Volume 7, Issue 1, January 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Energy Efficient based Opportunistic Routing Metric for Wireless Sensor Networks

Sharda Rani
Assistant Professor, Department of Computer Science, R.K.S.D College,
Kaithal, Haryana, India

DOI: 10.23956/ijarcsse/V7I1/0116

Abstract— Existing cryptographic methods are not suitable for sensor networks because of their limited resources and opportunistic behavior of wireless nodes. In last four years, reputation and trust aware methods are used to solve the issue of security in WSN. Data security in transit is an important issue for reliable delivery of data in WSN. In this paper, we have defined a new opportunistic routing (OR) metric for sensor networks. The metric is derived by using energy consumption and trustworthiness of sensor nodes. The simulation result shows that the metric is able to detect a malicious activity in the network segment. This metric effectively and efficiently prevent from malicious activities and maintain data integrity.

Keywords— Routing Metric, WSN, Trust, Secure Routing, Opportunistic Routing,.

I. INTRODUCTION

Cryptographic algorithms are not efficient in case of energy and storage in WSN, because of the limited resources available in sensor nodes [3]. Hence, there is a need of cooperation among sensor nodes in the network for security purpose. But, taking the assumption of hundred percent coordination is not valid. Sensor nodes in the deployment fields can easily be misconfigured, captured or hijacked by the attackers. The attackers may try to inject false information in the network or try to destroy the network. However in recent years, researchers [4-8] have proposed cryptography based routing algorithms/protocols, but these algorithms are mostly provide solution for outside attacks. These algorithms are ineffective when there are insider attacks from malicious sensor nodes. If we apply cryptographic algorithms for fighting with inside attacks, than a lot of energy will be wasted and network dies soon. Hence there should be cooperation and trust management between sensor nodes. To make successful deliveries of data packets at base station the trust management must be applied to routing process. The sensor nodes which are having low trust values must not be included in routing process.

As WSN are opportunistic networks in nature [9], rather than using fixed path routing, opportunistic routing is very useful. But, when we talk about secure opportunistic routing protocols/algorithms, either there are no proposed secure OR protocols/algorithms in literature or there are very few which are not much efficient in terms of energy and storage. The OR protocols must provide security and efficiency together. The security in opportunistic routing protocols can be improved by applying routing decisions on the basis of trust values of sensor nodes in the network. To increase the probability of a packet to reach destination, sensor nodes can utilize the trust based route dependability information.

In opportunistic routing major phases are: forwarder set selection and forwarder node selection. The source, when has data to be sent over wireless link, firstly choose the forwarder set from the neighbor set. For this purpose there is a requirement of certain criteria to be set. The forwarder set selection process exclude those nodes which are not able to fulfill the criteria. After this process the candidate forwarder is selected and given high priority on the basis of opportunistic routing metric (like ETX [10], mETX [11], EAX [12] etc.). The routing decision in OR is purely dependent upon the metric chosen for selecting candidate forwarder node [13].

In this paper, a novel trust aware and energy efficient opportunistic routing metric has been proposed which is specially designed for OR protocols in WSN. This metric will be compatible with previously proposed OR protocols for WSN. The metric not only improve the lifetime of the network but also the reliability and integrity of data. Major contributions of this research work are given below.

- A novel OR metric has been proposed, which considers the node trust value and energy efficiency as major design factors. The parameters for designing the trust aware and energy efficient OR metric are energy of the nodes, trust value of nodes, and link delivery probability among nodes.
- Simulation has been planned and executed to check the performance of the proposed OR metric and framework applied to existing OR protocols. Simulation results validate that incorporating the proposed trust metric into Destination Sequenced Distance Vector Routing (DSDV) protocol. It can considerably increase the performance of DSDV communications in hostile environments.

II. RELATED WORK

The first and popular OR protocol has been proposed by Biswas and Morris [2], and called as EXOR [10]. The authors shown that this new idea of routing can work more efficiently and effectively in wireless networks. Authors have proposed a metric, called as Expected Transmission Count (ETX) [10], for forwarder candidate set selection. This metric calculates the number of transmissions required for a data packet to reach destination. Forwarder candidate nodes was chosen from the set of neighbor nodes. Later Expected anypath transmission (EAX) [12] metric has been proposed by Dubois-Ferrie`re et al. [16]. On the basis of this metric they have proposed an OR protocol and named it as LCOR. But, EAX is computationally complex and expensive for large scale wireless networks. Similar to EXOR, [17] presented SOAR which uses ETX as a metric for candidate forwarder selection, but it mainly tries to decrease the number of duplicate data packets to be received at destination node. In existing OR protocols the focus has been given on timely data delivery and no or very little emphasis has been given to security of data and routes in communication.

Security is always crucial in wireless networks, as the data packets are sent on unsecured and open wireless links [18]. Cryptography methods provide external security to the network, so that any attacker from outside cannot harm the network [3]. But to cope with internal attacks there is a need of coordination among nodes and security within the network. To provide internal security in WSN there is a need of lightweight methods. Because, sensor nodes have less capabilities like less energy, low storage and small computation power etc. Trust and management systems are very lightweight and easily computable and improve security of communication within the network.

Researchers in recent year have developed trust and reputation management protocols and algorithms for ad hoc networks, internet of things and other mobile wireless networks. Some common names of protocols include CONFIDANT [19], CORE [20] and SORI [21] etc. Salehi et al. [22] has proposed some metrics and a trust aware routing framework for wireless networks recently. There have proposed three routing metrics i.e. RTOR [22], TORDP [22] and GEOTOR [22], for opportunistic routing protocols for calculating the trust value. They have proposed a trust aware opportunistic routing protocol previously, which is also developed for wireless networks. But these all are not purely meant for WSN and does not work well in sensor networks. Also for opportunistic routing, to the best of our knowledge, very few trust based systems have been proposed.

Trust management in WSN has also been focused during last three years. As sensor nodes have limited resources, researchers try to balance between security and utilization of resources. Deng et.al. have proposed a dynamic routing framework for WSN, which incorporates social network theories of trust and named it as TARF [23]. TARF uses conventional cryptographic approaches as complementary methods and provide security solutions for WSN. Energy efficiency is an issue in this protocol. Working in WSN security EMPIRE [24] protocol has been proposed. This is probabilistic and distributed monitoring approach. It tries to decrease monitoring tasks per node and save energy, by maintaining the appropriate security level. Another trust based routing protocol for WSN has been proposed and named as ETARP [25]. This protocol define routing paths on the basis of maximum utilization of resources with lesser communication cost. But this is also not, much energy efficient approach having greater overhead. Recently, TESRP [26] has been proposed by Ahmed et.al which is also designed to save energy and lower the cost and overhead in routing process for WSN. TLAR [27] has been proposed especially for WSN. TLAR calculates the consolidated trust values using direct and indirect observations of its neighbors. This routing scheme adjust the route weight values dynamically again and again. This increase the overhead and communication delay introduces.

In this paper we have presented a trust aware energy efficient opportunistic routing metric for WSN. It is being evaluated by extensive simulations to check the effect of new metric on various performance parameters. The routing metric proposed here has been checked with existing broadcasting algorithm DSDV.

III. TRUST AWARE ENERGY EFFICIENT OR METRIC

As discussed in literature very few researchers have focused on security and energy efficiency in opportunistic routing for WSN. In this research a new trust aware energy efficient opportunistic routing metric has been proposed, provide security of data in transit and improve lifetime of the network. Energy cost model will be the same as in our research paper published recently [28].

In opportunistic routing the most important phase is considered is the forwarder candidate set selection. In wireless sensor network, after sensing data, each sensor node form a list of its neighbors. From neighbor list, the forwarder candidates has been chosen and is given a priority value. The highest priority node will first transmit the data first. Opportunistic routing make it possible to utilize broadcasting nature of wireless links. To find the best wireless link routing metrics have been applied to OR.

In this section a new opportunistic metric has been introduced especially for OR protocols in WSN. This metric is distributive in nature. This metric needs information about forwarder nodes' ID, energy and packet reception ratio. After collection of these values, the node calculates forwarding ratio, acknowledgement impact and energy consumption. By including these all values trust value has been calculated. Distance (*D*) between nodes is not required as major criteria, especially for opportunistic routing in WSN. Hence, distance will be used only for checking the packet forwarding progress (*PFP*) towards destination (Eq. 1 and Eq. 2).

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$$

$$\text{where } 0 \le i, j \le k \text{ , and } i \ne j \qquad (1)$$

$$PFP_{n_i}^{s,d} = D_{s,d} - D_{n_i,d}$$

where s=source, d=destination, $0 \le n_i \le k$ (2)

A. Proposed Metric

In opportunistic routing the forwarder node and the path of data packets have been decided at the time of transmission. Each sensor node maintain a matrix of trust evaluation factors about other nodes and calculate the trust value for each forwarder candidate in neighbor list. Metric calculation involves two step process as described in below.

Step 1: Trust Evaluation

In this step, sensor node, when has data to send, form its neighbor list and extract the forwarder candidates on the basis of packet reception ratio (*PRR*) as calculated below in Eq. 3.

$$PRR_i = \frac{P_{recieved}}{P_{sent}}$$

where $0 \le PRR_i \le 1$ (3)

As soon as the forwarder list has been made, the nodes now start calculating the trust value for each node in the forwarder list. The trust evaluation consists of following trust factors.

1) Node Identification (*ID*): This factor contains the location information and the identity of the forwarder candidate node. Source node collect this information from each node in the forwarder list.

$$ID_i =< NodeID_i, Location\_coordinates_i, Energy_i >$$

where $0 \le i \le k$

2) Forwarding Sincerity (*F*): This factor represents, whether the forwarder candidate node is forwarding the data packets successfully or not. This record is maintained by using the calculation of success and failure counts. Initially this value will be 1 for each forwarder node.
   - F_i : Forwarding sincerity value of node i
   - FS_i : Forwarding success count of node i
   - FF_i : Forwarding failure count of node i.
3) Energy Depletion (*E*): This factor calculates the energy consumption for each transmission made by a node. This factor is based on the information of node's total energy. Also. This factor is used to calculate the lifetime of the node and the network. This factor is used to check whether the energy depletion is greater than threshold or not. If it is greater than threshold than the node cannot transfer data packets and excluded from the forwarder set. Otherwise a priority has been set according to the value of this factor.
   - E_{total_i} : Total energy impact of node i

$$E_{total} = E_{total} - (E_{tx} + E_{rx} + E_{ack}) \quad (4)$$

where, E_{tx} : Transmission energy, E_{rx} : Receiving energy, E_{ack} : Acknowledgement sending and receiving energy.

4) Acknowledgement Sincerity (*ACK*): This factor calculates the acknowledgement sending and receiving sincerity among nodes. This record is maintained by using the calculation of success and failure counts of acknowledgements transmissions. Also, this value is useful to calculate the probability of retransmission of packets. Initially this value will be 1 for each forwarder node.
   - ACK_i : Acknowledgement sincerity value of node i
   - $SACK_i$: Acknowledgement success count of node i
   - $FACK_i$: Acknowledgement failure count of node i.
5) Trust Value (*T*): This factor gives the total trust value of a node and it will be evaluated on the basis of all trust evaluation factors. This value is dynamic in nature, because it needs to update again and again for every new transmission of data packets.
   - T_i : Trustworthiness of node i.

Step 2: Trust Value Calculation

All trust evaluation factors, discussed above, values has been recorded in a matrix. As these values are discrete, we cannot directly judge the value in a logical decision of trusting a node or not. Hence, the next step is to quantize the values of trust factors, so that the values will be transformed into continuous values from -1 to +1. Here -1 means no trust and +1 means full trust. Trust quantification for each trust factor can be calculated as follows:

1) Forwarding Sincerity Value

$$F_i = \frac{FS_i - FF_i}{FS_i + FF_i}, \text{ subject to } -1 \le F_i \le 1 \quad (5)$$

2) Energy Depletion Value

$$E_{total_i} = \frac{E_{tx} + E_{rx} + E_{ack}}{E_{total}}, \text{ subject to } -1 \le E_{total_i} \le 1 \quad (6)$$

3) Acknowledgement Sincerity Value

$$ACK_i = \frac{SACK_i - FACK_i}{SACK_i + FACK_i}, \text{ subject to } -1 \le ACK_i \le 1 \quad (7)$$

Finally using these values total trust has been computed, which involves the weighting process. Each trust evaluation factor has been assigned a weight. The weights represents the importance of each trust factor. The value will be 0 for unimportant factor and 1 for most important factor. These weights are dependent on the type of the applications of WSN. After the completion of this process the trust value will be calculated by the following equation.

$$T_i = \frac{\alpha * F_i + \beta * E_{total_i} + \gamma * ACK_i}{\alpha + \beta + \gamma}, \text{ where } -1 \le \alpha, \beta, \gamma \le 1 \quad (8)$$

Here, α is the weight adjustment for forwarding sincerity, β is the weight adjustment for Energy depletion and γ is the weight adjustment for acknowledgement sincerity. If the energy value is lower than a specified threshold, than the node will be excluded from the forwarder list, because this node is not able to forward data packets. And the value of trust, T_i in this case will be -1.

As each sensor in involved in calculating the trust value in the network, some malicious nodes which are creating problems like inconsistent data, malicious data, and blocking data packets at one point can be detected and reported in this step.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the security and energy performance of proposed trust aware opportunistic routing metric. The metric has been applied in DSDV protocol and simple DSDV [29], Ad-hoc On Demand (AODV) [30] and modified DSDV (proposed) has been tested in WSN scenario. The security performance comprises the average number of malicious nodes have encountered during a transmission. A specific malicious ratio has been given in every simulation. On the other hand, energy performance is calculated by checking the energy efficiency of each node after each successful or unsuccessful transmission in the presence of malicious nodes.

A. Simulation Setup

The simulations has been carried out by using MATLAB. The scenario considered over here contains single base station with static sensor nodes in a field area of 500 x 500 m. The transmission has been considered successful only when base station receives the packet. Many experiments has been conducted considering single base station and continuous communication model with N sensor nodes. The source has been chosen randomly, which will initiate the communication.

Table 1 Simulation Parameters

Parameter	**Description**
Area	500 x 500 m
Range of Radio	200 m
Number of Nodes	50-100
Traffic Type	CBR
Packet Size	127 bytes
Data Rate	20 kbps
SNR Threshold	10
Initial Energy	10.0 J
Electronic Energy	$50 * 10^{-9}$ J

At a time only one source node has been selected and it will forward the data towards base station using multiple hops. The simulation will terminate the sensors having energy lower than 0.001 joules. For physical and data link layers, IEEE 802.15.4 framework has been chosen, which perfectly fits for low data rate applications and it provides long lifetime of batteries of nodes [31]. As mentioned in [31], constant bit rate traffic with a data rate of 20 kbps with a packet size of 127 bytes has been simulated here. Table 1 shows the simulation settings in MATLAB.

B. Experimental Results

The number of nodes considered here varies from 50 to 100 deployed in the simulation area. One can deploy nodes in any field of application as the position of nodes is random. This metric can be applied to any application of WSN.

a) Safety Performance: The safety performance has been measured for three protocols i.e. DSDV, AODV and modified DSDV. The different malicious nodes percentages (5%-20%) has been considered during simulation. It has been assumed that as the malicious sensor nodes ratio increases in the network, the difficulty in managing security in route setup has been increases. It can be seen from figure 1 that the average risk level of modified DSDV has been lower as compared to DSDV and AODV protocols. This is because, in AODV and DSDV while choosing the next-hop for data transmission do not consider the values of number of successful transmission and node energy. When a malicious node is

selected as next-hop it will not forward the packet or drop the packet. This malicious node will be detected in modified DSDV using proposed trust aware metric and will be avoided for the next transmission. This conclude that trust aware metric can attain a high level of security.

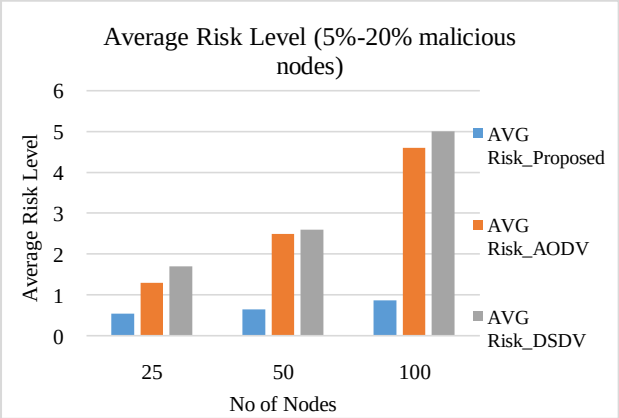

Figure 1: Average Risk Level

From figure 1 the average risk level increases with respect to increase in the number of malicious nodes in network. The risk level for all three protocols increase as the malicious nodes increase in the network, because of the problem in choosing nodes as next-hop. Every time a malicious node drop the packet, there is a need of setting up route again and retransmitting missing packets. As the average risk level in AODV and DSDV is high, we can conclude that, there is no security has been considered in the routing metric of these protocols.

b) Energy Efficiency Performance: To test the energy performance of three protocols, general energy model has been considered from our previously published research paper [28]. Figure 2 shows average energy cost for different simulations under different malicious nodes ratios (5%-20%). It can be seen from the figure 2 that modified DSDV with proposed metric shows high energy efficiency as compared to AODV and DSDV. AODV and DSDV shows poor performance in terms of energy efficiency. Figure 3 shows the average network lifetime which varies with number of nodes and the number of malicious nodes. Proposed metric shows good performance in maintain good lifetime, but reduces in performance when the malicious nodes increases in the network. The energy efficiency decreases because, if there are larger number of malicious nodes in the network, there will be problems in route setup. The end-to-end delay will be increases and also the path loss increases (figure 4 and figure 5) in this case.

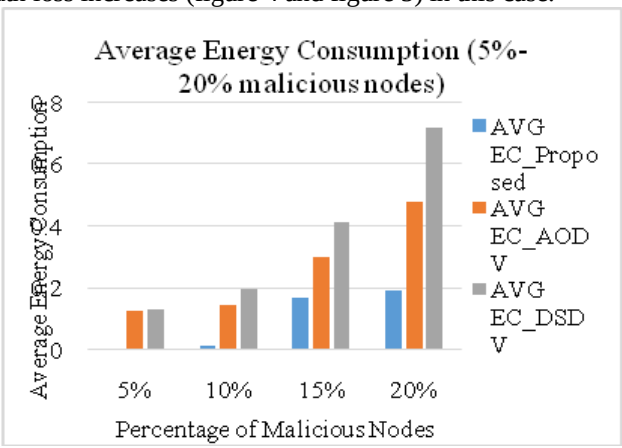

Figure 2: Average Energy Consumption

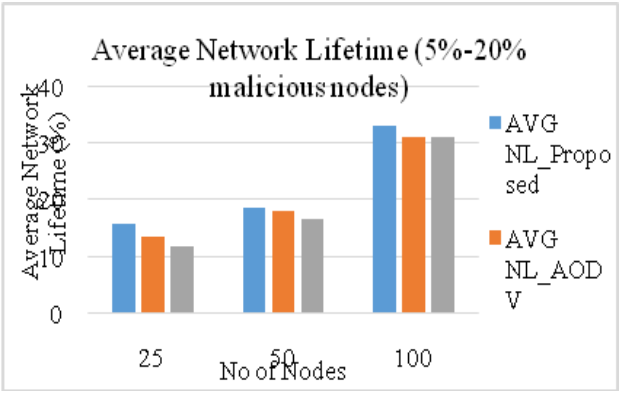

Figure 3: Average Network Lifetime

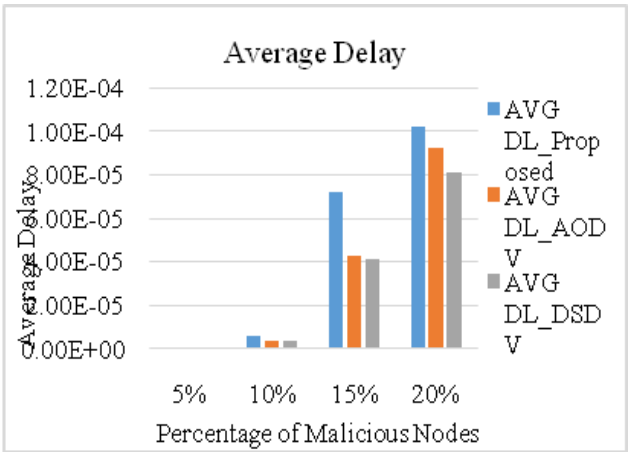

Figure 4: Average End-to-End Delay

From overall results obtained above it can be concluded that the proposed metric works well with DSDV in maintaining the safety and energy efficiency in the network. Proposed metric has advantages of equal energy load distribution and maintaining security, over existing route setup metrics used in AODV and DSDV. The only disadvantage is that the end-to-end delay will be high due to little computation overhead.

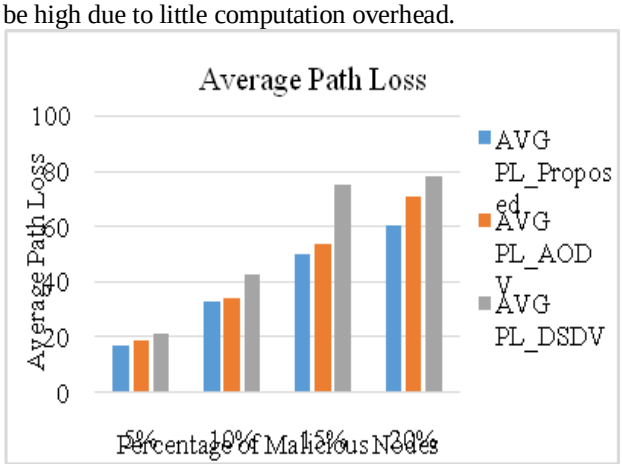

Figure 5: Average Path Loss

V. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed a new trust and energy aware routing metric and applied it to DSDV protocol. The routing metric focuses on the trustworthiness and energy efficiency of the nodes in the network. The trustworthiness can be computed as a factor of forwarding sincerity, energy cost and acknowledgement sincerity of a node. These factors are most essential for the survival and successful operation of WSN in hostile environment and malicious attacks. The routing metric can be viewed as a composite metric. It assigns weights for energy, forwarding sincerity and acknowledgement sincerity of a node. If a node is not satisfying in these three sincerity conditions, it will not be considered as next-hop for data transmission. The route selection has been improved and false link failure notifications has been avoided. The simulation results have shown the betterment of the proposed metric in terms of safety and energy efficiency.

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] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci, E.: 'Wireless sensor networks: a survey', Computer networks, 2002, 38, (4), pp. 393-422

[3] Mohindru, V., and Singh, Y.: 'Efficient Approach for Securing Message Communication in Wireless Sensor Networks from Node Clone Attack', Indian Journal of Science and Technology, 2016, 9, (32), pp. 1-7

[4] 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

[5] 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

[6] 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

[7] 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, 2006), Vancover, BC, pp. 437-446

[8] 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), 2010, pp. 18-23

[9] 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

[10] 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

[11] Koksal, C.E., and Balakrishnan, H.: 'Quality-aware routing metrics for time-varying wireless mesh networks', IEEE Journal on Selected Areas in Communications, 2006, 24, (11), pp. 1984-1994

[12] 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

[13] 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

[14] 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

[15] Boukerche, A., and Darehshoorzadeh, A.: 'Opportunistic routing in wireless networks: Models, algorithms, and classifications', ACM Computing Surveys (CSUR), 2015, 47, (2), pp. 22

[16] 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

[17] 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

[18] Hui-hui, D., Ya-jun, G., Zhong-qiang, Y., and Hao, C.: 'A wireless sensor networks based on multi-angle trust of node', in Proceedings of International Forum on Information Technology and Applications (IEEE, 2009), Chengdu, China, pp. 28-31

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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, 2010), Miami, Florida, USA, pp. 153-157

[24] 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

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

[26] 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

[27] 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

[28] 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

[29] Perkins, C.E., and Bhagwat, P.: 'Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers', in Proceedings of SIGCOMM computer communication review (ACM, 1994), New York, USA, pp. 234-244

[30] Perkins, C., Belding-Royer, E., and Das, S.: 'Ad hoc on-demand distance vector (AODV) routing', No. RFC 3561, 2003

[31] Chang, J.-H., and Tassiulas, L.: 'Energy conserving routing in wireless ad-hoc networks', in Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE, 2000), Tel Aviv, Israel, pp. 22-31

