc networks, the degree of reliable data delivery depends on the co-operation of the intermediate nodes that exists between the source and destination. The co-operation among the active mobile nodes is more crucial mainly due to the resource constraint challenge of ad hoc networks. Besides, the byzantine behavior of mobile nodes degrades the survivability of the network. Hence detecting and mitigating byzantine attack is considered as one of the significant research issue to be resolved. In this paper, we propose a Cohen Kappa Reliability Coefficient based Reputation Mechanism (CKRCRM) for detecting and mitigating byzantine attack through a statistical reliability coefficient called Cohen Kappa and further re-confirmation of maliciousness is achieved through Pareto resilience factor. The performance of CKRCRM is analyzed using ns-2 simulator and is observed the proposed mitigation approach outperforms the PCMA and the CONFIDANT benchmark mechanisms considered for study by improving the performance of the network in terms of packet delivery ratio and throughput by 34% and 29%respectively. Furthermore, CKRCRM detects and mitigates byzantine nodes at a rapid rate of 33% than the existing mitigation mechanisms proposed for isolating byzantine nodes from the routing path.

Keywords: Byzantine node, AODV,Cohen Kappa Reliability Coefficient, Paretoresilience factor, Mobility Proportion, time of connectivity.

Introduction

Mobile ad hoc network is defined as a collection of autonomous mobile nodes that performs the act of routing without relying on any 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. 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 [3]. The reputation factor of a mobile node reflects the reliability and cooperation 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 the packets without transmitting to the next intermediate or to the destiny node. In general, such classes of nodes are known as malicious nodes, which by its activity drastically reduce the network performance. Even though the required resources are adequate for data transmission, the networks will function properly only when the participating nodes are cooperative in routing and forwarding. Due to the selfishness character some nodes won't cooperate with others.

Although, researchers have put forward large number of techniques, to detect and mitigate various types of malicious attacks in MANETs, most of the proposed approaches were mainly framed for unicast type of routing activity. This paper focuses on detecting and mitigating malicious nodes in the routing activity by making use of AODV protocol. The AODV 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. In this paper, we propose a Cohen Kappa Reliability Coefficient based Reputation Mechanism (CKRCRM) for mitigating byzantine nodes. The proposed approach CKRCRM quantifies the trust of the group leader is estimated through the Kappa statistical factor computed and re-confirms a node's maliciousness based on Pareto resilience factor that quantifies the impact of byzantine nodes on the performance of the network.

The remaining part of the paper is organized as follows. Section 2 presents a brief literature review on the existing mitigation mechanism proposed for detecting byzantine attacks in ad hoc networks. Section 3 and 4 elaborates on the proposed CKRCRM mechanism with its associated algorithms. Section 5 presents the simulation setup used for the implementation of CKRCRM and the comparative study carried out with PCMA and CONFIDANT. Section 6 concludes the paper with future plan of research.

Related Work

In the recent past, a number of byzantine node mitigation mechanisms have been contributed by the researchers. Some of the existing mitigation approaches for detecting byzantine attack are enumerated below.

Tarag Fahad and Robert Askwith [2] have proposed an algorithm namely Packet Conservation Monitoring Algorithm (PCMA) to detect selfish nodes. It avoids the trust for the selfish node based on the information from the direct neighbouring nodes of malicious nodes and excludes the malicious nodes relying on its neighbour information. No reliability analysis has been carried on the obtained neighbour information.

Kumar Das et al., [4] contributed a reactive multicast protocol that enables reliable transmission of data by organizing nodes into shared multicasting determined based on node behaviour. The authors investigated the issue of multicasting based on link stability, energy efficiency and expiration time. They also developed a framework for efficient detection of malicious activity that could decrease the network survivability. L. Buttyan and J.P Hubaux[5] contributed a trust oriented framework that enforces cooperation between mobile nodes of an ad hoc environment. They implemented a tamper resistance module for detecting and mitigating rendezvous point attack. They also prove that malicious activity can be identified efficiently based on path-rater and watch dog mechanism.

Further, S.Roy et al., [6] contributed a mitigation mechanism that could deal with the exhaustive sets of attacks that could originate in a multicasting environment. This mitigation mechanism investigates wide range of issues that could arise during route establishment and route maintenance by incorporating control packets like RREP-INV, MACT (P), MACT (J) and MACT (J)-MTF.Bing Wu et al., [7] proposed a Watchdog and Path-Rater dependent intrusion detection system that monitors the trustworthiness of the mobile nodes participating in group communication. Watch dog and Path-Rater were utilized for computing reputation of the mobile nodes through which the decision of identification may be incorporated.

Furthermore, Chi-Yang Chang et al., [8] proposeda mechanism for recovering compromised nodes of the network by utilizing a bootstrap router that enables efficient routing. This mechanism is based on the principle of tit for tat strategy where malicious nodes are punished with -1 and the normal routing nodes are rewarded with +1. Depending upon the number of punishments and rewards gained by a mobile node, the decision of isolating malicious nodes were taken into account. C. Demir and C.Comaniciu et al., [9] proposed a novel detection mechanism based on the concept of auction. This mechanism selects the optimal routing path by computing the minimum cost obtained by the mobile nodes in each and every individual bids. This mechanism further manipulates the optimal routing path based on the payment which is equal to the magnitude of second lower valued bid.

In addition, H. Yang et al., [10] contributed a detection mechanism that utilizes one way hash function for predicting the gentility parameter of a mobile node. The utilized hash function depends on the second hand information obtained from the neighbour nodes of the shared multicast group leader. They also contributed a fault tolerance mechanism that aids in enhancing delivery of data packets. An evidence based trust aided mitigation mechanism was proposed by Thomas M.Chen et al., [11] which identify the attacker nodes based on the rule of Dempster-Shafer Theory. This approach also computes the trust factor based on second hand information using the concept of posterior probability.

Buchegger and Boudec [12] proposed a protocol namely CONFIDANT to detect and exclude the misbehaving nodes from forwarding activity .Trust manager is used to evaluate the level of trust of nodes and to prepare alert reports of it. As the Manets are resource constraint in nature it is not better to use a trust manager which consumes more bandwidth to transmit the trust details to ensure the reliability of participating nodes.

Extract of the Literature

From the review of the literature from the research works available for mitigating rendezvous point attack, the following shortcomings are identified:

- A swarm intelligence based mechanism for byzantine node attack mitigation based on energy availability has not been proposed to the best of our knowledge.
- A distributed mitigation mechanism that detects a group leader as compromised and elects a new group leader based on mobility proportion has not been much explored.

These limitations of the literature are the motivation factors for proposing Swarm based Energy Aware Mitigation Mechanism for mitigating rendezvous point attack based on Optimal Energy Factor and swarm intelligence paradigm.

Cohen Kappa Reliability Coefficient Based Mitigation Mechanism (CKRCMM) For Byzantine Attack In Manets

In this section, we present a Cohen Kappa Reliability Coefficient based mitigation mechanism (CKRCRM) for Byzantine attack in an ad hoc scenario. In this approach, the detection of byzantine attach is achieved through the following two steps

a) Identification of Routing loops.
b) Estimation of the reliability of mobile nodes

When a Source Node 'S' wants to communicate with the destination node 'D', the source node 'S' broadcast control packets to all possible paths from 'S' to 'D'. But, when a node or group of nodes present in the routing path between 'S' and 'D' gets compromised by Byzantine attack. Then, the intermediate nodes are monitored by their neighbours for a timestamp (Ts) and if the monitoring node does not gets updated through an acknowledgement then the node is confined as attacked by further computing a parameter called Cohen Kappa Reliability Coefficient (CKRC).

Suppose a node 'N_i' is monitored by 'N_h' and 'N_j' for identifying whether it is Byzantine and compromised .Then, the expected forward probability of 'N_h' and 'N_j' about 'N_i' is given by (1) as

$$P_{me} = P_{fp(h)} * P_{fp(j)} \quad \text{--------- (1)}$$

Here,

The forward probability '$P_{fp\ (h)}$' estimated by neighbour 'N_h' on 'N_i' calculated through (2) as

$$P_{fp\ (h)} = N_{pfi\ (h)}/N_{pri\ (h)} \quad \text{--------- (2)}$$

Similarly,

'P_{fpi}' is the forward probability calculated by neighbour 'N_j' on 'N_i' estimated through (3) as

$$P_{fp\ (j)} = N_{pfi\ (j)}/N_{pri\ (j)} \quad \text{--------- (3)}$$

Where,

$N_{pfi(h)}$, $N_{pfi(j)}$,$N_{pri(j)}$and $N_{pri(j)}$ denotes maximum number of packets forwarded and maximum number of packets received by 'N_i' as monitored by 'N_h' and 'N_j' respectively.

Further,

The chance agreement probability for computing the expected reliability of the monitored node 'N_i' is given by (4) as

$$P_{ep} = P_{me} * P_{be} + (1 - P_{me})(1 - P_{be}) \quad \text{---------- (4)}$$

Furthermore, the observed probability about 'Ni' by 'N_j' is given by (5) as

$$P_{op} = P_{me}(1 - P_{be}) \quad \text{---------- (5)}$$

Then, the Cohen kappa Reliability Coefficient (CKRC) is manipulated by (6) as

$$P_{os}(CKRC) = (P_{op} - P_{ep})/(1 - P_{ep}) \quad \text{---------- (6)}$$

Thus, the Cohen kappa Reliability Coefficient (CKRC) estimates the degree of survivability of a mobile node towards byzantine compromised behaviour on the routing path. Based, on the degree of attack vulnerability, the byzantine node is isolated from the routing bath based on re-confirmation through Pareto resilience factor as given by (7) as,

$$R_{i(t)} = \left(\frac{\Omega(i)}{\Omega(i)+t}\right)^{\alpha} \quad \text{---------- (7)}$$

Where, 'α' and't' is defined as the mobility proportion and time of connectivity of a mobile node with respect to their neighbors. When the Pareto resilience factor ($R_{i(t)}$) is below a threshold of 0.4, then the byzantine compromised mobile node will be isolated from the routing path.

The Cohen Kappa Reliability Coefficient Based Mitigation Algorithm For Byzantine Attack

Algorithm1: $\boldsymbol{Computation\_CKRC()}$
Notations: ***n - Number of mobile nodes in the network*** ***r - Number of sessions*** ***R_P- Number of packets received by a mobile node*** ***F_P- Number of packets forwarded by a mobile node*** ***T_{rep}-Timestamp at which acknowledgement is received*** ***T_s - Timestamp at which acknowledgement is expected to be received*** ***P_{me} – Probability of malicious estimation*** ***P_{be} - Probability of normal behaviour estimation***
1. Begin *2. For each mobile node in the network, $i = 1$ to n do*

3. For each session of packet transmission, check(T_{rep}<=T_s)
4. The node 'N_i' is detected as byzantine compromised.
5. Then, Find the expected forward probability $(Pme = Pfp(h) * Pfp(j))$ *based on forward probability estimated by Neighbor 'N_h' and 'N_j'*
6. Estimate chance agreement probability $P_{ep} = P_{me} * P_{be} + (1 - P_{me})(1 - P_{be})$
7. Also, Manipulate the observed probability about 'Ni' by 'N_j' and 'N_h' as

$$Pop = Pme * (1 - Pbe)$$

8.Calculate the Cohen kappa Reliability (CKRC) is manipulated by
P_{os} (CKRC) = (P_{op}-P_{ep})/ (1-P_{ep})
9.If(P_{os} (CKRC) <=P_{op}) then
10.Confirm 'N_i' is byzantine compromised
End for
End for
End

Simulations and Experimental Analysis

The comparative analysis of CKRCRM with the existing benchmark mitigation solutions PCMA and CONFIDANT protocols are thoroughly investigated through simulation using network simulator ns-2.26.The simulation environment used for investigation contains 50 mobile nodes randomly distributed in a terrain size of 1000x1000m. Itpossess the channel capacity of 2 Mbps with a constant bit rate of 80 packets/sec and refresh interval ,time of simulation being 20 seconds and 150 seconds respectively .Further, the CKRCRM ,PCMA and CONFIDANT algorithms used for comparative analysis is evaluated based on the network related parameters packet delivery ratio, throughput, total overhead and control overhead.

Table 1: Simulation Setup

Parameter	**Value**	**Description**
No. of mobile nodes	50	Number of Simulation Nodes
Type of Protocol	AODV	Ad hoc On demand Distance Vector Protocol
Type of Traffic	80 packets per Second	Constant bit rate
Type of Propagation	Two Way Ground	Radio propagation model
Simulation Time	150 s	Maximum simulation time.
Number of packets used	1000	Maximum number of packets used in simulation.
Channel capacity	2 Mbps	Capacity of the wireless channel

Performance analysis for CKRCRM

The performance of CKRCRM is exhaustively studied based on two experiments viz.

a) **Experiment 1**: Varying the number of mobile nodes with number of byzantine compromised node set as 10:
b) **Experiment 2**: Varying the number of byzantine nodes in increments of 5.

The following section enumerates on the performance of the CKRCRM when compared to PCMA and CONFIDANT protocol:

Experiment 1: Varying the number of mobile nodes with number of byzantine compromised node set as 10

Figure. 1 depicts the performance of CKRCRM over PCMA and CONFIDANT, PCMA based on packet delivery ratio. The proposed CKRCRM approach improves the performance of the network in terms of packet delivery ratio by16% to 22% and by 25% to 28% than the benchmark mechanisms schemes like CONFIDANT and PCMA.This significant improvement in the packet delivery rate is achieved since CKRCRM detects and mitigates byzantine attack at a rapid rate of 33%.

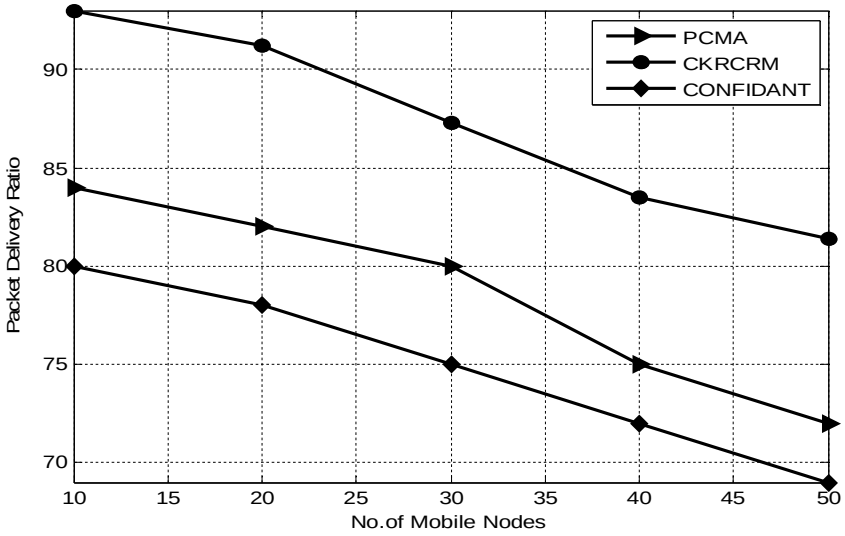

Figure 1: Experiment 1- Performance Chart For CKRCRM Based On Packet Delivery Ratio

Further, it is also obvious that CKRCRM in an average increases the packet delivery rate to a maximum extent of 35% than PCMA and CONFIDANT.

Figure. 2 represent the superior performance of CKRCRM over PCMA and CONFIDANT based on control overhead. Further, the proposed statistical reliability based CKRCRM approach drastically minimizes the control overhead from 23% to 18% and from 17% to 13% than PCMA and CONFIDANT.

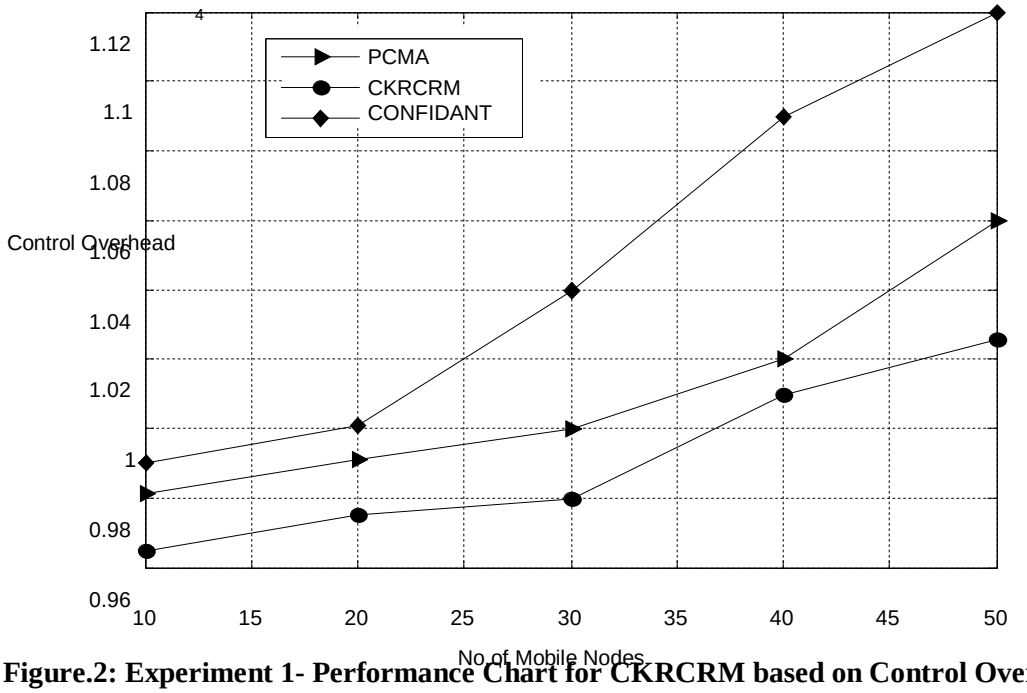

Figure.2: Experiment 1- Performance Chart for CKRCRM based on Control Overhead

It is also transparent that the proposed CKRCRM mitigates the byzantine node attackers and in average reduces the control overhead by 21%.

Figure.3portrays the superior performance of CKRCRM over PCMA and CONFIDANT with respect to total overhead. The proposed CKRCRM approach reduces the total overhead from 25% to 29% and from 31% to 35% over PCMA and CONFIDANT.

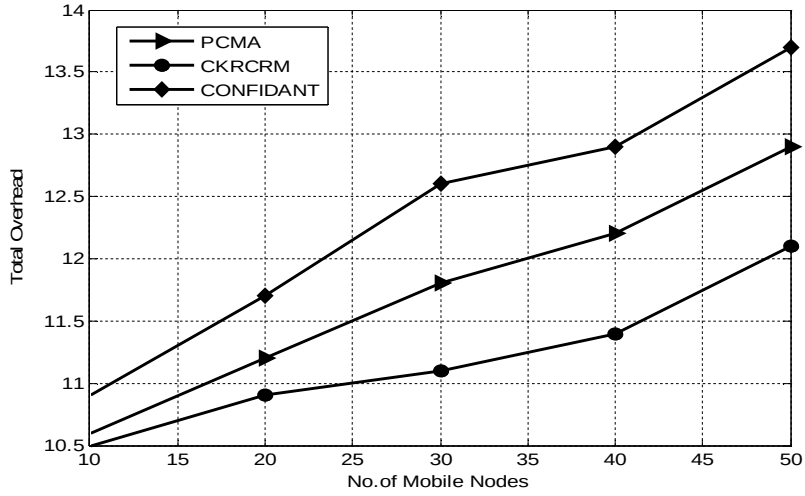

Figure 3: Experiment 1-Performance Chart for CKRCRM based on Total Overhead

It is evident that, CKRCRM approach in an average reduces the total overhead by 25% than the existing mitigation mechanisms like PCMA and CONFIDANT.

Figure.4exhibits the performance of CKRCRM over PCMA and CONFIDANT based on throughput. The proposed CKRCRM mitigation approach shows a phenomenal improvement in throughput than the byzantine existing approaches like CONFIDANT from 16% to 29% and from 23% to 33% over PCMA.This improvement in throughput is due to the efficient energy mechanism incorporated for detecting byzantine node attackers that maliciously drops packets.

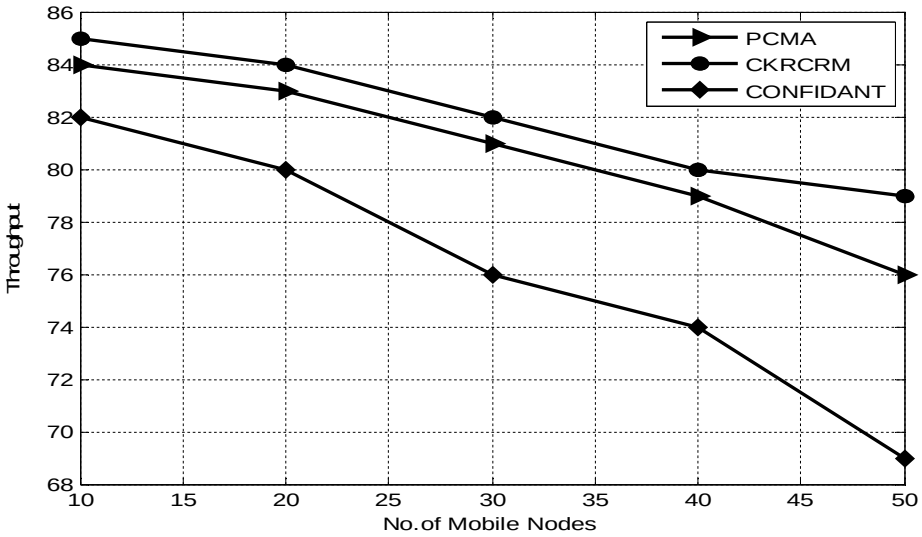

Figure 4: Experiment 1-Performance Chart for CKRCRM based on Throughput

It is also obvious that our CKRCRM approach mitigates byzantine node compromised nodes rapidly and increases the throughput by reducing packet drops in an average of 18%.

Experiment 2: Varying the number of byzantine nodes in increments of 5.

The performance of CKRCRM is compared with the existing reputation approach named CONFIDANT and PCMA based on packet delivery ratio is presented in figure.5. The proposed CKRCRM approach exhibits a phenomenal improvement in packet delivery ratio than PCMA and CONFIDANT by 19% and 14% respectively.

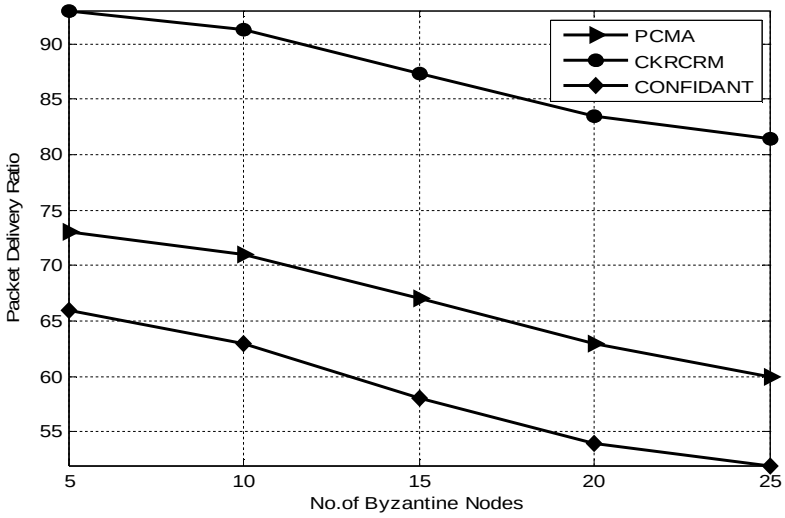

Figure 5: Experiment 2- Performance Chart For CKRCRM Based On Packet Delivery Ratio

It is also evident that CKRCRMeffectively and efficiently detects byzantine compromised nodes and mitigates them at faster rate of 34% and further increases the packet delivery ratio to a maximum level of 21%.

The performance of CKRCRM is compared with the existing byzantine nodes mitigation approaches like PCMA and CONFIDANT based on throughput is presented in figure.6. The proposed CKRCRM approach exhibits a remarkable improvement in throughput than PCMA and CONFIDANT by 31% and 36% respectively.

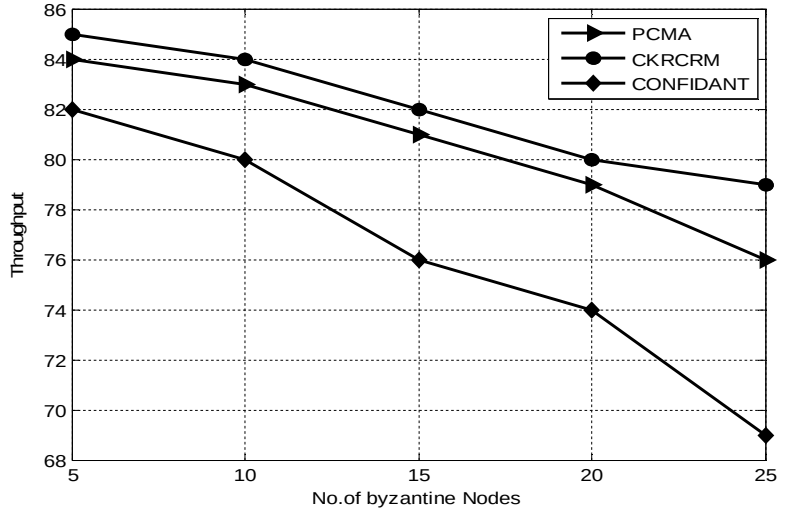

Figure 6: Experiment 2- Performance Chart for CKRCRM based on Throughput

It is also transparent that, CKRCRM effectively and efficiently detects byzantine attacker nodes and increases the throughput to a maximum level of 21%.

Figure.7depict the performance of CKRCRM overPCMA and CONFIDANT based on total overhead. The proposed CKRCRM approach exhibits a phenomenal decrease in total overhead of about 23% and 31% than CONFIDANT and PCMA.

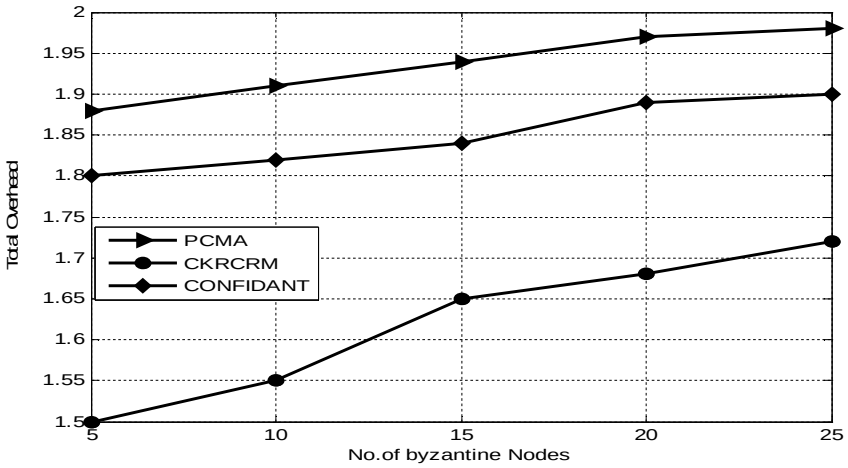

Figure 7: Experiment 2- Performance Chart for CKRCRM based on Total Overhead

It is also obvious that, the CKRCRM effectively and efficiently detects byzantine nodes and in an average reduces the total overhead to a maximum level of 26%.

Figure.8depict the performance of CKRCRM overPCMA and CONFIDANT based on control overhead. The proposed CKRCRM approach exhibits a phenomenal decrease in control overhead from by 24 % and 19% than PCMA and CONFIDANT.

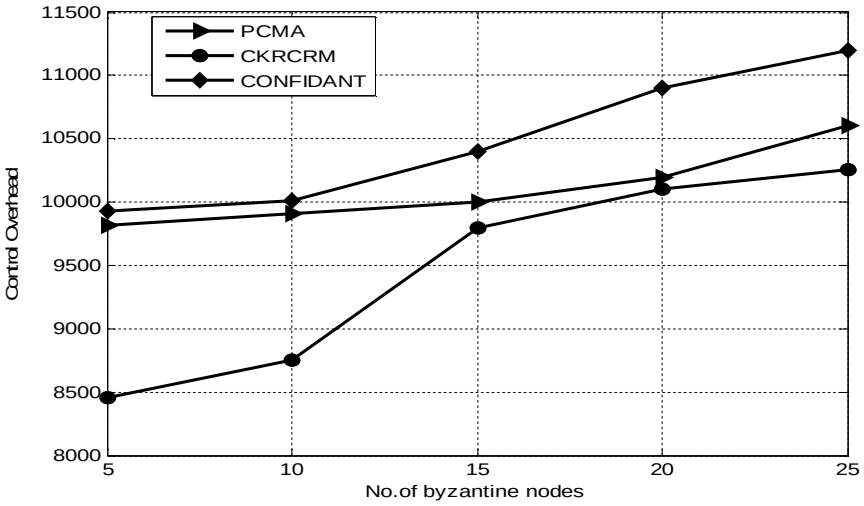

Figure 8: Experiment 2- Performance Chart for CKRCRM based on Control Overhead

It is also transparent that CKRCRM effectively and efficiently detects byzantine attacker nodes and in an average reduces the control overhead to a maximum extent of 18%.

Conclusion

This paper has presented a Cohen Kappa Reliability coefficient based Reputation Mechanism (CKRCRM) for mitigating byzantine compromised mobile nodes based on Cohen Kappa statistical reliability coefficient and re-confirming the isolation of the malicious nodes based on Pareto resilience factor. The exhaustive simulation experiments and analysis clearly exhibits that this reputation approach isolates byzantine nodes and improves the performance of the network with respect to packet delivery ratio, total overhead, throughput and control overhead in an average by 34% than the benchmark mitigation mechanisms considered for comparative analysis. As a part of future research, a mitigation mechanism based on cornbach alpha reliability coefficient may be formulated for detecting and isolating byzantine attacked nodes from the routing path.

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.

[2] Tarag Fahad and Robert Askwith., 'A Node Misbehaviour Detection Mechanism for Mobile Ad hoc Networks', PGNet. 2006.

[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] Subir Kumar Das, B.S. Manoj, and C. Siva Ram Murthy. 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, pages 24–35, June 2002.pp 33-46

[5] L.Buttyan and J-P, Hubaux, (2003), 'Stimulating Coperation in Self – organizing Mobile Ad hoc Networks", Mobile Computing and Networking' pp 255-265.

[6] S. Roy, V.G. Addada, S. Setia and S.Jajodia, Securing AODV: Attacks and countermeasures, in Proceedings of. SECON'05, IEEE, 2005.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei. A Survey on Attacks and Counter measures in Mobile Ad Hoc Networks. WIRELESS/MOBILE, NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) 2006 Springer.

[8] Chi-Yuan Chang, Yun-Sheng Yen. Chang-Wei Hsiesh Han-Chieh Chao an Efficient Rendezvous Point Recovery Mechanism in Multicasting Network, International Conference on Communications and Mobile Computing, 2007.

[9] Demir, C and Comaniciu C. An Auction based AODV Protocol for Mobile Ad Hoc Networks with Selfish Node. Communications ICC'07. IEEE International Conference in June 2007.

[10] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

[11] Chen, T.M, Varatharajan,V (2005) Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks. IEEE Internet Computing.pp 233-245.

[12] S. Buchegger and J. Boudec,(2002) "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp, Mobile Ad Hoc Networking and Computing.