Pervasive and Mobile Computing 44 (2018) 58–73

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs

Manjula R. *, Raja Datta

Department of Electronics and Electrical Communication Engineering , Indian Institute of Technology, Kharagpur 721302, India

ARTICLE INFO

Article history:
Received 18 September 2017
Received in revised form 25 December 2017
Accepted 14 January 2018
Available online 6 February 2018

Keywords:
Local adversary
Network lifetime
Source location privacy
Wireless Sensor Networks

ABSTRACT

In this paper, we propose a two-phase routing technique using multiple virtual sources to provide enhanced source location privacy in Wireless Sensor Networks (WSNs). We use the concept of *escape-angle* and *random walks* that is based on potential energy. The proposed method routes packets to the base station via different virtual sources located at various positions in the network. The key idea of this work is to exploit the excess energy available in the non-hotspot areas of the network to generate dispersive routes between source node and the virtual sources. This approach maximizes *safety-period* without hampering the network lifetime. We present mathematical models to estimate the overall energy expenditure that incurs at each node during Min Hop Routing phase (phase two). We then determine the remaining amount of energy which could be used for Stochastic and Diffusive Routing phase (phase one). Simulation results show that the proposed technique achieves improved safety-period without hampering the network lifetime.

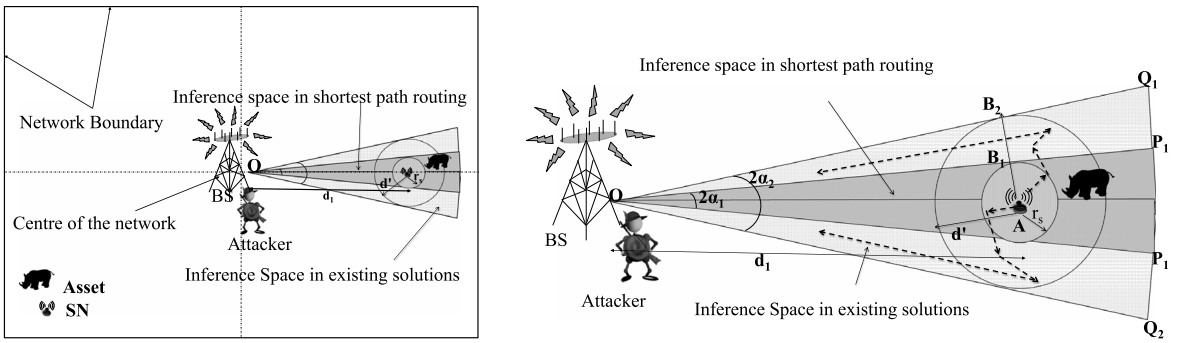
1. Introduction

Source location privacy (SLP) in Wireless Sensor Networks (WSNs) has gained importance in the recent past. One of the promising and most challenging applications of WSNs, besides environmental monitoring [1], smart grids, health care and smart homes, is asset/event monitoring in unattended and hostile environments [2]. The main challenge stems from the inherent characteristics of sensor nodes such as limited energy resources and their open nature of wireless communication links. These features of sensor nodes pave the way to a plethora of security and privacy issues such as packet interception, DoS attacks, fake packet injection, etc. We find several habitat and environmental monitoring applications with WSNs in the literature [2,3]. Several measures have been taken by various non-profit organizations across the globe to protect the wildlife. WSNs are deployed in the natural habitats to monitor the endangered animals like Panda, Rhinos, Tigers [4,5], etc. The purpose of these networks is to collect the event information such as locations, movements, health status of these animals (interchangeably, we call them as assets in our work) and report the event information to the Base Station (BS), also known as *Sink*. The hunter (adversary) exploits the wireless nature of the communication links to eavesdrop on the message flows so as to backtrack the communication path with the aim of poaching these assets [6,7].

Phantom routing schemes are widely recognized as one of the effective routing strategies to preserve the source location privacy in WSNs [8]. Source location privacy protection deal with hiding the physical location of the source of the event and make it difficult for the adversary to backtrack the origin of information. In phantom routing techniques [6,7,9,10], the source node randomly selects one of its neighbors and forwards a packet to it. On receiving the packet, the neighbor decrements the hop count H by one and then relays it to another randomly chosen neighbor. The node at which the hop count H

* Corresponding author.
E-mail addresses: rajamanjula@ece.iitkgp.ernet.in (Manjula R.), rajadatta@ece.iitkgp.ernet.in (R. Datta).

https://doi.org/10.1016/j.pmcj.2018.01.006
1574-1192/



(a) As seen from the center of the network.

(b) Zoomed version.

Fig. 1. Inference space.

(of the packet) becomes zero is termed as the virtual source or phantom source. The phantom source now acts as a decoy node and forwards the data packets to the base station using a shortest path routing technique. In Fig. 1 we present a scenario that depicts working of existing phantom routing techniques [6,7,9,10]. Figs. 1(a) and 1(b) shows the network scenario in which the BS is situated at the center of the network and an asset under observation is detected by the sensor node (having the radio range r_s units) that is at a distance d_1 units from the BS. Fig. 1(b) shows the zoomed version with more details. After the packet is randomly relayed for H number of hops, the random walk terminates within the circular region having the radius d' units. The dotted arrow lines in Fig. 1(b) shows the routing paths taken by the packets in these techniques. It may be observed that all the routing paths between the phantom nodes and the BS gets concentrated within the conic section Q_1OQ_2. Therefore, an adversary positioned at the BS can receive majority of the packets arriving at the BS and it can easily backtrack to the source of the information. Therefore we see that in these type of routing techniques the random walk tends to stay around the real source of the event as shown in Fig. 1(a). Also, the authors in [7] and [11] have shown that the probability of a phantom source to be present within 20% of H hops from the source is $1 - e^{-H/25}$. As the number of hops (H) increases, the probability tends to one. Therefore, H is preferably chosen to be of smaller value and is often set to 10 [7]. Hence, these schemes suffer from insufficient privacy preservation level.

Chen et al. in [12] proposed a forward random walk (FRW) method in which every node in the network divides its neighbors into three groups: (i) *closer neighbor set* containing only those nodes which are one hop closer towards the BS than the node itself, (ii) *farther neighbor set* containing those nodes which are one hop farther away from the node of interest and (iii) *equivalent set* containing those neighbors whose *depth* is same as that of the node of interest (*depth* is the number of hops a node is away from the base station). Here the source node randomly chooses one of the neighbors from the closer set and forwards the information packet to it. The process is repeated at each intermediate node till the packet reaches the base station. This technique also suffers from weaker privacy level. This is because the adversary's backtracking time is smaller compared to that of the phantom single path routing technique (PSPR) [7] as the random walk is biased towards the base station. In the literature there are several other papers based on the random walk scheme [9,10,13] which suffer from similar problems.

It may be noted that in all these techniques the level of source location privacy, usually measured in terms of *safety period*, increases as the distance between the source node and the base station (BS) increase. The *safety period* here is defined as the number of messages sent to the base station before the adversary reaches the origin of information (i.e., the source node). One straight-forward solution to improve the *safety period* (i.e., the privacy level) is to have a network-wide routing technique. This technique would make the adversary difficult in making predictions regarding the direction of the origin of the traffic and thus lead to increased backtracking period. Admittedly, such a solution would lead to high energy consumption due to longer and network-wide routes from the source to the BS. As a result, the researchers are challenged with the contradictory objectives of achieving the higher level of privacy without hampering the network lifetime. In this paper we try to address these issues with the help of a new stochastic routing technique.

Typically, applications involving multi-source and single destination paradigm suffer from reduced network lifetime due to uneven distribution of the traffic load among the nodes in the network. In particular, the sensor nodes within the base station's radio range carry all the traffic load arriving from the nodes that are far away from it. Similarly, nodes in the hotspot (high traffic) regions also expend more energy in transmitting the event information to the BS. As a result, the nodes lying far away from the BS and those lying in the non-hotspot regions of the network have approximately 90% of the energy remaining when the first node in the network dies [14]. Further, the routing paths in these techniques [5–7,12,13,10] are not dispersive in nature, i.e., despite using phantom routing techniques, each packet's path from the source node is confined to a small geographical region between the source and the BS. The repeated usage of the same paths leads to a phenomenon called *hotspot* and this, in turn, leads to energy hole problems in the network. Problems such as network partitioning, non-coverage areas, etc. also pop up due to this, which makes routing infeasible and reduces the network lifetime.