Journal of Network and Computer Applications 41 (2014) 300–311

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks

Govind P. Gupta [a,*], Manoj Misra [a], Kumkum Garg [b]

[a] Department of Computer Science & Engineering, Indian Institute of Technology, Roorkee 247667, India
[b] Dean, Faculty of Engineering, Manipal University Jaipur, Jaipur 302026, Rajasthan, India

ARTICLE INFO

Article history:
Received 14 December 2012
Received in revised form
16 October 2013
Accepted 14 January 2014
Available online 6 February 2014

Keywords:
Wireless sensor networks
Mobile agents
Trust
Itinerary design
Security
Migration algorithm

ABSTRACT

Recently, the use of mobile agents in wireless sensor networks (WSNs) has emerged as the topic of extensive research due to their efficient utilization of network bandwidth and energy, and flexibility of their use for different WSN applications. Most of the proposed mobile agent based schemes use static itineraries for agents' migration that are computed at the sink using a centralized algorithm. These centralized algorithms require global knowledge of sensor distribution, which is difficult to obtain accurately. Other issue with static itinerary based agent migration is that an agent may not move along its itinerary due to node failures or malicious node attacks. In order to solve these issues, we first propose a framework for trust evaluation to identify the malicious behavior of sensor nodes and then give a localized distributed protocol, called energy and trust aware mobile agent migration (ETMAM) protocol for periodic data gathering application. The results of our simulation study show that the ETMAM protocol is effective in improving resilience against node failures or malicious nodes attacks.

1. Introduction

Recently, mobile agents computing paradigm has been advocated in the context of wireless sensor networks (Chen et al., 2007, 2010a, 2010b, 2011; Shakshuki et al., 2008; Konstantopoulos et al., 2010). A mobile agent is an autonomous software agent that migrates among nodes, following a certain itinerary and carries out data aggregation locally at each sensor node (Chen et al., 2007). The efficiency and effectiveness of the mobile agent based data aggregation depends on the agent's migration path (i.e. itinerary). In the literature, two types of approaches are proposed to decide the itineraries of the agent: dynamic and static. In dynamic approach (Chen et al., 2007), itinerary of an agent is decided at run time, while in static approach, the sink node computes itineraries before agents are dispatched for data aggregation. The problem with the static itinerary based agent migration approach is that it incurs significant additional cost in periodic collection of network topology information at the sink and an agent may not move along its itinerary due to node or link failures. However, dynamic approach offers extra flexibility to find a way around node or link failures (Konstantopoulos et al., 2010; Xu and Qi, 2008). Another benefit with the dynamic approach is that the size of the agent packet is much smaller than the static approach because an agent does not carry a pre-computed itinerary list.

Besides energy efficient agent migration another critical issue is the protection of mobile agent against malicious, or compromised nodes. In mobile agent based WSNs, each sensor node provides an execution environment for the mobile agent. When sensor nodes are compromised by a malicious adversary, the malicious adversary gets access to security keys and reprograms the sensor nodes to severely spoil the execution of an agent by corrupting or modifying its code or state information, denying agent service requests, simply not executing the agent's processing code or even terminating the agent without notification (Jansen, 2000; Varadharajan et al., 1998). In order to prevent such attacks, basic cryptography mechanisms such as symmetric key based authentication and integrity protection alone are not sufficient, because compromise nodes know secret keys and behave as a legitimate node (Karlof and Wagner, 2003; Chen et al., 2009). The use of computation-intensive cryptography mechanisms such as public-key cryptography involves considerable storage and computation overheads. Thus it cannot be employed in WSNs because sensor node has limited resources such as battery power, memory, computation, and communication capabilities. 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 during the agent's migration within network. This can protect mobile agents from malicious nodes.

* Corresponding author.
E-mail addresses: gpg.india@gmail.com, gpgupta@outlook.com (G.P. Gupta).

http://dx.doi.org/10.1016/j.jnca.2014.01.003
1084-8045

Taking the aforementioned issues into consideration, we propose a dynamic, distributed scheme called energy and trust aware mobile agent migration (ETMAM) which combines energy and trust as selection criteria to build routes on the fly for the traveling agent to complete the data aggregation tasks. The main technical contributions of this paper are

(1) First, we propose a trust evaluation framework for mobile agent based WSNs to evaluate the trustworthiness of sensor nodes. Trustworthiness of node is used to identify the malicious or compromised sensor nodes. To the best of our knowledge, this is the first work for mobile agent based WSNs.
(2) Second, we propose a novel dynamic and distributed protocol, ETMAM for energy and trust aware agent migration. ETMAM not only provides reliable migration paths for the traveling agents but also uses cloning mechanism to optimize agent migration path and reduces agent's payload. With the ETMAM protocol, faulty or malicious nodes can be detected early and are bypassed during agents' migration.
(3) We evaluate the proposed protocol ETMAM, by comparing it with the state of art protocols using Castalia3.2 (Boulis, 2011) WSN simulator. The simulation results show that ETMAM is more efficient and effective in the presence of faulty and malicious nodes. In particular, ETMAM improves success rate of the agents' round trip and reduces energy consumption as well as overall response time.

The remainder of this paper is structured as follows: Section 2 reviews related work. In Section 3, we present the network model and assumptions. Next we present the framework for trust evaluation in Section 4, followed by our proposed ETMAM protocol in Section 5. The simulation setup and performance analysis are presented in Section 6. We conclude the paper in Section 7 with some suggestions for future work.

2. Related work

In recent years, extensive studies have been conducted on mobile agent based data aggregation in WSNs. Much research effort has been dedicated to efficient itinerary planning for agent migration and several schemes have been proposed (Shakshuki et al., 2008; Konstantopoulos et al., 2010; Chen et al., 2010a, 2010b, 2011; Xu and Qi 2008; Qi and Wang, 2001; Wu et al., 2004). One of the first solutions for the mobile agent migration problem has been proposed in (Qi and Wang, 2001), where Qi et al. in year 2001 described 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 center of deployment area as its next destination. The effectiveness of LCF depends on current location of the agent. Wu et al. (2004)) have proposed a genetic algorithm (GA) based approach for computing the itinerary of an agent. It uses global knowledge of network topology to design a static itinerary for the agent. This gives better performance than LCF and GCF protocols in terms of energy consumption. The protocols proposed in Qi and Wang (2001) and Wu et al. (2004) employ single agent to visit all sensor nodes and their performance is adequate for small network; however, it declines as the network size grows.

Shakshuki et al. (2008) proposed a software agent based directed diffusion protocol where the mobile agent visits only a subset of sensor nodes. The first phase of directed diffusion (Intanagonwiwat et al., 2003) 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. The mobile agent itinerary is determined by sink but authors have not given the procedure. Chen et al. (2010a, 2010b) 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.

Konstantopoulos et al. (2010) 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.

Chen et al. (2010) proposed a centralized algorithm called directional source grouping based multi-agent itinerary planning (DSG-MIP). The algorithm executes at sink and statically determines the number of mobile agents and their itineraries. The main idea of this algorithm is to divide the network area into sector zones and the center of each sector zone is the immediate neighbor node of sink node. In each sector zone, itinerary of mobile agent may be determined by using any single agent itinerary planning algorithm.

The survey of multiple mobile agent based itinerary planning is remarkably reviewed in Wang et al. (2011) with their merits and demerits. Most of these proposed algorithms are centralized and executed at sink node to derive static itineraries. Three limitations are associated with these algorithms. The first limitation is that the additional communication overhead is involved to get up-to-date global network topology information to design itineraries for mobile agents. The second limitation is that a mobile agent may not move along its itinerary due to nodes or links failures. The third limitation is that none of the above protocols consider security issues. They only focus on how to decide efficient itineraries for mobile agents. A malicious or compromised node can disrupt the operations of mobile agent by modifying its code, state, or itinerary, denying requested services or terminating it absolutely (Lin and Varadharajan, 2010; Ching et al., 2005). To overcome these challenges, we propose a dynamic and distributed algorithm for mobile agent migration, where malicious or compromised nodes are detected at an early stage and bypassed during migration.

3. Network model and assumptions

We consider a wireless sensor network similar to (Konstantopoulos et al., 2010; Karlof and Wagner, 2003; Rachuri and Murthy, 2010) that consists of a large number of low-cost sensor nodes, uniformly distributed in a monitoring field of radius R. It is shown in Fig. 1. All sensor nodes are static and have same computation, communication and sensing capabilities. There is only one sink node placed at the center of the monitoring area. Each sensor node is aware of its own location coordinate either by low power GPS device or using any localization algorithm (Capkun et al., 2002; Mao et al., 2007; Yun et al., 2009) which is similar to assumption used in Rachuri and Murthy (2009, 2010). Since the sensor nodes are stationary, assigning location coordinate to each sensor nodes is a onetime task and it is part of network setup phase.

We assume that the sink node is equipped with a steerable beam directional antenna with transmission power control capability as used in Liu et al. (2011a, 2011b) and Mao and Hou (2007). The sink node uses steerable beam directional antenna for creation of concentric rings and equiangular wedges (Olariu et al., 2004)