Ad Hoc Networks 47 (2016) 16–25

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Energy efficient fuzzy adaptive selection of verification nodes in wireless sensor networks

Muhammad Akram, Tae Ho Cho*

College of Information and Communication Engineering, Sungkyunkwan University, Suwon 16419, Republic of Korea

ARTICLE INFO

Article history:
Received 15 July 2015
Revised 5 April 2016
Accepted 25 April 2016
Available online 26 April 2016

Key terms:
WSNs
Fuzzy
Energy

ABSTRACT

In Wireless Sensor Networks, sensor nodes are highly vulnerable to several security attacks because they are usually installed in hostile environments. These energy and hardware–resource-constrained nodes, without suitable safeguards, may be compromised by adversaries. Adversaries launch two major types of attacks: false-report injection and false-vote injection attacks via these compromised nodes. These attacks drain significant amounts of energy and drop valid reports. PVFS[1] by F. Li et al. [1] counters these two major attacks. One of the reasons to launch false-report injection attack is to drain the energy resource of the entire network to render it unresponsive. We propose Fuzzy-based adaptive selection of the intermediate verification nodes in PVFS to achieve optimal energy savings. We demonstrate that our proposed method achieves better energy conservation in the presence of both the aforementioned security threats while providing the same high filtering control of the PVFS.

1. Introduction

Wireless sensor networks (WSNs) are an economically viable solution with an extraordinary ability to regularly monitor random events in the physical world and to manipulate them with the help of tiny resource-constrained nodes that are densely deployed in a variety of environments often hostile in nature [2,4,12,13]. WSNs tend to have a significant impact on efforts to improve the efficiency of military and civil applications including battle field surveillance, and disaster and security management [7,16]. Energy constraint is one of the serious challenges in WSNs. Some energy efficiency schemes have to be developed to increase lifetime of the network [2]. Several cryptography-based security methods can provide the resilience equivalent to that of others, however, their energy consumption behaviors are quite varying from one another [8]. There are several attacks that can happen to WSNs. Two attacks that are of a major concern are False Vote Injection Attack (FVIA) and False Report Injection Attack (FRIA) [6,8]. In FVIA, one or more nodes cast a false vote on a legitimate report after an event is detected. These false votes are appended to the report and the report is forwarded along a designated path towards the sink. There is a chance that the report may be filtered out at an intermediate verification node immediately after the number of verified false votes reaches its predetermined threshold value. This attack leads to denial of service. FVIA may also cause some consumption of the finite energy resources of the sensor network by resending reports to the sink until sink acknowledges its receipt. In FRIA, a false report is fabricated by a collection of colluding nodes within the cluster. The compromised nodes cast false votes on the fabricated report and the report is forwarded to the sink. The propagation of such false reports greatly contributes to the rapid depletion of the energy resources of the intermediate verification nodes [9].

PVFS exploits a voting mechanism in conjunction with cluster-based organization and probabilistic selection of intermediate verification nodes and key assignment [1]. Although the probabilistic key assignment mechanism in PVFS aims to save energy, it does not take into account the dynamics of the network during observation and use them in the selection of the intermediate verification nodes in order to conserve more energy.

We propose Fuzzy rule-based selection of intermediate verification nodes. Our scheme helps to improve the verification node proximity to the event reporting cluster (referred to as the original cluster hereafter) in order to save energy. While choosing closer intermediate verification nodes, it considers the attack ratio and the energy consumption for selection of the verification nodes. The contribution of this paper is as follows:

i. We propose a fuzzy rule-based intermediate node selection method that aims to achieve higher energy saving as compared to that achieved by PVFS.
ii. Our method considers three important factors as input parameters while choosing verification nodes during observation:

* Corresponding author. Tel: +82 312907221.
E-mail addresses: akram.khan@skku.edu (M. Akram), thcho@skku.edu (T.H. Cho).

[1] Probabilistic voting-based filtering scheme

http://dx.doi.org/10.1016/j.adhoc.2016.04.010
1570-8705/

a. The residual energy level
b. Compromise attack attempts.
c. Proximity of individual verification nodes to the original cluster.

The decision making process takes place in the original cluster to

a. Substitute intermediate verification nodes
b. Exclude upstream cluster heads from considering as verification nodes in the future

We analyze our proposed method and present simulation results that show that our proposed method achieves significant energy saving in the presence of increasing security attacks and considerably increases the network lifetime.

The rest of this paper is organized as follows. In Section 2, we provide a background overview of the PVFS algorithm and the motivation for our research. We present our proposed method in Section 3, followed by the simulation results in Section 4, related works in Section 5 and a conclusion in Section 6.

2. Background and motivation

The aforementioned two attacks pose serious security threats to all WSN and FRIA also causes rapid depletion of the limited energy resources in networks [1]. In the forthcoming section, we concisely describe the operation of the PVFS in WSNs to counter these two attacks. We also discuss the motivation behind our proposed work.

2.1. PVFS

PVFS uses a voting method for the authentication of real reports. It exploits cluster-based orientation in combination with a probabilistic key assignment method. PVFS considers the cluster-based model because of its natural suitability for filtering mechanisms. WSNs are broken into clusters, each of which has L nodes, and a set of keys is attached to each cluster. CHs are elected and their one-hop neighbors join to form clusters. It assumes that the formation of clusters, distribution of keys and discovery of routes takes place soon after sensor deployment and that no nodes are compromised. Intermediate cluster heads are chosen as verification nodes using a designed probability method with the cluster head which is responsible for reporting the event. During the route discovery phase, every cluster head gets the IDs of all the intermediate CHs in the upstream between original cluster and the base station (BS), their distance to the BS in hop-count and its own distance to the BS. The original CH selects intermediate CHs as verification nodes using the probability p, which is given by:

$$p = d_i/d_o. \tag{1}$$

Where

d_i = distance between CH_i and the BS.
d_o = distance between the original CH and the BS.

The original CH notifies one of the nodes in the cluster to securely exchange its generation key with one of the selected verification nodes using the session key created through pairwise key establishment protocols. Each CH also shares another symmetric key with the BS which is used to generate the verification signature. A report is not immediately dropped after a verification node finds a false vote attached to it; instead the result of the current verification is recorded and the report is forwarded along the path. The report will only be dropped when the number of verified false votes reaches a predetermined threshold.

2.2. Motivation for the proposed method

After having identified FVIA and FRIA as two major attacks in WSNs, it is necessary to devise an energy-efficient scheme to improve the energy saving and increase the life-time of sensor networks while simultaneously providing maximum safeguards against two types of attacks [5,10]. PVFS counters these two attacks using a general en-route filtering framework as its basis and probabilistically selects intermediate verification nodes using the probability given by Eq. (1).

Li et al. propose that the probabilistic selection of intermediate verification nodes ensures early verification and dropping of fabricated reports which leads to significant energy conservation in WSNs [1]. However, static security threshold selection in PVFS renders it not ideal for deployment in an environment with dynamic characteristics in which there are clusters with different statuses such as the number of nodes in the cluster and the assignment of keys [3,4,6]. In addition, PVFS is not adaptive with respect to the frequency of the attacks and the energy status of nodes involved in the verification. PVFS does not use back check key and drop report acknowledgment.

Sensor nodes conserve battery power to prolong network lifetime. Two common reasons of energy consumption in WSNs are communication and verification of reports. Energy consumed during transmission is directly proportional to the distance between the source and the recipient, as given by Eq. (2).

$$E_{Tx} = E_{elec(k)} + \varepsilon_{amp} \times k \times d^{\alpha}, \tag{2}$$

Where k is the size of data, d is the distance between the source and the recipient, $E_{elec(k)}$ is the energy consumed to run the radio electronic and ε_{amp} is the energy consumed to amplify the signal. α is 2 for the free-space. Therefore it is very important to detect and drop false report at the early stage to save energy. We propose a Fuzzy logic-based adaptive selection of verification nodes that saves the energy resources of the verification nodes. Our proposed method tries to improve the proximity of the intermediate verification nodes to the original cluster to ensure earlier dropping of false reports than is possible in the original PVFS.

3. Fuzzy adaptive selection of verification nodes

In this section, we present a detailed description of our proposed method.

3.1. Assumptions

We consider a large-scale dense wireless sensor network with a cluster-based orientation. We assume that the nodes do not move after the initial deployment and remain stationary. The cluster-based hierarchical model is best for multi-hop communication and facilitates a general en-route filtering mechanism [1]. The sensing rang of all sensor nodes is greater than their transmission range and every CH has longer transmission range than the ordinary nodes in the network [1,8].

Predetermined node IDs are assigned to all nodes before network deployment, and the nodes with the smallest node IDs are elected as CHs in their respective clusters [1]. For simplicity, we assume that the cluster formation, distribution of keys and discovery of routes take place immediately after sensor deployment when no nodes have been compromised. Only two types of attacks i.e. FRIA and FVIA, can happen to the sensor network. Consideration of all other possible attacks is beyond the scope of this paper.

3.2. Threat model

In our work, we assume that the intensity of the attack increases with the time as more and more nodes are getting