Trust Based Path Selection for Mobile Agent Migration in Wireless Sensor Networks

[1]Dr.K.Sangeetha, [2]K.Renuga Gayathri
[1]Assistant Professor, [2]PG Scholar
Department of Computer Science and Engineering,
Kongu Engineering College, Perundurai, India

***Abstract*— Data aggregation is the process of collecting and aggregating the useful data. End-to-end data aggregation, without degrading sensing accuracy, is a very relevant issue in wireless sensor networks (WSN) that can prevent network congestion to occur. Recently, mobile agents have been used for aggregation due to their efficient utilization of network bandwidth and energy. Most of the mobile agent based schemes use static pre-planned route for agent's migration. The issue with static route based agent migration is that an agent may not move along its route due to node failures or malicious node attacks. The proposed system uses dynamic route which offers more flexibility to find a way around node or link failures. When sensor nodes are compromised by the attacker, the attacker gets access to security keys and reprograms the sensor nodes to spoil the execution of an agent. Thus in order to provide an efficient solution to overcome these attacks, proposed system uses trustworthiness of nodes to be used to identify and bypass the malicious or compromised nodes. The performance is evaluated using NS2 simulator.**

***Index Terms*—Wireless sensor networks, sector, trust, wedges.**

I. INTRODUCTION

A mobile agent is a software abstraction that can migrate across the network (hence mobile) representingusers in various tasks (hence agents). Each agent is typically composed of the agent code, the agent execution thread along with an execution stack, and the agent data part, which corresponds to the values of the agent's global variables. The efficiency and effectiveness of the mobile agent based data aggregation depends on the agent's migration path. The problem with the static route based agent migration approach is that the agent may not move along its path due to node or link failures. However, dynamic approach offers extra flexibility to find a way around node or link failures.

When sensor nodes are compromised by the attacker, the attacker gets access to security keys and reprograms the sensor nodes to severely spoil the execution of an agent. In order to prevent such attacks, basic cryptographic mechanisms are not sufficient. Thus in order to provide an efficient solution to overcome these attacks, trustworthiness of nodes should be used to identify and bypass the malicious or compromised nodes. In proposed method two techniques are involved. They are

1. Trust evaluation framework has been developed to evaluate trust worthiness of sensor nodes. Trustworthiness of node is used to identify the malicious or compromised sensor nodes.
2. TEBM- Trust and Energy Based Migration Algorithm has been developed. With the TEBM algorithm, malicious nodes can be detected early and are bypassed during agent's migration.

II. RELATED WORK

Capra and Musolesi [1] proposed the notion of human trust which could be formed from three sources: direct experiences, credentials and recommendations. In particular, recommendations are trust information coming from other nodes in the social context. Only two sources are considered in calculating trust value namely, direct experiences and recommendations, since it is hard for SNs with limited resources to carry credentials.

Chen et al [2] proposed Multi-agent Itinerary Planning (MIP) algorithm. MIP is also centralized algorithm executed at the sink and performs grouping of deployed sensor nodes into different subgroups. In each subgroup, a single mobile agent based algorithm like LCF, GCF or GA is used to compute mobile agent itineraries.

Haiyun et al [3] proposed that infrastructureless networks rarely have a real defense mechanism against most of the attacks, including both outsider and insider attacks such as compromised node attacks. The suggested system design is like this – if one node is named trusted by certain number of its neighbouring nodes, that particular node is trusted locally and globally. However, since the system uses a minimum number of trusted nodes it is not so applicable to sensor networks where the nodes are randomly spread out.

Konstantopoulos et al [4] proposed a tree based itinerary design (TBID) algorithm. TBID is a centralized algorithm which is executed at the sink node and computes number of mobile agents to be used for data gathering and their itineraries. This algorithm assumes that the sink knows the geographic location of all sensor nodes. TBID uses greedy techniques for grouping sensor nodes and designs near optimal itineraries to explore them.

Qi et al [8] proposed two heuristic algorithms, Local Closest First (LCF) and Global Closest First (GCF), for the itinerary planning. In LCF, an agent starts its migration from the sink and looks for the next node with the shortest distance to the current node as its next destination. In GCF, each agent begins its migration from the sink and looks for the next sensor node with the shortest distance to the centre of deployment area as its next destination. The effectiveness of LCF depends on current location of the agent.

Shakshuki et al [9] proposed a software agent based directed diffusion protocol where the mobile agent visits only the subset of sensor nodes. The first phase of the directed diffusion protocol is used for determining a subset of sensor nodes. Mobile agents are dispatched by the sink for data gathering from this subset of sensor nodes.

III. SYSTEM MODEL

Wireless sensor network consists of a large number of low cost sensor nodes, uniformly distributed in a monitoring field. All sensor nodes are static and have same computation, communication and sensing capabilities.

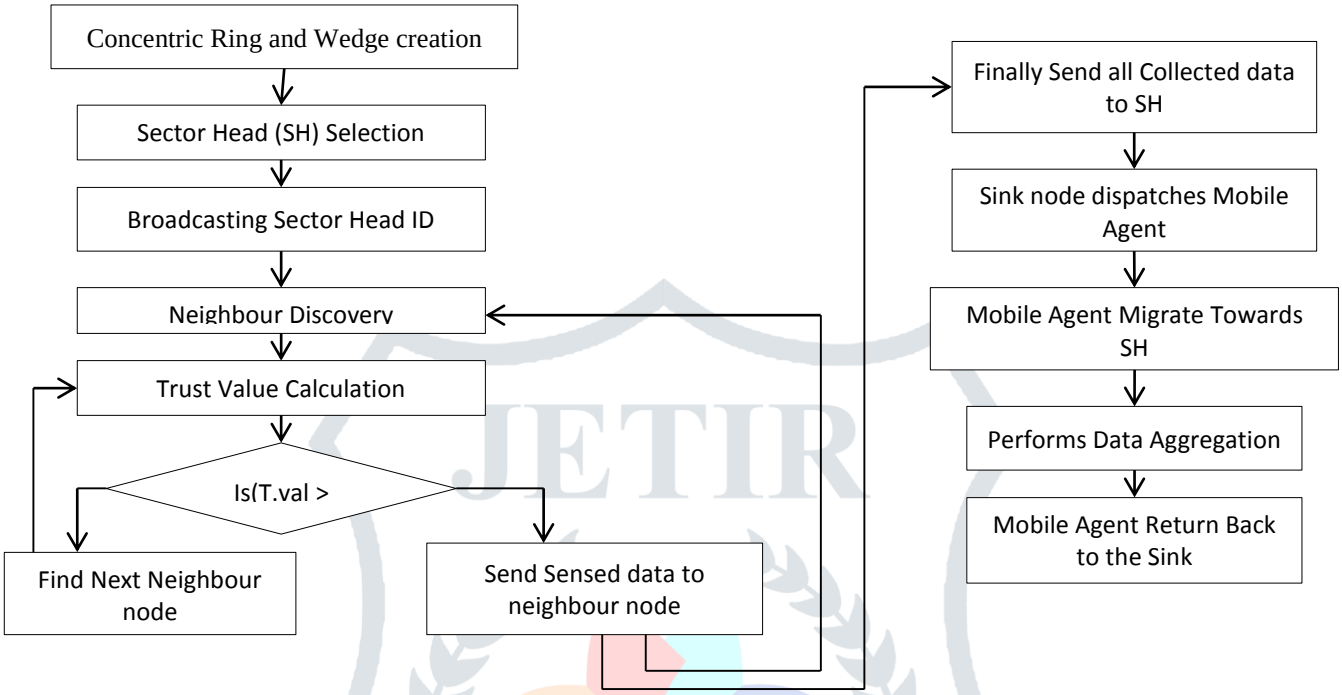

Figure 1. Flow Graph of Agent Migration

There is only one sink node placed at the centre of the monitoring area. The sink node is equipped with a steerable beam directional antenna with transmission power control capability. The sink node uses steerable beam directional antenna for creation of concentric rings and equiangular wedges. Concentric ring is the circular region of width r2-r1 between two concentric circles of radius r1 and r2 centred at the sink where r1<r2 and a wedge is an angular region centred at the sink. It is assumed that sink node is a powerful and trusted data collection device.Each node is assigned a unique identifier (ID). Here sink node is most powerful and trusted data collection and that every sensor node is equipped with trust manager component (TMC) which stores node's trust value.

IV. PROPOSED METHODOLOGY

A. TRUST VALUE CALCULATION

In order to identify and bypass malicious or compromised nodes, each node evaluates the trust value of its neighbors locally. Direct trust value depends on the local monitoring results of neighbour's behaviours such as dropping, misrouting, delaying, replaying or modifying packets. Indirect trust values are computed from peer recommendations. Peer recommendations are trust values reported by the neighbour nodes that have had previous interaction with the nodes for which recommendation is requested.

Calculating direct trust value,

$$T_{direct} = 100 \times \frac{\text{Number of successful forwarding of packets}}{\text{Number of packets forwarding}} \quad (1)$$

Calculating indirect trust value,

$$T_{indirect} = \frac{\text{Sum of trust values from peers recommendations}}{\text{Total number of neighbors reported trust value}} \quad (2)$$

The trust value is considered to be an unsigned integer in [0,100], where 0 represents the most untrusted state while 100 represent the most trusted state. Using final trust value, each sensor node can select the most trusted neighbour node to forward mobile agents.

B. TRUST AND ENERGY BASED MIGRATION ALGORITHM

Trust Based Mobile Agent Migration (TEBM) algorithm is used for data aggregation in WSNs. The basic idea of TEBM algorithm is to identify and bypass the faulty or malicious nodes during mobile agent migration process.Here the sink node dispatches the mobile agents for data aggregation. The mobile agent migration depends on the trust value of each node

CONCENTRIC RING AND WEDGE CREATION

In concentric ring creation phase, the sink node divides the whole circular monitoring area into concentric rings. Each node in a concentric ring can communicate with only nodes in the previous, within the current and nodes in the next ring. At the end of this phase each node knows its ring number.

In wedge creation phase, the sink node divides the whole circular monitoring area into angular wedge region. The number of angular wedge is equal to number of nodes in first concentric ring.

SECTOR HEAD SELECTION

In Sector Head (SH) selection, node with maximum remaining energy is selected as Sector Head in each sector. Sector Head ID is broadcasted to all other nodes within same sector.

NEIGHBOUR DISCOVERY

In neighbor discovery, each node broadcasts a HELLO packet to its one hop neighbors. The node receiving the HELLO packet compares the ring and wedge number to identify whether the neighbor node is in previous, current or next ring.

AGENT MIGRATION

In agent migration, the sink node dispatches mobile agents concurrently to the Sector Head (SH) nodes of each wedge region for data aggregation and collection. Each agent has the following four basic local operations executed :

- AgentVisitSH()
- AggregateData()
- updateAgentBriefcase()
- Migrate()

When a mobile agent arrives at any Sector Head for data fusion/aggregation, it requests different services to middleware to accomplish its task at the node and these services are provided by middleware system to the mobile agents. When an agent visits a SH, it executes AggregateData() to perform the data aggregation of the sensed data at the visited node with the data carried by the agent. After data aggregation, updateAgentBriefcase() function executes to update agent's brief-case (i.e. data area) by the aggregated data. Then, an agent calls Migrate() function to decide the next SH to move on. These operations are executed at each visited SH.. After traversing the SH of each sector region, agent returns back to the sink with all aggregated data.

V. EXPERIMENTAL SETUP

The hardware required for the experiment are Intel Core i5 processor, 4 GB RAM and 20 GB hard disk drive. The like software required are Fedora 14 Operating System, NS2 simulator tool for running simulation and the language used is TCL and C++. The parameters used for simulation is listed below.

Table 1 Experimental Setup

Parameters	Specifications
Simulation Area (m × m)	700 × 700
No. of Sensor Nodes	25 – 100
No. of Sink Node	1
Transmission Range of each node	25m
Simulation Time	300 seconds
Antenna Type	Omni Directional
Radio Propagation Model	Two Ray

VI. PERFORMANCE EVALUATION

The following are the parameters considered for the performance evaluation of network in the presence of malicious nodes during agent migration for data aggregation.

Energy Consumption per Round

It is defined as the amount of energy consumed per one round of data aggregation.

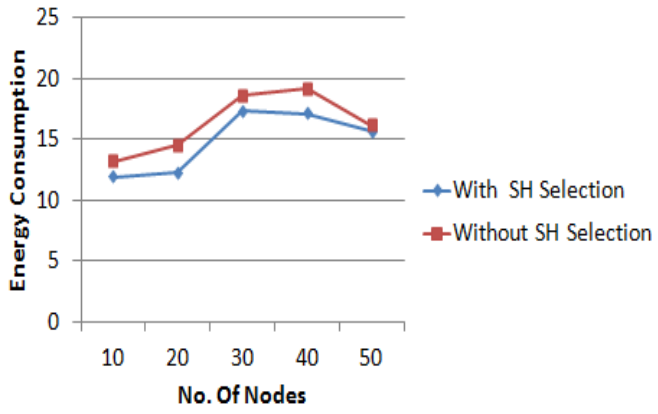

Figure 2. Energy Consumption

Packet Delivery Ratio

It is defined as the ratio of total number of packets received to the total number of packets sent by the node.

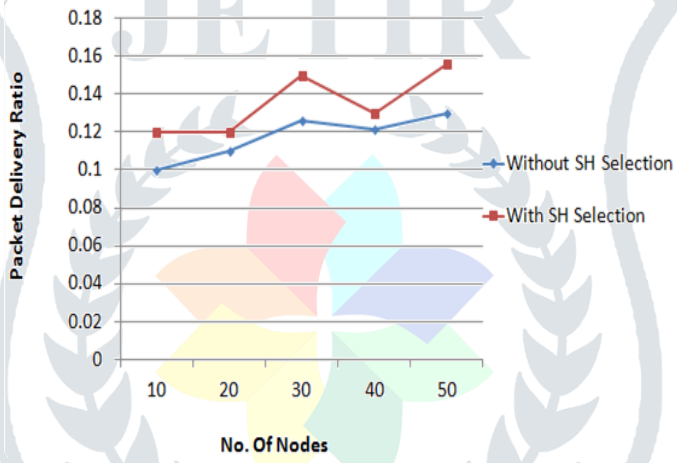

Figure 3. Packet Delivery Ratio

VII. CONCLUSION

Trust and Energy Based Migration (TEBM) algorithm has presented an integrated solution for reliable agent migration within network. In TEBM, energy and trust are both considered for forwarding the sensed data to the neighbour node. In addition, TEBM uses sector head selection features to reduce the itinerary length of the agent.

REFERENCES

[1] Capra L and Musolesi M., (2006), 'Autonomic Trust Prediction for Pervasive Systems,' International Conference on Advanced Information Networking and Applications, Vol. 2, No.6, pp. 1-5.

[2] Chen M., Cai W., Gonzalez and Leung VCM (2010a), 'Balanced Itinerary Planning for Multiple Mobile Agents in Wireless Sensor Networks', Ad Hoc Network, Vol. 6, No. 12, pp. 416-428.

[3] Chen M., Gonzalez-Valenzuela S and Leung V (2010b), 'Directional Source Grouping for Multi- agent Itinerary Planning in Wireless Sensor Networks', IEEE International Conference on Information and Communication Technology Convergence, Vol. 6, No. 12, pp. 207-212.

[4] HaiyunLuo, PetrosZerfos, Jiejun Kong, Songwu Lu and Lixia Zhang (2002), 'Self Securing Adhoc Wireless Sensor Network', IEEE Symposium on Computer and Communication, Vol. 2, No. 3, pp. 473-481.

[5] Konstantopoulos C., Mpitziopoulos A., Gavalas D and Pantziou G (2010), 'Effective Determination of Mobile Agent Itineraries for Data Aggregation on Sensor Networks', IEEE Transaction on Knowledge Data Engineering, Vol. 22, No. 12, pp. 1679-1693.

[6] Marchang N and Datta R (2012), 'Light-Weight Trust-Based Routing Protocol for Mobile Ad hoc Networks', IET Information Security, Vol. 2, No. 6, pp. 77–83.

[7] Ozdemir S (2007), 'Secure and Reliable Data Aggregation for Wireless Sensor Networks', 4th National Conference on Ubiquitous Computing System, Vol. 4836, No. 4, pp. 102-109.

[8] Qi H and Wang F (2001), 'Optimal Itinerary Analysis For Mobile Agents In Adhoc Wireless Sensor Networks', Proceedings of 13th International Conference on Wireless Communications, Vol. 1, No. 11, pp. 147-153.
[9] Shakshuki E., Malik H and Denko M (2008), 'Software Agent-Based Directed Diffusion in Wireless Sensor Network', Telecommunication System, Vol. 38, No. 3-4, pp. 161-174.
[10] Wu Q., Rao NSV., Barhen J., Iyenger S., Vaishnavi VK and Qi H (2004), 'On Computing Mobile Agent Routes for Data Fusion in Distributed Sensor Networks', IEEE Transaction Knowledge Data Engineering, Vol. 16, No. 6, pp. 740-753.