International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Trust and Energy-Inspired Threshold Packet Relaying Capability Technique (TEITPRCT) for Reliable Routing in MANETs

V. Vijayagopal, K. Prabu

Abstract*: The data dissemination in MANET completely depends on the packet relaying capability attributed by the mobile nodes of the network. This packet relaying potential of the mobile node completely depends on the energy possessed by the mobile nodes. In this paper, a Trust and Energy-Inspired Threshold Packet Relaying Capability Technique (TEITPRCT) is proposed for achieving reliable data forwarding in the network. This proposed TEITPRCT approach utilized the benefits of factors that includes Frequency Index of Interaction (FII), Intimacy Index (II) and Honesty Index (HI) for quantifying the trust attributed by each mobile node in the network. It also inherently estimates the energy possessed by the mobile nodes of the network through the utilization of probe packets. The simulation experiments are conducted using ns-2 based on evaluation metrics that include throughput, latency, and energy consumptions with respect to different mobile nodes of the network. The simulation results proved the potentiality of the proposed TEITPRCT approach over the other benchmarked schemes considered for investigation.

Keywords* : Mobile Ad hoc NETworks (MANETs), Frequency Index of Interaction (FII), Intimacy Index (II), Honesty Index (HI), Energy.

I. INTRODUCTION

Dynamic modifications in network topologies, restricted battery capacity and unreliable nature of wireless links pose a major challenge for reliable routing in MANET [1]. The selection of long-lasting stable path is an important routing issue in MANET [2-4]. The open infrastructures of MANET make it vulnerable to a wide range of attacks [5-7]. These attacks are mainly due to the dynamic network topology and constrained energy of mobile nodes [8]. The attacks are divided into external attacks and internal attacks. A number of mitigation schemes were proposed in the literature with the aimed of detecting and preventing external attacks [9-11]. But the majority of the external attack mitigation techniques fail to achieve the detection when malicious nodes have entered into the network and specific nodes of the network are compromised by attacker [12].

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
V.Vijayagopal*, Research Scholar, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India.
Dr. K.Prabu, Associate Professor, PG & Research Department of Computer Science, Sudharsan College of Arts & Science, Pudukkottai – 622104, Tamilnadu, India.

In this paper, a Trust and Energy-Inspired Threshold Packet Relaying Capability Technique (TEITPRCT) is proposed for facilitating reliable data forwarding in the network by isolating malicious nodes. This proposed TEITPRCT approach is contributed by estimating the factors such as the Frequency Index of Interaction (FII), Intimacy Index (II) and Honesty Index (HI). These three factors were used for evaluating the degree of trust attributed by each mobile node in the network. The simulation experiments are conducted using ns-2 to performance the metrics of throughput, latency, and energy consumptions with respect to different mobile nodes and malicious adversaries in the network. The simulation experiments are also conducted using packet drop rate and false alarm rate under an increasing number of malicious adversaries and CBR connections established in the network.

II. RELATED WORK

From the recent past, a considerable number of energy and trust-based routing approaches were formulated in the literature. In this section, some of the predominant approaches are reviewed based on their merits and limitations.

Ermis et al [13] devise new measures that have the capability for adapting the behaviour of a node with respect to the mobility factor of neighbour nodes in MANET to design a routing protocol. The authors used scope of per-hop Round Trip Time (RTT) related to the time duration of a node for sending a probe packet and receiving the same from its 1-hop neighbors. Then Sarkar et al [14] explored the distribution of the probe as well as probe acknowledgement packets to get RTT values in a regular time which leads to high bandwidth consumption and more network contention. However, it is not suitable for dynamic and dense networks. Chen et al [15] proposed a new metric known as contact-related mobility metric based on the idea of encountering of nodes. Two nodes are said to encounter each other while the distance between the two nodes is found to be lesser than the transmission range. Santhi et al [16] propounded a new metric called ETX, which assists a routing technique to identify the path which offers high throughput. ETX of a link is measured in terms of the expected number of transmissions required for data communication over the link between two nodes for sending a packet and also including retransmissions in the MAC layer.

Another method using Mobility Factor (MF) was proposed by Dhananjayan et al [17] proposed a T2AR: trust-aware ad-hoc routing protocol in order to include the properties of the protocols as one of the criteria. In such protocols mobility is measured by means of preserving the neighbor's history resulting in more number of control packets and more complexity in maintenance of long queue of neighbors. Yasin et al [18] contributed a detection mechanism using a new metric namely Active Interactive Rate (AIR) has been introduced as a measure in the proposed routing protocol. In the proposed approach the source node selects the neighbor node based on AIR offering the best metric towards the destination. This scheme only uses the local knowledge of the neighbourhood similar to position based routing. The main advantage is the increase network scalability which is a major constraint in large and dense Mobile Ad hoc Networks. Rajesh Babu et al., [19] proposed a detection approach termed Novel Honeypot Based Detection and Isolation Approach (NHBADI) based on energy metric. This energy metric is quantified using energy consumption due to transmission, reception and overhearing is considered for neighborhood selection, then there exist two approaches. The first is that it always selects the same node with minimum power dissipation which results in a sharp reduction of battery energy. In addition, Merlin et al., [20] proposed an approach named Novel Trust Based Energy Aware Routing Mechanism (NTEARM) that enables non-uniform energy consumption among the nodes. Therefore, the minimum energy drain rate is considered. The authors formulated and used the energy metric based on the residual energy and the initial energy of the node.

III. TRUST AND ENERGY-INSPIRED THRESHOLD PACKET RELAYING CAPABILITY TECHNIQUE (TEITPRCT)

In TEITPRCT, the malicious adversaries are detected effectively based on the utilization of three Trust parameters (TR) called Frequency Index of Interaction (FII), Intimacy Index (II) and Honesty Index (HI). All the three factors are computed based on the past experiences derived through the interaction of each mobile node to the directly connected communicating nodes for sustaining reliable data dissemination.

Computation of Frequency Index of Interaction (FII),

The Frequency Index of Interaction (FII) refers to the degree of interaction or number of interactions that exists between the nodes of the network. This FII is determined using the probe packets that are sent from the source to the destination nodes of the network. In this context, the probe packets help the monitoring nodes to estimate the degree of interaction made feasible by the monitored node at any particular point of time. The maximum number of interactions between the monitored nodes and its closer neighbouring monitoring node infers better FII. Thus FII is calculated using Equation (1) which is the ratio of maximum number of interactions existing between the monitored and the monitoring nodes ($M_{n(i)}$) to the cumulative number of interactions made possible by the monitored node to the other nodes of the network except the monitoring node (N_T).

$$TR_i^{FII} = \frac{M_{n(i)}}{N_T} \quad (1)$$

Calculation of Intimacy Index (II)

Index of Intimacy (II) is the second factor essential for the computation of mobile nodes' trust. This II determines the time period in which the interaction between the monitored nodes and the monitoring nodes is maximum on par with the time period of interactions happening between the monitored nodes and the other neighbouring nodes of the network. Thus II computed using Equation (2) represents the time incurred in the interaction between the monitored nodes and the monitoring nodes ($CTS_{l,m}$) to the cumulative time spent for interaction among the monitored node and their interacting nodes ($CTS_{l,n}$) of the network.

$$TR_i^{II} = \frac{CTS_{l.m}}{CTS_{l,n}} \quad (2)$$

Calculation of Honesty Index (HI)

Index of Honesty **(**HI) is the third factor used for quantifying the trust of the mobile nodes which is estimated using Equation (3) through the positive and negative interactions of the monitored mobile based on the viewpoint of the monitoring mobile nodes.

$$TR_i^{HI} = \frac{f_i}{f_i + g_i} \quad (3)$$

Where ' f_i ' and ' g_i ' represents the positive and negative interactions existing between the monitored and the monitoring mobile nodes of the network. Then, the Cumulative Trust Factor (CTF) for quantifying a node as benevolent or malicious is determined based on Equation (4)

$$CTF_i = \alpha TR_i^{FII} + \beta TR_i^{II} + \gamma TR_i^{HI} \quad (4)$$

Finally, the estimated CTF is compared with the computed threshold parameter which is discussed in the forthcoming section.

Computation of threshold Parameter

The estimation of the Threshold parameter (TH_p) also depends on the past experience of the mobile node. This past experience relates to the activity of the mobile node monitored over the number of session time ' k ' till the recent past. Thus the threshold parameter is calculated based on Equation (5)

$$TH_p = \frac{\sum_{s=1}^{k} PD_C}{k} \quad (5)$$

Where PD_c refers to the Packet Delivery capability of the mobile nodes during the process of data dissemination. In this context, if the value of CTF_i is less than TH_p then the specific node is determined as malicious during data dissemination.

Algorithm of the proposed TEITPRCT scheme

Input: Node N_i, N_j….N_n Clock Synchronization time t_n
Output: Malicious Node Detection
Begin:

for {i=0; i<n; incr i}
{
N_i broadcasts → R_{REQ} to n node // time t1
Receive R_{REQ} ← N_n // time t2
N_n send → R_{REP} N_i // time t3
Receive R_{REP} ← N_i // time t4
Calculate $CTF_i = \alpha TR_i^{FII} + \beta TR_i^{II} + \gamma TR_i^{HI}$ based on the estimation of FII, II and HI and Trust (TR)
}
{
Calculate the threshold parameter using

$$TH_p = \frac{\sum_{s=1}^{k} PD_C}{k}$$

If ($CTF_i > TH_p$)
{
Normal Node
}
Else
{
Abnormal Node
}

End If
End For
End.

IV. SIMULATION RESULTS AND DISCUSSION

The significance of the proposed TEITPRCT scheme is determined by conducting simulation experiments using the network simulator (ns-2.34). This simulation setup used for implementing the proposed TEITPRCT scheme comprises of the network terrain area of 1500x1500 with 200 mobile nodes under the random motion in the network. The simulation parameters used for the deployment of the proposed TEITPRCT scheme are tabulated in Table 1.

Table 1: TEITPRCT Simulation Setup Parameters

Parameters	Values
Mobile nodes	200
Antenna type	Omni Antenna
Mobility model	Random Way Point
Model of Radio Propagation	Two Ray Ground
Traffic model	Constant Bit Rate (CBR)
Time for Simulation	250 secs
Transmission Range	250m

In the first fold of investigation, the predominance of the proposed TEITPRCT scheme is evaluated based on throughput, energy utilizations and average latency by varying the mobile nodes of the network. Figure 1 demonstrates plots of throughput related to the proposed TEITPRCT scheme compared with the baseline NTEARM, T2AR and NHBADI approaches. The throughput of the proposed TEITPRCT scheme is comparatively high compared to the benchmarked schemes independent to the number of mobile nodes of the network, since the utilization of contextual parameters plays an anchor role in identifying the trustworthiness of mobile nodes that directly influences their forwarding capability. Thus, the throughput of the proposed TEITPRCT scheme is improved by 10%, 13% and 16%, on par with the NTEARM, T2AR and NHBADI approaches. Figure 2 and 3 exemplars the plots of energy consumption and latency associated with TEITPRCT scheme and the compared NTEARM, T2AR and NHBADI approaches. The energy consumptions of the proposed TEITPRCT scheme is determined to be highly sustained even when the number of mobile nodes is increased in the network. This significant performance of the proposed TEITPRCT scheme with respect to energy consumptions is mainly due to the inclusion contextual energy factor that aids in balancing the energy of individual mobile nodes. Similarly, the packet latency of the network is also realized to be comparatively minimized even when the number of mobile nodes is increased, since the link stability of the wireless links is also quantified in terms of energy and trust. Thus, the energy consumptions of the proposed TEITPRCT scheme are minimized by 9%, 14% and 17%, on par with the NTEARM, T2AR and NHBADI approaches. The packet latency of the proposed TEITPRCT scheme is also minimized by 11%, 13% and 15%, on par with the NTEARM, T2AR and NHBADI approaches.

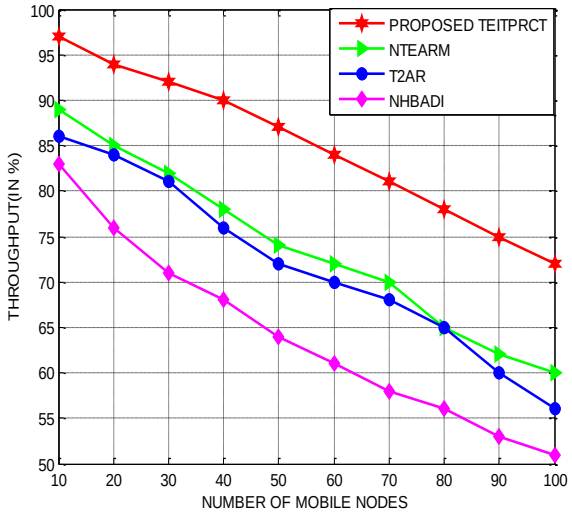

Figure 1: TEITPRCT-Throughput-Different Number of Mobile Nodes

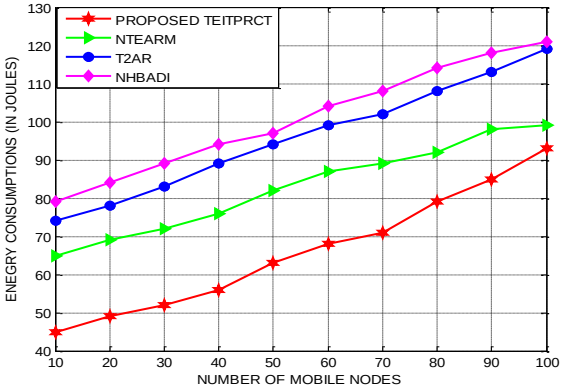

Figure 2: TEITPRCT-Energy Consumptions-Different Number of Mobile Nodes

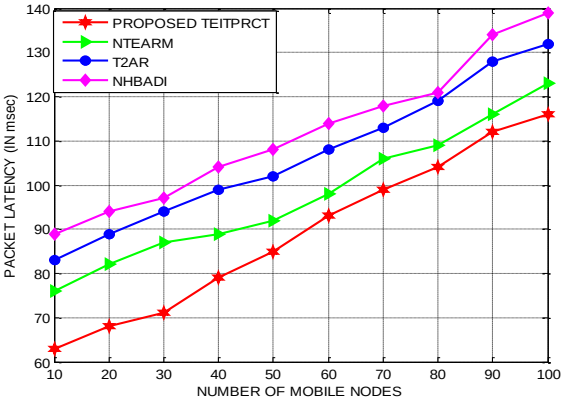

Figure 3: TEITPRCT-Latency - Different Number of Mobile Nodes

In the second fold of investigation, the predominance of the proposed TEITPRCT scheme is evaluated based on throughput, energy utilizations and average latency by varying the number of malicious adversaries in the network. Figure 4 glorifies the plots of throughput related to the proposed TEITPRCT scheme compared with the baseline NTEARM, T2AR and NHBADI approaches evaluated with respect to the increasing number of malicious adversaries. The throughput of the proposed TEITPRCT scheme is comparatively high compared to the benchmarked schemes independent to the number of malicious adversaries compromised in the network, since the use of energy and trust factor aids in the significant categorization of mobile nodes into genuine and malicious nodes. The throughput of the proposed TEITPRCT scheme with different malicious adversaries is enhanced by 13%, 15% and 19%, on par with the NTEARM, T2AR and NHBADI approaches. Figure 5 and 6 demonstrates the plots of energy consumption and latency associated with TEITPRCT scheme and the compared NTEARM, T2AR and NHBADI approaches with different count of malicious adversaries. The energy consumptions of the proposed TEITPRCT scheme are determined to be phenomenally maintained inspite of increasing malicious adversaries, since it incorporates a flexible detection strategy depending on the change in malicious nodes of the network. Further, the packet latency of the network under different number of malicious adversaries is also realized to be comparatively reduced, since the routing of data packets through malicious nodes designated through energy and trust is maximally included. Thus, the energy consumptions of the proposed TEITPRCT scheme under different malicious adversaries are minimized by 7%, 10% and 13%, on par with the NTEARM, T2AR and NHBADI approaches. The packet latency of the proposed TEITPRCT scheme under different malicious adversaries are also minimized by 9%, 12% and 14%, on par with the NTEARM, T2AR and NHBADI approaches.

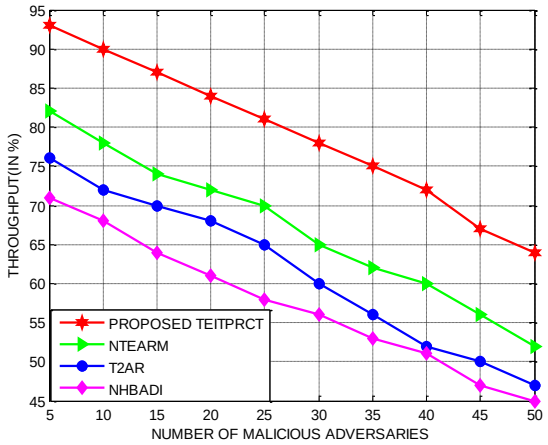

Figure 4: TEITPRCT-Throughput-Different Number of Malicious Adversaries

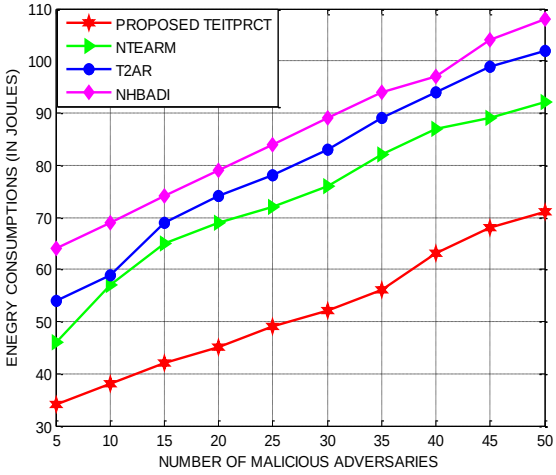

Figure 5: TEITPRCT-Energy Consumptions - Different Number of Malicious Adversaries

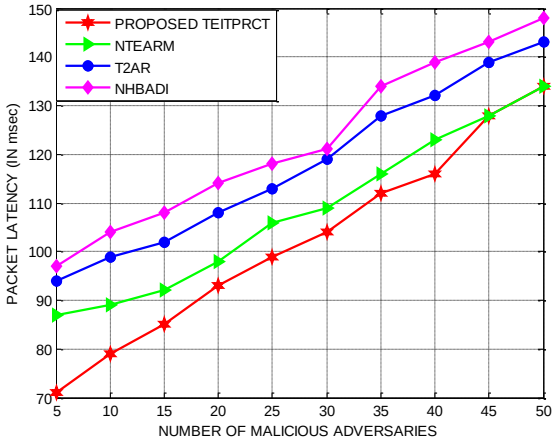

Figure 6: TEITPRCT-Latency - Different Number of Malicious Adversaries

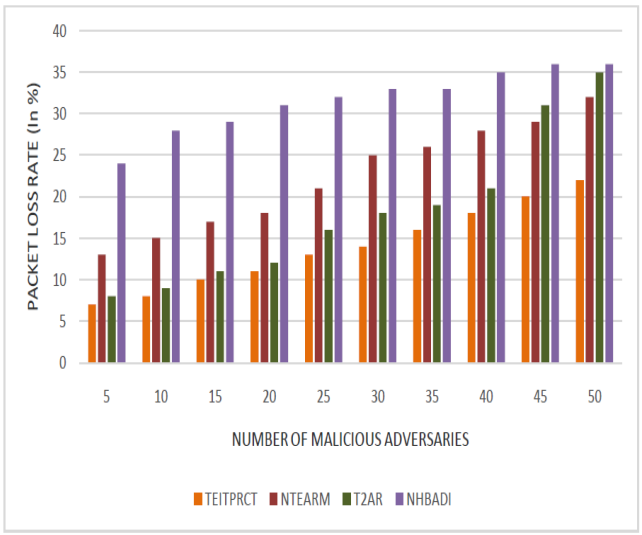

Figure 7: TEITPRCT-Decrease in Packet Loss Rate-Malicious Adversaries

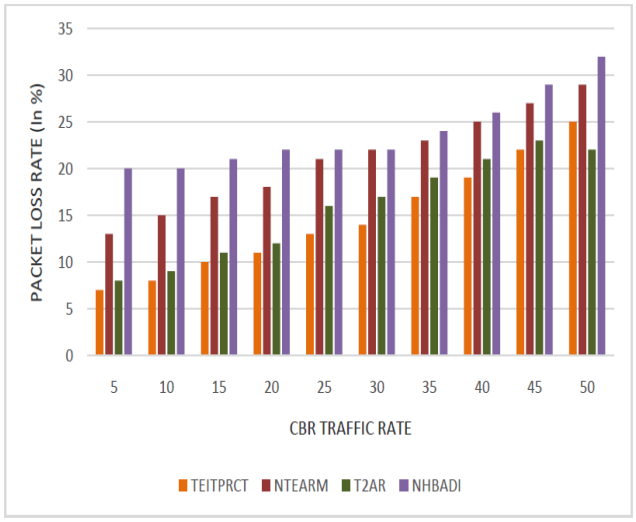

Figure 8: TEITPRCT-Decrease in Packet Loss Rate-CBR Traffic Rate

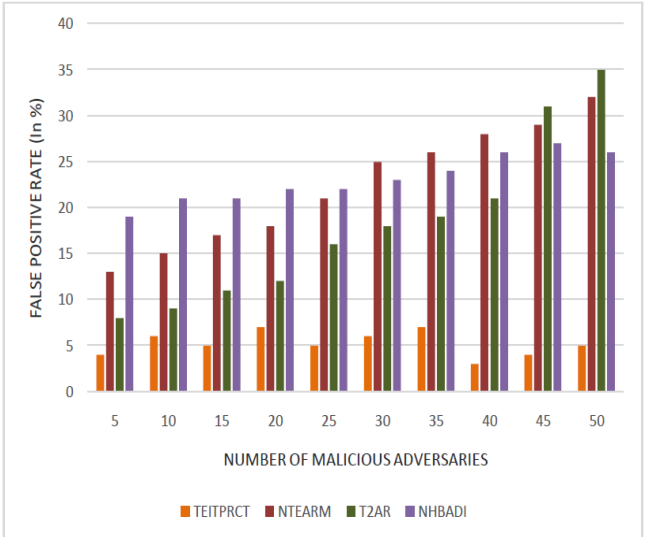

Figure 9: TEITPRCT-False Positive Rate -Malicious Adversaries

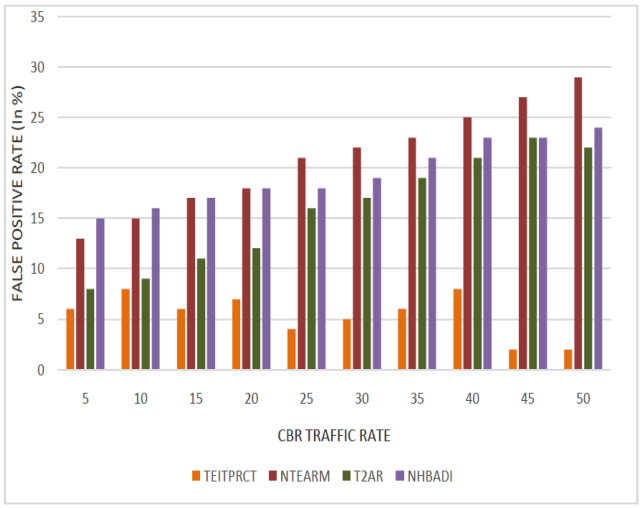

Figure 10: TEITPRCT-False Positive Rate-CBR Traffic Rate

In addition, the potential of the proposed TEITPRCT scheme is also compared with the baseline NTEARM, T2AR and NHBADI approaches using packet drop rate and false alarm rate with different number of malicious adversaries and CBR traffic rate. Figure 7 and 8 presents the packet drop rate of the proposed TEITPRCT scheme and the benchmarked NTEARM, T2AR and NHBADI approaches with different number of malicious adversaries and CBR traffic rate. The packet drop in the network is considered to be considerably reduced independent to the number of malicious adversaries and CBR traffic rate in the network. This predominant performance of the proposed TEITPRCT scheme is mainly due to the utilization of different factors that aids in estimating the trust and energy of the mobile nodes in a potential manner. Thus, the packet drop rate of the TEITPRCT scheme is considerably reduced by 8%, 11% and 13% compared to the benchmarked NTEARM, T2AR and NHBADI approaches with different number of malicious adversaries. Likewise, the packet drop rate of the TEITPRCT scheme is also considerably reduced by 10%, 12% and 14% compared to the benchmarked NTEARM, T2AR and NHBADI approaches with different CBR traffic rate.

Figure 9 and 10 presents the false alarm rate of the proposed TEITPRCT scheme and the benchmarked NTEARM, T2AR and NHBADI approaches with different number of malicious adversaries and CBR traffic rate. The false alarm rate in the network is considered to be considerably reduced independent to the number of malicious adversaries and CBR traffic rate in the network. This predominant performance of the proposed TEITPRCT scheme is mainly due to the high detection rate that uses significant isolation of malicious adversaries. Thus, false alarm rate of the TEITPRCT scheme is considerably reduced by 9%, 12% and 15% compared to the benchmarked NTEARM, T2AR and NHBADI approaches with different number of malicious adversaries. Likewise, the false alarm rate of the proposed TEITPRCT scheme is also considerably reduced by 7%, 10% and 13% compared to the benchmarked NTEARM, T2AR and NHBADI approaches with different CBR traffic rate.

V. CONCLUSIONS

The proposed TEITPRCT scheme was presented as an attempt for achieving reliable data dissemination between mobile nodes by including the merits of the three factors such as Frequency Index of Interaction (FII), Intimacy Index (II) and Honesty Index (HI). This proposed TEITPRCT scheme is a reliable process in quantifying the trust attributed by each mobile node in the network based on the energy possessed by the mobile nodes of the network estimated probe packets. The simulation result proved that the packet drop rate of the TEITPRCT scheme is considerably reduced by 8%, 11% and 13% compared to the benchmarked NTEARM, T2AR and NHBADI approaches with different number of malicious adversaries. Likewise, the packet drop rate of the TEITPRCT scheme is also considerably reduced by 10%, 12% and 14% compared to the benchmarked NTEARM, T2AR and NHBADI approaches with different CBR traffic rate.

REFERENCES

1. Naseer. (2012). EMPIRE - Energy efficient trust-aware routing for wireless sensor networks. Dynamic Ad-Hoc Networks, 1, 391-412.
2. Biradar, R., Manvi, S., & Reddy, M. (2010). Mesh Based Multicast Routing in MANET: Stable Link Based Approach. International Journal of Computer and Electrical Engineering, 1(1), 371-380.
3. Venkanna, U., Agarwal, J. K., & Velusamy, R. L. (2014). A Cooperative Routing for MANET Based on Distributed Trust and Energy Management. Wireless Personal Communications, 81(3), 961-979.
4. Ali, S. S., & Prasad, B. V. (2017). Secure and energy aware routing protocol (SEARP) based on trust-factor in Mobile Ad-Hoc networks. Journal of Statistics and Management Systems, 20(4), 543-551.
5. Moh, S., Kang, M., & Chung, I. (2011). Link Quality Aware Robust Routing for Mobile Multihop Ad Hoc Networks. Mobile Ad-Hoc Networks: Protocol Design, 2(1), 67-74.
6. Anusha, N., & Radha, N. (2016). An Improved Trust Based Approach For Detecting Malicious Nodes in MANET. International Journal of Computer Trends and Technology, 41(1), 54-58.
7. Carvalho, T. C., Ferreira Júnior, J. J., & Francês, R. L. (2016). Reliable Energy-Efficient Multilayer Mechanism with Realistic Battery Model and QoE Support in Wireless MANETs. Journal of Microwaves, Optoelectronics and Electromagnetic Applications, 15(1), 30-48.
8. Gupta, D. (2016). A Trust Model Based Routing Protocol For MANET. International Journal Of Engineering And Computer Science, 1(1), 89-94.
9. Kaur,D.(2016).view-performance-estimation-of-best-ad-hoc-routing-protocol-with-trust-mechanism-in-manet-2. International Journal of Engineering and Computer Science, 5(2), 54-64.
10. Fotino, M., & De, F. (2011). Energy Issues and Energy Aware Routing in Wireless Ad Hoc Networks. Mobile Ad-Hoc Networks: Protocol Design, 1(1), 56-65.
11. Biswas, S., Nag, T., & Neogy, S. (2014). Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. 2014 Applications and Innovations in Mobile Computing (AIMoC), 2(1), 34-45.
12. Jhaveri, R. H., Patel, N. M., & Jinwala, D. C. (2017). A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks. Ad Hoc Networks, 2(1), 67-74.
13. Ermiş, O., Bahtiyar, Ş., Anarım, E., & Çağlayan, M. U. (2017). A secure and efficient group key agreement approach for mobile ad hoc networks. Ad Hoc Networks, 67(3), 24-39.
14. Sarkar, S., & Datta, R. (2016). A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Ad Hoc Networks, 37(2), 209-227.
15. Chen, D. (2016). An energy-efficient QoS routing for wireless sensor networks using self-stabilizing algorithm. Ad Hoc Networks, 37(2), 240-255.
16. Santhi Sri, T., Rajendra Prasad, J., & Kiran Kumar, R. (2018). Distributed and Adaptive Efficient Energy Aware Routing Procedure for MANETs. International Journal of Engineering & Technology, 7(3.12), 841.
17. Dhananjayan, G., & Subbiah, J. (2016). T2AR: trust-aware ad-hoc routing protocol for MANET. SpringerPlus, 5(1).34-45.
18. Yasin, A., & Abu Zant, M. (2018). Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 2018(1), 1-10.
19. Rajesh Babu, M., & Usha, G. (2016). A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET. Wireless Personal Communications, 90(2), 831-845.
20. Merlin, R. T., & Ravi, R. (2019). Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. Wireless Personal Communications, 104(4), 1599-1636.

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.