Reputation-based Energy Efficient Opportunistic Routing for Wireless Sensor Networks

Nagesh Kumar[1], Yashwant Singh[2], Pradeep Kumar Singh[1]
[1]Department of Computer Science and Engineering,
Jaypee University of Information Technology,
Waknaghat, Solan, INDIA-173234
[2]Department of Computer Science and Information Technology
Central University of Jammu, INDIA
engg.nagesh2@gmail.com

***Abstract*—Selection of the best next-hop in Opportunistic Routing (OR) is a crucial task in wireless sensor networks (WSN). To increase the throughput, network lifetime and reliability of WSN, there is a need of an optimal OR protocol. To improve the reliability of network, reputation management is important. Reputation management gives a chance to nodes to transmit data on secure and reliable routes. This paper gives a new reputation based OR metric and protocol, in which the next hop selection is based on its reputation. The proposed OR metric considers the reputation level as a primary selection parameter for next-hop. New OR metric relies on energy efficiency and packet delivery ratio of next-hop. Proposed OR protocol selects all middle position neighbors as next-hop and potential forwarder will be decided on the basis of new OR metric. Energy consumption is considered to be dynamic. The protocol has been compared with Middle Position Dynamic Energy Opportunistic Routing (MDOR), and Trust and Location Aware Routing Protocol (TLAR). Simulation results depict that the proposed OR protocol optimized the throughput and network lifetime.**

***Index Terms*—End-to-end Delay; Energy Efficiency; Next-Hop Selection; Reputation; Trust; Opportunistic Routing; Throughput.**

I. Introduction

WSN are most demanded networks in present scenario because of their abundance of applications in real life like defense, environment, and health. In most of the applications the sensor nodes are left unattended, and expected to operate on their own [1, 7]. Although, sensor nodes in WSN are resource constraints having less capabilities, less energy and less storage capacity. Hence, the researchers have to focus on the development of protocols which are able to work with these constraints. Also, the unattended nodes are prone to several attacks, which in turns reduces the capabilities of the network. Most important capability parameters for WSN are throughput, end-to-end delay, and network lifetime (energy efficiency). The performance of these parameters is dependent on routing protocols, and security methods used while transmitting data.

In recent years, OR has been introduced as a new routing paradigm to be used in ad-hoc and sensor networks. OR methods select a set of potential forwarder nodes, which will cooperate to forward data toward base-station (sink/destination) [7]. The idea of designing OR is to utilize the broadcasting property of wireless nodes. The selection of potential forwarders is based upon a routing metric, which is used to shortlist these forwarders from neighbor list. The set of shortlisted candidates is called as candidate set. Next-hop forwarder will be a node in between this candidate set, which is being chosen on the basis of next-hop selection metric.

Researchers [10, 11] have focused on developing new OR metrics [23] for candidate set selection and also forwarder candidate selection. These metrics can be implemented as end-to-end selection metrics or local selection metrics. The end-to-end selection method selects the candidate set on the basis of delivery probability of links from source to destination. While, in the case of local selection methods, candidate set has been decided on the basis of neighborhood information only. Local selection metrics introduces an improvement in reducing delays in the network [23]. In both candidate selection methods it is being assumed that sensor nodes will coordinate with each other. But in a real scenario, if a node has been affected by a malicious attack, then it may or may not coordinate with other nodes. For example, in a black-hole attack the affected node stop forwarding the packets towards other nodes. These types of problem need special treatment mechanisms in routing algorithms.

Working in this direction, there is a huge research has been carried out to tackle with security attacks on routing process. But most of the methods are based on cryptosystems [2-6] which are not efficient in resource constrained WSN. Hence, trust and reputation based methods have been introduced in recent years. These trust and reputation models are the subsets of security methods. These methods use trust based metrics, and if a node having inappropriate trust metric value it will be isolated from the neighbor list of each node.

This paper introduces a novel reputation based OR metric. This metric considers energy efficiency and reputation of a node on the basis of the packet forwarding ratio (PFR), to select next-hop candidate forwarders. The paper proposes an extension to the previous work, i.e. middle position dynamic energy OR algorithm. It is being extended to improve energy efficiency and provide reputation based security for network and data.

The structure of the rest of the paper is as follows. The next section of the paper presents the research related to OR and reputation based routing protocols by other authors. A broad description of the proposed reputation and energy aware OR protocol has been presented in section 3. Section 4 covers the performance analysis and simulation of the proposed work in view of various network constraints. Lastly, section 5 concludes the paper and discuss certain forthcoming works.

II. Related work

This section provides a brief view of related research work carried out for OR and reputation management, in recent years. This section describes energy efficient OR protocols, and reputation based routing protocols.

ExOR [8] the first OR protocol was introduced to increase the overall throughput of wireless ad-hoc networks. The idea was to utilize the broadcasting capabilities of wireless antenna. The protocol was based on a metric called as expected transmission count (ETX) [8]. This metric calculates the minimum number of transmissions required to send a packet from source to destination. Working in the same direction expected any path transmission (EAX) [9] was proposed, which was more efficient for WSN than ETX. Based on this metric an OR protocol was proposed named as LCOR [12]. This protocol was expensive in terms of energy for large scale WSN. SOAR [13] has been developed recently by using ETX as next-hop selection metric. It reduces the number of duplicate packets in the network. Middle position dynamic energy OR (MDOR) [24] was proposed to reduce the end-to-end delay and improve network throughput. MDOR is good in terms of optimizing the network lifetime and end-to-end delays. It selects middle sensor node from the neighbor list on the basis of the location of the node. In these simple OR protocols the focus has been given on timely data delivery and a little focus has been given on energy efficiency and security of communication process and data.

Trust and reputation management methods are of greater interest in WSN. Because, these methods are lightweight in terms of calculation and energy consumption. There are some trust and reputation aware protocols proposed in the last five years like CONFIDANT [14], CORE [15], and SORI [16] etc. As far as OR is concerned there are very few trust aware OR methods are available in the literature. Salehi et.al [17] have proposed OR framework on the basis of their proposed metrics (RTOR, TORDP and GEOTOR). But this framework is mainly concerned for wireless ad-hoc networks and performance will be degraded in wireless sensor networks. For WSN few researchers have developed trust aware routing methods like TARF [18], EMPIRE [19], ETARP [20], TLAR [22] and TESRP [21].

This paper presents a reputation based OR protocol, which is the extension to MDOR [24] and provide data reliability and good throughput in the presence of malicious nodes. The protocol will be briefly discussed in the upcoming section. New OR protocol is reputation and energy efficiency based and hence is more reliable than MDOR.

III. Proposed Work

The proposed OR protocol considers reputation and energy efficiency as major components of candidate selection metric. The reputation of a node is used to isolate the malicious sensor nodes from neighbor list. The energy efficiency component calculates the effect of each transmission on the energy of transmitting and receiving nodes. Every time the algorithm run in the network the new candidate set for each node may not be the same always. Following sub-sections discuss the proposed work in detail.

A. Forwarder Selection Metric

The proposed forwarder selection metric has two components: packet forwarding ratio and energy effect. Packet forwarding ratio is used to identify the nodes which are not sincerely forwarding the received packets and not acknowledging the packets forwarded toward them. *PFR* for a node i can be calculated by the following equation.

$$PFR_i = \frac{P\_fwd_{i->next\_hop}}{P\_sent_{source->i}} \tag{1}$$

where, $P\_fwd_{i->next\_hop}$ is the number of packet forwarded by the node i towards its next-hop node and $P\_sent_{source->i}$ is the number of packets sent by the source node towards node i.

The second component is the energy effect calculation on a node’s total energy. This effect is dependent upon the energy consumed during transmission, reception and sensing acknowledgements. This effect on energy consumption for each node can be calculated as follows.

$$E\_effect = \frac{E_{recieving} + E_{transmitting} + E_{ack\_sending}}{E_{total}} \tag{2}$$

Receiving ($E_{recieving}$), transmitting ($E_{transmitting}$) and acknowledgement ($E_{ack\_sending}$) sending energies have been calculated as given in MDOR [24]. Total energy (E_{total}) is the amount of energy remaining in the corresponding sensor node. After calculation of these two components the reputation value (*T_Value*) of a sensor node is calculated by the following equation.

$$T\_Value = \frac{\alpha.PFR + \beta.E\_effect}{\alpha + \beta} \tag{3}$$

Here, α and β are the adjustment values for both trust value components *PFR* and *E_effect* respectively. These are the weights according assigned to the components on the basis of the importance of each factor.

B. Reputation based Energy Efficient OR Protocol

In WSN the sensor node collects data from the field and send it toward base station. OR utilizes multiple routes advantage of wireless links, and selects one of the best suitable routes for data communication. As discussed in MDOR [24] it selects the forwarder nodes from the neighbor list, which are neither near nor too far away from the destination. This protocol optimizes the distance of the forwarder from source and destination. This process continues till the data packets reach the destination. But as we can see there is no mechanism of avoiding a malicious node in MDOR [24]. We have introduced a reputation management for the middle position nodes.

For the middle position sensor nodes, the trust aware forwarder selection metric has been calculated. If the *T_Value* is below a certain threshold, then it will not be selected as next-hop. This node will be removed from forwarder list. The trust value (*T_Value*) threshold has been fixed to 0.2 in our algorithm. This value has been fixed after extensive simulations has been carried out with different trust values like 0.1, 0.2, 0.3… 1. If the trust value is too higher than most of the nodes will not be able to transmit data after some energy consumption. This is because the trust value is dependent on energy consumption of the node. Also, if the trust value is very low than a single node will be selected again and again to transmit data. This is because we are selecting only middle nodes as next forwarder. This process of trust value calculation will be repeated for all nodes until the destination is reached. For every new data transmission the trust value has been updated by recalculation. The algorithm below shows the new Reputation based Energy Efficient OR Protocol. Also a flowchart has been given in Figure 1.

```
Input: source node S, target node D, dist(S, D).
Output: Successful transmission of data packet from node S to node D
1. Define S as Source Node
2. Create neighbor list NGH for S
3. Sort neighbor list according to distance
4. if D is neighbor of S
5. Send data packets to D
6. else
7. FNL is the subset of NGH (FNL is the forwarder node list)
8. Select the middle node (FWD) from FNL i.e. (neither near to S nor near to T).
9. Calculate trust value (T_Value) for each middle node using equation 3.
10. ifT_Value>= 0.2
11. Start communication with FWD
12. else
13. {
13. Discard FWD from FNL.
14. Select second middle node from FNL and name it as FWD.
15. Repeat from step 9 to 14
16. }
17. if FWD is equal to D then stop algorithm
18. else repeat step 2 to step 18 until D is reached
```

Whole algorithm works same as MDOR except that it calculates the trust value for each node on forwarder list and select forwarder on the basis of this trust value. As the trust value considers forwarding sincerity as a parameter, the attacks like a black hole, worm hole can be detected and prevented easily in this case. Also trust value considers the energy consumption effect also there will be improvement in lifetime of sensor node and obvious improvement in network lifetime of WSN.

IV. Simulation Results And Analysis

The performance of proposed protocol has been recorded in the presence of malicious nodes and compared to two other algorithms i.e. MDOR [24] and TLAR [22], which are proposed recently for WSN. TLAR is a trust and location aware routing protocol, which calculates trust value for the nodes in between the source and destination nodes. It has considered five trust metrics for trust value calculation.

A. Simulation Parameters

The performance of proposed algorithm has been tested by creating simulation using NS2. Table 1 shows the settings of parameters in NS2 simulation environments.

All the three protocols have been built over NS-2.35 and being tested for performance parameters. For the purpose of getting a better view of analysis the protocols have been tested by generating a different number of malicious nodes in the network. All the malicious node has been chosen randomly. The malicious node behaves differently in the network. Such as they do not forward the received packets, send no acknowledgements and do not coordinate properly with other normal nodes in the network.

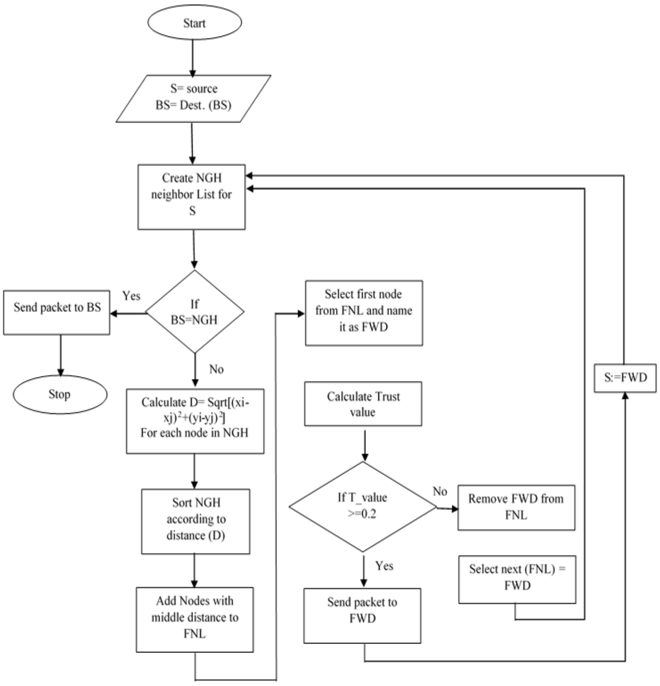

Figure 1: Reputation Based Energy Efficient OR Protocol

Table 1
Parameters for Simulation

Parameter	Value
Simulator	NS-2.35
Area of Deployment	500 x 500 m^2
Transmission Range	60 m
No. of Nodes (N)	100
No. of Malicious nodes	10, 20, 30, 40 and 50
Traffic Type	CBR (Constant Bit Rate)
Packet Size	32 bytes
Data Transmission Rate	5 packets/sec
Simulation Time	1000 sec
Initial Energy	100J
Initial Trust Value	1
Default α and β	0.4 and 0.3
Energy dissipation to run the radio ($E_{electronic}$)	50 nJ/bit
Buffer Length	30 packets

B. Results and Discussions

The network performance has been measured for all three protocols, and presented in the form of graphs. Figure 2 shows the performance of protocols on the basis of the packet delivery ratio (PDR) in the presence of malicious nodes. It can be seen that the proposed method has moderately high PDR as compared to MDOR [24] and TLAR [22]. This is due to the fast calculation of reputation value in the case of the proposed protocol. MDOR does not have any method to tackle with malicious nodes.

Hence, with the increase in malicious nodes packet delivery ratio for MDOR decreases rapidly. In TLAR, as discussed earlier, there is a need to calculate five trust metrics and hence this will increase overhead. Therefore, TLAR shows low performance as compared to the proposed approach.

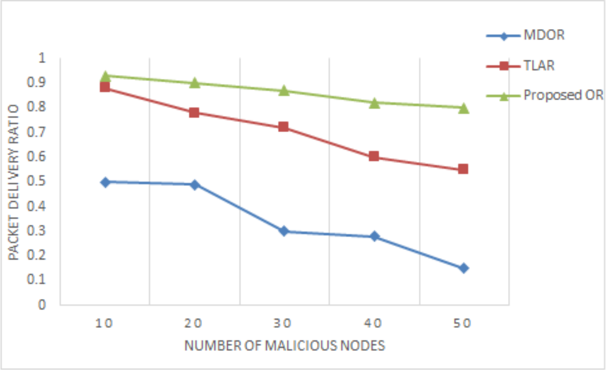

Figure 2: Comparison of MDOR, TLAR and Proposed OR in terms of Packet Delivery Ratio

Figure 3 presents the End-to-End delay. It can be depicted from the figure that end-to-end delay in case of MDOR is low because of the absence of reputation and trust methods. But in case of TLAR and Proposed protocol the end-to-end delay goes on fluctuating around similar values. If we talk about average End-to-End delay, proposed protocol shows little bit improvement over TLAR. This is because of the less overhead for the calculation of reputation values in the case of the proposed protocol.

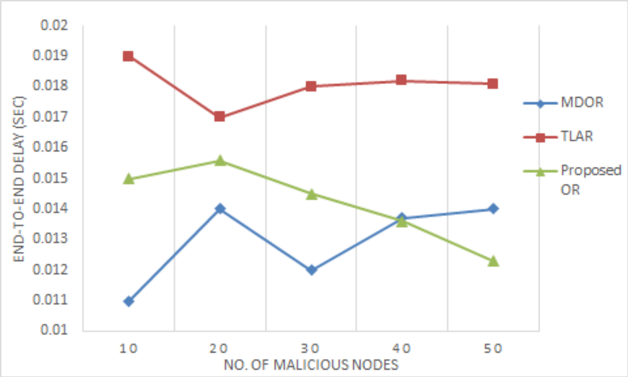

Figure 3: Comparison of MDOR, TLAR and Proposed OR in terms of End-to-End Delay

Figure 4 plots the energy consumption in the network. It is defined as the average energy consumption per node in the network, while performing the various tasks in the network. Most of the energy consumed in transmitting and receiving packets during network operation. Hence the energy consumption directly proportional to the radio energy consumption while transmitting and receiving packets. Proposed OR protocol has the lowest energy consumption as compared to TLAR and MDOR. MDOR mainly meant for dynamic energy consumption and do not work well when the energy consumption for transmission and reception of packets has been fixed. Similarly TLAR is mainly designed to provide secure routing and energy efficiency has not been paid much attention. Hence, proposed protocol works better. As far as the energy efficiency of the network has been improved, the network lifetime will automatically be increased.

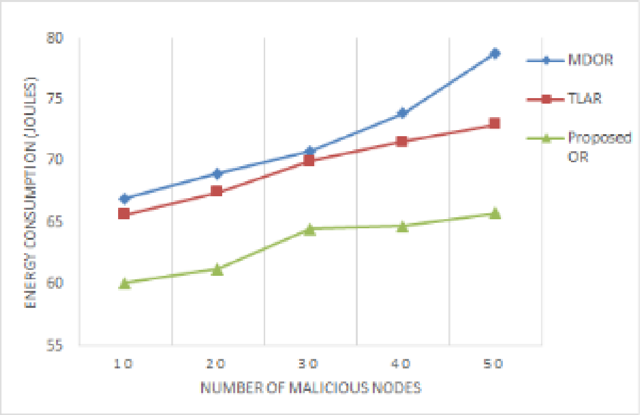

Figure 4: Comparison of MDOR, TLAR and Proposed OR in terms of Energy Consumption

V. Conclusion

In this paper, a novel OR protocol has been presented, which introduces reputation awareness in the next-hop selection. Reputation management is an important feature. It can be used to avoid a number of unnecessary and duplicate transmissions in the presence of malicious nodes. Also the proposed protocol if energy efficient, because it considers the effect of each transmission and reception of packets on node's total energy. The proposed protocol's candidate forwarder selection metric is composed of these two components. The simulation and performance analysis has been done by comparing the proposed protocol, MDOR and TLAR. The results showed that proposed OR protocol has good performance in the presence of malicious nodes. The proposed method optimizes the energy efficiency, end-to-end delay and packet delivery ratio in WSN. In the future direction we can consider more parameters and metrics' components to improve network performance by considering the properties of WSN.

References

[1] Akyildiz, I.F., and Kasimoglu, I.H.: 'Wireless sensor and actor networks: research challenges', Ad hoc networks, 2004, 2 (4), pp. 351-367.

[2] Lyu, C., Gu, D., Zhang, X., Sun, S., Zhang, Y., and Pande, A.: 'SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs', Computer Communications, 2015, 59, pp. 37-51.

[3] Shaikh, R.A., Jameel, H., d'Auriol, B.J., Lee, H., Lee, S., and Song, Y.-J.: 'Group-based trust management scheme for clustered wireless sensor networks', IEEE transactions on parallel and distributed systems, 2009, 20 (11), pp. 1698-1712.

[4] Yao, L., Man, Y., Huang, Z., Deng, J., and Wang, X.: 'Secure Routing based on Social Similarity in Opportunistic Networks', IEEE Transactions on Wireless Communications, 2016, 15 (1), pp. 594-605.

[5] Yao, Z., Kim, D., and Doh, Y.: 'PLUS: Parameterized and localized trust management scheme for sensor networks security', in proceedings of International Conference on Mobile Ad Hoc and Sensor Systems (IEEE), Vancover, BC, 2006, pp. 437-446.

[6] Zhou, Y., Tan, X., He, X., Qin, G., and Xi, H.: 'Secure Opportunistic Routing for Wireless Multi-Hop Networks Using LPG and Digital Signature', Information Assurance and Security Letters 1, 2010, pp. 18-23.

[7] Kumar, N., and Singh, Y.: 'Routing Protocols in Wireless Sensor Networks', in Niranjan, K.R., and Ashok Kumar, T. (Eds.): 'Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures' (IGI Global, 2016), pp. 86-128.

[8] Biswas, S., and Morris, R.: 'ExOR: opportunistic multi-hop routing for wireless networks', in Proceedings of 35th SIGCOMM Computer

Communication Review (ACM, 2005), Philadelphia, Pennsylvania, USA, pp. 133-144.

[9] Zhong, Z., Wang, J., Nelakuditi, S., and Lu, G.-H.: 'On selection of candidates for opportunistic anypath forwarding', ACM SIGMOBILE Mobile Computing and Communications Review, 2006, 10 (4), pp. 1-2.

[10] Hsu, C.-J., Liu, H.-I., and Seah, W.K.G.: 'Opportunistic routing: A review and the challenges ahead', Computer Networks, 2011, 55 (15), pp. 3592-3603.

[11] Liu, K., Abu-Ghazaleh, N., and Kang, K.-D.: 'Location verification and trust management for resilient geographic routing', Journal of Parallel and Distributed Computing, 2007, 67 (2), pp. 215-228.

[12] Dubois-Ferriare, H., Grossglauser, M., and Vetterli, M.: 'Valuable detours: Least-cost anypath routing', IEEE/ACM Transactions on Networking, 2011, 19 (2), pp. 333-346.

[13] Rozner, E., Seshadri, J., Mehta, Y.A., and Qiu, L.: 'SOAR: Simple opportunistic adaptive routing protocol for wireless mesh networks', IEEE Transactions on Mobile Computing, 2009, 8, (12), pp. 1622-1635

[14] Ganeriwal, S., Balzano, L.K., and Srivastava, M.B.: 'Reputation-based framework for high integrity sensor networks', ACM Transactions on Sensor Networks (TOSN), 2008, 4 (3), pp. 15.

[15] Michiardi, P., and Molva, R.: 'Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks': 'Advanced communications and multimedia security' (Springer, 2002), pp. 107-121.

[16] He, Q., Wu, D., and Khosla, P.: 'SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks', in Proceedings of Wireless communications and networking conference (IEEE, 2004), Atlanta, GA, USA, pp. 825-830.

[17] Salehi, M., Boukerche, A., Darehshoorzadeh, A., and Mammeri, A.: 'Towards a novel trust-based opportunistic routing protocol for wireless networks', Wireless Networks, 2016, 22 (3), pp. 927-943

[18] Deng, H., Yang, Y., Jin, G., Xu, R., and Shi, W.: 'Building a trust-aware dynamic routing solution for wireless sensor networks', in Proceedings of Globecom Workshops (IEEE), Miami, Florida, USA, 2010, pp. 153-157.

[19] Maarouf, I., Baroudi, U., and Naseer, A.R.: 'Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks', IET communications, 2009, 3 (5), pp. 846-858.

[20] Gong, P., Chen, T.M., and Xu, Q.: 'ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks', Journal of Sensors, 2015.

[21] Adnan, A., Kamalrulnizam Abu, B., Muhammad Ibrahim, C., and Abdul Waheed, K.: 'A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network', Mob. Netw. Appl., 2016, 21 (2), pp. 272-285.

[22] Vamsi, P.R., and Kant, K.: 'Trust and Location-Aware Routing Protocol for Wireless Sensor Networks', IETE Journal of Research, 2016, 63, pp. 1-11.

[23] Kumar, N., and Singh, Y.: 'An Energy Efficient Opportunistic Routing Metric for Wireless Sensor Networks', Indian Journal of Science and Technology, 2016, 9 (32), pp. 1-7.

[24] Sharma, M., & Singh, Y. Middle Position Dynamic Energy Opportunistic Routing for Wireless Sensor Networks. In IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 948-953.