POMSec: Pseudo-Opportunistic, Multipath Secured Routing Protocol for Communications in Smart Grid

Manali Chakraborty(✉), Novarun Deb, and Nabendu Chaki

University of Calcutta, Kolkata, India
manali4mkolkata@gmail.com

Abstract. Traffic engineering governs the operational performance of a network and its optimization. Splitting the network traffic using multipath routing is one of the standard techniques of traffic engineering. Multipath routing maximizes network resource utilization and throughput by giving nodes a choice of next hops for the same destination along with minimizing the delay. On the other hand, Opportunistic routing minimizes operational cost and the burden of redundant route maintenance by using a constrained redundancy in route selection. POMSec: Pseudo Opportunistic, Multipath Secure routing is one such algorithm that combines the advantages of both the routing methods and additionally implements an underlying trust model to secure the communication in Smart Grid.

Keywords: Opportunistic routing · Multipath routing · Wireless sensor network · Security · Energy efficiency · Smart Grid

1 Introduction

Wireless sensor networks are burdened with the task of transferring data from one node to another via wireless links and multiple hops, considering all the adversaries in the network. Each of the factors like unpredictable environmental behavior, dynamic network topologies, unreliable nature of communication or a combination of these may further contribute to failure of network services. Due to its dynamic nature, WSN is suitable for various types of applications [18]. However, security is one of the most important aspect of every application with different QoS requirements, such as, throughput, energy efficiency, delay, etc. Security of any application is generally determined by its attributes [21]. However, security solutions for sensor networks are different from ordinary networks having infrastructure. Besides, every application domain has its own unique characteristics and QoS parameters. Thus, it requires a secure and reliable routing protocol which will comply with application specific QoS parameters as well [5].

In traditional routing the route between a pair of nodes is always static and data packets are transmitted through intermediate nodes over that pre determined route. Whereas, multipath routing adds desired level of redundancy to

K. Saeed et al. (Eds.): CISIM 2017, LNCS 10244, pp. 264–276, 2017.
DOI: 10.1007/978-3-319-59105-6_23

overcome link failures utilizing alternative routes [7]. Besides, in multipath routing environment, link failures do not always result in the initiation of route discovery. This is because the network is k - fault tolerant, for small values of k and hence link failures do not bring network services to a halt [6]. Besides, multipath routing provides better load balancing and bandwidth aggregation [8].

There exist several works, [11–15] which propose to utilize multiple routes in order to provide stability and reliability in the network. However, in spite of all these benefits, multipath routing has several disadvantages: (1) Using multiple routes can increase significant energy cost, which is one of the most important QoS metric in WSNs; (2) Multiple route discovery and maintenance at every hop induces the operational cost of the network; and (3) Besides, multiple routes can introduce channel contentions and interference in the network, which result in the increment of delivery delay as well as cause transmission failures [12].

Opportunistic routing (OR) [17], or anypath routing, is another routing protocol which takes advantage of the broadcasting ability of nodes in wireless medium. It does not use multiple routes, but selects best possible relay nodes among a set of candidate nodes to improve reliability, efficiency and fault tolerance. In OR, first, a source node broadcasts a packet among its neighbors. Then these candidate nodes select a best relay node among itself using some coordination algorithm and forward the data packet through that node. The same process continues until the transmission is successful, i.e., the specified packet reaches its destination.

We have considered Smart Grid as an application domain of our proposed routing protocol. Now, due to specific demands of Smart Grid, the associated communication system should have these following characteristics [19,20]:

- It should consider different type of traffic patterns in the network, e.g., unicast, multicast and broadcast.
- It need to be scalable and flexible to incorporate new renewable sources and distributed energy resources in the network.
- Due to the large and evolving architecture of smart Grid, distributed or cluster based networks will be more suitable for it.
- The communication system should monitor the network devices and perform fault detection, isolation, and recovery.
- Every device should get uniquely identified and addressed.
- It should support different QoS parameters for a variety of applications and functions which have different latency and loss requirements, different bandwidth, different security requirements, different real time and non real time data constraints etc.
- Besides, the communication system should be interoperable, dynamic, cost effective, open to active standards and public interfaces, backward compatible and most importantly secure to all the vulnerabilities from inside and outside of the network.

Now, multipath routing and OR, both have their advantages and disadvantages. Multipath routing provides better reliability and fault tolerance, whereas

OR improves network performances and also supports different traffic patterns. However, multipath routing suffers from operational overhead of discovering and maintaining routes in every hop, which inturn increase the contention in the network. OR also suffers from duplicate reception problem at the destination and single path breakdown problem. Thus, it will be more effective to integrate the positive sides of both these paradigms in a single routing protocol.

The proposed work is a secure and pseudo opportunistic, multipath routing scheme that offers efficient load balancing. Like traditional OR methods, our protocol dynamically selects a set of forwarding nodes for packet transmission. However, the number of routes for packet transmission is not static, and the number of routes varies with the status of each intermediate node, at every hop along the path. The degree of routes at each hop depends heavily on the trust worthiness of neighbouring nodes. As an example, it may act like single-path routing, if the nodes are trustworthy and the communication is reliable and meets network requirements. Otherwise, the number of paths increased. The selection process is run-time and dynamic.

The idea of using selective multipath routing is first proposed in ETSeM [1]. In ETSeM each node is equipped to choose a set of forwarding nodes among its neighbours to transmit data. Route selection depends on the energy of nodes and number of paths set up through the nodes. However, the proposed routing protocol in [1] has not been associated with any security measures to detect threats and this inspires us to propose a new secure routing algorithm where an additional trust model [3] is combined with routing mechanism. In the proposed work, every node evaluate the trust value of its next hop neighbour and the routes are selected based on these trust values. The proposed protocol offers the flexibility that it may use multiple paths with high degree of multiplicity when the intermediate destinations are not that trusted. On the contrary, the protocol save resources, and checks congestion by choosing a single path or lesser number of alternate paths for the next hop according to the health value of its neighbour nodes. Because of these characteristics, our proposed algorithm has been referred as Pseudo Opportunistic, Multipath Secure (POMSec) routing protocol. We have simulated our protocol using QualNet 5.2 and also compares the results with [1] and another trust model proposed in [2].

The organization of this paper is described as follows: Sect. 2 gives the state of the art review on related works and Sect. 3 describes the proposed process in brief. The simulation results are presented in Sect. 4. Finally Sect. 5 concludes the paper.

2 State-of-the-Art Review

In this section, we discuss some of the significant works on multi-path as well as opportunistic routing for wireless networks. Besides, Sect. 2.3 discusses some of the existing trust models.

2.1 Multi-path Routing Protocols

Effectiveness of multipath routing protocols primarily rely on two aspects: route discovery and route selection process [4]. The multipath routing algorithm proposed in [9], has two different protocols: one for searching different multiple and node disjoint paths and another is for allocating the traffic optimally through those disjoint paths. Authors claimed that the algorithm works distributively and optimally balances the load in the network. In [12], each node first built a set of partially disjoint paths to destination among its neighbours.

REER [13] considers remaining energy level and available buffer size of a node, and Signal-to-Noise ratio to determine next hop forwarding node in the route. This algorithm has two methods of traffic allocation. First method selects a group of candidate nodes between every hop, and then the best route is chosen for data transmission. The second method breaks the transmitted message into several equal sized segments and then adds a XOR based error correction code with them and transmits them through different paths. Thus guarantees the arrival of the packet to the destination without any delay.

RELAX [14] effectively utilizes the relaxation technique of batteries to improve network lifetime. It also uses some metrics like remaining energy, Signal-to-Noise ratio, and other variables to predict the best next hop node. RELAX splits the transmitted message into several equal sized segments, and then add XOR based FEC with them and transmit them through different paths. Thus, the protocol does not require flooding when there is a link failure and hence the lifetime of the network is increased.

SEEMPr [15], tries to balance both the reliability and lifetime of a network, by providing the concept of criticality factor. The criticality factor determines the urgency of delivering a data packet. All packets do not have the same urgency. Thus, high priority packets follow optimal path, while other packets are sent through sub-optimal routes. Thus the energy consumption is distributed over the network.

The review above reflects that there already exist a good number of papers on multipath routing protocols. However, the trust worthiness of participating nodes is often not considered by the above protocols. In [6], a secret-sharing algorithm has been used to secure the network. However, the degree of multiple path selection on a hop to hop basis depending on the trust-value of the next hop destination has not really been considered in the existing approaches.

2.2 Opportunistic Routing Protocols

Several works have been proposed in the field of OR. [18] presents a survey of existing OR protocols in wireless network. Although OR is gaining a lot of attention due to its improved performance over other routing protocols in wireless environment, there is not much work present in Smart Grid area.

PLC-OR [22] is a power line communication based opportunistic routing in Smart Grid. Authors in this paper, uses static topological information of nodes to construct a routing table. It always selects a single path to the destination to avoid duplicate packet reception problem at the final destination. They used Dijkstra's algorithm for shortest path selection at each hop. Authors claim to reduce the transmission cost by using a static PLC-AN.

Authors of [23] proposed another OR for Smart Grid. However, this algorithm differs from the previous one in terms of its ability to handle varying topology in a network. They also introduced a new parameter depending on the transmission time for existing routes to calculate the best forwarding node among a set of forward nodes. The estimation method of transmission time is based on the outage probability of the PLC channel. Using simulation and theoretical methods, authors claimed to prove that the throughput of the network can be maximized if remaining transmission time is used to select and identify the forwarding nodes.

Analysing the existing works on opportunistic routing protocol reflects that it performs better in a static network, otherwise the operational cost exceeds the performance gain of the network. Thus, the tradeoff between progressing gain and processing delay and cost will be one of the main important concern for OR. OR does not come with any inherent security model. Thus, providing a secure transmission will be another important aspect while implementing OR in Smart Grid. Furthermore, duplicate packet delivery is another problem for OR. It generally causes due to broadcasting nature of wireless media and the use of isometric antennas. Authors of [22] claim to solve this problem by not allowing multipath routing, which restricted the selection of forwarding nodes within same transmission domain for a particular sender node. However, this inturn defeats the main purpose of OR, which exploits the broadcasting nature of wireless networks.

2.3 Trust Models

Authors in [2] proposed an honesty based intrusion detection system for MANETs. In HIDS, each node is tagged with an unique identifier and an honesty metric. This honesty metric of each node gets updated periodically based on the packet forwarding information provided by one-hop neighbours.

TIDS [3] is a another intrusion detection system for Wireless Ad-Hoc Networks that uses the trust evolution process to mitigate threats. Each node in the network is assigned a predetermined and fixed trust value. As the node spends time within the network, its trust value gets updated. Trust value of nodes get updated based on direct references and indirect recommendations. Trust values of one - hop neighbours are evaluated as part of two different processes.

In [10], another trust based model is proposed. The trust value of each node is calculated as a function of three different QoS parameters. A peer node will get rewarded every time it behaves properly with its neighbours. Thus the trustworthiness of each node depends on how it interacts and whether its neighbours are satisfied with its quality of service.

After reviewing several routing protocols and trust models we can conclude that neither multipath routing nor OR is perfectly tailor made for Smart Grid. In order to maximize the performance of Smart Grid, a combination of both the paradigms is necessary. Besides, there rarely exist some works, where trust models have been used in route discovery. This inspires us to propose an intelligent, selective and secure routing protocol which can use the perks of both opportunistic and multipath routing protocols with additional security mechanisms.

3 Description of the Process

This section briefly describes our proposed protocol for secure communication in Smart grid. Route selection in POMSec is dependent on energy depletion rate of the nodes, existing paths through the nodes and the trustworthiness of the nodes and their neighbours.

These following set of principles govern the proper execution of the proposed algorithm:

- Every node maintains two arrays – *Health* and *Trust*, of all its neighbour nodes.
- Every node has to store two variables – *Remaining Energy* and *Path.*
- Packet Receive (*PR*) and Packet Send (*PS*) counters are stored in nodes, along with the addresses of the nodes from which it receive the packets and to which it forward those packets. After a certain time frame (decided by the system operator), these counter values are sent to the node's one-hop neighbours.
- The health of each node N depends on trust-worthiness of the nodes, the remaining energy of it and on the number of paths through N.

3.1 The Trust Model

In order to secure our protocol we evaluated the trust of each node. The evaluation process is done by a node for its one hop neighbours and vice versa. The trust model has two main underlying concepts: *Direct Valuation* and *Indirect Reference* [3].

Direct Valuation refers to the trust value evaluated by a node. It is calculated using two different parameters: *Risk* and *Reputation.Risk* measures a node's behavior in recent past and *Reputation* assess a node's long term behavior. These two parameters helps to achieve an optimality by balancing the most recent behavior of a node in contrast to its long term behavior. On the other hand, *Indirect Reference* are considered from those entire one-hop neighbors that are common to both the evaluator node and the target node.

At time *t*, an evaluator node calculates the *Risk* and *Reputation* of its neighbour node i as,

$$Risk = \sum_{t} |PR_i - PS_i| \tag{1}$$

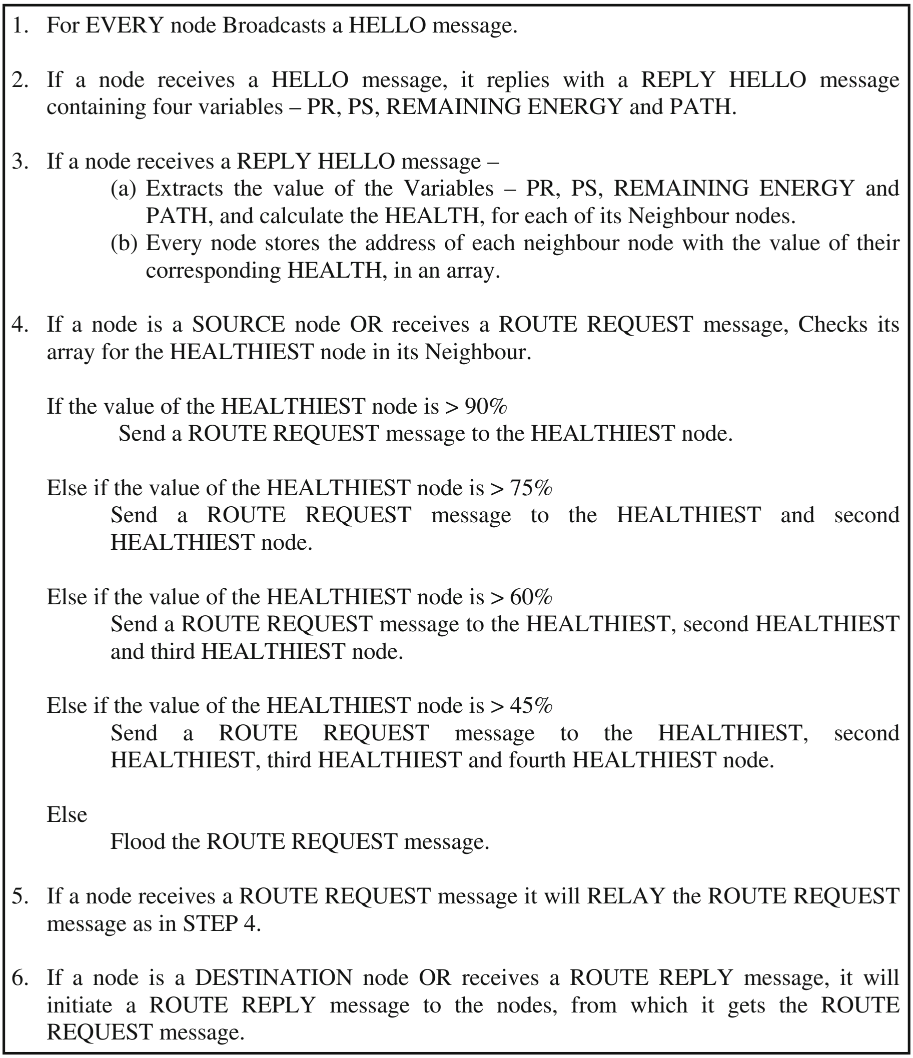
$$Reputation = \sum_{t}^{t-n} |PR_i - PS_i| \tag{2}$$

The *Indirect Reference* for m number of common neighbour Nodes (ND) between evaluator and target node, can be evaluated as,

$$Indirect\ Reference = \sum_{ND=1}^{m} \sum_{t}^{t-n} |PR_i - PS_i| \tag{3}$$

The reward for a node for the last time slice, is calculated using these three metrics as follows [3]:

$$\text{“}Reward = (\alpha * Risk) + (\beta * Reputation) + (\gamma * Indirect\ Reference)\text{”} \tag{4}$$



```
1. For EVERY node Broadcasts a HELLO message.

2. If a node receives a HELLO message, it replies with a REPLY HELLO message
   containing four variables – PR, PS, REMAINING ENERGY and PATH.

3. If a node receives a REPLY HELLO message –
       (a) Extracts the value of the Variables – PR, PS, REMAINING ENERGY and
           PATH, and calculate the HEALTH, for each of its Neighbour nodes.
       (b) Every node stores the address of each neighbour node with the value of their
           corresponding HEALTH, in an array.

4. If a node is a SOURCE node OR receives a ROUTE REQUEST message, Checks its
   array for the HEALTHIEST node in its Neighbour.

   If the value of the HEALTHIEST node is > 90%
           Send a ROUTE REQUEST message to the HEALTHIEST node.

   Else if the value of the HEALTHIEST node is > 75%
          Send a ROUTE REQUEST message to the HEALTHIEST and second
          HEALTHIEST node.

   Else if the value of the HEALTHIEST node is > 60%
          Send a ROUTE REQUEST message to the HEALTHIEST, second HEALTHIEST
          and third HEALTHIEST node.

   Else if the value of the HEALTHIEST node is > 45%
          Send a ROUTE REQUEST message to the HEALTHIEST, second
          HEALTHIEST, third HEALTHIEST and fourth HEALTHIEST node.

   Else
          Flood the ROUTE REQUEST message.

5. If a node receives a ROUTE REQUEST message it will RELAY the ROUTE REQUEST
   message as in STEP 4.

6. If a node is a DESTINATION node OR receives a ROUTE REPLY message, it will
   initiate a ROUTE REPLY message to the nodes, from which it gets the ROUTE
   REQUEST message.
```

Fig. 1. Working principle of POMSec.

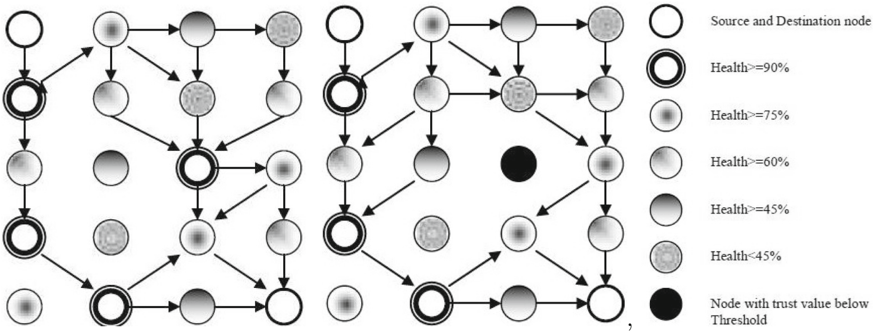
The above formula generates reward points for each nodes by assigning weights to α, β and γ. Also, these coefficients are normalized so that $\alpha + \beta + \gamma = 1$. Now, we can calculate the trust value as:

$$\text{“}Trust(t) = Trust(t-1) + Reward\text{”} \tag{5}$$

If the value for the variable *Trust* of a node, crosses the threshold value, then it considered as an attacker. The trust value of a node may vary according to Eq. (5).

3.2 Proposed Algorithm

An outline of our proposed algorithm using the above mentioned trust model is given in Fig. 1. The value of the metric *PATH* is increased by one, whenever a node receives a `ROUTE_REPLY` packet. A source node can transmits data using the path that's derived this way. The load to the destination node is distributed proportionally through the routes according to the health of each node.


Source and Destination node
Health>=90%
Health>=75%
Health>=60%
Health>=45%
Health<45%
Node with trust value below Threshold

(a) ETSeM (b) POMSec

Fig. 2. Data communication between Source and Destination using ETSeM and POMSec.

Figure 2(a) illustrates the route selection process of the ETSeM algorithm given in [1]. The significance of the algorithm after incorporating the trust model along the route selection process is depicted in Fig. 2(b). Figures 2(a) and (b) has the same set of nodes. The black node in Fig. 2(b) is detected as malicious in spite of its health more than or equal to 90%. This is because the trust value of the node is less than the threshold. POMSec can avoid all such malicious nodes in the route selection process with the help of the underlying trust model.

4 Experiments and Results

4.1 Simulation Settings

We have compared and analyzed the performance of POMSec with two different algorithms. First, another trust model, proposed in [2] is used with the ETSeM

Table 1. Parameter settings for simulation environment

Parameter	Value
Experimental area	$1500 * 1500\,\mathrm{m}^2$
Running time for each simulation	100 s
Mac Layer protocol	DCF of IEEE 802.11b standard
Traffic Model	CBR
Number of CBR traffics	10% of the total number of nodes
Mobility	Random Waypoint
Initial Energy level for each node	5000

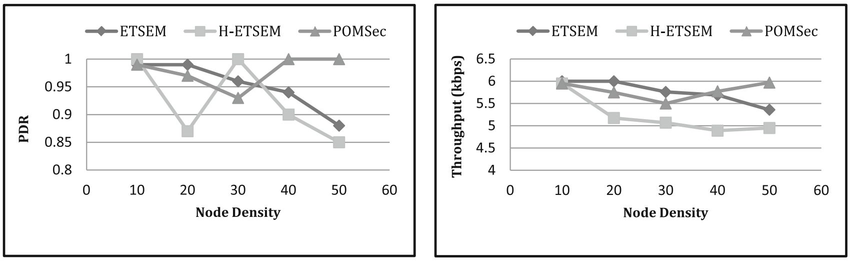
algorithm. Let's refer this change in the rest of this paper as H-ETSeM. Thereafter, extensive simulations of POMSec, ETSeM [1] and H-ETSeM have been successfully performed in QualNet and the results have been plotted as graphs and discussed accordingly. The simulation scenario and settings are described in Table 1 below:

4.2 Simulation Results

A quantitative analysis of POMSec and detailed comparison with ETSeM and H-ETSeM are presented in this section. The node density for each experiment varies between 10 nodes to 50 nodes and the mobility is set at 30 mps. We have used Constant Bit-Rate (CBR) traffic with 100 s runtime and 100 packets to transmit. A single CBR transmission is implemented for every 10 nodes, i.e., for forty nodes there will be four different CBR traffics in the experiment. Data has been collected for every variation in node density and then averaged for final results. These results are then plotted on graphs.

Packet Delivery Ratio. The first simulation checks the Packet Delivery Ratio (PDR) of POMSec and also compares it with others. PDR is an important parameter in routing and quite standard too. PDR represents the ratio of successfully receiving packets at destination over the packets sent by the sender through CBR traffic. Figure 3(a) shows the PDR for original ETSeM, H-ETSeM and POMSec. POMSec demonstrates more stable and higher PDR than the other two algorithms, inspite of having a trust based evaluation method in route selection.

Throughput. Throughput is a measurement of how much data passed through a network in unit amount of time. In this simulation we measured it in Kilobits/sec by observing CBR Server stats. The results in Fig. 3(b) shows that the throughput for POMSec is better comparing to the other two algorithms. POMSec obviously looks promising in terms of efficient path selection and decision-making and better throughput values.

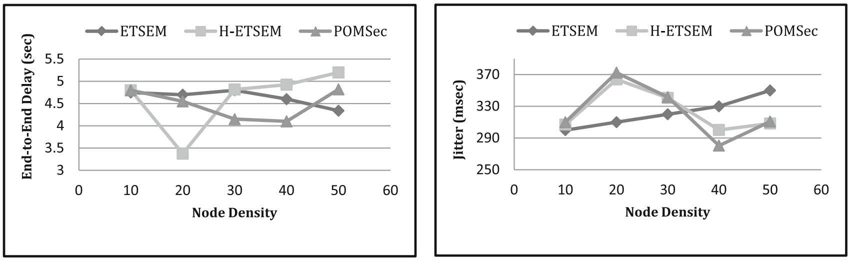


(a) Packet Delivery Ratio

(b) Throughput

Fig. 3. Comparative data analysis for PDR and throughput of ETSeM, H-ETSeM and POMSec.

End to End Delay. It represents the total time required by every CBR packet to reach its destination. Figure 4(a) depicts that POMSec offers much smaller delay than both the algorithms, which in turn proves the effectiveness of our trust model. H-ETSeM brings in more instability with increasing node density as compared to ETSeM. This actually confirms that the overhead for trust value updation increases with higher number of nodes.



(a) End-to-End Delay

(b) Jitter

Fig. 4. Comparative data analysis for End-to-end delay and Jitter of ETSeM, H-ETSeM and POMSec.

Jitter. In networking, the word jitter represents the average of the deviation of a packet against the mean latency of the network [16]. Figure 4(b) shows that the Jitter of H-ETSeM and POMSec are quite identical, and as the degree of nodes increase in the network, it appears to decrease and become stable after sometime.

Energy Depletion Rate. Energy efficiency is one of the most critical QoS metric for various Wireless environments. The calculations for energy depletion of each node according to their expenses for packet transmission, neighbourhood discovery, trust evolution and route maintenance, along with the updation rule

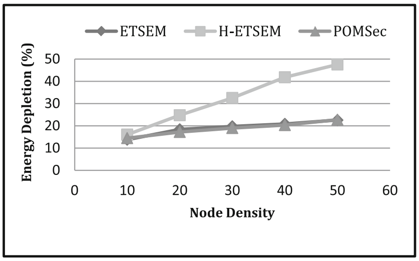


Fig. 5. Comparative data analysis for Energy depletion rate of ETSeM, H-ETSeM and POMSec.

has been additionally coded in simulation environment. The results in Fig. 5 are very interesting and informative. Inspite of additional trust evaluation overhead POMSec has almost similar trend as ETSeM. This confirms that our trust model is much light weight and it does not add extra burdens in the routing.

5 Conclusion

We have done a detailed study of the existing works in multipath routing and opportunistic routing in Sect. 2 of the paper. The survey reflects that many of them perform well in terms of throughput of the network and some of them are also energy efficient. However, none of these routing algorithms incorporate trust as a metric to determine the degree of multipath. Thats why we proposed an algorithm where trust evolution process is integrated with the route establishment process to provide security. Besides, a detailed comparison with other trust based approaches has been simulated in Qualnet and the results confirm that POMSec proves to be an improvement over existing algorithms, as it provides security as well as better throughput, PDA, delay and energy efficiency. POMSec has an unique feature that it distributed the traffic among nodes in such a way that the weaker nodes has lesser burden of routing than the nodes with more resources.

Acknowledgments. We would like to thank the Centre of Excellence in System Biology and Biomedical Engineering (TEQIP II), University of Calcutta for infrastructural and financial support towards publishing the results of our research work. This work is a part of the Ph.D. work of Manali Chakraborty, a Senior Research Fellow of Council of Scientific & Industrial Research (CSIR), Government of India. We would like to acknowledge CSIR, for providing the support required for carrying out the research work.

References

1. Chakraborty, M., Chaki, N.: ETSeM: a energy-aware, trust-based, selective multipath routing protocol. In: Cortesi, A., Chaki, N., Saeed, K., Wierzchoń, S. (eds.) CISIM 2012. LNCS, vol. 7564, pp. 351–360. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33260-9_30

2. Sen, P., Chaki, N., Chaki, R.: HIDS: honesty-rate based collaborative intrusion detection system for mobile ad-hoc networks. In: Computer Information Systems and Industrial Management, pp. 121–126 (2008)
3. Deb, N., Chaki, N.: TIDS: trust-based intrusion detection system for wireless ad-hoc networks. In: Cortesi, A., Chaki, N., Saeed, K., Wierzchoń, S. (eds.) CISIM 2012. LNCS, vol. 7564, pp. 80–91. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33260-9_6
4. Deb, N., Chakraborty, M., Chaki, N.: Honesty and trust bases IDS solutions. In: Chaki, N., Chaki, R. (eds.) Intrusion Detection in Wireless Ad Hoc Networks, pp. 111–145. CRC Press, Taylor & Francis Group (2014)
5. Lee, S.-W., Choi, J.Y., Lim, K.W., Ko, Y.-B., Roh, B.-H.: A reliable and hybrid multipath routing protocol for multi-interface tactical ad hoc networks. In: The Military Communication Conference, pp. 1531–1536 (2010)
6. Mueller, S., Tsang, R.P., Ghosal, D.: Multipath routing in mobile ad hoc networks: issues and challenges. In: Calzarossa, M.C., Gelenbe, E. (eds.) MASCOTS 2003. LNCS, vol. 2965, pp. 209–234. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24663-3_10
7. Marina, M.K., Das, S.R.: Ad hoc on-demand multipath distance vector routing, Computer Science Department, Stony Brook University (2003)
8. Ganjali, Y., Keshavarzian, A.: Load balancing in ad hoc networks: single-path routing vs. multi-path routing. In: IEEE International Advance Computing Conference, IACC 2009, pp. 32–34 (2009)
9. Lu, Y.M., Wong, V.W.S.: An energy-efficient multipath routing protocol for wireless sensor networks. Int. J. Commun. Syst. **20**, 747–766 (2007)
10. Xiong, L., Liu, L.: Building trust in decentralized peer-to-peer electronic communities. In: Proceedings of the 5th International Conference on Electronic Commerce Research (ICECR-5) (2002)
11. Zhang, J., Jeong, C.K., Lee, G.Y., Kim, H.J.: Cluster-based multi-path routing algorithm for multi-hop wireless network. Int. J. Future Gener. Commun. Netw. (2009)
12. Agrakhed, J., Biradar, G.S., Mytri, V.D.: Energy efficient interference aware Multipath Routing protocol in WMSN. In: 2011 Annual IEEE India Conference (INDICON), pp. 1–4 (2011)
13. Yahya, B., Ben-Othman, J.: REER: robust and energy efficient multipath routing protocol for wireless sensor networks. In: Global Telecommunications Conference, GLOBECOM, pp. 1–7. IEEE (2009)
14. Yahya, B., Ben-Othman, J.: RELAX: an energy efficient multipath routing protocol for wireless sensor networks. In: Proceedings of IEEE International Conference on Communications (ICC), pp. 1–6 (2010)
15. Varma, S., Tiwary, U.S., Jain, A., Sharma, T.: Statistical energy efficient multipath routing protocol. In: International Conference on Information Networking (ICOIN), pp. 1–5 (2008)
16. Comer, D.E.: Computer Networks and Internets, p. 476. Prentice Hall, Upper Saddle River (2008)
17. Hsu, C.-J., Liu, H.-I., Seah, W.K.G.: Opportunistic routing - a review and the challenges ahead. Comput. Netw. **55**, 3592–3603 (2011)
18. Boa, W., Chuanhea, H., Layuanb, L., Wenzhonga, Y.: Trust-based minimum cost opportunistic routing for Ad hoc networks. J. Syst. Softw. **84**, 2107–2122 (2011)
19. NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, U.S. Department of Commerce, January 2010

20. Cagri Gungor, V., Lambert, F.C.: A survey on communication networks for electric system automation. Comput. Netw. **50**, 877–897 (2006). Elsevier
21. Cheng, L., Niu, J., Cao, J.: QoS aware geographic opportunistic routing in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **25**(7), 1864–1875 (2014)
22. Yoon, S.-G., Jang, S., Kim, Y.-H., Bahk, S.: Opportunistic routing for smart grid with power line communication access networks. IEEE Trans. Smart Grid **5**(1), 303–311 (2014)
23. Qian, Y., Zhang, C., Xu, Z., Shu, F., Dong, L., Li, J.: A reliable opportunistic routing for smart grid with in-home power line communication networks. Inf. Sci. **59**, 1–13 (2016). Science China Press and Springer-Verlag Berlin Heidelberg