International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Cohen Kappa Reliability Factor-based Mitigation Mechanism for Enhancing Cooperation in Ad hoc Networks

V. Vijayagopal, K. Prabu

Abstract*: This paper presents a Cohen Kappa Reliability Factor-based Mitigation Mechanism (CKRFMM) for enabling trustworthy detection of Byzantine nodes. This detection process is achieved by estimating the reliability of the mobile nodes calculated through Cohen Kappa Reliability Factor (CKRF). CKRFMM reconfirms the byzantine behavior of active mobile nodes through Pareto function. Pareto function is a predominant re-test reliability estimator available in the classical theory of statistics. The simulation experimentation conducted using ns-2 of the CKRFMM is determined to be excellent in reducing energy consumptions, network delay compared to the benchmarked byzantine node detection schemes considered for investigation.

Keywords: **Byzantine Nodes, Cohen kappa, Reliability, Pareto function**

I. INTRODUCTION

In MANET, collaboration between mobile nodes are considered as the vital entity for establishing and maintaining reliable communication among the mobile nodes [1-3]. This co-operation ensures reliable network connectivity and enhances the resilience of the network [4]. However, the resilience or the connectivity of the network is greatly influenced by the presence of byzantine nodes [5]. Hence, a need arises for devising mitigation mechanisms that could handle byzantine behaviour in a more accurate and reliable way [6]. Traditionally, the mobile nodes in an ad hoc network is identified as byzantine when it intentionally refuses to forward packets for their neighbours in order to disturb the act of reliable packet delivery [7]. Therefore, the byzantine behaviour of mobile nodes can be effectively estimated by monitoring two significant parameters, viz., i) packet forwarding rate and ii) energy consumption rate [8]. The difference in packet forwarding and energy consumption of a mobile node can be calculated using statistical reliability factors available in the literature [9]. Further, the mitigation of byzantine nodes can be effectively performed by accessing their packet forwarding capability based on past experience of mobile nodes [10].

Revised Manuscript Received on March 17, 2020.
* Correspondence Author
Mr. V.Vijayagopal*, Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India. Email: vijayagopal1976@gmail.com
Dr. K.Prabu, Associate Professor, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India. Email: kprabu.phd@gmail.com

II. RELATED WORK

Buttyan and Hubaux [11] contributed a co-operation enforcement scheme that incorporates reliable packet forwarding process using a tamper robust hardware module for monitoring nodes' packet transmission behaviour. This hardware involves a nuglet counter which monotonically increases or decreases depending on the node's potential in forwarding or receiving packets. Every mobile node has to possess a positive counter value for participating in the routing activity. The tamper resistant feature of the incorporated hardware module enforces security to the nuglet counter from illegal computations. Fulai Liu and Ying Zhou [12] proposed a priority factor-based forwarding mechanism for motivating co-operative mobile nodes. This priority-based packet forwarding process is grouped into prized priority forwarding and un-prized best-effort forwarding. These prized priority forwarding and un-prized best-effort forwarding mechanisms are designed for efficiently discriminating critical issues that arise during the process of resolving misbehaviour actions.

Further, Sengathir and Manoharan [13] proposed a detection approach which considers communication in the network is achievable only through trustworthy nodes designated as broker nodes. In this scheme, byzantine behaviour of a mobile node is determined by the broker nodes. The receipt generated by the source node contains the virtual currency information that each mobile node pays to its neighbours for their forwarding service. The value of the virtual currency possessed by each and every mobile node dynamically changes based on the receipts forwarded by that node. Usha and Radha [14] propounded a credit-based scheme that analyzes the fairness attribute of mobile nodes by considering an assumption that emphasizes less credits to the nodes located in the periphery of the network than the nodes located at the centre. Zhong et al. [15] proposed another credit-based scheme known as simple, cheat-proof, credit-based system (SPRITE) that uses a receipt management system that stores forwarded and received messages of mobile nodes. SPRITE uses a Credit Clearance Service (CCS) which punishes or credits a mobile node based on its packet forwarding capability. In CCS, each mobile node gains more credits when it forwards maximum number of packets for their neighbouring nodes and it loses credits when it refuses to forward packets for their neighbours.

Demir and Comaniciu [16] proposed an auction based routing mechanism for mitigating misbehaviour of mobile nodes. This auction based routing mechanism is also an incentive-based approach that enforces collaboration by creating virtual economy in the network. Virtual economy refers to the payment given by a source node to intermediate nodes of the routing path for transmitting packets to the destination. At the same time, the source node possesses the option of choosing an optimal intermediate node for routing packets based on the lowest price in the virtual currency auction. This strategy makes the source node to neglect lowest energy node for transmission, since it may turn into root node attack compromised in the near future. Chong et al. [17] also proposed an incentive mechanism for rewarding mobile nodes with credits for participating in packet forwarding and for policing congestion and traffic. In this incentive mechanism, source node estimates price of congestion based on significant factors such as available bandwidth and transmission power for comparing it with willingness-to-pay. This willingness-to-pay factor is computed based on information that relates to the bandwidth and energy shared among the mobile nodes which is systematically adjusted by the nodes based on their personal observations.

III. COHEN KAPPA RELIABILITY FACTOR-BASED MITIGATION MECHANISM (CKRFMM)

CKRFMM is the significant statistical reliability factor-based mitigation mechanism proposed for mitigating byzantine attack from an ad hoc environment. In CKRFMM, the mitigation of byzantine compromised nodes are facilitated using two steps that include a) Calculation of reputation based on Cohen Kappa Reliability Factor (CKRF) and b) Isolation of byzantine nodes from routing based on computed CKRF.

a) Calculation of reputation based on Cohen Kappa Reliability Factor (CKRF)

Consider an ad hoc network in which each of the mobile nodes is monitored by their neighbouring nodes for 's' sessions. If there are 'n' nodes in the network and each node 'i' is monitored by its 'k' neighbouring nodes. The packet forwarding capability of each mobile node identified by first neighbour is given by

$$P_{PFC(1)} = \frac{NP_{f(1)}}{NP_{r(1)}} \qquad (1)$$

The packet forwarding capability of each mobile node identified by second neighbour is given by

$$P_{PFC(2)} = \frac{NP_{f(2)}}{NP_{r(2)}} \qquad (2)$$

Thus the packet forwarding capability of each mobile node identified by the 'kth'neighbour is given by

$$P_{PFC(k)} = \frac{NP_{f(k)}}{NP_{r(k)}} \qquad (3)$$

Where '$NP_{f(c)}$' and '$NP_{r(c)}$' denotes the packet forwarding and packet receiving probability as recommended by each monitoring neighbours and 'c' refers to each individual neighbouring node that varies between 1 and k.

The packet forwarding probability identified by each of the monitoring neighbours are independent of each other, then the Expected Packet Forwarding Potential ($EPFP_e$) is computed through

$$EPFP_e = P_{PFC(1)} * P_{PFC(2)} * \ldots\ldots * P_{PFC(k)} \qquad (4)$$

Similarly, the packet receiving capability of each mobile node identified by first neighbour is given by

$$P_{PRC(1)} = \frac{NP_{r(1)}}{NP_{s(1)}} \qquad (5)$$

The packet receiving capability of each mobile node identified by second neighbour is given by

$$P_{PRC(2)} = \frac{NP_{r(2)}}{NP_{s(2)}} \qquad (6)$$

The packet receivng capability of each mobile node identified by the 'kth' neighbour is given by

$$P_{PRC(k)} = \frac{NP_{r(k)}}{NP_{s(k)}} \qquad (7)$$

Where '$NP_{r(c)}$' and '$NP_{s(c)}$' refers to the number of packets actually received and the number of packets actually sent to it by their preceding neighbour nodes.

The packet receiving probability identified by each of the monitoring neighbours are independent of each other, then the Expected Packet Receiving Potential ($EPRP_e$) is computed through

$$EPRP_e = P_{PRC(1)} * P_{PRC(2)} * \ldots\ldots * P_{PRC(k)} \qquad (8)$$

Then the expected probability (P_{ex}) which quantifies the cumulative impact of both packet forwarding and packet receiving capability of mobile node is calculated using

$$P_{ex} = ((EPFP_e * EPRP_e) + ((1 - EPFP_e)(1 - EPRP_e))) \qquad (9)$$

The observed probability (P_{ob}) that infers the packet forwarding and packet receiving capability of mobile nodes is

$$P_{ob} = ((EPFP_o * EPRP_o) + ((1 - EPFP_o)(1 - EPRP_o))) \qquad (10)$$

Where $EPFP_o$ and $EPRP_o$ represents the Observed Expected Packet Forwarding Potential and Observed Expected Packet Receiving Potential of mobile nodes being monitored.

Then the Cohen Kappa Reliability Factor (CKRF) which quantifies the reliability of each mobile node under routing is computed using

$$P_{CKRF} = \frac{(P_{ob} - P_{ex})}{(1 - P_{ex})} \qquad (11)$$

b) Isolation of byzantine nodes from routing based on CKRF.

Further the reliability of the mobile nodes estimated through CKRF is re-estimated using Pareto function through

$$F_{PARETO} = (\frac{\varpi(i)}{(\varpi(i)+t)})^{\beta} \quad (12)$$

Where 'β' , 't' and ' $\varpi(i)$ 'refers to the mobility rate, connectivity time and resilience factor of each mobile node with respect to their neighbours.Pareto function is one of the re-test reliability estimation factor that verifies the validity of the preceding test. When the Pareto resilience factor F_{PARETO} is below a threshold of 0.4 (obtained from simulation and discussed in section 3.3) then the byzantine mobile node is isolated from the routing path.

The following algorithm 1 illustrates the steps involved in detecting byzantine nodes using Cohen Kappa Reliability Factor (CKRF) and retesting the trustworthiness of monitored mobile node using Pareto function for isolating them from the routing path.

Algorithm 1: Calculation of Cohen Kappa Reliability Factor (CKRF)

Notations

N-The number of nodes in the network
GN–Group of nodes of the routing path
SN-Source node
DN-Destination node
s-Number of sessions
u-any node in GN
k-Number of neighbouring nodes
c-Individual neighbouring node between 1 and k
P_{PFC} -packet forwarding capability of each mobile node identified by its neighbours
P_{PRC} -packet receiving capability of each mobile node identified by its neighbours
$EPFP_e$- Expected Packet Forwarding Potential of a node
$EPRP_e$ -Expected Packet Receiving Potential of a node
$NP_{r(c)}$ -number of packets actually received by a node
$NP_{s(c)}$ -number of packets actually sent to a node by their preceding neighbour nodes
$EPFP_o$ -Observed Expected Packet Forwarding Potential of mobile nodes
$EPRP_o$ -Observed Expected Packet Receiving Potential of mobile nodes
P_{ex}-expected probability
CKRF-Cohen Kappa Reliability Factor

Algorithm

begin
for every node in GN
Calculate $EPFP_e = P_{PFC(1)} * P_{PFC(2)} * ..... * P_{PFC(k)}$
Calculate $EPRP_e = P_{PRC(1)} * P_{PRC(2)} * ..... * P_{PRC(k)}$
Compute
$P_{ex} = ((EPFP_e * EPRP_e) + ((1 - EPFP_e)(1 - EPRP_e)))$
Manipulate
$P_{ob} = ((EPFP_o * EPRP_o) + ((1 - EPFP_o)(1 - EPRP_o))$
Determine $P_{CKRF} = \frac{(P_{ob} - P_{ex})}{(1 - P_{ex})}$
if ($P_{CKRF}(u) < 0.4$)
{
node u is byzantine compromised
Call Byzantine-Mitigation-Reconfirmation(u)
}
else
u is a normal node
}

Algorithm 2: Isolation of byzantine nodes from routing based on CKRF

Notations

β- the mobility rate
t- connectivity time
$\varpi(i)$ -resilience factor of each mobile node with respect to their neighbours
F_{PARETO} -Pareto function

Algorithm

Byzantine mitigation reconfirmation(u)
do
{
$$F_{PARETO} = (\frac{\varpi(i)}{(\varpi(i)+t)})^{\beta}$$
calculate Pareto function
if (FPARTEO(u) < 0.4)
{
{
node 'u' is byzantine reconfirmed
isolate node 'u' from routing path
}
else
node 'u' is reliable
}
while(GN<=N)
}

IV. ILLUSTRATIONS FOR CKRFMM

In this sub-section, the working of CKRFMM is illustrated with examples. Consider an ad hoc network in which the source node 'S' broadcasts RREQ packets through all possible routes to the destination 'D' in order to discover and establish route using RREP as shown in Fig 3.1. In CKRFMM, each intermediate mobile node between the source and the destination (S-A-B-C-E-D) is monitored by their neighbouring nodes with the aid of a CKRF reliability test call CKRF_CALC_TEST. This CKRF_CALC_TEST calculates the Cronbach alpha based reliability factor of each intermediate node for detecting and isolating byzantine nodes. If an intermediate node 'B' of the routing path is monitored by their neighbouring nodes A, C, E of the routing path. Then, the reliability of the mobile node 'B' is evaluated based on two scenarios that are categorized based on the number of packets dropped by that node.

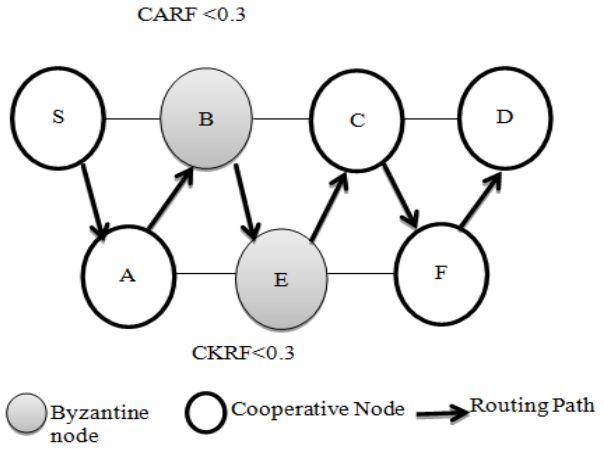

Figure 1-Scenario 1: When mobile nodes drops minimum number of packets

For instance, let the number of packets received by node 'B' from source node 'S' be 1000. But, the number of packets forwarded by that mobile node to its neighbouring nodes as monitored by A, C, E be 850, 650 and 750 respectively. Thus the mean deviation experienced are 150,350 and 200.Hence, the mean packet deviation of node 'B' as recommended by A, C, E is 233.Then Reliability Factor CARF for that node B is computed as 0.54 using the standard deviation and variation computed as 0.29 and 0.082 respectively. Hence the node is co-operative in routing.

Scenario 2: When mobile nodes drops moderate number of packets

In the Scenario 2, the number of packets received by B be 1000 but the number of packets relayed be 600, 500,400 to A, C, E respectively. Thus the mean deviation experienced are 400,500 and 600 respectively. Hence, the mean packet deviation of node 'B' as observed by A, C, E is 500.

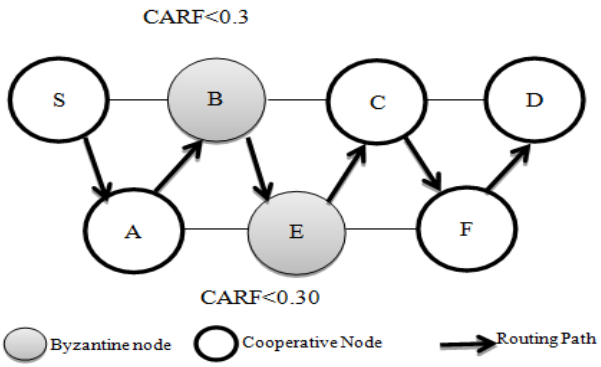

Figure 2-Scenario 2: When mobile nodes drops maximum number of packets.

Then Reliability Factor CARF for that node B is computed as 0.29 using the standard deviation and variation computed as 0.67 and 0.0036 respectively. Hence the node is exhibits byzantine behaviour in routing.

V. SIMULATION RESULTS AND DISCUSSIONS

The performance and characteristics of CKRFMM are thoroughly studied using ns-2.26 simulator. The performance of CKRFMM is compared with the proposed mitigation techniques like CONFIDANT, RTBD and PCMA.

Initially, CKRFMM is first investigated with the proposed mitigation approaches like CONFIDANT,RTBD and PCMA for identifying the mitigation point at which byzantine behaviour of nodes can be effectively handled. From the simulation result, is inferred that CKRFMM exhibits an effective performance at 0.40 since maximum numbers of byzantine nodes are detected by CKRFMM at this point than CONFIDANT, RTBD and PCMA considered for study. Hence, the mitigation point for detecting byzantine behaviour of nodesis considered to be 0.40 for comparative study. It is also inferred that CKRFMM is also equivalently capable of identifying maximum number of Byzantine nodes within the detection range of 0.35 and 0.45. Hence, maximum and minimum detection threshold detection point of CKRFMM is considered as 0.35 and 0.45 respectively.

Figures 3 and 4 depicts PDR and throughput of CKRFMM and the baseline schemes considered for analysis. The PDR and throughput of CKRFMM and the compared mitigation approaches considerably decreases as the number of mobile nodes increases. This is mainly due to the absence of a rapid routing process that handles an additional sum of data introduced into the network. But CKRFMM improves the packet delivery rate and throughput by enforcing a faster isolation rate of 30% greater than CONFIDANT, RTBD, and PCMA techniques.

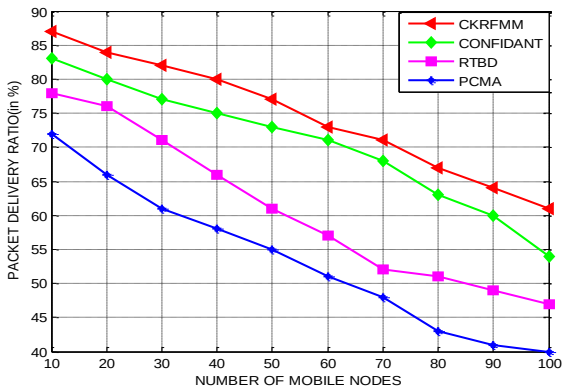

Figure 3-Experiment 1-Packet Delivery Ratio

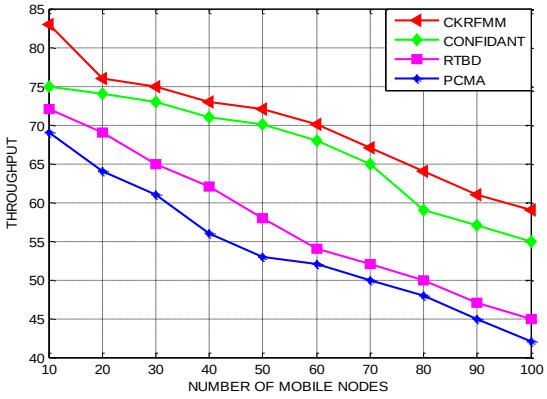

Figure 4-Experiment 1-Throughput

CKRFMM shows an improvement in PDR by 4%-6% over CONFIDANT, 8%-10% over RTBD and 14%-16% over PCMA. Similarly, CKRFMM improves the throughput by 4%-6% over CONFIDANT, 8%-10% over RTBD and 15%-17% over PCMA. In addition, CKRFMM enhances the PDR and throughput by 12% and 10%, respectively.

In figure 5 and 6 depicts Total overhead and control overhead of the network systematically improved with increase in number of transmissions. However, CKRFMM minimizes the control overhead by 6%-8% over CONFIDANT, 14%-16% over RTBD and 22%-25% over PCMA by enforcing Byzantine node mitigation at a rapid rate of 30%.

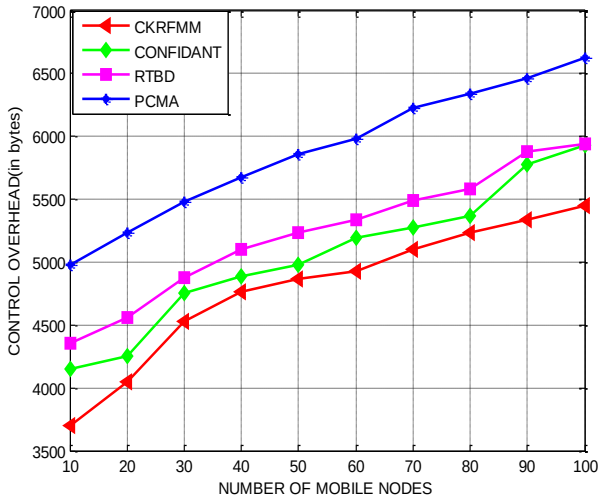

Figure 5-Experiment 1-Control Overhead

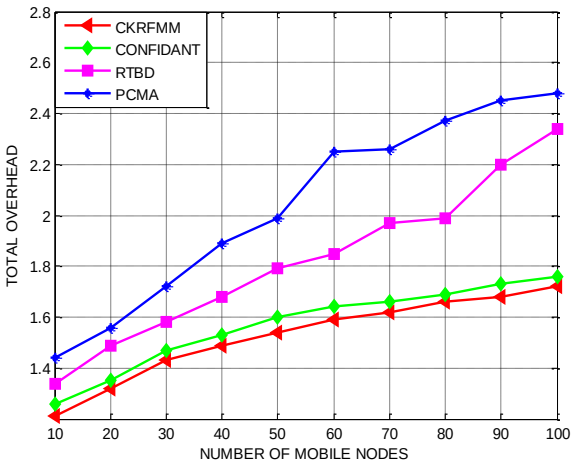

Figure 6-Experiment 1-Total Overhead

The total overhead of CKRFMM dramatically minimized the total overhead by 9%-12% over CONFIDANT, 14%-16% than RTBD and 21%-23% over PCMA. The results confirm that CKRFMM on an average minimized total overhead and control overhead by 22% and 18% respectively. In experiment 2, CKRFMM is investigated by varying the number of Byzantine nodes from 10 to 50. Figure. 7 demonstrates the PDR of CKRFMM analyzed by varying the number of Byzantine nodes. PDR decreases with increased number of Byzantine nodes as it forces the mobile nodes to exhaust energy. This intentional act affects the lifetime of an individual node and the routing path. However, CKRFMM handles this impact by utilizing CKRF for estimating the influence of byzantine nodes towards the lifetime of network. Hence, CKRFMM shows an improvement in PDR by 6%-8% over CONFIDANT, 9%-11% over RTBD and by 14%-17% over PCMA.

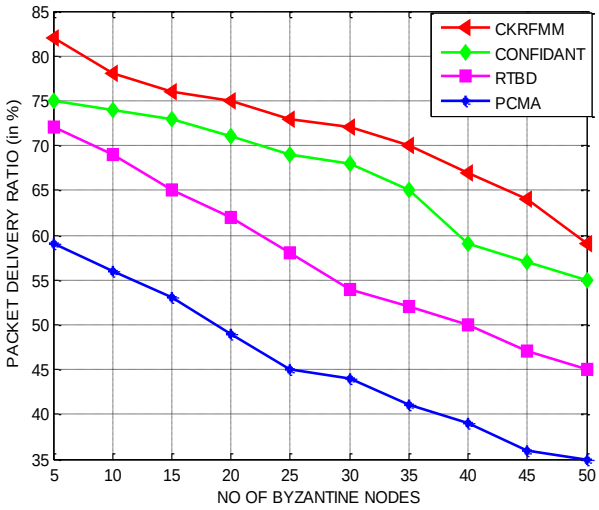

Figure 7-Experiment 2-Packet Delivery Ratio

Figures 8 and 9 spotlights the control overhead and delay estimated by varying the number of Byzantine nodes of an ad hoc network. The control overhead and delay is considered to enhance even when the influence of Byzantine nodes induces high energy consumption rate that crumbles the stability of the wireless link. Thus, CKRFMM demonstrates that control overhead is reduced by 10%-12% over CONFIDANT, 14%-16% over RTBD and from 18%-21% over PCMA. Further, CKRFMM portrays that the delay is reduced by 9%-12% over CONFIDANT, 14%-17% over RTBD and 19%-22% over PCMA. In addition, CKRFMM on an average reduced the control overhead and delay by 13.2% and 16.4% respectively.

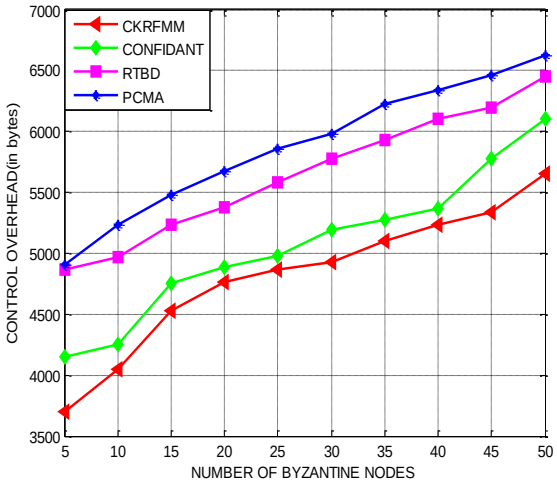

Figure 8-Experiment 2-Control Overhead

Retrieval Number: C6516029320/2020©BEIESP
DOI: 10.35940/ijeat.C6516.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

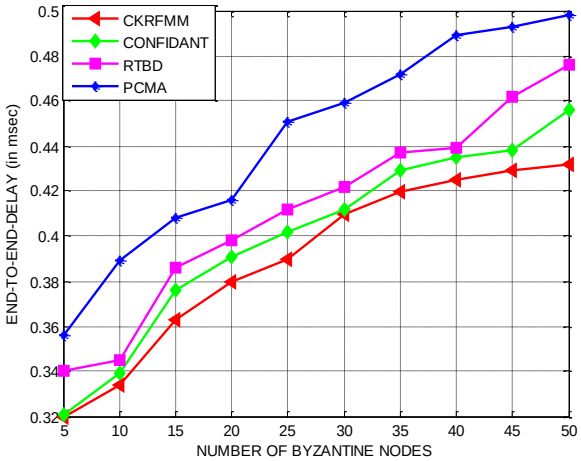

Figure 9-Experiment 2-End-To-End Delay

Figure 10 exemplars the results of CKRFMM estimated with respect to a detection rate on par with the benchmarked approaches. It is estimated that the detection ratio of CKRFMM increases with increase in the number of Byzantine nodes due to its rapid detection strategy. It is identified that CKRFMM improves the detection rate by 9%-11% over CONFIDANT, 14%-17% over RTBD and 19%-22% over PCMA.

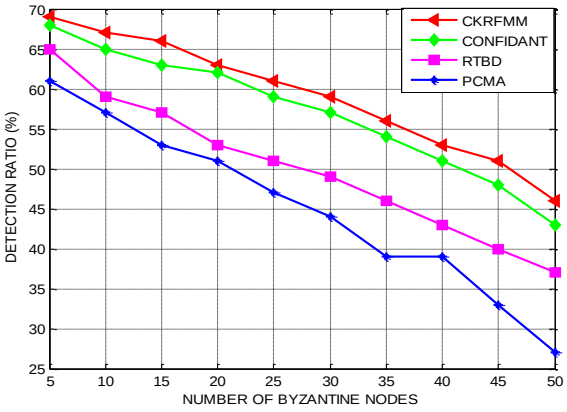

Figure 10-Experiment 2-Detection Ratio

Experiment 3 - Comparative Analysis of CKRFMM by varying the number of source and destination pairs

Finally, the performance of CKRFMM over CONFIDANT, RTBD and PCMA is also analyzed with varying the number of source and destination pairs. CKRFMM is determined to improve PDR independent to the number of source and destination pairs existing in the network. From Figure 11, it is obvious that CKRFMM increases the PDR by 11%-13% over CONFIDANT, 16%-19% over RTBD and 23%-26% over PCMA. Inaddition, it is observed that CKRFMM on an average improves the PDR by 14.6%.

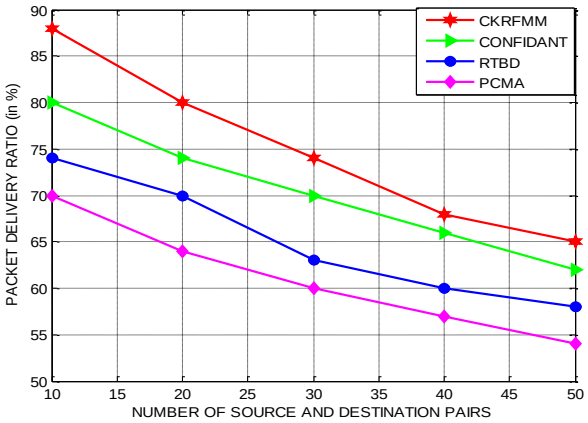

Figure 11-Experiment 3-Packet Delivery Ratio

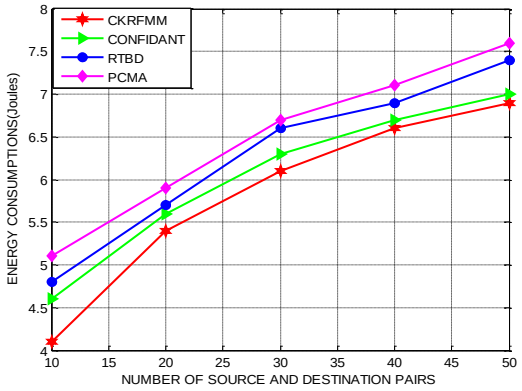

Figure 12-Experiment 3-Energy Consumption

Similarly, from Figure 12, it is transparent that CKRFMM reduced the energy consumptions by dynamic improving the detection rate on an average by 13% superior to the considered baseline mitigation schemes and thus energy consumptions are considerably reduced. It is also proved that CKRFMM decreases the energy consumptions by 8%-10% over CONFIDANT, 12%-15% over RTBD and 18%-21% over PCMA.

Figures 13 and 14 portrays the performance of CKRFMM in terms of end-to-end delay and packet drop rate obtained by varying the number of source and destination pairs. Figure 3.21 confirms that CKRFMM reduces the end-to-end delay by 9%-11% over CONFIDANT, 14%-18% over RTBD and 20%-23% over PCMA.

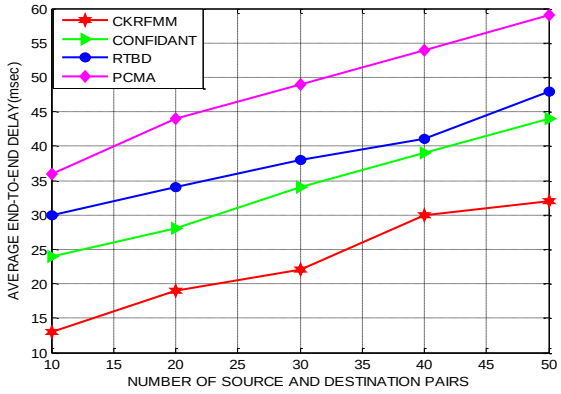

Figure 13 -Experiment 6-End-To-End Delay

Retrieval Number: C6516029320/2020©BEIESP
DOI: 10.35940/ijeat.C6516.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

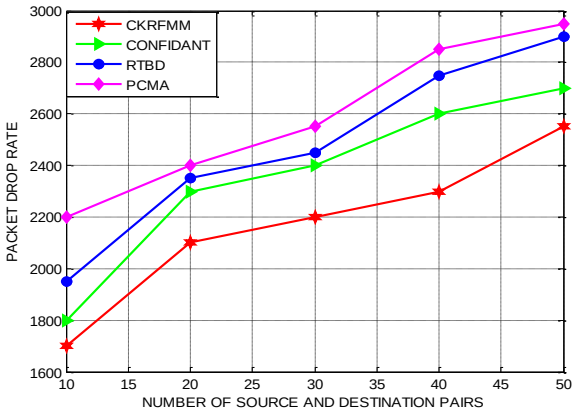

Figure 14-Experiment 6-Packet Drop Rate

In addition, Figure 14 demonstrates that CKRFMM reduces the packet drop rate by 12%-16% over CONFIDANT, 18%-22% over RTBD and 24%-28% over PCMA. Hence, it is obvious that CKRFMM is highly effective in reducing the end-to-end delay and packet drop rate on an average rate of 15% and 16.42% respectively.

VI. CONCLUSION

In this paper, Cohen Kappa Reliability Factor-based Mitigation Mechanism is presented for mitigating Byzantine nodes based on the past experience evaluated through their packet forwarding capability. CKRFMM facilitates mitigation by calculating CKRF and the reconfirms the node's malicious behaviour using Pareto function. The experimental results of CKRFMM outperform the proposed past history based mitigation approaches in terms of packet delivery, throughput, control overhead, total overhead and energy consumption. Further, CKRFMM aids in framing a detection threshold point for realizing the severity of impact induced by the byzantine behaviour of mobile nodes.

REFERENCES

1. J. Soryal and T. Saadawi, "Byzantine Attack Isolation in IEEE 802.11 Wireless Ad-Hoc Networks," 2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012), Las Vegas, NV, 2012, pp. 1-5.
2. S. K. Saini and P. Singh, "Analysis and detection of Byzantine attack in wireless sensor network," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3189-3191.
3. V.Vijayagopal, Dr. K.Prabu, 'An Trust and Energy-Inspired Threshold Packet Relaying Capability Technique (TEITPRCT) for Reliable Routing in MANETs', International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-12, October 2019, pp. 88-99.
4. V.Vijayagopal, Dr. K.Prabu, An Improved Integrated Energy and Trust-based Routing Mechanism for MANETs.', International Journal of Recent Technology and Engineering (IJRTE)', ISSN: 2277-3878 (Online), Volume-8 Issue-3, September 2019, pp. 8914-8919
5. V.Vijayagopal, Dr. K.Prabu, "Cronbach Alpha Based Reliability Factor-Based Mitigation Mechanism (CARFMM) for Energy and Trust Improved Routing Mechanism For MANETs", International Journal of Scientific & Technology Research (IJSTR) Volume 8 - Issue 10, October, 2019, pp.22-32.
6. B. Kailkhura, S. Brahma and P. K. Varshney, "Optimal Byzantine attacks on distributed detection in tree-based topologies," 2013 International Conference on Computing, Networking and Communications (ICNC), San Diego, CA, 2013, pp. 227-231.
7. Z. Sun, C. Zhang and P. Fan, "Optimal Byzantine Attack and Byzantine Identification in Distributed Sensor Networks," 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1-6.
8. S. Marano, V. Matta and L. Tong, "Distributed Detection in the Presence of Byzantine Attacks," in IEEE Transactions on Signal Processing, vol. 57, no. 1, pp. 16-29, Jan. 2009.
9. Lujie Zhong and Changqiao Xu, "Byzantine attack with anypath routing in wireless mesh networks," 2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), Beijing, 2010, pp. 711-715.
10. Lamba, G. K. (2016). Varying Number of Selfish Nodes based Simulation of AODV Routing Protocol in MANET using Reputation Based Scheme. International Journal Of Engineering And Computer Science, 1(2), 34-42.
11. Buttyan, and J. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks. ACM/Kluwer Mobile Networks and Applications (MONET) 8 (2003).
12. Fulai Liu, Ying Zhou, Zhenxing Sun, Ruiyan Du, & Juan Sheng. (2016). Dynamic attack probability based Spectrum Sensing against Byzantine attack in Cognitive Radio. 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2(1), 23-32.
13. Sengathir, J., & Manoharan, R. (2013). A split half reliability coefficient based mathematical model for mitigating selfish nodes in MANETs. 2013 3rd IEEE International Advance Computing Conference (IACC), 1(1), 32-43.
14. Usha, S., & Radha, S. (2011). Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks. International Journal of Computer and Electrical Engineering, 1(1), 524-528.
15. S. Zhong, J. Chen, and Y.R. Yang, Sprite - A simple, cheat-proof, credit-based system for mobile ad-hoc networks. Technical Report 1235, Department of Computer Science, Yale University (2002).
16. Demir, C., & Comaniciu, C. (2007). An Auction based AODV Protocol for Mobile Ad Hoc Networks with Selfish Nodes. 2007 IEEE International Conference on Communications, 1(1), 23-34.
17. Chong, Z., Tan, S., Goi, B., & Ng, B. C. (2012). Outwitting smart selfish nodes in wireless mesh networks. International Journal of Communication Systems, 26(9), 1163-1175.

AUTHORS PROFILE

Mr. V. Vijayagopal received his M.Sc and M.Phil from Madurai Kamaraj University, Madurai, India. Now doing his Ph.D research in Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India. His Research interested is Adhoc Networks, MANET. He has published more than 5 technical papers at various National / International Conferences and Journals.

Dr. K. Prabu received his MCA and M.Phil from Annamalai University, Chidambaram, India. He received his Ph.D Degree in Computer Applications from Manonmaniam Sundaranar University, Tirunelveli, India. He is now working as an Associate Professor in PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India. He is a Reviewer of 06 National/International Journals. His Research interested is Adhoc Networks, Wireless Networks & Mobile Computing, and Wireless Sensor Networks. He has published more than 75 technical papers at various National / International Conferences and Journals. He is a life member of ISTE, IACSIT, IAENG, and also senior member of IASED, and IRED.