IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Integrated Poisson and Hyper-exponential Bayesian Probabilistic Factor-oriented Efficient Routing Mechanism for MANETs

V.Vijayagopal[1*], K.Prabu[2]

[1,2]PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai, Tamilnadu, India

[*]*Corresponding Author: vijayagopal1976@gmail.com, Tel.: +91-9940311819*

Available online at: www.ijcseonline.org

Accepted: 06/Jul/2018, Published: 31/July/2018

Abstract— Reputation is considered as the significant reliability index for measuring the degree of participation rendered by each mobile node towards co-operation. Reputation decreases drastically under the influence of byzantine nodes as they intentionally drop maximum number of packets. Byzantine nodes decrease packet delivery rate and throughput of the network in spite of consuming network resources. The existing Bayesian conditional probability based mitigation approaches fail to utilize the benefits of conditional probabilistic distributions like Poisson and Hyper-exponential distribution for detection. This paper presents an Integrated Poisson and Hyper-exponential Bayesian Probabilistic Factor-based Mitigation Mechanism (IPHBFMM) for investigating the influence of byzantine nodes and mitigate them for ensuring better routing process. IPHBFMM is potential in combining two independent variables for discriminating co-operative nodes from byzantine nodes based on past and present behaviour. Simulation results proved that the energy consumptions and communication overhead of IPHBFMM is excellently minimized by 26% and 34% compared to the existing Bayesian probability-oriented techniques considered for analysis.

Keywords- Byzantine nodes, Poisson Factor, Hyper-Exponential distribution, Bayesian Probability. Co-operative Packet Forwarding Factor, Packet Forwarding Normalization Factor

I. INTRODUCTION

The establishment and maintenance of Mobile Ad hoc Network (MANET) is the optimal choice for various critical applications like military communication and disaster recovery operation in which infrastructure less communication is the only possibility [1]. But when the mobiles nodes in this kind of self-organized ad hoc network refuse to co-operate, i.e., behave in a byzantine manner, the core objective of an ad hoc network is even more crucial and the degree of survivability of network becomes a critical issue to be investigated [2]. The specific issue that is highly focused in this paper is the mobile nodes' trustworthiness in performing network layer functionalities of data forwarding. This act of packet forwarding is mainly achieved by routing packets through co-operative nodes rather than misbehaving nodes. Further, misbehaving mobile nodes may be co-operative for a time period but may suddenly change its behaviour into byzantine node depending on the unfavourable situation like energy scarcity prevailing in them [3]. Therefore, a mobile node may initially agree to forward packets but later fails to carry out its activities due to its byzantine behaviour. Hence, it is evident that byzantine nodes utilize maximum network resources but refuse to forward packets for their neighbouring nodes [4]. Thus byzantine nodes invalidate the premise of co-operation in maximum of the routing algorithms proposed for MANET. Moreover, maintaining co-operation between mobile nodes in the presence of byzantine node is a challenging issue because, i) ad hoc network fails to possess a well-defined line of defence than its wired and infrastructure counterpart and ii) the topology of MANET is unpredictable and energy-constrained in nature [5]. Furthermore, considerable number of reputation-based mitigation approaches contributed for preventing byzantine nodes fails to consider past or present behaviour of mobile nodes for detecting byzantine nodes [6-8].

This paper presents Integrated Poisson and Hyper-exponential Bayesian Probabilistic Factor-based Mitigation Mechanism (IPHBFMM) for investigating the influence of byzantine nodes that intentionally crumbles the resilience of the network. IPHBFMM uses Poisson and Hyper-exponential distribution parameters as they are predominant and capable in discriminating genuine nodes from byzantine nodes as they can combine two independent variables that influence the past and current behaviour of mobile nodes. The simulation study of IPHBFMM is also performed for quantifying its excellence in mitigating byzantine nodes on par with the compared byzantine prevention techniques.

Extract of the Literature

From the literature survey, it is identified that conditional probabilistic detection approaches are considered to be superior to history-based detection mechanisms. Since they facilitate the detection of byzantine behaviour by monitoring the current characteristics of mobile nodes based on the assumption that they are reliable in the past. But most of the conditional probabilistic mitigation approaches available in literature address byzantine nodes by calculating conditional probability using naive probability, Bayes probability or Dempster Shafer theory of evidences. It is evident that they have not utilized any advanced conditional probabilistic techniques like Poisson and Hyper-Exponential distribution for computing reputation of mobile nodes. Moreover, Poisson and Hyper-Exponential distribution based reliability factor estimation is identified as the predominant conditional probability computation techniques that possess the capability of integrating two independent events of nodes' behaviour [19-20]. Hence, IPHBFMM is proposed for effectively identifying and isolating byzantine nodes by utilizing the merits of Poisson and Hyper-Exponential distribution for reliability factor estimation.

II. PROPOSED IPHBFMM

IPHBFMM is a reliability factor-based mitigation mechanism that derives the benefits of Poisson factor for effectively mitigating byzantine nodes. In IPHBFMM, the mitigation of byzantine nodes are facilitated through four steps viz., a) Estimation of Co-operative Packet Forwarding Factor (CPFF), b) Computation of Poisson Factor-based density function for mobile nodes based on CPFF, c) Calculation of joint density function for integrating discrete and continuous probability mass function of mobile nodes and d) Detection and isolation of byzantine nodes using computed Bayesian Conditional Probabilistic Poisson Factor (BCPPF).

a) Estimation of Co-operative Packet Forwarding Factor (CPFF)

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

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

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 receiving 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

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

Then the Co-operative Packet Forwarding Factor (CPFF) which quantifies the cumulative impact of both packet forwarding and packet receiving capability of mobile node is calculated using

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

b) Computation of Poisson Factor-based density function for mobile nodes based on CPFF

The computation of Poisson varied density function is based on the use of mixed distribution that employs the combination of discrete and continuous behaviour of mobile nodes. The mixed distribution is used mainly because the survivability of mobile nodes mainly depends on discretely or continuously changing source of influence originated by byzantine attacks.

Initially the discrete behaviour of mobile nodes are analysed based on Poisson distribution. In general the behaviour of mobile nodes towards routing depends on the availability of energy possessed by them. The amount of energy possessed by each mobile node is

$$AV_{energy} = \frac{E_U}{R_A} \quad (10)$$

Where AV_{energy}, E_U and R_A represents the amount of available energy, utilized energy and residual energy of the mobile nodes. This energy parameter AV_{energy} is exponentially distributed the probability mass function $DP_{s(i)}$ of survivability of mobile node is

$$DP_{s(i)} = e^{AV_{energy}} \left(\frac{(AV_{energy})}{PFNF}^{PFNF}\right) \quad (11)$$

In this context, PFNF denotes the Packet Forwarding Normalization Factor which is computed based on CPFF. This PFNF is normalized between the ranges of 1 to 100.

Next, the behavioural analysis of mobile nodes is performed based on continuous distribution that inspires exponential distribution. The exponential distribution based probability mass function $CP_{s(i)}$ for identifying the resilience rate of mobile nodes of the network is

$$CP_{s(i)} = \kappa(1 - P_{FC})^{\kappa - 1} \quad (12)$$

Where 'P$_{FC}$ 'and 'k' represents the packet forwarding capability and constant mean rate of packet delivery.

c) Estimation of joint density function for integrating discrete and continuous probability mass function of mobile nodes

The two probability mass functions called $DP_{s(i)}$ and $CP_{s(i)}$ are integrated into an integral value to quantify the impact of discrete and continuous analysis of life time of mobile nodes using

$$IP_{s(i)} = DP_{s(i)} * CP_{s(i)} \quad (13)$$

Further, the Complementary Bayesian Probabilistic Poisson Factor (CBPPF) which quantifies the reliability of the routing path based on $IP_{s(i)}$ is

$$CBPPF = \sum_{r=1}^{c} IP_{s(r)} \quad (14)$$

Furthermore, the reliability of both the mobile nodes (m) and their resilient routing path(r) is expressed based on BPPF as

$$BPPF(m,r) = (1 - CPPF(m,r)) \quad (15)$$

d) Detection and isolation of byzantine nodes using Bayesian Probabilistic Poisson Factor (BPPF)

The value of BPPF aids in deciding the contribution level rendered by the mobile nodes towards packet forwarding ability is evaluated based on their discrete and continuous behavioural parameters. The detection and isolation of byzantine nodes is triggered when the conditional probabilistic threshold of 0.35 is identified (obtained through simulation and portrayed through Table 1)

III. Conditional Probabilistic Poisson Factor based Mitigation (IPHBFMM) algorithm

The following algorithm 5.1 illustrates the steps involved in detecting byzantine nodes using BPPF and isolating them from the routing path.

Algorithm 1. Conditional Probabilistic Poisson Factor based byzantine node detection and isolation

1. Let the number of nodes in the network be N.
2. GN–Group of nodes of the routing path, in which two significant nodes are labelled as SN (source node) and DN (destination node) respectively.
3. Set of nodes in the routing path can be established by sending `RREQ' message by the SN to all other nodes in the network
4. Mobile nodes which are ready for data transmission replies to the source node by `RREP' message.

5. Let the algorithm steps (6 -19) be executed for a node say, u, which belongs to the list GN, that uses 't' number of sessions for transmission.
6. for every node 'u' of GN in the routing path.
7. Calculate Expected Packet Forwarding Potential ($EPFP_e$) using $EPFP_e = P_{PFC(1)} * P_{PFC(2)} * ..... * P_{PFC(k)}$
8. Calculate Expected Packet Receiving Potential ($EPRP_e$) using $EPRP_e = P_{PRC(1)} * P_{PRC(2)} * ..... * P_{PRC(k)}$
9. Compute CPFF based on $EPFP_e$ and $EPRP_e$ using $CPFF = ((EPFP_e * EPRP_e) + ((1 - EPFP_e)(1 - EPRP_e)))$
10. Calculate the availability of energy possessed by the mobile node towards routing using $AV_{energy} = \frac{E_U}{R_A}$
11. Estimate discrete probability mass function $DP_{s(i)}$ for survivability of mobile node using $DP_{s(i)} = e^{AV_{energy}}(\frac{(AV_{energy})}{PFNF}^{PFNF})$ through Poisson distribution.
12. Estimate continuous probability mass function $CP_{s(i)}$ that identifies resilience of mobile nodes using $CP_{s(i)} = \kappa(1 - P_{FC})^{\kappa-1}$ based on exponential distribution.
13. Integrate discrete and continuous mass functions $DP_{s(i)}$ and $CP_{s(i)}$ for quantifying the lifetime of mobile nodes using $IP_{s(i)} = DP_{s(i)} * CP_{s(i)}$
14. Compute CBPPF using $CBPPF = \sum_{r=1}^{c} IP_{s(r)}$ for estimating the reliability of the routing path based on reliability of mobile nodes.
15. Calculate reliability of mobile nodes and their participating resilient routing path using $BPPF(u) = (1 - CPPF(u))$
16. If (BPPF (u) < 0.35) then
17. Node u is byzantine compromised
18. Call Byzantine-Mitigation (u)
19. Else
20. Node u is reliable.
21. End if
22. End for
23. End for.

IV. ILLUSTRATIONS

In this sub-section, the working of IPHBFMM is illustrated by considering 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 Figure 1. In IPHBFMM, 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 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 using the cumulative sum of data packets forwarded by the node to their interacting neighbours.

Scenario 1: When mobile nodes drops moderate number of packets

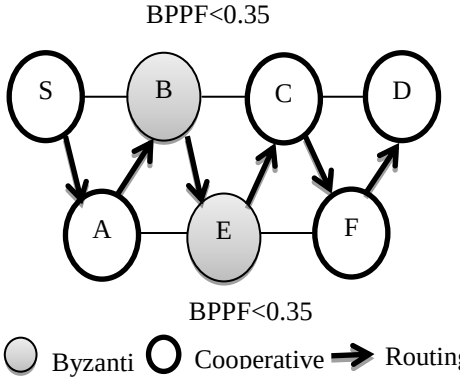

Figure 1-Mobile nodes dropping moderate number of packets

For instance, let the sum of packets actually received by node 'B' from source node 'S' is 1000. The actual number of packets forwarded by mobile node 'B' to its neighbouring nodes as monitored by A, C, E is 850, 650 and 750 respectively. Thus the mean deviation experienced is 150,350 and 200. Hence, the mean packet deviation of node 'B' as recommended by A, C, E is 233. Then the value of BPPF for node ' B' is determined as 0.3 as the CBPPF's for the node B is was estimated to be 0.69. Hence the node 'B' is towards byzantine behaviour in routing.

Scenario 2: When mobile nodes drops maximum number of packets

Similar to scenario 1, let '1000' be the sum of packets received by B from source node 'A'. In this context, the number of packets forwarded to their neighbours A, C and E are 600, 500 and 400 respectively**.** Then the mean deviations experienced are 400,500 and 600 respectively. Hence, the

mean packet deviation of node 'B' as observed by A, C, E is 500.

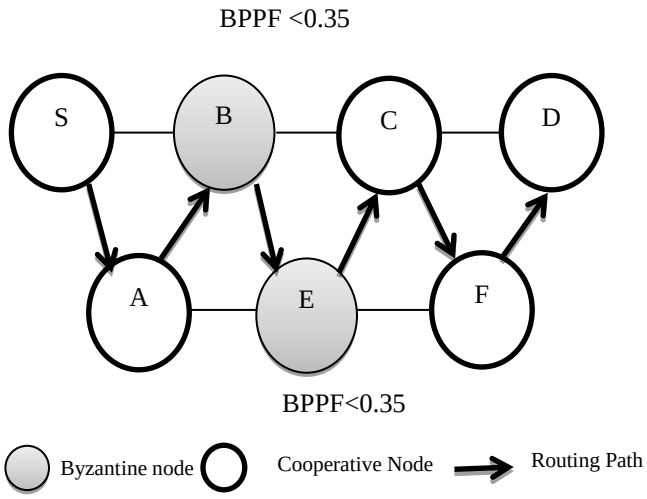

Figure 2-Mobile nodes dropping maximum number of packets

Then Reliability Factor CBPPF for the node B is determined to be 0.81 and hence BPPF is estimated at 0.19. Hence the node 'B' exhibits byzantine behaviour in routing.

V. SIMULATION-BASED EXPERIMENTAL EVALUATION OF IPHBFMM

The importance of IPHBFMM in mitigating Byzantine nodes is determined based on its comparison with the techniques of BGABMT, NMSBCKF and SARP. The significance of IPHBFMM is investigated using evaluation parameters such as energy consumptions, detection rate, packet drop, increase in communication overhead and accuracy rate of detection based on different number of benevolent nodes, number of attacker nodes, pause time and pairs of source and destination. The simulation parameters set up used for comparative analysis is detailed as follows.

Simulation Environment

Simulation experiments for IPHBFMM, BGABMT, NMSBCKF and SARP are conducted using the network simulator version ns-2.34. For investigating the performance of IPBHFMM, BGABMT, NMSBCKF and SARP, the network topology containing 100 nodes are created for the nodes to exhibit random motion and move around the terrain area of 1500x1500 meters. The mobile nodes in the simulated network are considered to possess 150 joules of energy out of which 15 joules of energy are used for each round of communication. In addition, Table 1 unveils some of the significant simulation parameter used for comparative study of IPHBFMM with BGABMT, NMSBCKF and SARP.

Table 1-Significant simulation parameters used for implementing IPHBFMM

Simulation Parameters	Simulation Parameter Values
Routing Protocol	AODV
Channel capacity	2 Mbps
CBR(Constant Bit Rate) rate	50 packets/second
Capacity of queue in MAC layer	40 packets
Minimum And Maximum Variation in CBR	5 packets to 50 packets/ second
Mobility Speed	10 meter/second
Size of packets	512 bytes

Results and Discussions

Initially, the conditional probabilistic threshold of 0.35 is determined based on empirical results estimated using different thresholds of detection probability. Table 1 demonstrates and identifies the reason for choosing conditional probabilistic threshold as 0.35 for Byzantine attack detection. Table 1 also emphasis the percentage of attacker nodes detected as byzantine under different detection probabilities varied from 0.20 to 0.50 under implementation.

Table 1- Determination of Bayesian conditional probabilistic threshold for IPHBFMM

Byzantine Prevention Scheme	Detection probability (0.41-0.50)	Detection probability (0.36-0.40)	Detection probability (0.30-0.35)	Detection probability (0.20-0.29)
IPHBFMM	61%	68%	93%	72%
BGABMT,	53%	56%	78%	63%
NMSBCKF	45%	48%	66%	56%
SARP	38%	42%	60%	48%

The significance of IPHBFMM is then studied using energy consumptions, throughput and communication overhead under different number of benevolent nodes. Figure 3, 4 and 5 bespeak the performance of IPHBFMM using energy

consumptions, communication overhead and throughput based on different number of benevolent nodes. The energy consumptions of IPHBFMM infers to be excellent than the compared BGABMT, NMSBCKF and SARP approaches by 22%, 18% and 14% since the energy utilized by the mobile nodes for forwarding data in the network is minimized due to the rapid updating of continuous and discrete information related to the current and past characteristics of mobile nodes during interaction. Likewise, the communication overhead of IPHBFMM is also estimated to be decreased to an appreciable level by 26%, 23% and 17% as the re-transmission of data packets is reduced due to fast update of reputation corresponding to the nodes of the network. Similarly, the throughput of the network based on the deployment of IPHBFMM is determined to be substantial by an appreciable margin of 20%, 17% and 12% respectively as the act of packet delivery is facilitated with greater reliability in the network.

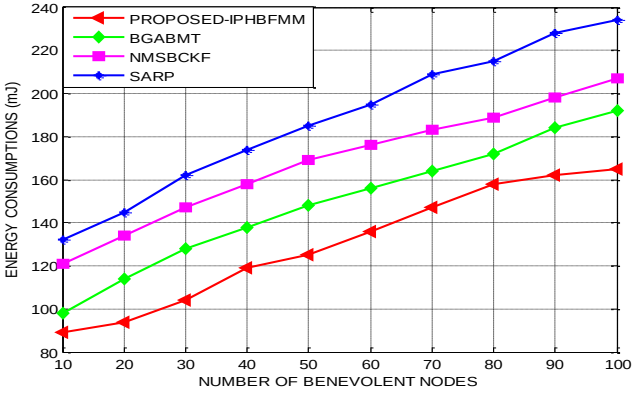

Figure 3: IPHBFMM-energy consumptions-different benevolent nodes

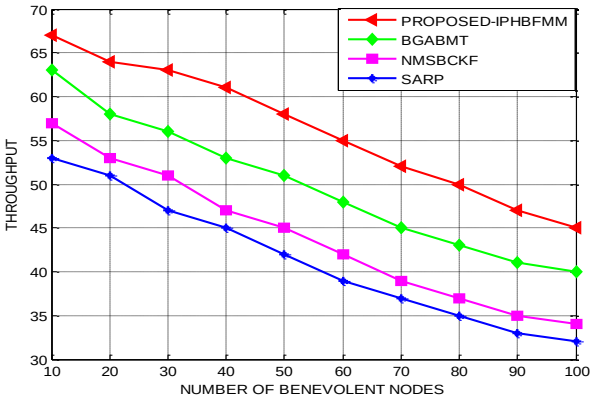

Figure 4: IPHBFMM-throughput-different benevolent nodes

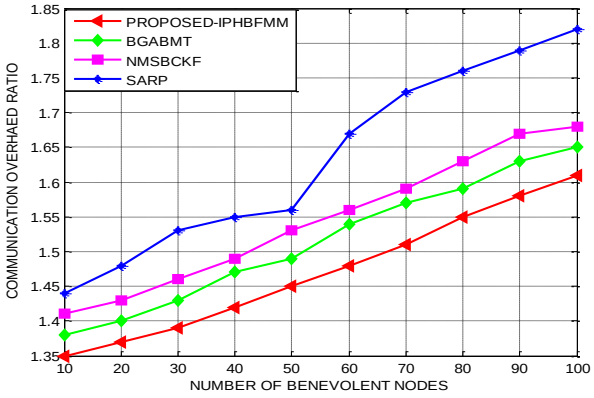

Figure 5: IPHBFMM-communication overhead ratio-different benevolent nodes

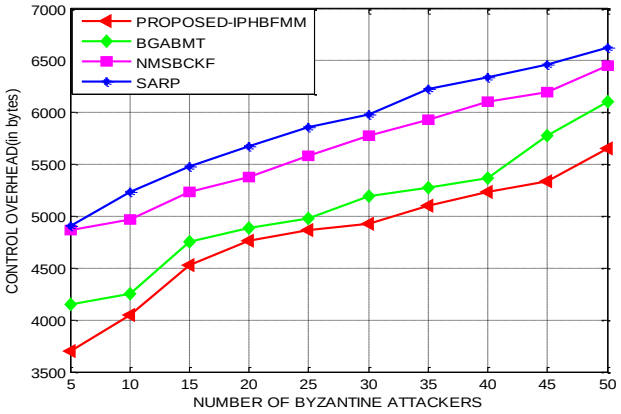

Figure 6: IPHBFMM-control overhead-byzantine attackers

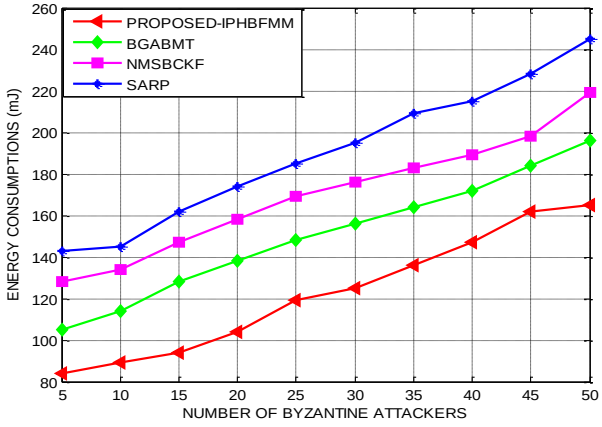

Figure 7: IPHBFMM-energy consumptions-byzantine attackers

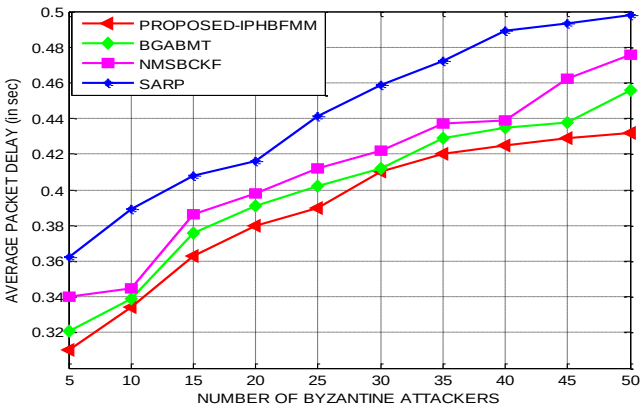

Figure 8: IPHBFMM-average packet delay-byzantine attackers

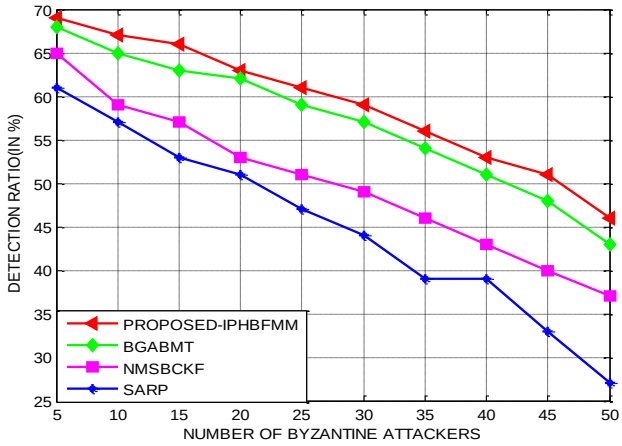

Figure 9: IPHBFMM-detection ratio-byzantine attackers

Further, the importance of IPHBFMM is then studied using control overhead, energy consumptions, average end-to-end delay and Detection ratio under the influence of different number of byzantine attackers. Figure 6, 7, 8 and 9 manifests the performance of IPHBFMM using control overhead, average end-to-end delay and detection ratio studied based on different numbers of byzantine attackers. The control overhead of the proposed IPHBFMM scheme is minimzed by 21%, 16% and 13% superior to the compared BGABMT, NMSBCKF and SARP approaches.The energy consumptions of the proposed IPHBFMM scheme is reduced predominatly by 24%, 20% and 16% better to the compared approaches. Likewise, the proposed IPHBFMM scheme reduces the average end-to-end delay by 31%, 26% and 21% optimal to the compared baseline approaches. In addition, the detection ratio is improved by 26%, 21% and 16% better to the benchmarked schemes utilized for investigation.

VI. CONCLUSION

The proposed IPHBFMM was an attaempt for reliable detection of byzantine nodes that degrades the packet forwarding capability of the mobile nodes under routing. The core merits of the conditional probability factor which is estimated based on Bayesian probability is considered as the vital decisive parameter for reliable detection of byzantine attacker nodes. The simulation results of the proposed IPHBFMM scheme confirmed an average 16% superiority in term of throughput and packet delivery ratio. The results of IPHBFMM scheme also highlighted a predominant minimization in the mean control overhead, average energy consumption and mean packet latency of 23%, 21% and 17% compared to the benchmarked schemes. The computational complexity of the proposed IPHBFMM scheme was confirmed to be essential over the compared BGABMT, NMSBCKF and SARP techniques. In the near future, it is planned to formulate a novel Fleiss Kappa Reliability-based mitigation scheme that rapidly and influentially detects and eliminates Byzantine attacker compromised node from the network for enforcing cooperation.

References

[1] Buttyan, L and Hubaux, J-P, (2003) 'Stimulating Coperation in Self–organizing Mobile Ad hoc Networks', MONET Journal of Mobile Computing and Networking, Vol. 8, No. 1, pp. 579-592.

[2] Marti, S, Gulli, T.J, Lai, K and Baker, M, (2000) 'Mitigating routing misbehaviour in mobile ad hoc networks Mobile Computing and Networking', in Proc., 6th ACM Annual International Conference on Mobile Computing and Network (ACM-MobiCom), Boston, USA, Vol. 1, No. 1, pp. 255-265.

[3] Pusphalatha, M, Revathy, V, Rama Rao, P, (2009), 'Trust based Energy aware reliable reactive protocol in mobile ad hoc networks', World Academy of Science, Engineering and Technology, vol. 3, no. 27, pp. 335-338.

[4] Rizvi, S and Elleithy, M, (2009) 'A new scheme for minimizing malicious behavior of mobile nodes in Mobile Ad Hoc Networks', Internation Journal of computer Science and Information Security, Vol.. 3, No. 1, pp. 25-34.

[5] Michiardi, P and Molva, R, (2002) 'CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks', in Proc., 6th IFIP Conf. on Security, Communications and Multimedia, Protoroz, Solvenia, vol. 228, no. 1, pp. 107-121.

[6] S. Goswami and S. Das, (2014),"A probabilistic approach to detect selfish node in MANET," International Journal of Computer Applications, vol. 3, no. 1, pp.23-26.

[7] B. Wang, S. Soltani, J. K. Shapiro, and P. T. Tan, \Local detection of selfish routing behavior in ad hoc networks," in Proceedings of International Symposium on Parallel Architectures, Algorithms and Networks, vol. 2, no. 3, pp 23-34, December 2005.

[8] Buchegger, S and Boudec, J-Y, (2002), 'Performance Analysis of the CONFIDANT protocol: Cooperation of Nodes – Fairness in Distributed Ad-hoc Networks', in Proc., 3rd ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc '02), New York, USA, Vol. 1, No. 1, pp. 226-236.

[9] Kargl, F, Klenk, A,.Schlott, S and Weber, M, (2004), 'Advanced Detection of selfish or Malicious Nodes in Ad hoc Networks', in Proc.,

First European Workshop on Security in Ad-Hoc and Sensor Network (ESAS 2004), Heidelberg, Germany, Vol. 1, No. 1, pp. 255-263.

[10] B. Kailkhura, Y. S. Han, S. Brahma and P. K. Varshney, (2015) "Asymptotic Analysis of Distributed Bayesian Detection with Byzantine Data," in *IEEE Signal Processing Letters*, vol. 22, no. 5, pp. 608-612.

[11] C. Hortelano, T. Calafate, J. C. Cano, M. de Leoni, P. Manzoni, and M. Mecella,(2010), "Black-hole attacks in p2p mobile networks discovered through Bayesian Filters," Proceedings of OTM Workshops, vol. 2, no. 6, pp. 543-552.

[12] B.G. Chun, K. Chaudhuri, H. Wee, M. Barreno, C. H. Papadimitriou, and J. Kubiatowicz, \Sel_sh caching in distributed systems: A game-theoretic analysis," in Proceedings of the 23th Annual ACM Symposium on Principles of Distributed Computing, vol. 7, no. 4, pp. 21-30, November 2004.

[13] B. Wang, S. Soltani, J. K. Shapiro, and P. T. Tan, "Local detection of selfish routing behavior in ad hoc networks," in Proceedings of International Symposium on Parallel Architectures, Algorithms and Networks, vol. 2, no.3, pp 23-34, December 2005.

[14] Chen, T.M, Varatharajan, V, (2009), 'Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks', IEEE Internet Computing, vol. 3, no. 1, pp 234-241.

[15] Sengathir, J., & Manoharan, R. (2015). Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs. *Egyptian Informatics Journal*, *16*(2), 231-241.

[16] N. M. Webb, J. Richard, Shavelson, and E. H. Haertel, (2006), "Reliability Coefficients and Generalizability Theory", Handbook of Statistics. Elsevier press, vol. 26.

[17] Steutel, F. W, and Harn, V. K, (2004)." Infinite divisibility of probability distributions on the real line". MarcerDekkar, 2004.

[18] Annapourna, P Patil, Rajani Kanth, Bathey Sharanya,Dinesh Kumar, M.P, Malavika, J, (2011) 'Design of Energy Efficient Routing protocols for MANETs', International Journal of Computer Science Issues, vol. 8, no. 1, pp. 215-220.

[19] Hernandez-Orallo, Manuel, D, Serraty, Juan-Carlos Cano, Calafate, T and Manzoni's, (2012) 'Improving Selfish Node Detection in MANETs Using a collaborative Watchdog', IEEE Communication Letters, Vol. 16, No.5, pp.

[20] Sengathir, J., & Manoharan, R. (2015). A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs. *EURASIP Journal on Wireless Communications and Networking*, *2015*(1).

