International Journal of Communication Technology for Social Networking Services
Vol.3, No.2 (2015), pp.1-16
http://dx.doi.org/10.21742/ijctsns.2015.3.2.01

Graded Reliance Based Routing Scheme for Wireless Sensor Networks

Poornima G.[1], Suresh Babu K.[2], Raja K. B. [2], Venugopal K. R.[2] and Patnaik L. M.[3]

[1, 2]University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India
[3] Indian Institute of Science, Bangalore, India
gpoornima.ece@bmsce.ac.in[1],ksb1559@gmail.com[2]

Abstract

In this paper Graded Reliance based routing algorithm is proposed to deal with defective nodes in Wireless Sensor Networks (WSN's).The algorithm is intended to validated or build evidence that, by dynamically learning from previous experience and adapting the changes in the operational environment the application performance can be maximized and also enhance operative agility. Quality of service and social network measures are used to evaluate the confidence score of the sensor node. A dynamic model-based analysis is formulated for best reliance composition, aggregation, and formation to maximize routing performance. The results indicate that reliance based routing approaches yields better performance in terms of message delivery ratio and message delay without incurring substantial message overhead.

Keywords*: QOS, Social Reliance, Delivery Ratio, End to End Delay, Message Overhead, Fault Tolerance, Energy*

1. Introduction

A wireless sensor networks (WSNs) consists of spatially scattered autonomous sensors to supportively monitor physical or environmental conditions, such as temperature, humidity, light, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on [1]. The sensor nodes are usually battery-powered and operate in an attendant open environment for a relatively long period of time, energy efficiency and fault tolerance has becomes a critical issue of concern. Therefore, resource constraint wireless sensor networks, needs refined methods to manage resource and also provide efficient means for fault tolerance. The deployment of wireless sensor networks in many application areas, *e.g.* aggregation services, requires self-organization of the network nodes into clusters [2]. In these cases, sensors in different regions of the field can collaborate to aggregate the information they gathered. For instance, in habitat monitoring applications the sink may require the average of temperature; in military applications the existence or not of high levels of radiation may be the target information that is being sought. It is evident that by organizing the sensor nodes in groups *i.e.*, clusters of nodes, we can reap significant network performance gains. Clustering not only allows aggregation, but limits data transmission primarily within the cluster, thereby reducing both the network traffic and the contention for the channel.

ISSN: IJCTSNS

Most communication happens when data has to be routed from source to the destination i.e., identifying routes, sending sensed data to the sink or base station. In data gathering from Region of Interest (ROI) of the network, data loss often happens due to external faults and internal faults such as random link faults and hazard node faults, interference, atmospheric changes, etc. Therefore it is essential to have a reliance path established for routing data.

Contributions: The Graded Reliance based routing algorithm is proposed to cope with unreliable nodes. QOS and Social Reliance are considered to deal with the defective nodes. The clustering follows grading and hence we can dynamically handle the reliance formation for changing environment conditions. The objective reliance is achieved by gathering the neighbour information and subjective reliance is got by executing the reliance management technique. Both objective and subjective reliance are obtained and validated. It targets application performance in presence of misbehaving nodes in terms of delivery ratio and message delay and threshold based reliance formation for faulty nodes in terms of false alarm probability.

Organization: The rest of the paper is organized as follows. The literatures of various exiting schemes to handle reliance based fault tolerance are surveyed in section 2. Section 3 reliance in wireless sensor network is discussed and Section 4 and 5 features the proposed model. In Section 6 results of technique and their performance are discussed. The concluding comments are detailed in Section 7.

2. Related Work

Ganeriwal *et al.*, [3] proposed a reputation-based framework for data integrity in WSNs. To directly monitor and observes malicious nodes and invalid data the system collects information from each node using a watchdog device.Hierarchical clustering technique is discussed in [4] to detect DoS attaches and alert the cluster head about the abnormal behaviour of the nodes. Rone Ilidio da Silva *et al.*, [5] proposed a fault tolerant energy efficient in-network spatial query processing mechanism for wireless sensor networks. A location based routing protocol is used to avoid failed nodes. Only those nodes in the region of interest receive the query and respond to it there by saving energy. Akos Orosz *et al.*, [6] proposed a fault tolerant ring topology to provide energy efficient and real time operation using Time Division Multiple Access (TDMA) in sensor networks. Algorithms are used to find braided-Hamiltonian cycles in the region of nodes. Node failure and link failure is overcome by using alternate path. The algorithms are able to find solutions in large networks when the simple depth-first algorithm fails.

Mohamed Lehsaini *et al.*, [7] proposed two Efficient Clusters based Fault-tolerant Schemes (ECFS) enabling to reduce communication and processing overhead. ECFS-1 tolerates link failures and ECFS-2 tolerates both sensor faults and link failures. A clustered architecture with primary cluster-head and secondary one are used to avoid node failure. ECFS-1 ensures reliable delivery of data to the base station while minimizing the energy consumption to allow a long network lifetime. ECFS-2 ensures the reliability of collecting data and data delivery. Yi Xie *et al.*, [8] proposed a Fault Tolerant Target Tracking (FTTT) strategy, which transforms the tracking problem into a vector matching process in order to improve the tracking flexibility, increase the tracking accuracy and reduce the influence of in-the-field factors.

Shih-Hao Chang and Teh-Sheng Huang proposed a new knowledge based for fault detection and diagnosis using fuzzy logic approach and challenge approach in Wireless Sensor Networks (WSNs) [9]. A fault tolerance algorithm based framework is used in heterogeneous WSNs to find fault nodes and this algorithm adopts Bayesian approach to observe and estimate nodes reputation regarding message forwarding.Yao *et al.*, [10] proposed a parameterized and localized trust management scheme for WSN security, particularly for secure routing, where each node only maintains highly abstracted

parameters to evaluate its neighbors. Aivaloglou and Gritzalis [11] proposed a hybrid trust and reputation management protocol for WSNs by combining *certificate-based* and *behavior-based* trust evaluations. However these only considered a node's QoS property in trust evaluation for a flat WSN architecture that cannot be scaled. Liu *et al.*, [12] and Moraru *et al.*, [13] proposed trust management protocols and applied them to geographic routing in WSNs. However, no hierarchical trust management was considered for managing clustered WSNs. Their work again evaluated trust based on QoS aspects such as packet dropping and the degree of cooperativeness.

Background: Zhang *et al.*, [14] followed hierarchical trust architecture and considered multi-attribute trust values. Intrusion detection is the last defense to cope with malicious nodes for WSNs in which Sensor Nodes (SNs) can be compromised due to capture or virus infection. Existing work was mostly based on anomaly detection [15] techniques to discover deviations from expected behaviors, including rule-based [16-17], weighted summation [18], data clustering [19], and Support Vector Machine (SVM) [20].

3. Reliance in Wireless Sensor Networks

3.1 Attacks in Wireless Sensor Networks

Wireless sensor networks are prone to various attacks as the nodes are normally deployed in open environment. Some of the major kinds of attacks are energy drain, sink hole, sniffing, hello flood, Acknowledgement spoofing, black hole, grey hole, replayed, DoS attack. The cryptographic techniques are not able to detect these attacks but however reliance based systems can detect such attacks by periodically or continuously monitoring the node behaviour in the network.

3.2 Reliance in Sensor Network

The key design issues addressed are reliance composition *i.e.*, the factors to be considered for reliance, reliance aggression *i.e.*, information collected for each factor considered and reliance formation *i.e.*, reliance formed from each factor. In a network each node collects the information about the services provided by peer entities. Based on the past experience of interaction of peer entity a node can evaluate the reliance for taking decision on further communication. A node in wireless sensor networks builds reliance based on results of interaction with its neighbouring node. The reliance valve calculated by a node about its neighbour depends on the various parameters used to observe the behaviour over past interactions. For example the number of interactions related to packet forwarding, data consistency and energy drain. Based on the observed interaction with neighbouring node, a node calculates the reliance valve. The factors influencing the reliance valve of peer entity under various conditions are as follows:

i. The peer entities exhibit high level of reliability, availability and accuracy under high reliance condition.
ii. Under low reliance condition the peer entities conduct reveals it is defective or malicious. This instigates to provide ways to improve network performance.
iii. When all the peer entities are in high trust, the performance of the network measured in terms of reliable data transfer increases.

4. Proposed Model

The proposed model is designed to efficiently handle reliance based data collection and define the optimal parameters to be considered to validate a node dynamically based on QoS and social network and then identify the application level optimization. The network area is initially divided into zones and then form clusters to detect the compromised nodes

and revoke them from communication. The heterogeneous network is modelled as an undirected graph *G = (V, E, c)* where, *V* is the set of nodes, this set consist of *N* sensor nodes and *M* super nodes and *E* is the set of edges, representing the communication links between node-pairs. The nodes are randomly deployed in the network area and then the area is divided into *Z* zones. Each zone has *N/Z* nodes placed in them on an average. The nodes communicate with their neighbour nodes that lay within the radio range; they evaluate each other based on direct observations. The notation used in the proposed algorithm is given in Table 1.The algorithm has two components viz., (i) objective reliance; the objective reliance estimation is achieved by social network or the neighbour information's to deal with selfish or unreliable nodes and (ii) subjective reliance estimator. The algorithm implements the modules for approximating average delay, delivery ratio and throughput that contribute to subjective reliance calculation. The packet delay is calculated at the node itself and packet delivery ratio by the neighboring nodes. These valves are updated to all the nodes.

4.1 Reliance Formation

The algorithm forms two levels of reliance estimation periodically, one peer to peer level and the other cluster head to sensor node level [21-23]. For peer to peer reliance estimation the reliance components considered are closeness, morality, energy, and selflessness. The evaluation is done considering the one hop neighbours. The reliance value that node *i* evaluates towards node *j* at time *t*, $R_{ij}(t)$, is represented as a real number in the range between *0* and *1* where *1* indicates complete reliance, *0.5* ignorance, and *0* distrust. i.e., the worthiness of a node must be calculated by considering nodes interaction related to data forwarding [24-25], data aggregation, broadcast packets, control packets, location information, energy etc.

$$R_{ij}(t) = w_1 R_{ij}^{closeness}(t) + w_2 R_{ij}^{morality}(t) + w_3 R_{ij}^{energy}(t) + w_4 R_{ij}^{selflessness}(t) \quad (1)$$

Where *w1, w2, w3,* and *w4* are weights associated with these four trust components with *w1 + w2 + w3 + w4 = 1*.

$R_{ij}^{closeness}(t)$: It is a measure of number of interaction levels. It is given by the ratio of number of interaction between n_i and n_j to the maximum number of interactions between n_i and any neighbour node over the time period *0* to *t*.

$R_{ij}^{morality}(t)$: It is a measure of confidence of node i on node j based on its observations over a time interval.

$$R_{ij}^{morality}(t) = 1 - \frac{Dishonest\ Count}{R^{th}} \quad (2)$$

$R_{ij}^{energy}(t)$: It is a measure of node j's remaining energy as heard by node i.

$R_{ij}^{selflessness}(t)$: It is a measure of degree of selflessness of node *j* as evaluated by node *i* based on its observations over a time interval. Node *i* track the misbehaviour of node *j* in performing the sensing, reporting and data forwarding tasks.

The reliance R_{ij} computed by the nodes is reported to the cluster head and then the cluster head computes the average reliance AR_{ij} valve i.e., compared with the reliance threshold. Similar strategy is applied to compute the reliance of cluster head by the base station. The base station extracts the reliance information received from cluster head.

$$CR = \begin{pmatrix} AR_{ij} < \Gamma\ compromised \\ AR_{ij} \geq \Gamma\ not\ compromised \end{pmatrix} \quad (3)$$

4.2 Reliance Aggregator Nomination

The Reliance Aggregator (RA) are initially nominated randomly and later based on the trust valve generated. The time slot for each zone and *RA* is divided equally and *RA* gets shuffled for every time slot. The node n_i estimates the neighbourhood-reliance in zone Z at time slot T_i in accordance with the difference between the probability distributions of the information generated by n_i and the information sent to n_i by n_i*'s* neighbouring nodes. This validation is to know how much of information is shared between the two.

4.3 Reliance Composition

In the proposed algorithm a minimum reliance threshold, R^{th}, is selected such that a node having reliance valve below threshold is considered as compromised and needs to be excluded from sensor reading and routing duties. The nodes with true reliance are only considered for reliance path construction, other nodes are excluded from communication. The routing path thus built is used for packet delivery and hence more reliable [26]. The basic principle is that a compromised node will exhibit several social and QoS reliance behaviors, ***i.e.***, low *closeness* and low *morality* (for social trust) as well as low *energy* and low *selflessness* (for QoS trust), thus revealing itself as a compromised node under graded reliance evaluation.

Table 1. Notations Used in Methodology

Symbol	Definition
A	Network Area
N	Set of Nodes
M	Cluster Head
$dist(x,y)$	distance between node pair
CST	Carrier Sense Threshold
$E_{residue}$	Residual Energy Level
α	Scale factor for Direct Reliance
β	Scale factor for Indirect Reliance
Δt	Reliance update interval
$R_{ij}(t)$	Valve of Reliance of n_{ij} @ t
f_c	Fraction of Compromised Node
R^{th}	Reliance Threshold
Γ	Zone/Cluster Reliance Threshold
CR	Cluster Reliance
P	Probability of self-information
q	Probability of neighbour information.
D	Divergence
AR_{ij}	Average Reliance valve

5. Algorithm Description

The proposed algorithm in Table 2 must provide a much secured, efficient, reliable path in the network for data communication. The proposed scheme is based on zone and cluster based mechanism so that communication range for each node is reduced due its power limitation [27-28]. It should also provide a basis for obtaining the ground truth status of nodes in the system, at zone and cluster level and limits the cost of false positives. In the network model considered the nodes once deployed and are uniformly placed in grid distribution they are static and do not change their location. The communication between nodes is always direct and bidirectional. The base station is considered to be reliable entity. Only one hop neighbor information is considered and

each node is aware of its cluster status (*i.e.* node position, residual energy levels, link reliability, neighbors and cluster head).

Table 2. GRMT: Graded Reliance Based Routing Algorithm

Input	Initiate transaction at the start of sensing time.
Output	Data packets received at the destination node through a trusted path at the end of the sensing time.
Step1	Zone Discovery and Reliance Aggregator Selection Mechanism.
Step2	If the zone reliance is false then zone is declared compromised else not
Step3	If the zone reliance is true then peer and graded reliance is estimated.
Step4	The nodes with true reliance are only considered for reliance path construction
Step5	The nodes without true reliance are withdrawn from the communication.

Step1: The nodes are randomly deployed in a network area *A i.e.*, divided into *z* non overlapping zones. The Zone size will affect the cost of communication; the size should not be too large or too small as it affects intra-zone communication cost. Hence the zone size is optimized to $r^2/2$, such that all nodes can directly communicate with each other. The node placement follows a uniform grid distribution and each node identifies its location and the zone to which it belongs. Each node is assigned a unique ID. The node discovers all of its home members using pairwise key. The Reliance Aggregator is then selected in round robin schedule and acts as an aggregator for a predefined timeslot that is pseudo randomly set.

Step2: In each time slot the Reliance Aggregator computes the current reliance and reports that valve to base station. The zone computes the reliance based on the self–information and the neighbour information in the zone. The neighbour reliance indicator is the amount of information exchanged between the nodes. Higher the valve higher will be the closeness and morality between the nodes. The node uses equation 4 and 5 to compute the reliance. The valves of *p* and *q* are based on the distribution of sensed data. Here $p=0.5$ and $q \leq p$ for better accuracy; *i.e.* majority of the information generated by the node is within the expected range.

$$D = p * \log (p/q) + (1-p) * \log ((1-p) / (1-q)) \quad (4)$$

$$\text{Neighbour Reliance} = \min (1, 1. / (1+D)) \quad (5)$$

If the computed reliance is below the threshold Γ the zone is declared compromised else not by the base station.

Step3: The received report from the reliance aggregator is checked for its validity along with time status of the report is generated. Based on this information the base station makes its decision on declaring the cluster head as compromised or not. Similarly Peer to Peer, Sensor Node (SN) to Cluster Head (CH), Cluster Head to base station reliance is computed and the report is submitted to base station.

Step4: The data from the source is moved to the only truthful aggregators to which zone and cluster it belongs and then it is forwarded to the base station.

Step5: The zone or cluster that does not satisfy the required reliance is barred from communication.

6. Performance Evaluation

The performance of the proposed technique is tested by implementing the algorithm using *NS-2* simulator. The result demonstrates the performance and benefits of graded reliance based routing algorithm over previous methods.The proposed algorithm provides a much secured, efficient, reliable path in a network for communicating data from source to destination. The scheme is based on zone and cluster based mechanism. In the algorithm a minimum reliance threshold, R_{th}, is chosen such that a node below threshold is considered compromised and needs to be omitted from sense and routing responsibilities.

A WSN with *101* SNs evenly spread out in a *500m*× *500m* operational area based on uniform grid distribution with the base station at the center is considered. The network area is divided into *5* equal grids of uniform size on both the *x* and *y* axis to form *25* zones. Nodes are uniformly distributed in the zone such that each zone accommodates *4* nodes. The radio ranges of a Sensor Node and a Cluster Head are $r = 440m$ and $R = 200m$, respectively. The cluster range considered forms *8* clusters for graded evaluation. All nodes are initially treated as fault free. The simulation run time is *200sec* for one iteration. We conduct performance analysis to compare graded reliance based routing algorithm with hierarchical routing scheme [21]. In the proposed algorithm node n_i forwards a message to a maximum of *1*-hop neighbours not only closest to the destination node but also with the highest reliance values $R_{ij}(t)$. The source sensor and a sink node randomly selected the algorithm is evaluated for a data delivery of 45000 message packets. The performance parameters considered for evaluating the algorithm are Packet Delivery Ratio (PDR), Throughput (S), End to End Delay (EED), Message Copies (MC) and Energy (E).

Table 3. Network Parameters

Parameter	Value	Parameter	Value
Simulator	NS2, V3.4	Initial energy	100J
Topology size	500m **x** 500m	Cluster radius	200m
Transmission Range	250 m	Receive power	0.01J
Simulation time	200 sec	Transmit power	0.02J
Number of nodes	101	Start of Sensing time	35s
Traffic Type	CBR	End of Sensing time	190s
Threshold value	0.5	MAC Type	MAC 802_11

Initially all nodes are good and later become bad based on the compromised ratio introduced. The degree of compromised nodes is varied from *0%* to *90%*. Reliance $R_{ij}(t)$ is either *1* or *0* for a node depending on its behavior. The false positive probability is varied in the range of *1%* to *20%*.The reliance update interval is set to $\Delta t = 20sec$ for the node. After total run of *200sec* the energy status of the nodes is noted. The scale factor for direct and indirect reliance is set to $\alpha = 0.6$ and $\beta = 0.8$ setting a mean square error of less than *0.25%*. The best α and β values are set to ensure subjective reliance is close to objective reliance, intrinsically it depend on the nature of each reliance property as well as a given set of parameter values as those listed in Table 4 characterizing the environmental

and operational conditions. The valves of *PDR, S, MC,* and *E* decreases as compromised nodes increases, whereas delay increases with compromised nodes. The zone reliance is computed and informed to the base station.

The base station performs the Progressive Likelihood Assessment from the received information. Based on the assessment report the zone's reliability is declared. As a second level of Assessment graded mechanism is adapted i.e., peer to peer and cluster to sensor reliance is also calculated. Once the clusters are formed and cluster head is elected, then all communication between nodes is always through cluster head. Reliance is calculated between sensor nodes, cluster head and base station. The base station communicates through cluster head.

Table 4. Performance Parameters of Proposed GRMT Algorithm

CN	PDR (%)	S(bps)	EED(ms)	MC	E(J)
0	90	40169	1.98018	18	6.60732
0.1	73.7	30178.6	1.986	17	5.90293
0.2	62.5771	21289	2.2525	18	6.47355
0.3	62.0894	23599.8	2.00425	19	5.0712
0.4	51.7264	11491.5	1.95302	17	5.06493
0.5	40.7869	13134	1.923	17	4.0915
0.6	32.1475	9337.03	2.17172	18	4.90069
0.7	26.4705	7005.03	1.98512	15	3.81892
0.8	20.973	5290.21	2.08823	16	3.23447
0.9	8.85658	538.98	2.54638	12	2.79025

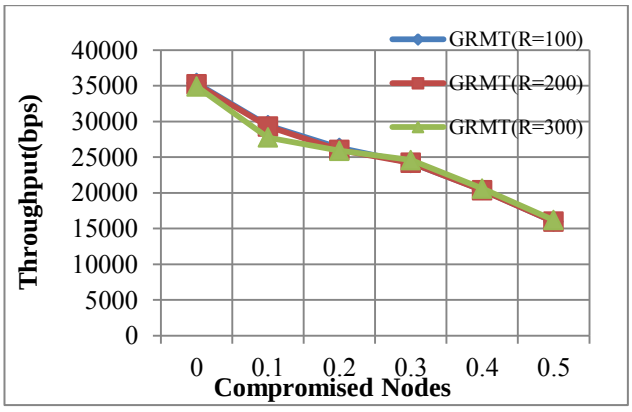

Figure 1. Variation of Throughput with Compromised Nodes for Variable Range

The variation of performance parameters with CN is observed for variable cluster range is shown in Figure 1. The cluster range is varied and throughput is observed for three different cases of *R*, *i.e.*, when *R* is set to *100m, 200m* and *300m* keeping the SNs range at *250m*. It is noticed that the throughput drops with increase in CN for all the three

cases. It is also observed from Table 5 that as long as SNs range is greater than CH range the throughput of the network is restored.

Table 5. Performance of Throughput with Cluster Range

Sensor Node Range =250mts Cluster Range	Throughput (%)
100	83.0924
200	82.6633
300	6.64894

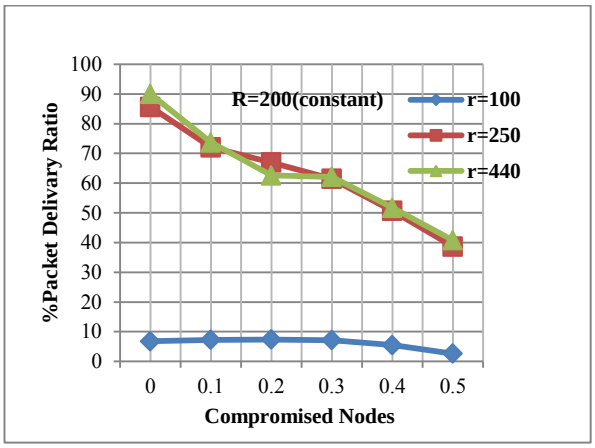

Figure 2. Variation of PDR for Varying Transmission Range(r)

The variation of percentage PDR for variable sensor transmission range is shown in Figure 2 keeping the cluster range constant at *200m*. It is observed that the success ratio of packet delivery is better when the transmission range is higher than the cluster radius, *i.e.* for valves *r=250m* and *440m* and the PDR drops when *r=100m* this is because *r<R*.

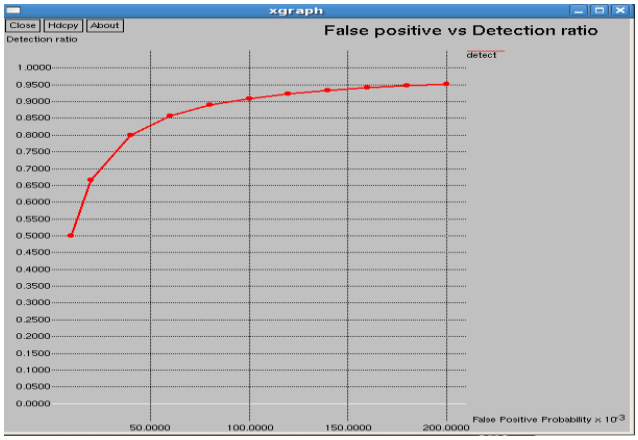

Figure 3. Performance of GRMT in Terms of Detection Ratio

The variation of detection ratio with respect to false positive probability is shown in Figure 3. The number of compromised nodes is kept constant at *0.1*, the false positive probability is varied from *0.05* to *0.2* and detection ratio is noted. It is observed that, as the false positive probability increases, the detection ratio also increases. This method features nearly zero false positives, implying that truthful nodes will not be unreasonably

detached from the network. However, to realise a high node compromise detection capability, these schemes require every sensor node to be confirmed periodically.

Figure 4 show the performance of the proposed in terms of throughput varying with compromised node. It is observed that the PDR is above *41%* for proposed scheme even when *50%* of the nodes are compromised. It is also observed that overall the GRMT has *5%* enhancement in performance compared to existing scheme and this improvement can be attributed to ability of the algorithm to perform reliance Progressive Likelihood Assessment both at zone and cluster level.

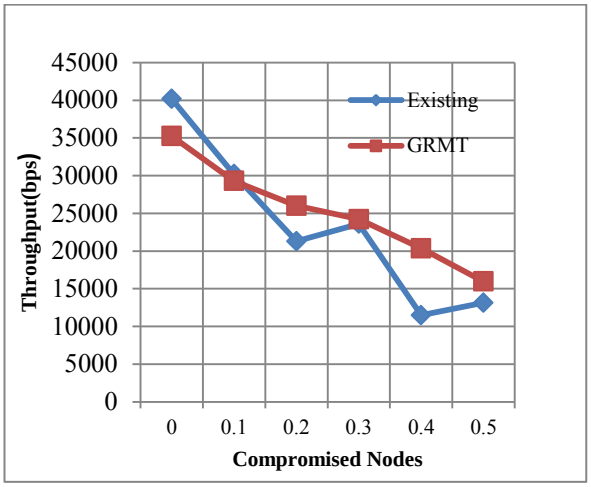

Figure 4. Variation of Throughput with CN for Existing [21] and GRMT

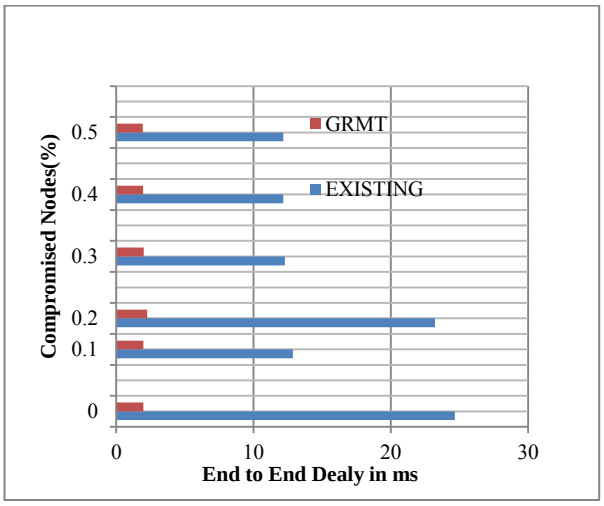

Figure 5. Comparison of Average Delay for Existing [21] and GRMT with CN

The variation of end to end delay with CN for existing algorithm presented by Bio *et al.*, [21] and proposed method is shown in Figure 5.It is observed that the message delivery delay increases with the increase in percentage of compromised or selfish nodes due to more messages being dropped by compromised or selfish nodes. The proposed model produces better performance compared to existing scheme since the packets are transmitted through a reliable path.

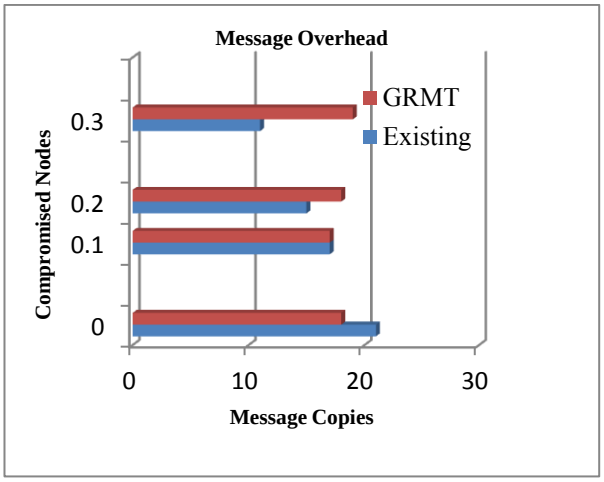

Figure 6. Comparison of Message Overhead for Existing [21] and GRMT

The message overhead foe existing [21] method and proposed method with compromised nodes is shown in Figure 6. According the GRMT method the path taken by the data to travel from source to destination is not always the shortest path but only a reliable path of data delivery this has contributed to the slight increase in message overhead compared to existing scheme as seen in Figure 6.

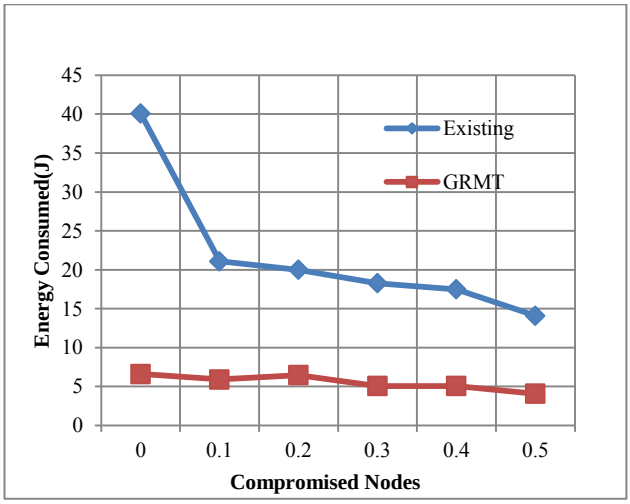

Figure 7. Comparison of Total Energy Consumed for Existing [21] and GRMT

The total energy consumption for existing [21] and GRMT is shown in Figure 7 for varying CN. It is observed from the results that there is significant reduction in the amount of energy consumed by the proposed algorithm compared to existing method. The energy saving can be attributed to the fact that graded mechanism is followed to aggregated the information at two levels i.e., zone and cluster followed by a revocation of the compromised zones and clusters by software attestation.

The variation of detection ratio with false positive for existing [23] and the proposed method is given in Table 6. It is observed that as the false positive probability increases, the detection ratio also increases for both existing [23] and proposed method. The advantage of subjective selection is that even a relatively small number of honest nodes can send zone-reliance report with low-reliance values, leading to detection.

Table 6. Performance of Proposed grmt

False Positive	Detection Ratio	
	EXISTING[23]	Proposed GRMT
0.01	0.567895	0.500342
0.02	0.75879	0.666966
0.04	0.91267	0.800213
0.06	0.921452	0.857305
0.08	0.979011	0.889019
0.1	0.9845	0.9092
0.12	0.9899	0.92317
0.14	0.99235	0.933415
0.16	1.000	0.941249
0.18	1.0	0.947434
0.2	1.0	0.95244

7. Conclusion

In this paper, a graded reliance based routing algorithm for wireless sensor networks is projected considering two aspects of credibility, namely, zone based reliance and cluster based reliance. In the proposed GRMT model a reliable path from source to destination is established, all unreliable nodes that are selfish, malicious and dishonest are removed from the path of communication. Here initially compromised nodes are detected and they are corrected using zone based approach. Later in cluster based approach three levels of reliance is calculated for the nodes in the network *i.e.*, at the node level, cluster level and base station level; hence the method can also be viewed as Enhanced hierarchical trust management scheme. A probability model is used to analyse and validate both subjective and objective reliance based on the actual node status including properties for QOS and social support. The proposed technique shows better performance in terms of packet delivery ratio, average end to end delay, throughput and detection ratio and energy while maintaining low false positive. There are some impending research directions that including examining the effect of the zone and cluster size, the reliance update interval to the protocol performance and lifetime of a given WSN and also probing the viability of applying GRMT to more dynamic networks such as mobile and autonomous WSNs.

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Network's," IEEE Communications Magazine, vol. 40, no. 8, (**2002**), pp. 102–114.
[2] S. Bandyopadhyay and E. J. Coyle, "Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," IEEE Conference on Information and Communication, (**2003**).
[3] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava," Reputation-Based Framework for High Integrity Sensor Networks", ACM Transactions on Sensor Networks, vol. 4, no. 3, (**2008**), pp. 1–37.
[4] D. Mansouri, L. Mokda, J. B. Othman and M. Ioualalen, "Detecting DoS Attacks in WSN based on Clustering Techniques", IEEE Conference on Wireless Communication and Networking, (**2013**), pp. 2215-2219.
[5] R. I. da Silva, D. F. Macedo and J. M. S. Nogueira," Fault Tolerance in Spatial Query Processing for Wireless Sensor Networks", IEEE Network Operations and Management Symposium, (**2012**), pp. 97-104.
[6] A. Orosz, G. Roth and G. Simon, "TDMA Scheduling in Fault Tolerant Wireless Sensor Networks", IEEE International Instrumentation and Measurement Technology Conference, (**2012**), pp. 1169 - 1173.
[7] M. Lehsaini, M. Feham, and H. Guyennet, "Efficient Cluster-Based Fault-Tolerant Schemes for Wireless Sensor Networks", Fifth International Conference on New Technologies, Mobility, and Security, (**2012**), pp. 1-5.

[8] Y. Xie, G. Tang, D. Wang, W. Ziao, D. Tang and J. Tang, "A Fault Tolerant Target Tracking Strategy Based on Unreliable Sensing in Wireless Sensor Networks," Twenty Sixth International Parallel and Distributed Processing Symposium Workshops & PhD forum, vol. 978, (**2012**), pp. 7695-4676.
[9] S.-H. Chang, and T.-S. Huang, "Fuzzy Based Fault Tolerance Algorithm in Wireless Sensor Networks", Twenty Sixth International Conferences On Advanced Information Networking And Application Workshops, vol. 978, (**2012**), pp. 7695-4652.
[10] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and Localized Trust Management Scheme for Sensor Networks Security," Proceedings of IEEE International Conference on Mobile Adhoc Sensor Systems, (**2006**), pp. 437–446.
[11] E. Aivaloglou and S. Gritzalis, "Hybrid Trust and Reputation Management for Sensor Networks", Journal of Wireless Networks, vol. 16, no. 5, (**2010**), pp. 1493–1510.
[12] K. Liu, N. Abu-ghazaleh, and K. D. Kang, "Location Verification and Trust Management for Resilient Geographic Routing," Journal of Parallel Distributed Computing, vol. 67, no. 2, (**2007**), pp. 215–228.
[13] L. Moraru, P. Leone, S. Nikoletseas, and J. D. P. Rolim, "Near Optimal Geographic Routing with Obstacle Avoidance in Wireless Sensor Networks by Fast-Converging Trust-Based Algorithms," Proceedings of ACM Workshop QoS Security Wireless Mobile Networks, (**2007**), p. 31–38.
[14] J. Zhang, "Trust Management Architecture for Hierarchical Wireless Sensor Networks," Proceedings of IEEE International Conference on Local Computer Networks, (**2010**), pp. 264–267.
[15] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks", IEEE Transaction on Wireless Communication, vol. 15, no. 4, (**2008**), pp. 34–40.
[16] V. Bhuse and A. Gupta, "Anomaly Intrusion Detection in Wireless Sensor Network", Journal of High Speed Networks, vol. 15, no. 1, (**2006**), pp. 33–51.
[17] A. da Silva, "Decentralized Intrusion Detection in Wireless Sensor Networks", Proceedings of ACM International Workshop on Quality of Service Security Wireless Mobile Networks, (**2005**), pp. 16–23.
[18] H. Hu, "Weighted Trust Evaluation-Based Malicious Node Detection for Wireless Sensor Networks", International Journal of Information Computer Security, vol. 3, no. 2, (**2009**), pp. 132–149.
[19] C. E. Loo, M.Y. Ng, C. Leckie and M. Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks", International Journal of Distributed Sensor Network, vol. 2, no. 4, (**2006**), pp. 313–332.
[20] S. Rajasegarar, C. Leckie, M. Palaniswami, and J.C.Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", Proceedings of IEEE International Conference on Communication, (**2007**), pp. 3864–3869.
[21] F. Bao, I.R. Chen, M. Chang, and J. H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust Based Routing, "Proceedings of ACM Symposium on Applied Computing, (**2011**), pp.1732–1738.
[22] F. Bao, I. R. Chen, M.Chang, and J. H. Cho, "Trust-Based Intrusion Detection in Wireless Sensor Networks", Proceedings of IEEE International Conference on Communication, (**2011**), pp. 1–6.
[23] J. Ho, M. Wright, and S.K. Das, "Zone Trust: Fast Zone-Based node compromise Detection and Revocation in Wireless Sensor Networks using Sequential Hypothesis Testing", IEEE Transactions On Dependable and Secure Computing, vol. 9, no. 4, (**2012**).
[24] G. Theodorakopoulos and J. S. Baras, "On Trust Models And Trust Evaluation Metrics for Ad Hoc Networks", IEEE Journal on Selected Areas of Communication, vol. 24, no. 2, (**2006**), pp. 318–332.
[25] P. Ebinger and N. Bissmeyer, "TEREC: Trust Evaluation and Reputation Exchange for Cooperative Intrusion Detection in MANETs", Proceedings of Communication, Network Services Research Conference, (**2009**), pp. 378–385**.**
[26] F. Wang, C. Huang, J. Zhao, and C. Rong, "IDMTM: A Novel Intrusion Detection Mechanism Based on Trust Model for Ad hoc Networks", International Conference of Advances in Information Networks and Applications, (**2008**), pp. 978–984.
[27] Banwari, D. Sharma, and D. Upadhyay, "Routing Algorithms for MANET: A Comparative Study", International Journal of Engineering and Innovative Technology, **v**ol. 2, no. 9, (**2013**), pp. 193-197.
[28] M. Beldjehem, "Toward a Multi-Hop, Multi-Path Fault-Tolerant and Load Balancing Hierarchical Routing Protocol for Wireless Sensor Network", Journal of Wireless Sensor Network, vol. 5, no. 11, (**2013**), pp. 215-222.

Authors

Poornima. G, she received the BE degree in Electronics and Communication Engineering from Bangalore University and the M.E. degree in Digital Communication from Bangalore University, Bangalore. She is pursuing Ph.D. in Computer Science and Engineering at University Visvesvaraya College of Engineering, Bangalore University. She is a faculty in the Dept. of Electronics and Communication Engineering, BMS College of

Engineering. Bangalore. Her research interests include Computer Networks, Digital Signal Processing. She has research publications in refereed National, International Journal and Conference Proceedings. She is a life member of Indian Society for Technical Education, New Delhi.

Suresh Babu, he is an Associate Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 30 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, Signal Processing, and Computer Networks.

K B Raja, he is an Associate Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 60 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, and Computer Networks.

K R Venugopal, he is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 250 research papers to his credit. His research interests include computer networks, parallel and distributed systems, digital signal processing and data mining.

L M Patnaik, he is the Vice Chancellor, Defence Institute of Advanced Technology (Deemed University), Pune, India. During the past 35 years of his service at the Indian Institute of Science, Bangalore, He has over 550 research publications in refereed International Journals and Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to high performance computing and soft computing. His areas of research interest have been parallel and distributed computing, mobile computing, CAD for VLSI circuits, soft computing, and computational neuroscience.