I. J. Computer Network and Information Security, 2017, 7, 59-66
Published Online July 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.07.07

Reciprocity based Energy Efficient Cooperative Routing Protocol for WSNs

Prasanna Shete
Electrical Engineering Dept. V. J. T. I, Mumbai, 400019, India
E-mail: prasannashete@somaiya.edu

R. N. Awale
Electrical Engineering Dept. V. J. T. I, Mumbai, 400019, India
E-mail: rnawale@vjti.org.in

Abstract—Prolonging network lifetime by salvaging the energy of low battery capacity nodes is a prime concern in Wireless Sensor Networks. Energy efficient routing protocols try to improve the node lifetime by restricting their participation in the routing process. This leads to selfish node behavior causing disruption of inherent network cooperation. This paper proposes an elegant routing mechanism based on direct reciprocity principle, named energy efficient cooperative ad hoc on-demand distance vector (EECoAODV). Proposed protocol correctly differentiates between inherently selfish nodes that use the energy of other nodes to relay their packets, but refuse to reciprocate; and the energy critical nodes that have turned non-cooperative for their own survival. Selfish nodes are punished and eliminated from the routing process thus prolonging the battery capacity of energy critical nodes to improve the overall network performance. EECoAODV is implemented in Qualnet simulator and its performance is compared with conventional AODV and reinforcement based state-action-reward-action (SARSA) routing mechanism. Results show that EECoAODV improves the lifetime of energy critical nodes and thus delivers improved packet delivery ratio than SARSA-AODV and conventional AODV.

Index Terms—WSN, MANET, Reciprocity, AODV, Energy efficiency.

I. Introduction

Wireless Sensor Networks (WSNs) are networks comprising of tiny low powered and energy constrained nodes [1], [2]. Packet delivery in such networks is based on multi-hop relaying. The primary concern in such networks is to improve the network lifetime by preventing the energy depletion of nodes that lose their energy to relay packets of other nodes. Routing protocols [3], [4] used in such networks follow the notion of indirect reciprocity [5], assuming all participating nodes act cooperatively to forward packets of other nodes. For energy efficient operation optimized routing schemes are proposed [6], [7], [8]. These approaches try to conserve the battery capacity of nodes by controlling the number of packet forwarding requests served (of other nodes) i.e. for energy efficient routing the nodes may deny cooperation and act selfishly. To address the selfish node behavior and bring cooperation in the ad hoc network various schemes have been proposed. These are broadly classified into credit based systems [9], [10], [11], reputation based systems [12], [13], [14] and trust based systems [16], [17], [18], [19], [20]. Reference [15] provides a survey of cooperation enforcement schemes. The principle adopted in these approaches is to either punish the selfish/misbehaving nodes or give incentive to cooperative nodes, so as to bring in cooperation in the network. In this paper we assume nodes solely use trust system.

As long as the entire network is under the control of same authority, all nodes will be aware of the decided policy and thus abide by it to achieve the desired results. But in real world heterogeneous scenarios like IoT (Internet of Things), the nodes range from sensors to laptops having different battery capacity levels; and may belong to different authorities governed by their own policies and preferences. Some of these may be altruist and always act cooperatively; some may be rational and self-regarding aiming to maximize their own gains by minimizing their contribution to packet forwarding, whereas some may be reciprocators that mimic the actions of others. Under such scenario it becomes necessary to properly handle the node behavior. In trust systems, the interactions among the nodes are accounted for identifying a particular node as misbehaving (selfish) or well-behaving (cooperative). e.g. Reference [21] proposed self-adaptive trust model (SATM) for secure geographic routing in WSNs, that calculates trust through direct observations. This strategy is well studied and has displayed good results in identifying malicious nodes. Also it works equally well in identifying intentionally selfish nodes that try to free ride on the resources/services of other nodes, but refuse to render theirs. However energy optimized routing protocols that try to salvage the node lifetime for sensing critical data, conserve the node energy by reducing their participation in forwarding requests of other nodes when a control condition is met. The nodes in such scenario should neither be treated as fully cooperative nor fully selfish; they act altruistically

when they have resources in abundance, and start behaving selfishly when there is deficit of resources. So, in order to achieve energy efficient operation as well as sustain network wide cooperation, it becomes important to correctly identify whether the node is intentionally selfish (i.e. selfish by nature), or it is compelled to behave selfishly for the matter of its own survival (i.e. selfish due to resource constraint).

Thus defining node cooperation involves human behavioral and social factors. These factors are also influenced by behavior of other nodes. The conventional tools used in ad hoc and sensor networks are not suitable to model this situation hence alternative techniques were proposed. In [18], [19], [20] the packet forwarding interactions among the nodes is represented using game theoretic framework. In this paper we propose reciprocity based cooperative energy efficient routing extension to widely adopted routing protocol- Ad hoc On Demand Distance Vector (AODV) [3], which improves the lifetime of energy critical nodes by avoiding free riding of selfish nodes. The proposed algorithm is based on the notion of strong reciprocity that follows the tit-for-tat (TFT) principle of [19] in the packet forwarding decision to punish the selfish nodes by eliminating them from the routing process.

The contributions of this paper are two fold; firstly it proposes direct reciprocity based mechanism to correctly identify non energy-critical nodes that behave selfishly, and adopts a stable TFT strategy to punish them. Next, it salvages the battery of critical nodes by selecting the path comprising of nodes with maximum remaining energy, to achieve increased path/network lifetime.

Rest of the paper is organized as follows; the AODV routing mechanism is briefed in section II, section III elaborates reciprocity based trust model to handle selfishness. Section IV briefs the network cooperation model, the proposed energy efficient cooperative ad hoc on-demand distance vector (EECoAODV) algorithm is presented in section V and its performance is evaluated in section VI. Section VII provides concluding remarks.

II. AODV Routing Mechanism

Due to its ability to scale with network size, Ad hoc On Demand Distance Vector (AODV) [3] is widely accepted routing protocol in wireless ad hoc networks like MANETs, WSNs etc. AODV is an on-demand routing protocol in which nodes initiate route discovery procedure when they have packets to be delivered to destination, for which path is not readily available. The route discovery procedure relies on flooding of control packets called route request (RREQ) packets. The route is discovered through broadcast/re-broadcast of RREQs by intermediate nodes till the destination is reached. When the RREQ reaches the destination, the reverse path is set up. The destination node reverses this path and sends reply (RREP) packet to the source following unicast transmission along this path. When RREP reaches the source, forward path is set that is used for data packet transmission. The RREQ forwarding mechanism of AODV is based on the principle of indirect reciprocity, in which every intermediate node forwards the request of other nodes in the hope that some other node/s will forward its request. The inherent altruistic behavior of nodes to forward packets of others inculcates network wide cooperation among the participating nodes. However, this cooperation costs the nodes to consume their energy (battery) for relaying packets of other nodes. In the conventional AODV operation, all nodes are treated equal and thus every node has to participate in packet forwarding, even if its residual energy is critically low. Hence energy critical nodes will exhaust their battery capacity in forwarding the packets of others and die soon to reduce the path lifetime.

III. Reciprocity Principle and Trust Model

Human social interactions are based on reciprocity principle. In behavioral science, reciprocity is broadly categorized into direct reciprocity and indirect reciprocity [22]. The notion in former category is “you help me and I will help you”, whereas the later follows “you help me and someone else will help you” principle. Direct reciprocity can be treated as personal enforcement of cooperation, whereas indirect reciprocity is general enforcement based cooperation [23]. Further reciprocity is also classified as strong and weak reciprocity. Strong reciprocity is defined as altruistically rewarding cooperators and punishing defectors even if the punishment incurs hefty cost to the punisher [24]. Hence, strong reciprocators cooperate only with other cooperators and punish the defectors even if that does not provide short or long term benefits to them. On the other hand in weak reciprocity the clause of punishment is relaxed, and the reciprocator may cooperate even with the non-cooperator if there is possibility of long term benefits.

Reciprocity principle can be applied to packet forwarding interactions in WSNs. The notion is now modified as “you forward my packets and I will forward yours” (direct reciprocity) or “you forward my packets and someone will forward yours” (indirect reciprocity). Reciprocity based cooperation requires node to use trust system that can differentiate between selfish and cooperative nodes. In direct reciprocity, nodes are required to remember their bilateral packet forwarding interactions in the form of personal trust data, while in indirect reciprocity nodes are expected to keep track of packet relaying interactions of all participating nodes as general trust data. Cooperation can be developed on direct, indirect or on both reciprocity mechanisms with personal trust data or combination of personal and general trust data for decision making. Recent research has demonstrated that if packet forwarding follows the reciprocity principle, in which nodes use tit-for-tat (TFT) strategy to forward packets of others, cooperation can be sustained [17], [18], [19], [20]. Although, most of the early research assumes cooperation can be only based on weak reciprocity, it has been pointed in [19] referring to [25] that strong reciprocity can also induce cooperation in situations, where strong reciprocators ready to bear the

cost associated with the strategy, are present in the network.

We apply the reciprocity principle to the packet forwarding mechanism, for achieving energy efficient routing in WSNs. By addressing the node selfishness, we try to conserve the battery of energy critical nodes. This work relies only on personal trust data related to direct reciprocity among nodes for forwarding decisions. This is in tune with the findings of [20] that suggest, in network scenarios with many unconditionally cooperative nodes, cooperation can be sustained on the basis of direct reciprocity. Since goal of this work is to prolong node lifetime of critical nodes, hence in the proposed scheme behavior of selfish nodes will not be made to change from non-cooperative to cooperative throughout the simulation.

IV. Network Cooperation Model

As discussed in earlier sections, this work relies solely on trust system to model reciprocity based cooperation. Cooperation among the nodes is judged on two parameters; the help extended by a node to forward request packets of other nodes, and its capability to render help. The number of packet forwarding requests relayed by a node from total number of requests received is taken as node cooperation degree, and its remaining energy/battery capacity as its capability. Together, this is considered as a measure of node cooperation defined as "node credibility" that is used by nodes in making the forwarding decision.

We first formally define various terminologies used in this paper and then enlist the assumptions made.

***Cooperative Node*:** Node that unconditionally forwards the packet forwarding requests received from other nodes to next hop by consuming its energy.

***Selfish Node*:** Node that routes its packets to the intended recipient using the relaying services of other nodes, but is not available for forwarding packets of others. The selfish node consumes the energy of other nodes to route its packets, but refuses to expend its energy for others even when it has in ample.

***Critical Node*:** A node which has very limited energy as compared to the average energy of the network (i.e node that has energy less than some predefined energy threshold) is defined as critical node. Such node does not forward packets of other nodes as it is not capable of doing so. Since nodes in WSN are supposed to conserve their energy for own survival, critical node should not be treated as selfish, even if it does not forward packets of other nodes.

***Cooperation Degree*:** Cooperation degree of node *j* from the perspective of node *i*, is defined as the ratio of number of *i's* requests relayed by *j*, to the total number of requests received from *i* given as:

$$\gamma_i^j = \frac{Number\ of\ i's\ requests\ relayed\ by\ j}{Total\ Number\ of\ requests\ received\ from\ i}$$

$$\gamma_i^j = \frac{[Nrreq]_i^j}{[Nrreq]_i} \quad (1)$$

***Node Credibility* ($\mathcal{C}$):** It is the measure of node's cooperation calculated on the basis of cooperation degree and its capability given as:

$$\mathcal{C}_i^j = \gamma_i^j * \left\{ \frac{Average\ Network\ Energy}{Remaining\ Node\ Energy} \right\}$$

$$\mathcal{C}_i^j = \gamma_i^j * \left\{ \frac{\sum_i^n RE_i}{n * RE_j} \right\} \quad (2)$$

where, γ_i^j is the cooperation degree, *n* is total number of nodes in the network and *RE* is residual energy of observing node. As $\mathcal{C}_i^j$ increases, node *i* treats *j* as cooperative, otherwise selfish.

***Credibility Score* ($\mathcal{CS}$):** It is the measure of path credibility, and is calculated by summing the credibility of all precursor nodes along the path traversed. For RREQ received along path *p*, credibility score is defined as:

$$\mathcal{CS} = \sum_p \mathcal{C}_i^j \quad (3)$$

Assumptions

- The network is self-organizing, in which the topology changes dynamically and thus node locations are unpredictable.
- Every node transmits at same power level that is radiated equally in all directions using omni-directional antennas. i.e. radio range of every node is equal.
- Network consists of cooperative (well-behaving) as well as selfish (misbehaving) nodes, but not malicious nodes.
- The nodes are capable of recording past interactions with other nodes.
- Reputation system is not present in the network.

V. EECoAODV Protocol

This section explains proposed energy efficient cooperative routing protocol named EECoAODV that extends the AODV routing protocol with two additional functions; detecting the selfish nodes and selecting the best path for data forwarding that comprises of cooperative nodes with sufficient energy.

EECoAODV algorithm is based on direct reciprocity principle in which packet forwarding events recorded by the node itself are used as trust data. Notwithstanding the earlier approaches [18], [19], [20] in which the packet forwarding events till packet delivery to the destination are used in the trust data collection, we only consider single hop interactions with direct neighbors during route discovery phase for collecting trust data. Trust data is collected on the basis of whether a route request was

actually relayed by the expected forwarding node/s. This is so, because if a node behaves selfishly during the route discovery phase and does not forward route request packets of other nodes, it will not be part of discovered route, and thus will refrain itself from forwarding packets of other nodes.

For implementing the EECoAODV algorithm, nodes are required to maintain additional data structures. Each node maintains a neighbor table that stores remaining battery capacity and cooperation degree of its 1-hop neighbors. Moreover, the route request (RREQ) packet structure is modified to carry node energy and credibility score of nodes as shown in Figure 1. We utilize the unused reserved bits of RREQ packet to carry credibility score and additional row is added after originator sequence number field to represent the remaining node energy (remaining battery).

Type	J	R	G	D	U	Credibility Score	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							
Remaining Node Energy							

Fig.1. Modified RREQ Packet Format

A. Reciprocity based route Discovery

When a source node wants to send data to a destination for which path is not readily available, it formulates a route request (RREQ) packet (with credibility score value initialized to zero) and broadcasts it. Intermediate nodes use their personal trust system and decision mechanism for relaying the received route requests following the TFT approach of [19]. An intermediate node (other than critical or selfish), on receiving RREQ, evaluates credibility of precursor node as described in Section IV. Comparing precursor node's credibility with predefined credibility threshold, an intermediate node judges whether the request is from a cooperative or selfish node and decides whether to forward or drop it, as represented below.

$$Decision = \begin{cases} forward, & if\ \mathcal{C}_i^j \geq [\mathcal{C}_i^j]_{Th} \\ drop, & if\ \mathcal{C}_i^j < [\mathcal{C}_i^j]_{Th} \end{cases} \quad (4)$$

where, $\mathcal{C}_i^j$ and $[\mathcal{C}_i^j]_{Th}$ are the node credibility and credibility threshold respectively.

If the request is from selfish node the intermediate node/s punish the locally observed selfishness by dropping the request. Whereas, if the request is from cooperative node, the intermediate nodes add the calculated credibility score to the credibility score value contained in the RREQ and relay it to next hop. Since node's remaining battery is accounted in the credibility calculations, EECoAODV can easily differentiate between inherently selfish nodes from those that have turned selfish due to resource (battery) constraint.

// Algorithm 1. RREQ Handling at Intermediate node//

```
RREQ_receipt ( )
 {
   calculate C_i^j of precursor node using equation (2);
   //compare credibility (C_i^j) of precursor node with
 threshold
   if (C_i^j <  [C_i^j]_Th) then            // [C_i^j]_Th = 0.5
        discard RREQ;
    else
        add C_i^j value to Credibility score in the RREQ packet;
        flood RREQ;
 }
```

Route Reply

When the RREQ reaches destination, the destination node rather than instantly replying with RREP, buffers the received RREQ and waits for some predetermined time *T*, that is fractional multiple of RREQ interval, to receive the copy/ies of same RREQ along different path/s. Destination node compares the credibility scores of all received RREQs, and selects the path that has maximum credibility score to send the RREP.

// Algorithm2. Route selection; RREQ handling at Destination//

```
First RREQ received ( )
{
  buffer the path and credibility score CS, corresponding to
 this
   RREQ ;
while (RREQ_interval)
   {
    buffer the CS and path of all received RREQs;
   }
 //compare credibility score of all paths  and select the path
 that
    has maximum credibility score //
    [path]_D-S = max(CS);
    send RREP along max(CS);
}
```

Cooperation Degree Initialization and Updation

Every node initializes the cooperation degree of its neighbors to 0.5, so as to treat first request altruistically. This setting is helpful for correctly handling the request from a neighbor with which the node has not interacted earlier. Cooperation degree is later updated based on the request forwarding interactions among the nodes.

//Algorithm 3. Cooperation Degree Initialization/Updation//

```
for (every neighbor j)
     if  ([Nrreq]_i ≤ 1)
        γ_i^j = 0.5; //initialize γ_i^j = 0.5
     else
        γ_i^j = [Nrreq]_i^j / [Nrreq]_i ;
```

VI. Performance Evaluation

This section presents the performance evaluation of EECoAODV. For evaluating the performance, two network scenarios were designed; a) 25 nodes arranged in a static grid with 4 traffic connections, and b) 25 mobile nodes moving at a speed of 10 m/s according to RWP mobility model.

Performance is evaluated on the metrics of packet delivery (PDR), throughput, end-to-end delay, residual battery capacity, and battery dead time. The performance of EECoAODV is compared with conventional AODV and reinforcement learning based SARSA-AODV algorithm.

A. EECoAODV performance in Static Grid Scenario

The objective of this experiment is to analyze the ability of proposed EECoAODV to improve the lifetime of energy critical nodes by handling node non-cooperation arising from selfish behavior. For this a small 2-d lattice network of 25 nodes and 4 traffic connections each of 512 kbps is simulated in Qualnet 5.0 network simulator. The network comprised of selfish as well as critical nodes along with normal nodes. The nodes are assigned different initial battery capacity in order to differentiate them as critical, normal and selfish. The critical nodes are assigned least initial battery capacity and the selfish nodes have the highest battery capacity as shown in Table 1. Two selfish and two critical nodes act as traffic sources. Since no restriction on number of packets to be transmitted is set in the simulation parameters, source nodes keep on sending packets throughout simulation time or till they exhaust their battery. Table 1 presents detailed simulation parameters.

Table 1. Simulation Parameters for Static Grid Network

Parameter	Value
No. of Nodes and Area	25 and 1500m * 1500m
Node Placement Strategy	Grid [Grid unit = 200m]
Channel Frequency	2.4 GHz
Transmission Range	300 m
Antenna Model	Omni-directional
Battery Model	Linear
Energy Model	Generic
Path Loss Model	Two ray Model
PHY / MAC Layer Protocol	IEEE 802.11b
Traffic Sending Rate	32 kbps
Payload size	512 bytes
No. of Traffic Connections	4
Critical Energy/Battery Threshold	2.4 mAh
Critical Node Numbers with initial battery capacity	{7, 9, 17, 19}; 3.0 mAh
Normal Node Numbers with initial battery capacity	{1,2,4,5,6,8,10,12,13,14.16,18, 20,21,22}; 12 mAh
Selfish Nodes Numbers with initial battery capacity	{3, 11, 15, 23}; 13 mAh

The simulation results are recorded for different simulation durations. Figure 2 and 3 present the average packet delivery ratio and end-to-end delay of network as function of simulation time. EECoAODV delivers better PDR than other two, however the end-to-end-delay experienced is bit higher than AODV. As seen from Figure 2, initially for simulation time up to 420 s, EECoAODV delivers poor PDR as compared to AODV, thereafter it is same as AODV. This is so because, for lesser simulation duration no node in the network exhausts its energy and thus all nodes remain alive till the end of simulation. Thus for these simulation durations, path to destination discovered by AODV doesn't experience breakage arising from node failure. Since AODV follows the notion of shortest path in route selection, as against the best energy path notion of the energy efficient schemes, it's PDR and delay performance will be better than other two. However, since there is no provision in AODV protocol to salvage the energy of critical nodes, when the experiment is run for longer simulation duration the critical nodes will consume their battery to forward packets of other nodes and die early. This results in path failures and thus, degrades the AODV performance. On the other hand, when EECoAODV is used, nodes forward packets based on reciprocity principle and conserve their energy by not relaying the packets of selfish nodes. Thus critical nodes survive for longer time, and hence PDR is improved.

Although SARSA-AODV is an energy efficient algorithm intended for balanced energy consumption of nodes that aims to improve the node lifetime, it too doesn't have provision for punishing the free riding of selfish nodes. SARSA-AODV follows the state-action-reward-action metaphor of reinforcement learning in which the node's energy drain rate observed for some predefined duration (usually a multiple of RREQ interval), is used to judge the state and corresponding action of a node. SARSA is a complex algorithm and is slow in responding to dynamic energy changes of sensor nodes; action (packet forwarding decisions) taken on the basis of present state remains fixed throughout the next action interval. It may happen that some of the nodes might have selected an action of forwarding packets based on their energy value in previous state, but during the action phase they drain their energy and turn critical. SARSA algorithm cannot handle this situation and nodes with critical battery have to continue with the selected action of packet forwarding throughout the state, even if that causes their complete energy depletion. Also SARSA-AODV incurs large delay due to wait time involved at the destination in selecting the least energy drain path. Hence its performance is poor as compared to other two.

The individual node statistics are presented in Figure 4 to Figure 7. Figure 4 and Figure 5 show the battery dead time of critical nodes that are acting as data source and destination respectively. The PDR statistics for critical and selfish node are presented in Figure 6 and Figure 7 respectively. It is clear from the results that EECoAODV prolongs the lifetime of critical nodes as well as improves their PDR as compared to both; AODV and SARSA-

AODV. The node lifetime of critical nodes is improved by 12.76% and their PDR is improved by 7.7% as compared to AODV; whereas improvement of 13.18% and 11.52% is seen as compared to SARSA-AODV on these parameters. However, as EECoAODV punishes selfish nodes, their PDR is degraded.

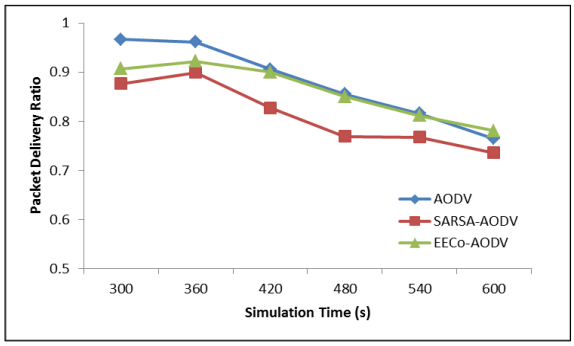

Fig.2. Packet Delivery Ratio vs Simulation Time

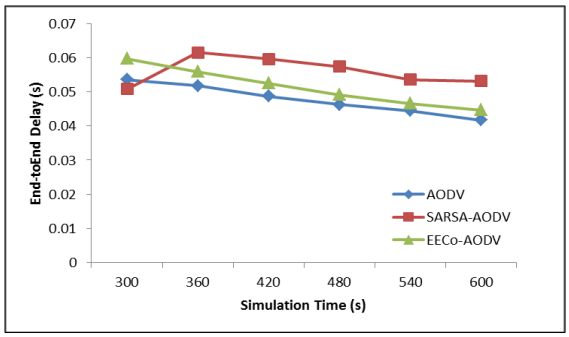

Fig.3. End-to-End Delay vs Simulation Time

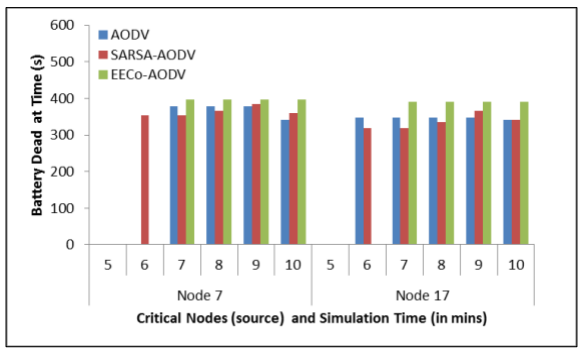

Fig.4. Battery Dead Time of Critical Node (data source) vs Simulation Time

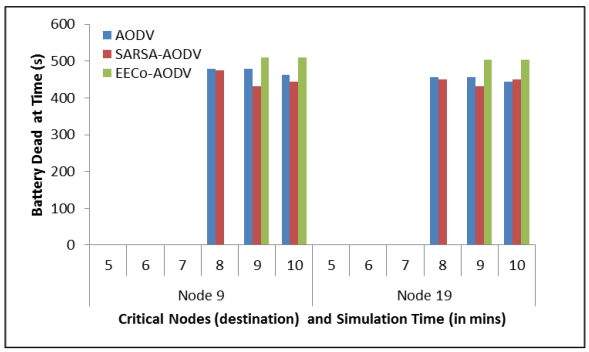

Fig.5. Battery Dead Time of Critical Node (destination) vs Simulation Time

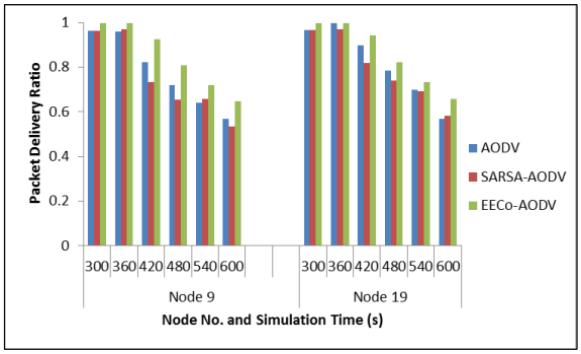

Fig.6. Packet Delivery Ratio of Critical Nodes

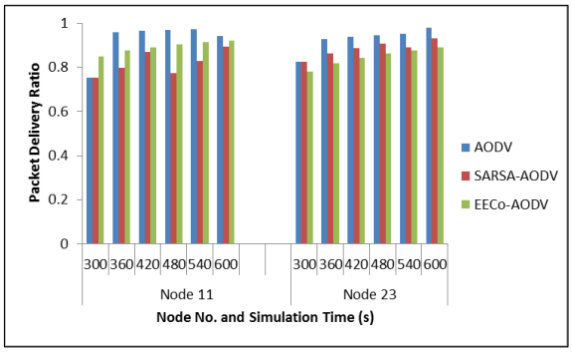

Fig.7. Packet Delivery Ratio of Selfish Nodes

B. EECoAODV performance in Node Mobility Scenario

Here more realistic network scenario is considered, consisting of 25 nodes placed uniformly in the terrain of 500 * 500 m. The nodes move according to RWP mobility model with a speed of 5 m/s. Traffic connections are set between randomly selected source destination pairs that do not comprise of critical or selfish nodes i.e. these nodes act as intermediate nodes that are only meant to forward the packets of other sources, and do not generate any traffic by themselves.

The network comprises of 5 critical, 5 selfish and 15 normal nodes. Number of traffic connections is varied from 1 to 5 and performance is analysed. The results are presented in Figure 8-9. One can easily anticipate that as number of traffic connections increase, the critical nodes need to forward more packets and thus will lose more energy and their battery capacity will be depleted soon. Since there is no provision in conventional AODV or SARSA-AODV to handle the non-cooperation of selfish nodes, their performance is expected to degrade when number of traffic connections is increased. Whereas EECoAODV punishes the non-cooperation of selfish nodes and tries to conserve energy of critical nodes, hence it is expected to deliver better performance than other schemes.

The above notion is justified by the results. As can be observed from the graphs, for scenarios with up to 3 traffic connections all schemes deliver more or less same performance. For simulation scenarios with more than 3 traffic connections EECoAODV outperforms AODV as well as SARSA-AODV; PDR is improved (Fig.8), at the same time the dead-time of critical nodes is delayed (Fig. 9).

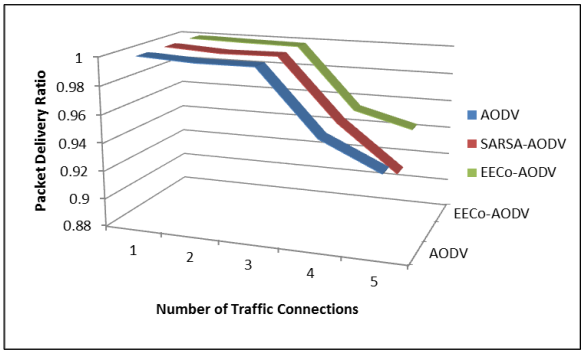

Fig.8. PDR vs No. of Traffic Connections

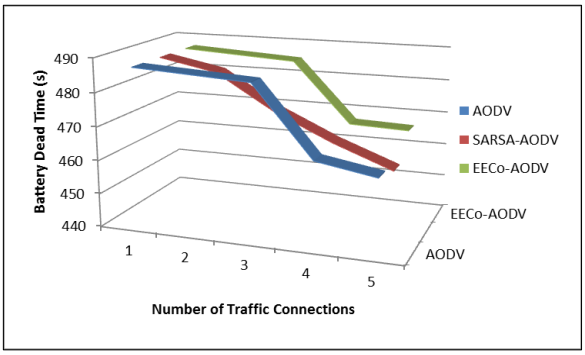

Fig.9. Battery Dead Time of Critical Node vs No. of Traffic Connections

VII. Conclusion

This paper addressed the energy depletion of critical nodes resulting from selfish node behavior of some nodes, which adversely affected the performance of ad hoc wireless sensor networks. Using the principal of direct reciprocity, energy efficient algorithm named EECoAODV is proposed that punishes the non-cooperating selfish nodes, by not forwarding their requests and thus improves the node lifetime of critical nodes.

The proposed algorithm is implemented in Qualnet 5.0 simulator and its performance is evaluated for different metrics. The work presented in this paper is limited to improving the battery capacity and performance comparison of proposed solution with conventional and energy efficient routing protocols only (e.g. AODV and SARSA-AODV). Simulation results show that EECoAODV addresses the early energy depletion of critical nodes by restricting them from relaying requests of selfish nodes. Since the battery capacity of critical nodes is conserved, the path failures arising from battery exhaustion of these nodes is reduced. EECoAODV outperforms conventional AODV as well as SARSA-AODV on networks metrics viz., node lifetime and PDR of critical nodes. In static scenario with EECoAODV, the battery dead time of energy critical nodes is prolonged by 12.76% and 13.18% respectively as compared to AODV and SARSA-AODV. Moreover, the PDR results show with EECoAODV, energy critical nodes deliver 11.52% and 7.7% more packets as compared to SARSA-AODV and conventional AODV respectively. EECoAODV punishes the non-cooperation of selfish nodes and tries to conserve energy of critical nodes; and thus delivers better performance than other schemes.

References

[1] K. Sohraby, D. Minoli and T. Znati,(2007) “Wireless Sensor Networks: Technology, Protocols and Applications,” Wiley Interscience.

[2] M. Perillo and W. Heinzelman (2004), “Wireless Sensor Network Protocols”.

[3] C. E. Perkins, S. Das (July 2003) “Ad Hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561.

[4] D. B. Johnson, D. A. Maltz (Feb 2007), “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4,” RFC 4728.

[5] M. Nowak and K. Sigmund (Oct. 2005), “Evolution of Indirect Reciprocity,” Nature 437, pp. 1291-1298.

[6] Chettibi and S. Chikhi (May 2012), “An adaptive Energy Aware Routing Protocol for MANETs using SARSA Reinforcement Learning Algorithm”, Proc. of IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS), pp. 84- 89.

[7] H. Farooq and L. Jung (2013), “Energy, Traffic Load, and Link Quality Aware Ad Hoc Routing Protocol for Wireless Sensor Network Based Smart Metering Infrastructure,” Intl. Journal of Distributed Sensor Networks, pp. 1-13.

[8] S-H. Park, S. Cho and J-R. Lee (2014), “Energy-Efficient Probabilistic Routing Algorithm for Internet of Things,” Journal of Applied Mathematics, pp. 1-7.

[9] J-P. Hubaux, T. Gross, J-Y Le Baudec, and M. Vetterli (2001), “Towards Self-organized Mobile Ad Hoc Networks: The Terminodes Project”, IEEE Communications Magazine.

[10] S. Zhong, J. Chen and Y. R. Yang(Mar-Apr 2003), “Sprite: A Simple Cheat-Proof, Credit Based System for Mobile Ad hoc Networks”, Proc. of INFOCOM.

[11] L. Anderegg and S. Eidenbenz (Sep. 2003), “Ad hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents,” Proc. of 9th Intl. Conf. ACM MobiCom’ 03, pp.245-259.

[12] S. Marti, T. Giuli, K. Lai and M. Baker (Aug. 2000), “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. of 6th Intl. Conf. on Mobile Computing and Networking (MobiCom)”.

[13] S. Buchegger and J-Y Le Baudec (June. 2002), “Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness In Dynamic Ad-Hoc Networks)” Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC),.

[14] Y. Liu and Y. Yang (2003), “Reputation Propagation and Agreement in Mobile Ad Hoc Networks,” Proc.of IEEE Wireless Comm. and Networking Conference pp. 1510-1515.

[15] G. Marias, P. Georgiadis, D. Flitzanis and K. Mandalas (2006), “Cooperation enforcement schemes for MANETs: A survey,” Wireless Communications and Mobile Computing, Vol. 6(3), pp. 319-332.

[16] Srinivasan, P. Nuggehalli, C. Chiasserini and R. Rao (2003), "Cooperation in wireless ad hoc networks," Proc. of 22nd Annual Joint Conference of the IEEE Computer and Communications INFOCOM ‘03, pp. 808-817.

[17] L. Yu. And S. Hailes (May 2008), “Cooperative Packet Relaying Model for Wireless Ad hoc Networks,” Proc. of the 1st ACM Intl. Workshop on Foundations of Wireless Ad hoc and Sensor Networking and Computing, pp. 93-

100.
[18] M. Seredynski and P. Bouvry (Feb. 2012), "Direct Reciprocity based Cooperation in Mobile Ad hoc Networks," Intl. Journal of Foundations of Computer Science, Vol. 23, No. 2, pp. 501-521.
[19] M. Seredynski, G. Danoy and P. Bouvry (2012), "The Necessity for Strong Reciprocators in Mobile Ad Hoc Networks," Proc. of IEEE 26th Intl. Parallel and Distributed Processing Symposium Workshops & PhD Forum, pp. 609-616.
[20] M. Seredynski and P. Bouvry (Feb. 2013),"Analysing the development of cooperation in MANETs using evolutionary game theory", Journal of Supercomputing, Vol. 63- No. 3, pp. 854-870.
[21] Vamsi, P. Raghu, and Krishna Kant (Feb. 2015) "Self adaptive trust model for secure geographic routing in wireless sensor networks." International Journal of Intelligent Systems and Applications 7.3 (2015), pp. 21-28.
[22] E. Fehr and U. Fischbacher (2003), "The Nature of Human Altruism," Nature, Vol. 425, pp. 785-791.
[23] H. Brandt and K. Sigmund (2006), "The good, the bad and the discriminator – Errors in direct and indirect reciprocity," Journal of Theoretical Biology, Vol. 239 (2), pp. 183-194.
[24] H. Gintis(2000), "Strong Reciprocity and Human Sociality," Journal of Theoretical Biology, Vol. 206, pp. 169-179.
[25] E. Fehr, U. Fischbacher and S. Gachter (2002), "Strong Reciprocity, Human Cooperation, and the enforcement of social norms," Human Nature, Vol. 13 (1), pp. 1-25.

Authors' Profiles

Prasanna Shete received B.E degree in Electronics Engineering from Dr. B. A. M. University and M. Tech degree in Electronics and Telecommunication from V.J.T.I, Maharashtra, India. Presently, he is Research Scholar at V.J.T.I and Faculty in K. J. Somaiya College of Engineering, Mumbai, India. His research interests include Ad hoc Networks, Cross layer design for QoS in Multi-hop Wireless Ad hoc networks and Mobile Computing.

R. N. Awale received B E, M E and Ph D degree in Electronics Engineering from Marathwada University, Maharashtra India. Presently, he is working as Professor in Electrical Engineering Department, Veermata Jijabai Technological Institute (V.J.T.I), Mumbai, India. His research interests include Ad hoc Networks, Cross layer design for QoS in Wireless networks, Data Security and Coding Theory.

How to cite this paper: Prasanna Shete, R. N. Awale,"Reciprocity based Energy Efficient Cooperative Routing Protocol for WSNs", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.7, pp.59-66, 2017.DOI: 10.5815/ijcnis.2017.07.07

