Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure and Energy Efficient Node Scheduling Protocol for Target Coverage in Wireless Sensor Networks

Shoeb Ahmad, Muzammil Hasan
Department of CSE, Madan Mohan Malaviya University of Technology
Gorakhpur, Uttar Pradesh, India

Abstract— This wireless sensor network is an infrastructure formed by a group of sensing device known as sensor nodes which are randomly deployed in an area. Sensors are low power and low cost device and act as a powerful tool in the area of interest remotely. This property of sensor nodes makes it fit for various important application of monitoring and tracking. Trust is an observation and decision based parameter. In this paper we propose trust as multi-dimensional entity which insure security, reliability and accuracy. Security is one of the key issue, despite various mechanism intrusion is still possible so we utilize trust mechanism for a secure communication and also utilize coverage protocol to increase network lifetime by finding set active nodes.

Keywords— Wireless Sensor Network; Coverage; Scheduling

I. INTRODUCTION

In wireless sensor network numerous sensors are deployed in specific environment which remains unattended for a long period of time. Sensors nodes possess sensing, computation and wireless capabilities. From an intruders prospects both wireless nature as well as resource constraint serve are main reason for attack. Certain approaches which were proposed still undergo several vulnerabilities for example node capture attacks, denial of service (DOS) [1]. Another major problem is absence of energy reserve leads to discharging of sensor nodes as they are energy constrained necessary to maintain energy for effective communication. Architecture of wireless sensor network i.e. flat and hierarchical [2] has shown a need of effective communication where information from every cluster head is needed to be carried out securely. In this paper we consider environmental uncertainties and blended trust mechanism with subjective logic framework. A communication trust and energy trust are calculated along with uncertainty of neighbour as alone communication cannot be a trustworthy factor so energy has to be considered along with the underlying data. A subject logic framework for employing trust and trust is calculated as combination of direct and indirect or recommendation trust [3]. Recommendation is calculated by two factors: recommender nodes familiarity and reliability. The coverage is maximized with set of active nodes. This paper is organized as follows 2 coverage, security problem 3 trust mechanism and factors 4 proposed protocol 5 validation 6 conclusion

II. COVERAGE AND SECURITY IN WIRELESS SENSOR NETWORK

One of the critical problem related to energy efficiency is coverage. [5] Coverage problem is a measure of quality of service. Coverage refers to the monitoring or tracking ability of sensing field. Coverage is classified as follows:
Area coverage: It deals with a particular region being monitored, required that it should be monitored at least by a single node. The sensing region is called as boundary. Distance from node to boundary is called sensing radius.
Target Coverage: In this type of coverage targets are monitored in the area of deployment. This coverage has application in military to maintain target coverage while conserving energy.
A. Barrier Coverage: Detection of movement across barrier of sensors.
B. Sweep coverage [6]: A variation of barrier coverage can be thought as moving barrier problems. Secure communication is one of the necessities in wireless sensor network [6]. Wireless sensor network need to deal with inside as well as outside attack. It has been noticed that even a single malicious node can cause harm during communication. For transferring the data a trusted path is required. In wireless sensor network due to dense deployment in hostile area nodes are force to be less reliable or prone to overtaking by force. There are several malicious attack such as node replication, DOS etc. [1] several method such as cryptography, authentication etc. do not entirely provides secure communication. There are also several attacks in model such as good/bad mouthing attack. If bad then node give high trust value and in good high trust value for malicious nodes so we utilize the concept of trust familiarity and trust reliability so that correct recommendation value is received by nodes.

III. TRUST MECHANISM

Trust is a multi-dimensional entity so it's widely used to sort out numerous problems in wireless sensor network. Trust can also be considered as trustor's belief to rely on trustee.
It is also defined as function of uncertainty. Acc to Mcknight [4] the high level trust can be simplified as way of behaviour that is benevolent, competent and predictable. Trust depends upon the predictable behaviour of nodes [7].

GOALS

- Provide information that allows nodes to distinguish between trustworthy and non-trustworthy.
- Encourage or Discourage nodes to be either trustworthy or untrustworthy.
- Cope up with misbehaviour.
- Minimize damage caused by inside attacks

Properties

- Send and receive feedback about the current action taking place in network.
- Use feedback mechanism regularly to guide trust base decisions.

A. Asymmetric: Trust cannot be asymmetric because if node X trust node Y then it's not necessary that node Y also trust node X.
B.Transitive: Trust can be transitive because if node X trust node Y and node Y trusts Node Z then node X will absolutely trust node Z.
C. Reflexive: Trust can be reflexive. A node is bound to trust itself.
D. Context sensitive: Trust can be context sensitive because if node X trust node Y for task T1, it may not be necessary it also trusts node X for task T2 and T3.

IV. CLASSIFICATION OF TRUST

Trust can be classified in three ways.
A. Observation based: The system directly observes its own experience otherwise utilizes information provided by its neighbours. Here system can make use of neighbour's experiences.
B. Information Symmetry: Information can be symmetric or asymmetric as nodes may or may not have access to the same amount of information.
C. Centralization: It's further classified as;
(a) Centralized: Single entry maintains the reputation of all the nodes lying in a particular range.
(b) Distributed: Each nodes maintains information about other nodes. This information can be global or local. In this type there is a certain problem with consistency of data.

V. TRUST FACTORS (AS OBSERVATION BASED)

There are several trust factors which concludes towards coverage and security in wireless sensor network.
These factors are based on observation one node on another.
A. Direct trust: If subject node can be observe object node then direct trust is established. Due to presence of malicious attack a node cannot totally depend only on direct trust as its not feasible so we need to consider the number of communication to check whether node is normal, the data of particular node and also the residual energy are calculated. Hence direct trust is weighted average of data trust, energy trust and communication trust.
B. Communication trust: Communication trust is basically based on sensor node previous behaviours and often the communication is unstable and noisy which constitutes uncertainty. Hence to deal with uncertainty we use subject logic framework in which trust value is a triplet T= {b, d, u}, where b, d, u Ɛ [0, 1] are belief, disbelief and uncertainty and b+d+u=1. □ and □ represents successful and failed communications. Therefore communication trust is calculated as:

$$T_c = \frac{2b + u}{2}$$

$$b = \frac{\alpha}{a + \beta + 1} \; d = \frac{\beta}{a + \beta + 1} \; and \; u = \frac{1}{a + \beta + 1}$$

C. Data trust: Data trust can affect the trust of network nodes that created and manipulated data. We consider the percentage of current readings. Hence data trust is calculated as

$$T_{Data} = 1 - \frac{N_{err}}{\mathrm{N}}$$

Where N and Nerr are no communication and no of incorrect data readings.
D. Energy trust: Energy is an important metric in wireless sensor network. Nodes are dependent on amount of energy as it helps to distinguish between a normal node and malicious node. For calculation we define energy threshold θ. If Eres > θ the nodes cannot perform a particular task.

$$T_{eng} = \begin{cases} 1 - P_{eng} \;, & if \;\; E_{res} \geq \theta \\ 0 & else \end{cases}$$

Hence the direct trust is calculated as:

$$T_{direct} = \frac{W_1 T_c + W_2 T_{data} + W_3 T_{eng}}{W_1 + W_2 + W_3}$$

Where W1, W2, and W3 are weight values.
E. Recommendation trust: Recommendation is one of the most important factor in wireless sensor network. If there is no direct communication between subject and object node then recommendation is calculated by common neighbour between both the nodes. As there can be false recommendation by a malicious node there by we use to filter recommendation by using recommendation familiarity and recommendation reliability.

a. Recommendation familiarity: If represents the duration for which the subject node is neighbour of object node. If the durationis more, the trust value will be high. It's calculated as follows:

$$T_p = \frac{n}{\mathrm{N}} \times \alpha^{\frac{1}{n}}$$

Where n and N are no of successful communication between recommender R and node Y and total successful communication by recommender node R.

b. Recommendation reliability: If there is any faulty trust value then its filtered using trust reliability. It's computed as follows:

$$T_R = 1 - |\mathrm{T}_{\mathrm{R}}^{\mathrm{Y}} - \mathrm{T}_{\mathrm{AVG}}^{\mathrm{Y}}|$$

Where and represents rec. value of object node Y calculated by recommender and avg. value of all the recommendations.

Hence, Recommendation trust is calculated as follows:

$$T_{REC} = \frac{\sum_{i=1}^{n} 0.5 + (\mathrm{T}_{\mathrm{R}}^{\mathrm{Y}} - 0.5) \times T_F \times T_G}{n}$$

Where n is the number of recommenders.

F. Indirect trust: When subject node cannot observe object node directly and doesn't have common neighbour then we use indirect trust. Finally multi-hop recommenders are searched and trust is propagated to establish direct connection and choose the optimal trust chain by considering trust and distance value. After establishing trust chain all the recommender participate in trust propagation step as this avoids selection of malicious nodes and provides reliability. Indirect trust is calculated as:

$$T^{Y}_{IDR+1} = \begin{cases} \mathrm{T}_{\mathrm{R}+1} \times T^{Y}_{IDR} & if\ \mathrm{T}_{\mathrm{IDR}}^{\mathrm{Y}} < 0.5 \\ 0.5 + (T_{R+1} - 0.5) \times \mathrm{T}_{\mathrm{IDR}}^{\mathrm{Y}} & else \end{cases}$$

VI. TRUST VALUE UPDATION

The trust value is updated periodically as wireless sensor network are dynamic in nature and in order to avoid the wastage of energy it's updated as certain period not regularly. Previous trust values are needed to be considered as it provides the duration. If duration is long the value it doesn't reflect behaviour so sliding window concept is used to calculate updated value as follows:

$$T(i+1)_{new} = w_i T(i) + w_{i+1}\ T(i+1)$$

Where $w_{i\ and}\ w_{i+1}$ are weight values of previous and current values w_i= □ and w_{i+1} = □+1; T (i+1) represent trust value at $i^{th}$and $(i+1)^{th}$time slot.

VII. COMPONENT OF TRUST (AS DECISION MAKING)

For decision making it is important to follow some important points:

Information gathering- In this process, nodes keep information about those nodes which they want to keep. It is purely based on observation and experiences.

Information sharing- This component is concerned with dissemination of the information gathered by observation. In this component the information is also considered which is gathered by neighbour but this component makes system vulnerable. For sharing three factors are needed to be considered i.e. dissemination frequency, dissemination locality and dissemination content.

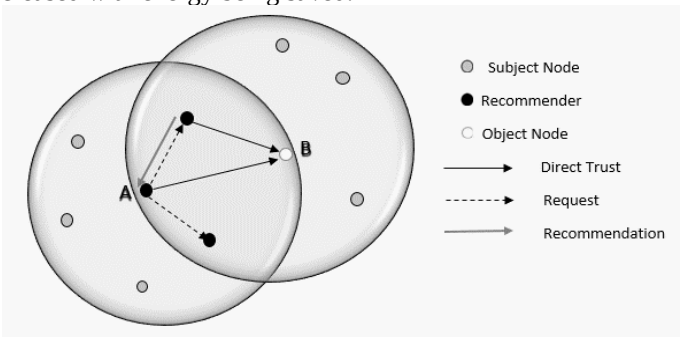
Information modelling- This component deals with the observation and neighbour information into a single metric. This metric is maintained and updated.

Information making- This component deals with taking decision which node to trust or not to trust. It is based upon the information given by the component information modelling. The decision tree can vary according to the trust value.

Hence trust can act as a decision making factor based on certain parameters such as security, energy etc.

VIII. PROPOSED MODEL

A sensor network is considered [1] which consist of n sensor nodes S= {s_1, s_2, …….s_n} and m target nodes T= {t_1, t_2……..t_n} In this protocol the objective function is to minimize sensor node in active state. As the few number of nodes are active so the data packets can be easily sent and received without information being lost and less the malicious node. The coverage can be increased with energy being saved.



Some assumptions of the protocol are:
A multi-hop network is considered. Sensor nodes are deployed in a rectangular field with the dimension m×n.
The coverage and sensing field are considered in a circle with radius r.
Initially all the nodes have same energy. They can alter on any among three modes active, observer and sleep. Two thresholds are considered as 0.2 and 0.5. If all nodes active network lifetime is 1 else depends on no of active node.

$$Mode = \begin{cases} active & if\ cov(i,j) \geq 0.5 \\ observer & if\ 0.2 \leq cov(i,j) < 0.5 \\ sleep & if\ cov(i,j) < 0.2 \end{cases}$$

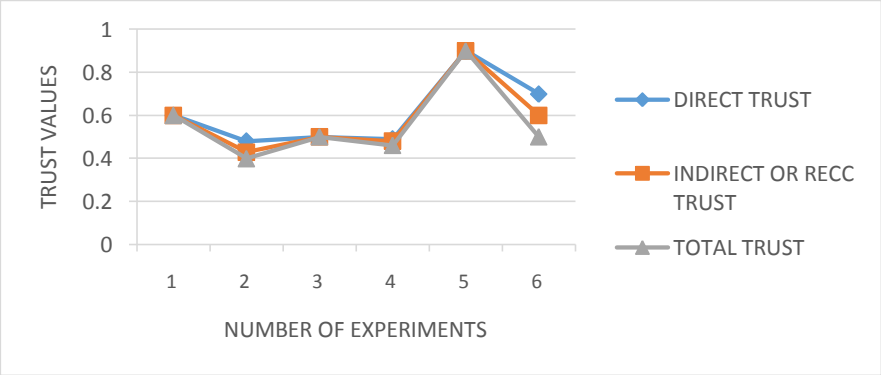
The following models are used to compute and solve coverage problems:
1. Probabilistic coverage model- Represents relation between target region and sensor node as follows:

$$Cov(i,j) = \begin{cases} 0 & if\ r_s + r \leq d(S_j, T_i) \\ e^{-\lambda a^{\beta}}\ observer & if\ r, -r < d(S_j, T_i) \leq r_s, +r_e \\ 1 & if\ r, -r \geq d(S_j, T_i) \end{cases}$$

2. State markov model represents good and faulty nodes.
3. Trust model represents trust between subject and object node.
The following steps describe working of trust model:
Step 1: The first step is SETUP in which base station gathers trust information of all the nodes. These information consist of node ID, key and address etc.
Step 2: The second step is SENSING PARAMETERS in which nodes sense the environment parameter according to the schedule of base station. Base station checks for all the active nodes based on trust value and coverage probability.
Step 3: The third step is DATA TRANSMISSION in which sensed data is reflected back to base station. For reliable transmission of data aggregator nodes are used selected on the basis of residual energy and link for active set.

IX. VALIDATION

According to our assumption we have considered a network of randomly deployed nodes in a rectangular field of 100 various parameters used in this network are:
1. Sensing range of sensor nodes
r_s = 22cm and detection error range r_e = 12cm.
2. Threshold value is 0.49 and trust value is calculated for a secure communication by utilizing trust factor. Every trust factor is calculated individually by varying certain parameters such as number of successful and unsuccessful communication and residual energy is considered of node.
Hence we calculated direct, indirect or recommendation trust.



The result of various experiments have been shown in above figure represents the no of nodes, direct trust, indirect trust and recommendation trust also TA^s the trust increases, more secure communication between nodes. It ranges from 0.4 and 0.9 with the nodes having trust 0.4 have moderate trust and one with 0.9 have high trust on nodes. Here the nodes are observed based on trust value and considering several parameters decision is taken by nodes.
Now according to our protocol, various sensor are ranging from 20-80 are varied with fixed target ranging are considered to carry our experiment.
The coverage quality with respect to distance is calculated as

$$Cov(i,j) = \begin{cases} 0 & if\ d \geq 22 \\ 0.7 & if\ 12 < d \leq 22 \\ 1 & if\ d \leq 10 \end{cases}$$

Here d is the distance between sensor node and target node. From the above obtained trust value we calculated the probability of node which determines ability of node to monitor target region as:

The node with maximum and optimized set covers O are generated from general set cover of nodes monitoring all the targets G_i. Where G_i represents the set of target covered and i is the node covering the targets. Following experiments are conducted and efficiency is calculated:

Experiment 1: In this experiment we have considered sensor node S=20 and target node T=10. The general set are as follows:

G_4 ={3,7}, G_5 ={3,7}, G_6 ={6,10} G_7 ={1,3,5,8}, G_8 ={1,3,5} G_9 ={2,9}

The optimized set derived from general set are as follows:

O_1 = {4, 13, 14, 19}, O_2 = {5, 13, 14, 19}, O_3 = {4, 13, 18, 19}, O_4 = {5, 13, 18, 19}

*Experiment 2:*In this experiment we have considered sensor node S=20 and target node T=10. The general set are as follows:

G_3 ={4,7}, G_4 ={5,7}, G_5 ={1,7} G_9 ={6,8,10}, G_0 ={1,8} G_3 ={7,8}G_4 ={1,4 5 9}, G_7 ={1,10}, G_8 ={1,4}

G_2 ={3,7,9,10}, G_3 ={1,2,4,7}, G_9 ={1,3,7} G_9={4,7,8,9,10}, G_3 ={4,10} G_5 ={2,5}

The optimized set derived from general set are as follows:

O_1 = {9, 14, 22}, O_2 = {9, 14, 29, 36}, O_3 = {9, 18, 22, 36}, O_4 = {9, 29, 30, 36}

Experiment 3: In this experiment we have considered sensor node S=20 and target node T=10. The general set are as follows:

G_4 ={2,4}, G_5 ={4,6,8}, G_7 ={1,7,8} G_8 ={2,4}, G_6 ={1,7} G_8 ={3,5}

G_2 ={3,6}, G_2 ={2,9}, G_3 ={3,8} G_3 ={8,9,10}, G_4 ={9,10} G_0 ={1,8} G_5 ={2,10} G_5 ={2,7}

The optimized set derived from general set are as follows:

O_1 = {5, 7, 18, 22, 53}, O_2 = {5, 7, 18, 43, 57}, O_3 = {5, 18, 35, 50, 57}, O_4 = {5, 16, 18, 22, 53}

X. CONCLUSIONS

This paper focuses on the study of an energy efficient node scheduling protocol for target coverage in wireless sensor network, we proposed a protocol for wireless sensor network which is divided into three steps. In first step, base station gathers trust information of all the nodes, in second step, node sense the environment parameter according to the schedule of base station and in third step sensed data is reflected back to base station. The proposed energy efficient coverage protocol enhance the network lifetime and reliability of data transmission to the base station.

ACKNOWLEDGMENT

I have completed my research paper with the support of my parents, teacher and my friends. I would like to thank Dr. U C. Jaiswal for his support and encouragement. I would like to thank my guide (mentor) for his complete guidance and support.

REFERENCES

[1] Jinfangjiang, Guangjie Han, Fang wang, Lei Shu, Mohsen Guizani, An effective trust model for Wireless Sensor Networks, IEEE Transaction on Parallel and Distributed System, 2014.

[2] Ado Adamou ABBA ARI 1 Abdelhalk SUEROUI, Nabila LABRAOUI and Blaise Omer YENKE, CONCEPTS AND EVALUATION OF RESEARCH IN THE FIELD OF WIRELESS SENSOR NETWORKS.

[3] International Journal of Computer Networks and Communications (IJCNC) Vol. 7, No.1 January 2015 DOI : 10.5121/ijcnc.2015.7106 81

[4] AvinashSrinivasany, Joshua Teitelbaumy, HuigangLiangz, JieWuyandMihaelaCardeiy, "Reputation and trust based system for an adhoc and sensor networks".

[5] D. H. Mcknight, N. L. Cherv "The Meanings of Trust" 96-04 MISRC Working Paper Series, University of Minesota, Management Information Systems Research Center, 1996.

[6] SANGEETHA S, RAMA LAKHMI K, "A Survey on Coverage Problem in Wireless Sensor Networks" International Journal of Advance Research in Computer Engineering and Technology (IJARCET) Volume 1, Issue 10, December 2012.

[7] Byers, J., and Nasser, G., "Utility- based decision making in wireless sensor networks", Proc of the 1st ACM International Symposium on Mobile Ad-Hoc Networking and Computing, November 2000, Boston, Massachusetts.

[8] Y. B. Reddy and RastkoSelmic., "Secure Packet Transfer in Wireless Sensor Networks – A Trust Based Approach", IARIA-ICN 2011, January 23-28, 2011 – St. Maarten.

