Future Generation of Communication and Internet of Things (FGCIOT)

Journal homepage: http://fgciot.semnaniau.ac.ir/

PAPER TYPE (Research paper)

Semantic and Trust based Data Aggregation in Wireless Sensor Networks

Mohammad Ahmadinia[1], Mohammad Davarpour[2]

[1] *Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran.*

[2] *Department of Computer Engineering, Semnan Branch, Islamic Azad University, Semnan, Iran.*

Article Info

Article History:

Received September 10, 2022
Revised October 5, 2022
Accepted October 15, 2022

Keywords:

Semantic sensor network, Trust modelling, Semantic data aggregation, Ontology

*Corresponding Author's Email Address: ahmadinia@gmail.com

Extended Abstract

Wireless sensor networks consist of a large number of sensor nodes spread in an environment. If the target-related data is collected semantically in the sensor network, it would be possible to be processed and reasoned intelligently. On the other hand, one of the most important challenges to do with all cases related to sensor networks is the limitation of energy consumption. Data aggregation technique is a way to reduce the energy consumed in wireless sensor networks. Although the techniques based on data aggregation extends the network lifetime through reducing the number of sent packets, they can decrease the accuracy and reliability of the received data. In this paper, Firstly, one strategy for semantic data collection and aggregation of information related to the targets located in sensor network environment are presented. Secondly, through semantic modelling of trust, a method is presented in aggregation technique in order to identify highly trusted sensors and increase their use in collection and aggregation of data about the sensed targets. Therefore, the system accuracy and trust would be generally improved. Modelling and simulation results show the desirable performance of the presented method compared to the previous works

Introduction

Wireless sensor networks are applied to monitor and control an environment. These networks consist of a large number of sensor nodes spread in an environment. In order to make the enormous data produced by these sensor networks, rational and understandable for the machine, semantic web technologies should be applied. These technologies can help sensor data aggregation and query to be managed in a better way.

One of the most important challenges to do with all cases related to sensor networks is the limitation of energy consumption. One way to reduce the energy consumed by wireless sensor networks is data aggregation technique.Data aggregation, through combination of related data, avoids the transmission of extra packets in order to reduce the total number of sent packets in the network. Some strategies should be presented to replace the extraction of raw sensor data in order to extract data based on its entity, because the end users usually aim to have access to information with an upper level of physical entity monitored by the sensor network. This can increase the usability of sensor network. Although the techniques based on data aggregation extend the network lifetime through reducing the number of sent packets, they can decrease the accuracy and reliability of the received data. It can be particularly deteriorated when sensors that

Doi:

collect and aggregate data are dealing with a problem or failure; Therefore, the accuracy of final decision is extremely reduced or a wrong decision might be made; thus, it is necessary to identify erred nodes and avoid using them in aggregation techniques as far as possible.

Considering what has been mentioned, this paper firstly aims to present some strategies to collect and aggregate information about the targets located in sensor network environment, through which the sensors that collect data related to a target can decrease the number of sent packets and increase the network lifetime through data aggregation. Through semantic and target-based data collection and using ontology, this paves the way for sensor data reasoning and knowledge extraction. Secondly, a method is presented in aggregation technique in order to identify highly trusted networks and increase their use in collection and aggregation of data about the sensed targets. Thus, the system accuracy and trust would be generally improved.

The rest of the paper has been organized as follows: In section two, the previous relevant works will be reviewed. Section three contains the suggested strategy for semantic and target-based presentation of sensor network data and modeling trust in sensor network. A method of semantic and trust-based collection of data in sensor network is described in the fourth section. The presented strategies are evaluated in fifth section. The sixth section includes the paper summary and conclusion.

I. PREVIOS WORKS

The previous research related to the subject of this paper can be divided into two parts: 1) semantic modeling of sensor networks and semantic gathering of sensor data, 2) trust management in wireless sensor networks.

The majority of works on semantic modeling of WSNs concerns to appropriate ontology design. In general, the ontologies presented in this regard can be divided into two main categories: Sensor-centric ontology and observation-centric ontology. The first has been developed to describe and infer from sensors and sensor networks such as CSIRO(Neuhaus and Compton, 2009), OntoSensor (Goodwin and Russomanno, 2007), CESN[1](Calder, Morris and Peri, 2010) and Ontonym-Sensor (Stevenson, Knox, Dobson & Nixon, 2009). The second has been developed to describe sensor observations and sensor-obtained data such as Stimuli-Centered (Stasch and et al, 2009), O & M (Werf and et al., 2009) and OOSTethys(Bermudez , 2010). However, ontology SSN (Compton & et al., 2012) is an appropriately perfect ontology based on OWL2 developed by the W3C Semantic Sensor Network called SSN-XG. This ontology describes the capabilities and properties of sensors, the act of sensing and the resulting observations.In (Roda and Musulin, 2014), an ontology-based framework is presented for the smart management of data collected from the sensor network. This work is based on a knowledge model that it is composed of the synthesis of two existing ontologies including SSN (a semantic sensor network ontology), SWRL (a temporal ontology) and a developed ontology as TAO (temporal abstracts ontology). Work (Kim and et al., 2013) presents a general methodology to manage the data collected from heterogeneous sensor networks. It introduces a set of words with rules related to network to connect various networks and manage them using OWL language and protégé tool. Concepts concerned with communications are not considered in SSN ontology and other ontologies of the sensor network. Hence, in work (Bendadouche and et al, 2012), an extension was done on SSN ontology which modeled data transfer between sensors and relations between sensors. In (Calbimonte and

[1] Coastal Environmental Sensor Networks

et al., 2012), an ontology-based model is presented to gain access to sensor network data and querying on data stream resources. In this work, authors allow users to express their needs on a conceptual level independent from language-related details and implementation via developing SPARQL and rewriting query. Work (Ibrahim and et al., 2013) presents a temporal-spatial model for sensor networks. The model makes it possible to reason based on sensors in any time and place. In this work, BFO and SSN ontologies are used. Work(Paul and et al., 2012) proposes a new method of characterizing and extracting semantic metadata via analyzing the observations of sensor raw data.

Several works have been proposed for trust management in WSNs. In the following, some of them explained: In (Ren and et al., 2014), the authors proposed a trust management scheme for UWSNs to provide efficient and robust trust data storage and trust generation. For trust data storage, they employed a geographic hash table to identify storage nodes and to significantly decrease storage cost. They used subjective logic based consensus techniques to mitigate trust fluctuations caused by environmental factors. In (Aivaloglou and et al., 2010) proposed a hybrid trust and reputation management protocol for WSNs by combining certificate-based and behavior-based trust evaluations. In (Bao and et al. 2012), the authors proposed a hierarchical trust management protocol leveraging clustering to cope with a large number of heterogeneous SNs for scalability and reconfigurability, as well as to cope with selfish or malicious SNs for survivability and intrusion tolerance. In (Krasniewski and et al., 2005) the authors designed a protocol to diagnose and mask arbitrary node failures in an event-driven WSN. In (Ganeriwal and et al., 2008), the authors proposed a Bayesian trust management framework where each node maintains reputation metrics to assess past behavior of other nodes and to predict their future behavior. The authors in (Yadav and et al., 2010) proposed iTrust, an integrated trust framework for WSNs. In (Anantharam and et al., 2011), an ontology has been presented, in order to model trust in wireless sensor networks and social networks, semantically.

II. SEMANTIC AND TARGET-BASED PRESENTATION OF SENSOR NETWORK DATA

In order to make the enormous data produced by sensor network, rational and understandable for the machine, semantic web technologies should be applied. Ontology is one of the most important semantic technologies applied in order to present and share knowledge. W3C Semantic Sensor Network group (SSN_XG) also has been presented a suitable and perfect ontology based on OWL2 which describes the abilities and attributes of sensors, the act of sensing, and observations. The main output of this group was to design SSN ontology(Compton and et al, 2012). This is a suitable ontology for semantic presentation of sensor networks and the data collected by them.

A. Linking of SSN ontology to domain ontologies

SSN ontology is a domain-independent model. Since the information is collected based on targets and not on sensors, other ontologies developed in each particular arena should be applied along with SSN ontology depending on the application of sensor network in that arena. For instance, if the sensor network is activated to do with agriculture, it would be applied in order to define agricultural concepts and entities such as plant, etc. In order to collect semantic information about the targets, SSN and domain ontologies must be linked properly. For instance, a method should be found to map the sensor perceptions to the dynamic attributes of the targets. On the other hand, the information stored in sensor network is recommended to be saved based on targets and not on sensors. The amount of extra information sent in the network and the stored information in the sensor network database can be largely decreased through target-based information saving.

The target-related information collected from sensor network falls into three categories: temporal, spatial, and thematic information, which together specify the target state at any time or place. This information exists in the applied domain ontologies. In this way, they can be linked to the SSN ontology.

B. Linking of thematic information

establish a thematic relation between SSN and domain ontologies of an entity, SSN:observation and SSN:sensor classes are connected to target attribute applying the SSN:observes and SSN:observedProperty parameters. Thus, it is specified that which entity attribute is monitored by each sensor.

C. Linking of spatial information

Applying the SSN:Platform object in SSN ontology, and also geographical ontologies such as WGS84, the geographical location of sensors can be presented. The location of a target can also be specified applying target locating methods and using position of several sensor nodes around the entity.

D. Linking of temporal information

The time of an observation is connected to a temporal class in OWL-time ontology (i.e. instance), using SSN:ObservationResultTime parameter. This can be equivalent with the change in quantity of a target attribute. Therefore, initialization time for an attribute is connected to OWL-time:instance class.

E. Semantic modeling of trust

In order to model trust in wireless sensor networks and social networks, an ontology has been presented(Anantharam and et al., 2012). This ontology is illustrated in Figure 1.

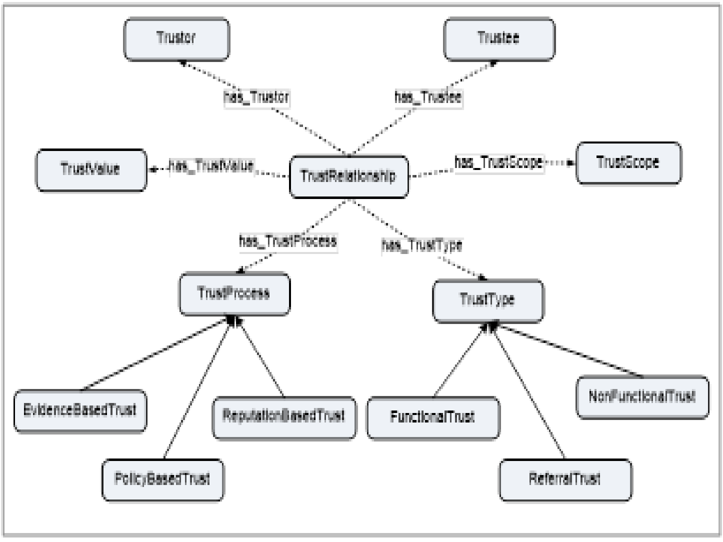

Fig. 1: Trust modeling ontology in wireless sensor networks and social networks (Anantharam and et al., 2012)

The proposed model for semantic modeling of sensor network trust is illustrated in Figure 2. The presented model expands Trust ontology that represented at (Anantharam and et al., 2012).

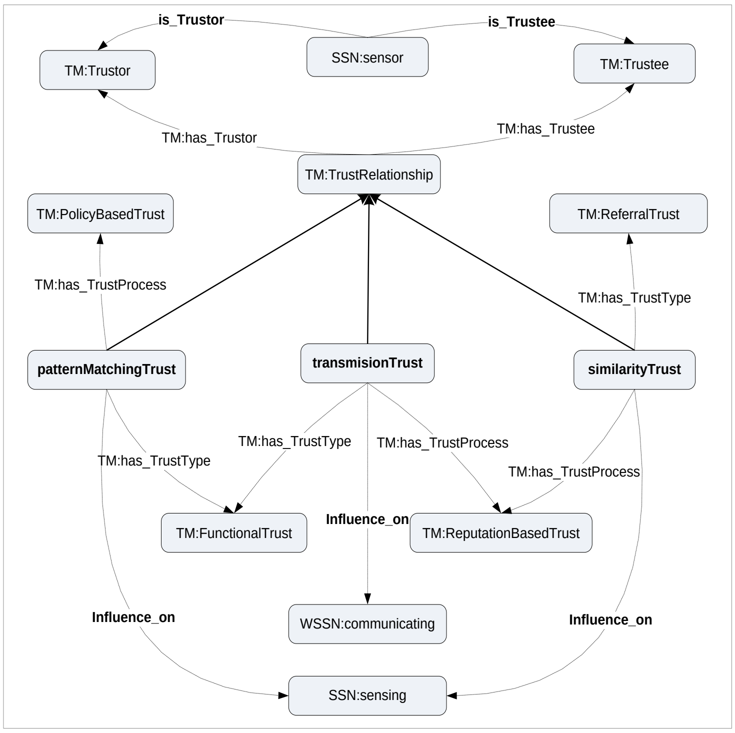

Fig. 2: Trust modeling through the proposed method and its connectivity to other ontologies

Sensor nodes are the effective agents in sensor networks. Thus, sensor class of SSN ontology is applied in modeling. Many parameters can be considered for calculating the trust of sensor nodes. Three parameters including non-similarity with the data received by neighbors, transmission error and not being matched with the expected pattern are applied in this work. Three classes including similarityTrust, transmissionTrust and patternMatching Trust have been applied to model these parameters. These factors have been introduced using suitable classes in TM ontology (Anantharam and et al., 2012). Thus, type of similarityTrust, ReferralTrust Class and its process, ReputationalTrust are considered that are extracted from TM ontology. Since these factors affect the sensitivity of sensor node, they would be connected to the sensing class of SSN ontology through Influence_on relation. As for the transmissionTrust class, FunctionalTrust type and ReputationalTrust process are extracted from TM ontology. As this factor affect the transmissibility of sensor node information, it can be connected to communicating class of WSSN ontology (Bendadouche and et al., 2012) through Influence_on relation (since sensor network communicational concepts have not been modeled in SSN ontology, they are modeled by WSSN ontology as an extension to SSN ontology). As for the patternMatchingTrust class, FunctionalTrust type and PolicyBasedTrust process are being considered. Since this factor affect the sensitivity of sensor node, it can be connected to sensing class of SNN ontology through Influence_on relation.

The effective parameters on trust that have been applied in this modeling are transmission accuracy, similarity with the data received by neighbors and being matched by the expected pattern.

III. SEMANTIC AND TRUST-BASED GATHERING DATA IN SENSOR NETWORK

This section aims to present a suitable strategy in order to collect semantic information related to the targets located in sensor network environment. Thus firstly, the more trusted nodes will play a more significant role in data collection and secondly, information will be collected semantically and based on targets. Software agents are applied in order to collect information about the targets located in the sensor network and trace the moving targets. In fact, one software agent is considered for each target located in the sensor network environment. This agent should migrate towards the target zone through the sensors, and settle in a suitable node near the identified target (leader node). Then, the agent should receive target-related information from the sensor nodes and send them to the sink. The target agent is created in the sink node. Fixed targets are usually settled in the sensor network from the beginning, but moving targets enter the environment while the sensor network is working. Therefore, the agent related to a particular target is either created from the beginning of sensor network operation, or when the sensor node identifies a target within the environment and informs the sink.

Target agent matches the SSN ontology which is related to the modeling of sensors and its observations and domain ontologies that model the sensed targets. Thus, the attributes perceived by the sensors is attributed to the target attributes. In order to connect sensor observations to the entity ontology, SSN:observation and SSN:sensor classes are connected to target attributes in domain ontology, applying SSN: observes, and SSN:observed Property parameters. Through this, it is specified that each sensor monitors which attribute of the target. In order to obtain the time of the change in target situation, or an event, temporal attributes of SSN ontology in the sensor node are directly mapped to target-related domain ontology.

In order to obtain spatial information about the target, each node is assumed to be aware of its location and capable of estimating its distance to the target. In this case, at least the information related to three sensor nodes around the target is needed to obtain its location. Therefore, target agent, which is located on one of the nodes around the target, receives the location of nodes and their distance to the target at least from three sensor nodes around it (leader node and two other ones). The target location is calculated in this way. Whenever the target agent receives different target-related information (temporal, spatial and thematic information), it sends them to the sink node in specific time intervals or when there is a change in situation or thematic or spatial information.

IV. Deployment the agent in a suitable node

A target might be placed in sensing range of several sensor nodes, simultaneously. Therefore, several nodes can monitor a particular target and collect its information. When the target is not a specific geographical location (but for instance a moving entity), the monitor nodes are those in its neighborhood and the target falls in their sensing range. Therefore, the software agent can be deployed in any of these nodes in order to receive target related information from the sensor nodes that are monitoring the target. But yet it would be better to deploy the software agent in a node with specific condition in order to collect information in a proper way and save energy in the network. Therefor, some parameters considered for selecting proper node, such as remaining energy, distance to the target, distance between leader and monitor nodes, multi-sensing, adjacency to the sink node and trust. The following part describes a method to calculate trust.

A. Calculation of the sensor node trust

This is how to calculate the effective parameters on trust:

B. Transmission Accuracy

In order to calculate this parameter, each node in the sensor network should firstly send a packet to all of its neighbors. Then it would demand and receive the same packet. This should be done by all of the network nodes. The next step is to investigate the sameness or difference of sent and received packets and inform the result to that node. Within a specific time, each node has the number of changed (N) and unchanged (P) packets. Thus the transmission error can be obtained through relation 1.

$P/(P+N) = \alpha$ (1)

C. Similarity with the data received by neighbors

Each node collects the data about the environment received by its neighbors and compares it with its own. Then, the mean value of those received by the neighbors is obtained. The difference between the date received by the considered node and the mean value is obtained in order to calculate the standard deviation of data received by neighbor nodes. The more difference between the value given by the considered node and the mean value of its neighbors, with this standard deviation, the more likely it is to have error and be less trusted.

β=1-(├|Δi-┤ ├ δ┤ |)/(├|Δi+┤ ├ δ┤ |) (2)

Δi = The difference between mean value of the data received by neighbors and data of that node

δ = Standard deviation

D. Being matched by the expected patter

If Δd is considered as the range of expected variation in sensed data, and the real range of variation (which is equal to the difference

between the data reported by the node and the expected value of data at the same moment) is represented by Δi, this parameter can be obtained through the relation 3:
(Δi-Δd)/(Δi+Δd) γ= (3)
In order to control the effect of each parameter, they must be weighted. Finally, the trust of each node is calculated through the relation 4:
W 3 * γ + β W2 *+ α =W1* t (4)
wi represents the weight given to each effective parameter in calculation of trust. The following conditions are met: W1+W2+W3 =1 و Wi ≤1 ≤0

V. Target recognition and selecting the leader node

If a target deploys in sensor network environment, it can be recognized by the sensor nodes that have this target in their sensing range. These are called the monitor nodes of that target. The task of sensor agents of monitor nodes is to elect one of the monitor nodes as the leader.To do this, each sensor agent calculates the competency of the corresponding node for being a leader according to predefined parameters, notifying the other sensor agents in the monitor nodes so as to elect the node with the highest level of competence as the leader node. In order to obtain the competence level (C), each of the effective parameters on selection of leader node are firstly calculated and normalized as shown hereunder.

A. Remaining energy(ek)

The amount of remaining energy (ei) in each node is divided by the maximum or initial energy of the nodes (emax) in order to obtain this parameter.
e_k=e_i/e_max (5)

B. Distance to the target

The node's distance to the target (di) is divided by its sensing range (rs). Then its ones' complement is obtained in order to calculate this parameter. When the sensor node is located on the target (e.g. target is a geographical zone), Zero can be considered as the distance to target. Also when the vicinity of node to the center is a matter of significance, the distance between the node and the center of target is considered as the value of this parameter.

$$d_k = 1 - \frac{d_i}{r_s} \qquad (6)$$

C. Multi-sensing($\boldsymbol{g_k}$)

The total number of different attributes of the target that can be obtained by the node (or the number of different sensors of the node), plus one (if the node is capable of positioning) is considered as the number of node sensing (gi) and it will be divided by the total number of attributes that can be sensed in the network (gtotal) plus one (that confirms the position).

$$g_k = \frac{g_i}{g_{total} + 1} \qquad (7)$$

D. Distance to sink node (Sk)

The distance between the monitor and sink nodes or the number of steps to the sink node (si) is divided by the biggest diagonal of sensor network or the maximum number of hops within the network (Smax), in order to calculate this parameter.

$$s_k = \frac{s_i}{s_{max}} \qquad (8)$$

E. Trust($\boldsymbol{t_k}$)

According to the suggested method in the previous part, trust is obtained through relation 4.

The competency of a node for becoming leader is considered as an outcome of the mentioned parameters. In order to adjust the effect parameters in calculating the competency, each parameter is assigned a value between zero and one so that the total weight is equal to one.

$$C_k = w_e \times e_k + w_d \times d_k + w_g \qquad (9)$$

$$w_e + w_d + w_g + w_s + w_t = 1 \qquad (1)$$

Thus the Ck value (which falls between 0 and 1) is calculated for each node, referring to its competence to be selected as leader node.

In the next stage, each sensor node broadcasts its C value to its neighbors. If L refers to the size of the biggest diagonal of the target (i.e. the distance between the farthest points on the target), there would be two situations. First, when the communicational radius of the sensor nodes is bigger than two times of sensing radius plus L. i.e. Rt> 2Rs +L. In this case, all the sensor nodes detecting the target are in each other's neighborhood. After one broadcast, all the monitor nodes entail the competency value of other nodes as the sensor agents deployed in the monitor nodes can specify, through comparison of C values, the leader node (i.e. the node with the highest C value).

The second scenario involves $R_t < 2R_s + L$. In this case, all the monitor nodes might not be neighbors. Therefore, after one broadcast, some of the monitor nodes might not have received the C value of some other monitor nodes. After the first-stage broadcast, each node has a list of neighbors and their C values, who are monitor nodes of entity. The proposed solution to receiving the list of entire monitor nodes by each of the monitor nodes is that each monitor node should send a list of attributes and competencies of its monitor neighbors to all the monitor neighbors. Thus, if two monitor nodes are two hops away from one another, they can receive each other's profile and complete their list. This will be repeated as long as the list of entire monitor nodes is completed. There is a limited number of repetitions (K), which can be obtained through relation 11 in case of network connectivity and full coverage of the environment by its sensors.

$$K = \left\lceil \frac{2R_s + L}{R_t} \right\rceil \qquad (11)$$

When all monitor nodes obtained the full list of other nodes that monitor the target and their level of competence, the one with the highest C value would be selected as the leader node. Afterward, the leader node sends a demand to the sink through other sensor nodes, where a suitable software agent is developed and sent towards the leader node.

VI. Scheduling of sensor agents

After the deployment of the target agent on the leader node, it would firstly receive the attributes of monitor nodes, so as to determine what information each sensor gathers, and whether or not it is capable of geographic positioning? How much is the remaining energy and how far is the node from the entity? Afterward, in order to save the energy consumption, the target agent designs a schedule for activities of the monitor nodes and informs them about it. Based on this schedule, monitor nodes would sense the target and send the related information to the target agent.

Since the target agent is deployed on the leader node that is constantly active and performs more data processing and transmission compared to the other monitor nodes, it loses its energy after a while and stops working before the others. In order to prevent this, the target agent must be transferred from the current node to another sensor node after a specific time. Therefore, another node with a higher C value should be firstly selected to replace the existing leader node according to the list of monitor nodes. Then that node and the others must be informed about the change in their role. That's when the target agent is transferred to the new leader node.

VII. EVALUATION OF THE PROPOSED METHODS

The presented strategies should be investigated from three aspects. Firstly, since these strategies are presented in order to model and collect the data sensed by wireless sensor networks, their efficiency in application of the suggested methods should be evaluated. Secondly, Recall and Precision parameters of information extraction should be investigated in order to evaluate the capability of the suggested method to model and extract the sensed data semantically. Thirdly, since one of the main objectives of the suggested method is to increase the trust in sensing and sending information, trust related parameters should be evaluated as well.

VIII. Simulation tools and conditions

J-sim network simulator was applied in order to evaluate the presented strategies. Java-based tool, Jena is applied in order to work with different ontologies. One of the main applications of sensor networks, i.e. collecting the information related to geographical zones, was used in line with investigation of the presented strategies. As it has been mentioned in the previous section, this system firstly models the information and attributes of the geographical zones semantically. Then the static information and those sensed by no sensor in the network are manually entered to the gateway. That is when the network is operated to collect dynamic information by the sensors through the foresaid methods. Climate data received from Meteorological Research Center of Kerman is considered as the set of data tested in this work. It includes the data collected by automatic weather stations in Kerman Province. A sensor network in a 1000*1000 m2 hypothetical environment is considered in this scenario. Ten different geographical zones are considered to exist in this environment. Sensors collect data from the environment and send it to the sink node each ten minutes. Each sensor node is assumed to be capable of sending to the sink in one step.

IX. Evaluation of the efficiency of functional parameters of WSN

It is necessary to evaluate the efficiency of the parameters related to the performance of the sensor network in the presented strategy. Considering the type of the suggested strategy, some of the previous works are selected for this comparison: 1) GPSR method (Karp and Kung, 2000): A method to collect basic information in sensor networks without clustering them; 2) LA-SleepScheduling (Ahmadinia and et al. 2014): That presents a Clustering algorithm based on environmental similarities, applying cellular learning automata technique. After clustering, a scheduling algorithm is also suggested in this work for alternative activation of sensor nodes for environmental sensing; 3) The algorithm presented in (Paul and et al., 2012) (acronymically called DSSM-RM): In this work, the collected data by the sensors is modeled applying an ontology. All the sensor nodes are activated in this method. Unlike the suggested method, the modeling is based on sensor, and not on the target; 4) Trust modeling method (TM) (Anantharam and et al. 2011): In which the sensor node trust is modeled semantically applying an ontology. All of the sensor nodes are activated in this method. The Comparative parameters are: network lifetime and algorithm overload.

The active nodes send their data to the sink node each ten minutes. There are several tests conducted for a number of sensor nodes n at 20, 50, 100, 150, 200 and 300. each test is repeated 10 times on each number of the sensors. The obtained result is the mean value of the ten operations.

Sensor lifetime is the first parameter applied to compare these different methods. The network lifetime in this research was considered the dissipation of the first node in the network (Ahmadinia and et al., 2014). The evaluation results illustrated in Figure 3 refer to the desirable performance of the suggested method. Figure 4 illustrates the energy consumed by the algorithm proportional to the total consumption energy during the sensor lifetime (algorithm overload) and compares this ratio in different methods. As to the suggested algorithm, the mentioned ratio is higher compared to the other algorithms. This is indeed because of the initial use of LA-SleepScheduling algorithm in the suggested method. Moreover, the use of software agents and semantic notation of information, and also the calculation of the trust of nodes cause an overload. But since the majority of nodes are inactive in most cases, the network lifetime is significantly increased. The higher energy consumption in learning phase compared to the other phases is acceptable as well (Figure 3).

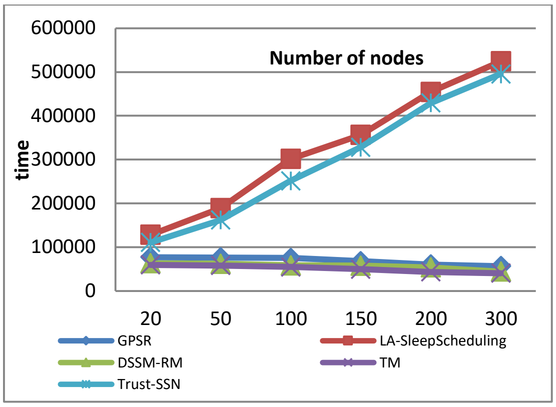

Fig. 3: Comparison of network lifetime in different methods

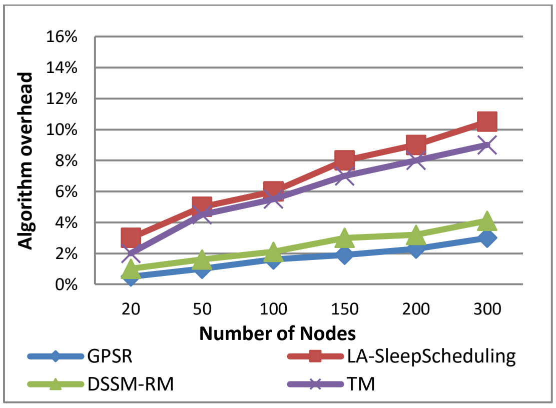

Fig. 4: Comparison of different methods with respect to algorithm overhead

X. Evaluation of semantic information extraction of sensed targets

After the semantic collection of target information from the environment, the target-related information can be extracted through semantic queries. This experiment aims to evaluate the accuracy of semantic information extraction. Therefore, the suggested method would be compared to DSSM-RM (Paul and et al., 2012) (in which the sensor network information is collected semantically and based on the sensors), TM (in which information is selected semantically and based on trust) methods. Recall and Precision variables are considered as the parameters under comparision.

Twenty sparql queries have been designed in order to compare the target-related information extraction through these methods. The results of the comparison considering these two variables are illustrated in Figures 5 and 6.

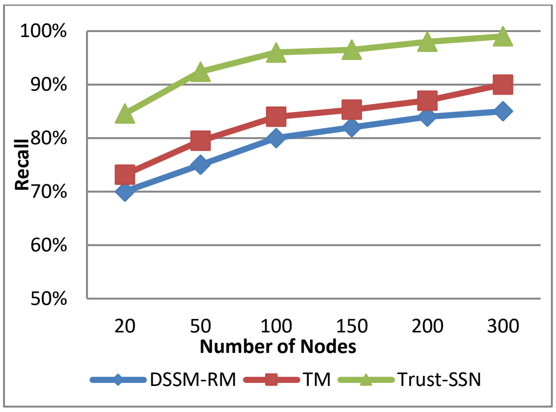

Fig. 5: Comparison of different methods with respect to Recall in query answering

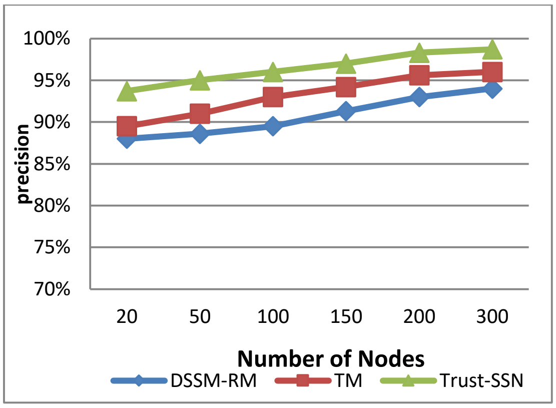

Fig. 6: Comparison of different methods with respect to Precision in query answering

Recall variable confirms the proportion of accurately extracted targets to the total number of targets desired to answer a query. Precision variable indicates the proportion of accurately extracted targets to the total number of extracted targets as the result of the query. In terms of Recall and Precision variables, the suggested method has a better performance compared to DSSN-RM and TM methods.

XI. Evaluation of trust in data gathering

One of the main objectives of the suggested method is to investigate the trust of sensor nodes and consider it as a parameter in data gathering. Two parameters are being considered in order to evaluate the calculation of sensor node trust in different methods: 1) the proportion of the mean trust of effective nodes to the mean trust of all network nodes; 2) the percent of packets that have been accurately received by the sink nodes compared to the total amount of data and packets sensed and sent by the sensor nodes. The suggested method would be compared to GSRM, LA-SleepScheduling, DSSM-RM and TM methods. Figure 7 compares the different methods considering first parameter (the proportion of the mean trust of effective nodes to the mean trust of all network nodes). Considering the different nature of functionality in different methods, the term “effective node” refers to the nodes that perform the main tasks of the network such as sensing or data transmission. Therefore, active nodes, cluster heads, monitor nodes or data transmitters might be considered as the effective nodes in different methods. Due to this parameter, the suggested method is the most desirable one.

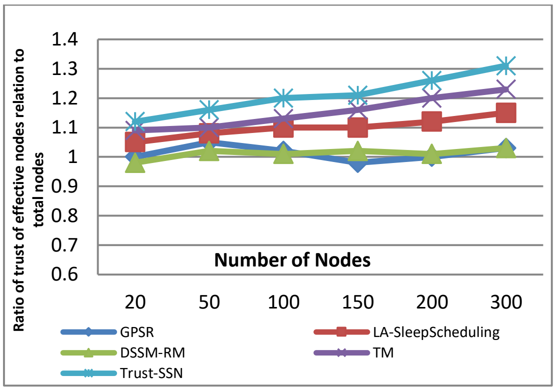

Fig. 7: Comparing the proportion of mean trust of effective nodes to mean trust of the total nodes

Figure 8 compares the different methods considering second parameter (the percent of packets that have been accurately received by the sink nodes compared to the total amount of data and packets sensed and sent by the sensor nodes). The suggested method is the most desirable one even in terms of this parameter.

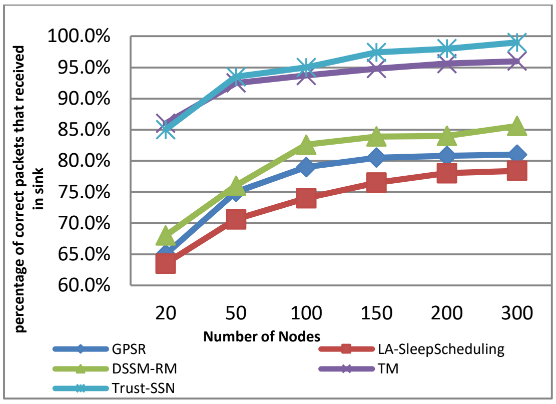

Fig. 8: Comparing the percent of packets accurately received by the sink to the total number of packets

CONCLUSION

Many studies have been performed on data gathering through sensor networks. This paper aims to present a strategy to collect and aggregate information about the targets located in sensor network environment, semanticaly and trust-based. Therefore, it firstly suggests dome strategies through which the sensors that collect data related to a target can decrease the number of sent packets and increase the network lifetime through data aggregation. Through semantic and target-based data collection and using ontology, this paves the way for sensor data reasoning and knowledge extraction. Secondly, a method is presented in aggregation technique in order to identify highly trusted networks and increase their use in collection and aggregation of data about the sensed targets. Thus, the system accuracy and trust would be generally improved. Finally, the suggested strategies were implemented and simulated through related software and simulators. Results confirmed the desirable performance of the suggested strategies.

REFERENCES

1.Ahmadinia M., Alinejad-Rokny H. and Ahangarikiasari H., " Data Aggregation in Wireless Sensor Networks Based on Environmental Similarity: A Learning Automata Approach", Journal of Networks, Vol. 9, No. 10, pp. 2567-2573, 2014.

2.Aivaloglou E. and Gritzalis S., “Hybrid trust and reputation management for sensor networks” Wireless Networks, vol. 16, no. 5, pp. 1493–1510, July 2010.

3.Anantharam P., Henson C., Thirunarayan K., and Sheth A., "Trust model for semantic sensor and social networks: A preliminary report," in Aerospace and Electronics Conference (NAECON), Proceedings of the IEEE 2010 National. IEEE, 2011, pp. 1-5.

4.Bao F., RayChen I., Chang M. and Cho J., &ldquo,”Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection",&rdquo,IEEE Trans. Network and Service Management, vol. 9, no. 2, pp. 169-183, June 2012.

5.Bendadouche R., Roussey C., De Sousa G., Chanet J., Hou K. M., “ Extension of the Semantic Sensor Network Ontology for Wireless Sensor Networks: The Stimulus-WSNnode-Communication Pattern”, In: 5th International Workshop on Semantic Sensor Networks in conjunction with the 11th International Semantic Web Conference (ISWC), Boston (2012).

6.Bermudez L.,” OGC Ocean Science Interoperability Experiment” Phase II Report. OGC Engineering Report Open Geospatial Consortium, 2010.

7.Calbimonte J.-P., Jeung H., Corcho O., and Aberer K., “Enabling query technologies for the semantic sensor web,” Int. J. Semant. Web Inf. Syst.,vol. 8, no. 1, pp. 43–63, Jan. 2012.

8.Calder M., Morris R. A. and Peri F., “Machine reasoning about anomalous sensor data”, In Ecological Informatics 5(1), pp. 9-18, 2010.

9.Compton M. and et al. “The SSN ontology of the W3C semantic sensor network incubator group”, Web Semantics: Science, Services and Agents on the World Wide Web, 2012.

10.Ganeriwal S., Balzano L., and Srivastava M., “Reputation-based framework for high integrity sensor networks,” ACM Trans. Sen. Netw., vol. 4, no. 3, pp. 1–37, May 2008.

11.Goodwin J. C., Russomanno D. J. “Survey of semantic extensions to UDDI: implications for sensor services”, In Proceedings of the International Conference on Semantic Web and Web Services, pp. 16-22, 2007.

12.Ibrahim A., Carrez F. and Moessner K., “Spatio-Temporal Model for Role Assignment in Wireless Sensor Networks”, European Wireless 2013, 16 – 18 April, 2013, Guildford, UK.

13.Karp B. and Kung H., "Greedy perimeter stateless routing for wireless networks", In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000), pp. 243-254, Boston, MA, 2000.

14.Kim D., Cha S., and Cho K., “Ontology-based methodology formanaging heterogeneous wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID610684, 9 pages, 2013.

15.Krasniewski M., Varadharajan P., Rabeler B., Bagchi S., and Hu Y., “TIBFIT: Trust index based fault tolerance for arbitrary data faults in sensor networks,” in Proc. DSN, 2005.

16.Neuhaus H. and Compton M. “The Semantic Sensor Network Ontology: A Generic Language to Describe Sensor Assets.” In AGILE Workshop Challenges in Geospatial Data Harmonisation, 2009.

17.Paul J., Yan Z., Jeung H., Corcho O., Aberer K., "Deriving Semantic Sensor Metadata from RawMeasurements", 5th International Workshop on Semantic Sensor Networks. Boston, 2012.

18.Ren Y., Zadorozhny V. I., Oleshchuk V. A., and Li F. Y., “A novel approach to trust management in unattended wireless sensor networks,” IEEE Transactions on Mobile Computing, vol. 13, no. 7, pp. 1409–1423, 2014.

19.Roda F., Musulin E. “An ontology-based framework to support intelligent data analysis of sensor measurements”, Expert Systems with Applications Journal, 41 , pp. 7914–7926, 2014.

20.Stasch C., Janowicz K., Braring A., Reis I. and Kuhn W. “A Stimulus-Centric Algebraic Approach to Sensors and Observations” In GSN '09: Proceedings of the 3rd International Conference on GeoSensor Networks, pp. 169, 2009.

21.Stevenson G., Knox S., Dobson S. and Nixon P. “Ontonym: a collection of upper ontologies for developing pervasive systems”, In CIAO '09: Proceedings of the 1st Workshop on Context, Information and Ontologies, pp. 1-8, 2009.

22.Wei W. and Barnaghi P. “Semantic annotation and reasoning for sensor data”, In EuroSSC'09: Proceedings of the 4th European conference on Smart sensing and context, pp. 66-76, 2009.

23.Yadav K. and Srinivasan A., “iTrust: An integrated trust framework for wireless sensor networks,” in Proc. ACM SAC, NewYork, NY, USA, 2010.