Available online at www.sciencedirect.com

ScienceDirect

Cognitive Systems Research 56 (2019) 14–22

Cognitive Systems RESEARCH

www.elsevier.com/locate/cogsys

A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks

A. Latha [a,*], S. Prasanna [b], S. Hemalatha [c], B. Sivakumar [d]

[a] Department of Electronics and Communication Engineering, Adhi College of Engineering and Technology, Kanchipuram, India
[b] School of Information Technology and Engineering, VIT, Vellore, India
[c] Department of Computer Science and Engineering, AdhiParasakthi Engineering College, Melmaruvathur, India
[d] School of Computer Science and Engineering, RGM College of Engineering and Technology, Nandyal, A.P, India

Received 27 July 2018; received in revised form 27 September 2018; accepted 13 November 2018
Available online 15 March 2019

Abstract

Security and energy optimization in Wireless Sensor Network (WSN) have a direct impact over device and network performance. The bridging gap between optimization and security needs to be curtailed so as to achieve secure optimization in this resource constraint networks. This manuscript presents as three-fold integrated scheme that governs secure neighbour selection, energy efficient routing and seamless aggregation that serve a multi objective purpose for WSN. We propose a Trust Assisted- Energy Efficient Aggregation (TA-EEA) scheme that improves overall aggregation precision with limited constraints in neighbour reliability and aggregation. The threefold process of TA-EEA ensures trusted neighbour selection, duty cycle based energy conservation and responsive congestion control for seamless transmission. These processes intend to minimize the energy utilization of the nodes to prolong the lifetime of the network with lesser control overhead. The trade-off between energy and security is exploited to progress efficient energy consumption under controlled overhead with higher packet delivery ratio.

Keywords: Congestion control; Duty cycle algorithm; Energy efficient routing; Secure data aggregation; Trust based neighbour selection

1. Introduction

Wireless Sensor Networks (WSNs) comprises of uncountable devices called sensor nodes that perform monitoring, sensing and transmitting operations with the interconnected similar devices. Sensor nodes are usually incompetent and inexpensive physical devices with assembled hardware elements and self-battery for operating the hardware (Alzaid, Foo, & Nieto, 2008). Sensor nodes relay the gathered information to a familiar node called sink. The sink node is present either in one-hop or multi-hop from the relaying node. Sensor nodes have multiple challenges, post deployment; the major is due to finite energy and secure neighbour availability. The power source of sensor nodes cannot be frequently recharged or they lack recharging capability depending upon the environment they are deployed. Both power and resource constraint emboss the network to be feeble that it must rely on additional optimization methods for retaining the service outcome of the network. Resource constraints have direct impact over network lifetime, energy dissipation, neighbour awareness, relaying and so on (Przydatek, Song, & Perrig, 2003).

Sensor nodes dispersed in distinct network region integrate sensed data forwarding to a common node called

* Corresponding author.
E-mail addresses: latha.arthanari@gmail.com (A. Latha), sprasanna@vit.ac.in (S. Prasanna).

https://doi.org/10.1016/j.cogsys.2018.11.006
1389-0417/

aggregator that successively forwards the same to the sink node. Sensor nodes due to their self-resource constraints may not find direct transmission to the sink node, for which aggregation is a solution. This prevents earlier energy drain of the node (Rajagopalan & Varshney, 2006). As the sensor nodes pursue a common transmitting fashion, energy consumption of the nodes at the time of relaying is less that aids to prolong the network endurance. Data aggregation emphasises a stronger energy optimization by reducing redundant transmission to the sink node (Fasolo, Rossi, Widmer, & Zorzi, 2007).

Sensor nodes are deployed in both favourable and adversary environments to carry out observations and sensing operations. In an adversary environment, there are chances for a node to be compromised or to infuse counterfeited information into the network. If an aggregator is influenced by the adversary, the aggregated value can be altered that would change the entire aggregation result in the sink (Gaikwad & Dhage, 2015; Ozdemir & Xiao, 2009). Therefore security becomes essential research area in data aggregation in WSNs.

In this manuscript, we intend to optimize WSN performance using a harmonized three-fold approach; energy optimization using region based duty cycle process, link capacity dependent aggregation and trust path selection using prolonged time consistency factor. Besides the overhead caused due to harmonizing the independent approaches is also intended to be minimized, with each process being restricted to the required levels of service provisioning.

The remainder of the manuscript is systematized as follows. Section 2 describes the review of the related works. Section 3 describes the System model and problem definition. Section 4 explains our proposed approach of the three-fold process in detail. Section 5 deals with the simulation results and discussion. Finally, the conclusion and future scope are briefed in Section 6.

2. Related work

This subsection describes some of the works proposed in the past that are designed for WSN performance improvement.

Roy, Setia, and Jajodia (2006) proposed a hierarchical durable data collection algorithm for data gathering in the existence of compromised sensor nodes. This method mitigates malicious aggregates but as the method authentication code along with the node address, number of MAC control messages generated is high.

Stealthy attack is a recurrent aggregation vulnerability that injects forged information into the aggregated data so as to deface the base station aggregation value. Passive scheme (Önen & Molva, 2007) with homomorphic encryption is proposed to improve data confidentiality among the sensor nodes. An improved cluster-based privacy homomorphism is proposed by Huang, Shieh, and Tygar (2010) which employs random key generation technique for improving data collection security intensity. This method lacks the key sharing information between sensor nodes and base station.

The authors of (Avokh & Mirjalily, 2010) designed a Dynamic balanced Spanning Tree Approach to reduce the drawback of hotspot caused in the static spanning tree method, to minimize energy utilization and to improve load balancing.

EBRP (Ren, Zhang, He, Lin, & Ren, 2011) is a loop eliminating algorithm that considers multiple routing factors like level, intensity and enduring energy of the nodes to improve packet flow rate. EBRP performs better load balancing and energy optimization. The authors of (Roy, Conti, Setia, & Jajodia, 2012) flourished a verification algorithm for aggregate authentication by the base station. This algorithm verifies the aggregation precision without exchange of message to the base station but the algorithm does not hold for verification in the active time of the attackers.

The authors in (Mathapati, Patil, & Mytri, 2012) proposed a cluster-based reliable energy efficient aggregation technique with co-ordinator nodes that perform monitoring and aggregation process. This clustering technique aids in minimizing energy consumption at the time of transmission and improved reliability of the transmission.

An anchor point based data aggregation method is proposed by Guo, Wang, and Yang (2013) to curtail multiple node energy dissemination due to varying data gathering instances. To improve confidentiality and integrity in data aggregation, Othman, Trad, Youssef, and Alzaid (2013) integrated authentication codes and ElGamal encryption scheme that minimizes communication overhead and computation complexity.

Mantri, Prasad, and Prasad (2013) flourished a bandwidth efficient inter and intra cluster aggregation to minimize redundancy and energy consumption. This method is designed for heterogeneous networks that require node information in forehand.

Xiang, Luo, and Rosenberg (2013) introduced a compressed sensing based data gathering scheme in random network deployment to accomplish effectiveness in energy utilization. This method also retains reliability post data gathering.

Xie and Jia (2014) proposed a cluster-based compressive sensing scheme for controlling redundant transmissions. An Adaptive Load Balancing Algorithm-Rainbow (ALBA-R) is proposed by Rao, Jana, and Banka (2016) for lowering energy consumption and overhead at the time of transmission. ALBA-R is a cross-layer method that resolved routing problem and efficiently balances load using special nodes called relays.

To minimize complexity in aggregator election that supports balanced energy consumption among the nodes, Chao and Hsiao (2014) proposed a light weight aggregator selection algorithm. To minimize energy consumption, the

authors have also proposed structure less data collection scheme that is an event driven reporting method for energy optimization.

To extend the energy efficiency for real time communications, Tyagi et al. (2014) proposed SAERP protocol. The distinguishable factor of SAERP from the other protocols is that it handles unforeseen transmission interludes. SAERP minimizes energy utilization and number of control messages generated.

WSNs have resource constraints and therefore the utilization of resources must be meaningful. In order to achieve profitable resource utilizations, Soltani, Hempel, and Sharif (2014) proposed a variable node - data fusion approach that results in efficient resource utilization in hefty WSNs.

In order to improve data gathering correctness and to restore energy for the depleted nodes, a mobile mediator called SenCar is designed by Zhao, Li, and Yang (2014). This mediator gathers data, delivers to sink and charges immobile nodes in the network for pursuing transmission.

A threshold based energy conserving method is proposed by Jain, Saini, and Bhooshan (2015). The nodes that do not exceed the threshold energy are iteratively connected to the sink with replacement. This improves network lifetime by minimizing energy drain constraints.

An integrated algorithm of itinerant sink and assignation sensor nodes models is proposed by the authors of (Mottaghi & Zahabi, 2015) that retains the merits of LEACH algorithm.

Xiao, Li, and Yuan (2015) considered the energy utilization optimization of a single node in a heterogeneous environment to improve the accuracy of data gathering. This approach minimized the bridging gap between aggregation value and energy utilization.

The methods discussed in the past focus on leveraging few metrics that are directly associated with security. Conventional security mechanisms improve network throughput and packet delivery ratio with the aid of detection and authentication mechanisms. Different from the traditional way of administering security in WSNs, our contribution is formulated as below:

(i) Trust Assisted Neighbour Selection (TANS) method in which a neighbour is assessed for its consistency time along with the trust value. This discovers selective neighbours that perform reliable communication over a prolonged time.
(ii) Energy Sustained Routing (ESR) for enhancing network lifetime by modifying the conventional duty-cycle process. The nodes are moved to active and sleep states based on their gained trust value. Besides, this routing determines the survival and replacement of the aggregators.
(iii) Congestion Aware Data Collection (CADC) assists congestion-free data migration between the nodes to improve reliability in communication. It accounts the packet count and buffer capacity of the nodes to ensure non-congested seamless transmissions.

3. System model

This subsection briefs the WSN model with the node density and its types and their energy model.

3.1. Network model

We contemplate a network with $\{n\}$ sensor nodes $\in N$ positioned in a random manner in a network region of dimension $X * Y$. The network consists of few source nodes (S_n), aggregator nodes (A_n) and a sink node (S_k). Source nodes transmit data to the sink directly or through intermediate nodes (I_n) in multi-hops. A_n initiate aggregation of data from S_n and transmits the same to S_k.

3.2. Energy model

Let E_{init} represent the pioneer energy of the node. A node utilizes its energy for routing and relaying data packets. Energy utilized by a node (E_{util})varies as the distance to the aggregator varies. If E_t and E_r represent the energy consumed by a node for transmitting and receiving data respectively, then

$$E_{util} = E_t + E_r \tag{1}$$

The inactive nodes in the network are shifted to sleep state so as to prevent the node being active for long time and thereby dissipating energy unnecessarily. A node with next higher enduring energy is transferred to active state for pursuing communication. This process is called duty cycle. The nodes in sleep state are said to keep its radio receiver in ON state so as to receive wake up messages. Therefore a least amount of energy is utilized by the nodes in sleep mode.

Considering a nodes' energy utilization in listening (E_{lis}) and sleep state (E_s), (1) can be rewritten as in (2)

$$E_{util} = E_t + E_r + E_{lis} + E_s \tag{2}$$

E_t and E_r can be computed using Eqs. (3) and (4) respectively.

$$E_t = d_{tr} \times e_t \times t_t \tag{3}$$

where d_{tr} is the data transfer rate, e_t is the transmission energy and t_t is the data transfer time.

$$E_r = d_{rr} \times e_r \times t_r \tag{4}$$

where d_{rr} is the data reception rate, e_r is the reception energy and t_r is the data reception time.

The duty cycle process is initiated over the communicating network region rather than path nodes. Duty cycle process of a node is distinct from aggregator replacement constraint i.e. the node is moved to sleep state based on its enduring energy monitored after each transmission.

3.3. Problem definition

Administering security in WSN despite resource constraints requires additional control messages for neighbour discovery. Neighbour discovery is frequent due to improper and false neighbour information update as the network lacks neighbour verification schemes and other central administration schemes. Through data authentication schemes, transmission is secured, leaving out prolonged chances in identifying a reliable neighbour. This degrades the quality of aggregation by minimizing transmission rate and accuracy in data gathering process. Our proposed approach minimizes chances for delayed neighbour selection and reliability check. The consistency of the node for measuring its reliability is evaluated and is updated post relaying. The preference for nodes is given in the order of higher consistency. Besides, the trade-off between security and energy by improving aggregation precision, using distinctprocesses of data collection and energy effective routing as a single venture, is also intended to be curtailed.

4. Proposed method

The description of the proposed TA-EEA scheme is given in this subsection with its phases and their functions for WSN improving WSN performance.

4.1. Trust Assisted Energy Efficient Aggregation (TA-EEA) scheme

TA-EEA is a harmonic scheme bonding the three distinct phases of optimization viz., Trust Assisted Neighbour Selection (TANS), Energy Sustained Routing (ESR) and Congestion Aware Data Collection (CADC).

For effective neighbour selection and to minimize complexity in security, we avoid in-node security provisioning schemes like message authentication and encryption schemes. This reduces complex algorithms being dumped at the same WSN that turns out to be hard for the network resources at the time of deployment or that would require multifaceted hardware support. The proposed TA-EES scheme is illustrated in Fig. 1.

4.2. Trust Assisted Neighbour Selection (TANS)

The aggregator node broadcasts a request for collecting data from the active S_n nodes in the network. Active source nodes are connected to the aggregator nodes in either one-hop or multi-hop. Initially, the active source nodes route to the aggregator node based on shortest distance. Each node in the network holds a consistency information record as shown in Fig. 2 below.

Where, NODE_ID is the physical address of the communicating node, NEIGHBOUR field indicates the direct one-hop neighbour, CURR_TV is the current trust value of the neighbour node at an instance 't', UT is the trust updated time and C_TIME is the consistency time which is the difference between previous and current trust update time.

The data forwarding node computes the trust (Sardar & Majumder, 2013; Venkanna & Velusamy, 2013) of its direct neighbour (T_{dn}) using (5)

$$T_{dn} = \frac{dp_i}{dp_j} \tag{5}$$

where dp_i is the count of successful data packets forwarded from node i and dp_j is the count of successful data packets received from j^{th} node and i and j are the direct neighbours.

On computing the direct trust of the neighbour, the current forwarding node updates its table with the neighbour ID, trust value and the time at which the trust is updated. CURR_TV holds the value of T_{dn}.

NODE_ID	NEIGHBOUR	CURR_TV	UT	C_TIME

Fig. 2. Consistency information record.

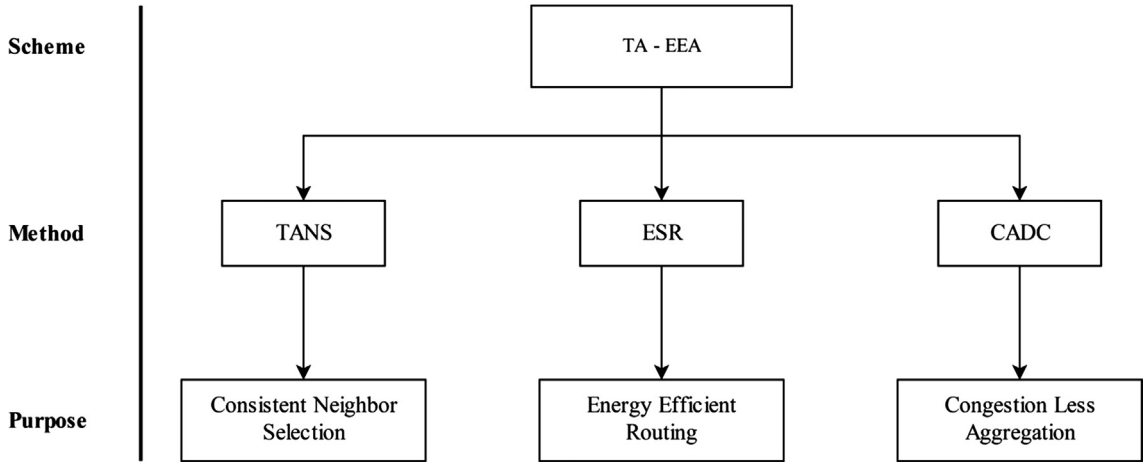

Fig. 1. TA-EEA illustration with functionalities.

Consistency time is computed using Eq. (6)

$$\Delta t(T_{dn}) = (UT - UT^{*}) \quad (6)$$

where $\Delta t(T_{dn})$ is the consistency time and UT^{*} represents the current trust updated time and UT represents the last trust updated time. The value of $\Delta t(T_{dn})$ is updated in the C_TIME field.

4.3. Forwarder selection conditions

An active forwarding node selects its next hop relaying node based on two conditions:

(i) The CURR_TV of the neighbour must be higher compared to the other direct neighbours and
(ii) C_TIME of the node must be large compared to the other direct neighbours.

Once the neighbour is selected the active source node relays all of its available data to the aggregator through the neighbour. This neighbour is regarded as the trusted node. The trust of the neighbour is updated post end of each transmission and a new trust value id updated. The default frequency of updating the T_{dn} value will be the time taken for the communication. Some special cases like facing larger drop or link failures and re-transmissions requires recurrent trust update and therefore the C_TIME of the nodes will be less.

4.4. Conditions for discarding a node from the routing path

A node can be discarded from the routing path if:

(i) The nodes' trust value is not updated or the node does not hold its neighbours trust information.
(ii) The nodes trust value is diminishing or the C_TIME is inflating.
(iii) The NEIGHBOR is replicated in two distinct nodes that are not in range.

A direct trust evaluation alone is preferred (discarding indirect trust computation) as duty cycle algorithm is employed for energy optimization. In duty cycle process, the indirect trust update from a node may not be expected if it is in sleep mode at the time of relaying.

4.5. Energy Sustained Routing (ESR)

For achieving energy efficiency in WSN, duty cycle process is employed, that prolongs a nodes' lifetime by switching transmission less nodes to sleep state and transmitting nodes to active state in a recursive manner. Our implication of duty cycle process is a diversified approach from the traditional duty cycle process. At the time of transmission initialization, the source nodes select I_n that route in a shortest path to the aggregator nodes. The rest of the nodes in the network are moved to sleep state with their radio receivers turned ON.

Fig. 3. List representation.

At the end of shortest path transmission, the active S_n nodes select their forwarder based on T_{dn} and $\Delta t(T_{dn})$. The nodes that are neglected this time from the routing path are moved to sleep state. To prevent unnecessary control message generation at the time of switching neighbours, the nodes hold two lists: Active List (AL) and Sleep List (SL). The lists can be represented as shown in Fig. 3.

The nodes that are involved in current transmission are present in AL and that are not participating in current transmission are moved to SL. Based on the trust value and C_TIME, the nodes in SL are sorted in descending order. When a node from AL is moved to SL, the a replacement for AL node is given from the top order of SL as the top level of SL holds the nodes with higher trust value and C_TIME after sorting.

Change of aggregator node relies on their half drain energy level. The aggregator node will be replaced when it drains half of the initial energy. Energy consumed by a aggregator is different from a common nodes' energy utilization. The energy consumed by a aggregator (E_{A_n}) is given (Chen et al., 2005) by Eq. (7)

$$E_{A_n} = k \times Y_a\left(\frac{d_{rr}}{k}\right) \quad (7)$$

where k is the aggregation level and Y_a is the function for aggregation.

Therefore it is necessary to keep monitoring the aggregator node energy. The half drain (E_{hd})of the node is given by (8).

$$E_{hd} = \frac{E_{init}}{2} \quad (8)$$

In order to monitor the aggregator nodes' energy level, its remaining energy needs to be computed subsequent to each aggregation. The remaining energy of the aggregator ER_{A_n} is computed using (9)

$$ER_{A_n} = E_{init} - E_{A_n} \quad (9)$$

when $ER_{A_n}$is equal to E_{hd}, the aggregator needs to be replaced.

4.6. Congestion Aware Data Collection (CADC)

In CADC phase, the aggregator accounts the forwarder capacity at the time of relaying collected data. Congestion control becomes essential as the forwarder node from the aggregator will not admit the same amount of data, the aggregator has collected. We intend the idea of verifying the acceptable limit of the direct forwarding neighbour

from the aggregator prior to each transmission. The packet accepting limit of the direct neighbour is verified using the transmission packet of the aggregator and the buffer utilization of the neighbour. If the count of packets transmitted by the aggregator is less or equal to the length of the neighbour buffer, then congestion is less. Therefore, the buffer length $B_L$is computed as given (Devi & Uthariaraj, 2013) in Eq. (10)

$$B_L = (1 - w_f) \times B_L + B_u \times w_f) \tag{10}$$

where w_f is the weight factor for transmission and B_u is the current buffer utilization.

The number of transmitted packets N_p is computed (Kumaravel & Prabha, 2012) using (11)

$$N_p = d_{tr}/L_r \tag{11}$$

where L_r is the link rate between A_n and I_n.

Prior to each transmission, the A_n needs to check if N_p is equal to B_L.

As stated in (Sirsikar & Anavatti, 2015), due to multiple packet reception, the aggregator may face the problem of replications that consumes further energy of the node. To minimize the impact of redundant transmissions, the aggregator is endowed with transmission verification and a counter broadcast. In transmission verification phase, the aggregator checks for the sequence numbers of each node that is indulged in communication. If the sequence number of a same node is found to be replicated at different instant of time 't', the aggregator discards the second transmission. This helps to minimize replicas from the same node at different instance of time.

In the counter broadcast, the aggregator broadcasts the last/recent observed transmission sequence number and binds the same with the each node address. It broadcasts the address and its associated sequence number to the next aggregator that is being elected. The new aggregator persists communication from the next sequence number received as a broadcast from the old aggregator node. The working of the proposed TA-EEA is illustrated in Fig. 4.

The process of the proposed TA-EEA is described in Algorithm 1.

Algorithm 1. TA-EEA Algorithm

Input: n, X * Y
$\forall n \in X * Y\{$
$S_n \rightarrow dataA_n \rightarrow dataI_n \rightarrow dataS_k$
Compute $T_{dn} = \frac{dp_i}{dp_j}, \forall I_n$ between A_n and S_k
Compute $\Delta t(T_{dn})$ using Eq. (6) $\forall I_n$ between A_n and S_k
if$\{curr_tv(I_{n_i}) > curr_tv(I_{n_j}) \&\& c_time(I_{n_i}) > c_time(I_{n_j})\}\{$
$next_intermediate = I_{n_i};$
$I_{n_i} :\rightarrow \{AL\};$
$AL \leftarrow: \{I_{n_j}\};$
Compute $E_{A_n} = k \times Y_a(\frac{d_{rr}}{k})$
if$\{ER_{A_n} < E_{hd}\}\{$
current$A_n :\rightarrow \{SL\}$
new$A_n = I_n, \max\{ER(I_{n1}), ER(I_{n2}), \cdots\}$
}endif
l1 :
for(next$I_n : S_k$){
Compute$B_L = (1 - w_f) \times B_L + B_u \times w_f)$
Estimate$N_p = d_{tr}/L_r$
if$\{N_p < B_L\}\{$
$A_n \rightarrow$ datanewI_n
nextI_n
GotoL1;
}endif
}endfor
}endif
}endfor
Output: trusted and energy efficient node n

The different methods in the proposed TA-EEA results in identifying an energy efficient trusted neighbour that is best-fit for consistent transmissions.

5. Simulation results and discussion

This section assesses the performance of the proposed scheme with the simulation background and the performance metrics. The considered metrics are compared with

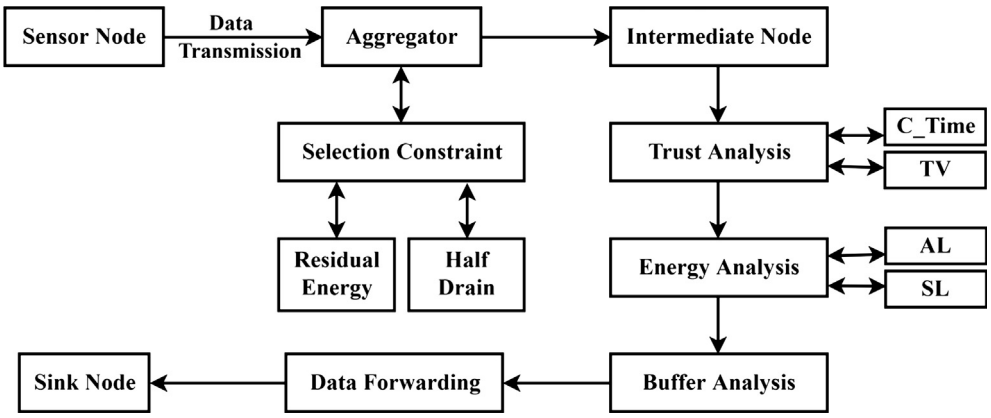

Fig. 4. TA-EEA working.

Table 1
Simulation parameters.

Parameter	Value
Network Area	1000 × 1000
Protocol	Dynamic source routing
No. of sensor nodes	100
Network topology	Flat grid
IEEE standard	802.11
Broadcasting Range	250 m
Application type	Constant bit rate
No. of packets	1500
Initial energy	10 J

the existing approaches to verify the reliability of the proposed scheme.

Our proposed TA-EEAs' performance metrics are compared with a Centralized Energy Allocation Algorithm (CEA) and SAERP that are implement using network simulator. Our proposed scheme is analyzed using the metrics: PDR, aggregation delay, control overhead, and energy utilization. We consider 100 nodes placed in a uniform manner in a 1000 m × 1000 m region with multiple transmitting nodes and a sink node. Table 1 shows the simulation parameters and its values.

6. Results

6.1. Packet delivery ratio

The above Fig. 5 illustrates the comparison of PDR for our proposed TA-EEA with EBRP (Ren et al., 2011) SAERP (Tyagi et al., 2014) and CEA (Xiao et al., 2015). In our proposed scheme, the aggregator is balanced between energy and congestion rate so as to transmit acceptable limit of packets to its forwarders. This lessens packet drop and augments the count of packets being delivered at the sink. Therefore, packet delivery ratio of our proposed TA-EEA is high comparatively.

6.2. Control overhead

The performance of EBRP, SAERP and CEA is compared with the proposed TA-EEA scheme with respect to the control overhead measured (Fig. 6). As the number of neighbours increases, the previous approaches discard the old neighbours to discover the new neighbours. This requires added control messages for both discovery and route establishment. In TA-EEA, the nodes are maintained in separate lists that are switched between the states without additional control messages. A node is discovered with a new broadcast if it has joined the network or the communication region of the active transmitting nodes. Therefore, unnecessary or non-periodic control message broadcast is restricted in our proposed approach.

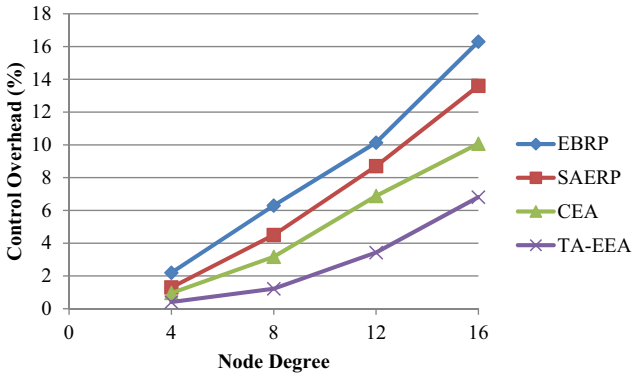

Fig. 6. Control overhead.

6.3. Aggregation delay

As flow rate increases, time taken for gathering the data increases (Fig. 7). In TA-EEA scheme, the CADC process minimizes retransmission post drop with the fore hand information of the forwarder buffer utilization. The time taken for aggregation is not interrupted due to retransmission, in TA-EEA scheme that consumes lesser time when compared to EBRP, SAERP and CEA.

6.4. Energy consumption

Fig. 8 illustrates the energy consumption compared between TA-EEA, CEA, SAERP and EBRP. In the proposed TA-EEA, ESR process retains an appreciable count of energy efficient nodes for further transmission by switch-

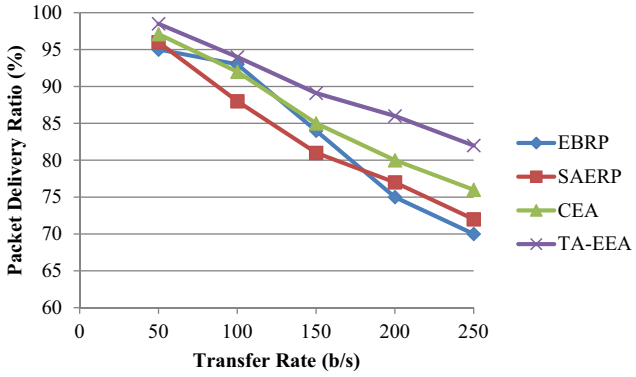

Fig. 5. Packer delivery ratio.

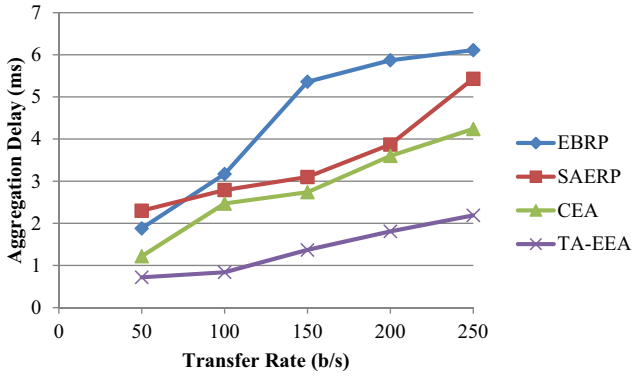

Fig. 7. Aggregation delay.

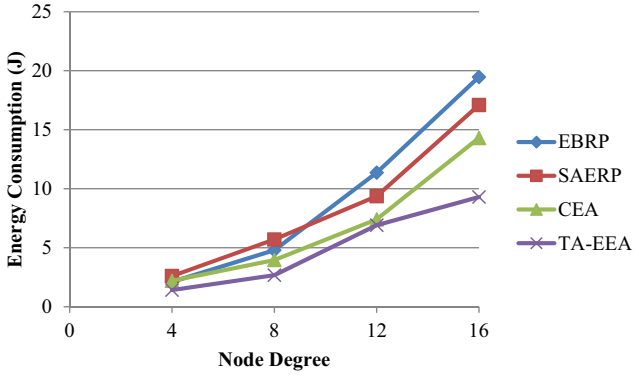

Fig. 8. Node degree vs energy consumption.

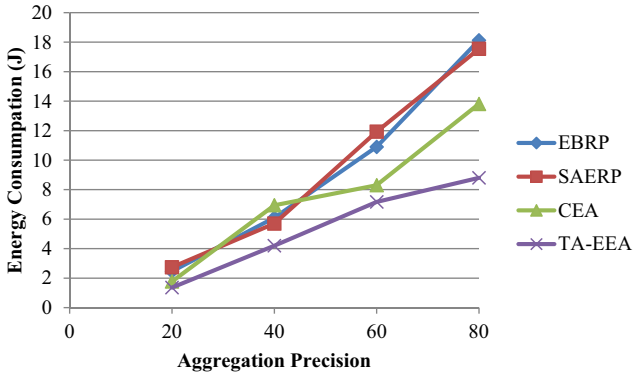

Fig. 9. Aggregation precision vs energy consumption.

ing them amid active and sleep state based on their consistency. This prevents a single node being utilized and drained once for all. As a result, not all nodes need to spend energy for a agreed transmission, minimizing the overall energy consumption.

The comparison for aggregation precision and energy consumption between EBRP, SAERP, CEA and the proposed TA-EEA is shown in Fig. 9. As aggregation precision increases, the level and rate of data collection increases, utilizing energy to the maximum limit. In TA-EEA, the aggregation is carried out through reliable neighbours as recommended by TANS and congestion is controlled by CADC. This helps to improve aggregation accuracy with lesser energy consumption as the methods prevent additional neighbour discovery and retransmissions.

7. Conclusion

We have analyzed and intended to minimize the trade-off factors prevailing in WSN and to exploit the same to improve the performance of the networks. Our proposed TA-EEA scheme is independent of the resource constraints of the network that performs optimization in a unanimous manner. Simulations conducted prove the consistency of our scheme by retaining networks' delivery ratio with controlled overhead which is quite high in selecting a secure neighbour with multi constraints. This approach succeeds in integrating the multi faced process as a single bind scheme with efficiency of its implication. The future of the work is planned to improve our TA-EEA scheme with scalability that would extend support for large scale Wireless Networks.

Appendix A. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.cogsys.2018.11.006.

References

Alzaid, H., Foo, E., & Nieto, J. G. (2008). Secure Data Aggregation in Wireless Sensor Network: A survey. *Information security conference (ACSC2008), Wollongong, Australia.* .

Avokh, A., & Mirjalily, G. (2010). Dynamic Balanced Spanning Tree (DBST) for data aggregation in wireless sensor networks. *2010 5th international symposium on telecommunications.* .

Chao, C.-M., & Hsiao, T.-Y. (2014). Design of structure-free and energy-balanced data aggregation in wireless sensor networks. *Journal of Network and Computer Applications, 37*, 229–239.

Chen, Y., Liestman, A., Liu, J. (2005). Energy-Efficient data aggregation hierarchy for wireless sensor networks. In Second international conference on quality of service in heterogeneous wired/wireless networks (QSHINE'05).

Devi, M., & Uthariaraj, R. (2013). Congestion based route recovery technique for MANET. *Journal of Theoretical and Applied Information Technology, 54*(1), ISSN: 1992-8645.

Fasolo, E., Rossi, M., Widmer, 1., & Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: A survey. *IEEE Wireless Communications [see also IEEE Personal Communications], 14*(2), 70–87.

Gaikwad, P. B., & Dhage, M. R. (2015). Survey on secure data aggregation in wireless sensor networks. *2015 International conference on computing communication control and automation.* .

Guo, S., Wang, C., & Yang, Y. (2013). Mobile data gathering with wireless energy replenishment in rechargeable sensor networks. *2013 Proceedings IEEE INFOCOM.* .

Huang, S. I., Shieh, S., & Tygar, I. D. (010). Secure encrypted-data aggregation for wireless sensor networks. *Wireless Network, 16*(4), 915–927.

Jain, T. K., Saini, D. S., & Bhooshan, S. V. (2015). Lifetime optimization of a multiple sink wireless sensor network through energy balancing. *Journal of Sensors, 2015*, 1–6.

Kumaravel, S., & Prabha, S. (2012). Adaptive data traffic control with wireless sensor networks. *International Journal of Computational Intelligence and Informatics, 2*(3), 200–208.

Mantri, D., Prasad, N. R., & Prasad, R. (2013). "BHCDA: Bandwidth efficient heterogeneity aware cluster based data aggregation for Wireless Sensor Network. *2013 International conference on advances in computing, communications and informatics (ICACCI).* .

Mathapati, B. S., Patil, S. R., & Mytri, V. (2012). Energy efficient reliable data aggregation technique for wireless sensor networks. *2012 International conference on computing sciences.* .

Mottaghi, S., & Zahabi, M. R. (2015). Optimizing LEACH clustering algorithm with mobile sink and rendezvous nodes. *AEU - International Journal of Electronics and Communications, 69*(2), 507–514.

Önen, M., & Molva, R. (2007). Secure data aggregation with multiple encryption. In *Lecture notes in computer science wireless sensor networks* (pp. 117–132).

Othman, S. B., Trad, A., Youssef, H., & Alzaid, H. (2013). Secure data aggregation with MAC authentication in wireless sensor networks.

2013 12th IEEE international conference on trust, security and privacy in computing and communications. .

Ozdemir, S., & Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: A comprehensive overview. *Computer Network, 53*(12), 2022–2037.

Przydatek, B., Song, D., & Perrig, A. (2003). SIA: Secure information aggregation in sensor networks. *Proc. ACM Conf. Embedded Network Sensor Systems*. .

Rajagopalan, R., Varshney, P. K. (2006). Data aggregation techniques in sensor networks: A survey. L.C. Smith College of Engineering and Computer Science at Surface.

Rao, P. C. S., Jana, P. K., & Banka, H. (2016). A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks. *Wireless Networks*.

Ren, F., Zhang, J., He, T., Lin, C., & Ren, S. K. D. (2011). EBRP: Energy-balanced routing protocol for data gathering in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 22* (12), 2108–2125.

Roy, S., Conti, M., Setia, S., & Jajodia, S. (2012). Secure data aggregation in wireless sensor networks. *IEEE international conference*. .

Roy, S., Setia, S., & Jajodia, S. (2006). Attack-resilient hierarchical data aggregation in sensor networks. *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks - SASN '06*. .

Sardar, M., & Majumder, K. (2013). A new trust based secure routing scheme in MANET. In *Proceedings of the international conference on frontiers of intelligent computing: theory and applications (FICTA) 2013 advances in intelligent systems and computing* (pp. 321–328).

Sirsikar, S., & Anavatti, S. (2015). Issues of data aggregation methods in wireless sensor network: A survey. *Procedia Computer Science, 49*, 194–201.

Soltani, M., Hempel, M., & Sharif, H. (2014). Data fusion utilization for optimizing large-scale wireless sensor networks. *2014 IEEE international conference on communications (ICC)*. .

S.B., K. Y., Tyagi, S. S., Soni, M. K., E., O. M. E. (2014). SAERP: An energy efficiency Real-time Routing protocol in WSNs. In 2014 International conference on reliability optimization and information technology (ICROIT).

Venkanna, U., & Velusamy, R. L. (2013). Mitigating the attacks on recommendation trust model for mobile ad hoc networks. In *Proc. ERCICA* (pp. 123–130).

Xiang, L., Luo, J., & Rosenberg, C. (2013). Compressed data aggregation: Energy-efficient and high-fidelity data collection. *IEEE/ACM Transactions on Networking, 21*(6), 1722–1735.

Xiao, S., Li, B., & Yuan, X. (2015). Maximizing precision for energy-efficient data aggregation in wireless sensor networks with lossy links. *Ad Hoc Networks, 26*, 103–113.

Xie, R., & Jia, X. (2014). Transmission-efficient clustering method for wireless sensor networks using compressive sensing. *IEEE Transactions on Parallel and Distributed Systems, 25*(3), 806–815.

Zhao, M., Li, J., & Yang, Y. (2014). A framework of joint mobile energy replenishment and data gathering in wireless rechargeable sensor networks. *IEEE Transactions on Mobile Computing, 13*(12), 2689–2705.