ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

A New Secure Geographical Routing Protocol Based on Location Pairwise Keys in Wireless Sensor Networks

[I]B.Tharika, [II]A.R.Jothimani
[I]M.Phil Scholar, [II]M.Phil Scholar
[I,II]Dept. of Computer Science, KG College of Arts and Science, Coimbatore – 35.

Abstract
Geographical and Energy Aware Routing (GEAR) is an effective routing protocol in wireless sensor networks (WSN). It performs well in the face of routing attacks, but it is incompetent of defending bogus routing information, sybil attack and selective forwarding. Directed at this problem, this paper present a location pairwise keys bootstrap scheme based secure geographical and energy aware routing protocol (SGEAR). SGEAR adapted to WSN rather suceessfully. Subsequently we give the performance analyses of SGEAR. Our performance analyses illustrate that our scheme is efficient to defend above-mentioned attacks.

I. Introduction

Wireless sensor networks (WSNs) are composed of a huge number of densely deployed sensors. A significant feature of such networks is that their nodes are unattended. Consequently, energy efficiency is a vital design consideration for these networks. Routing technology is the basic technology of the wireless sensor network communication layer. Geographic and Energy Aware Routing (GEAR) algorithm uses energy aware and geographically informed neighbor selection heuristics to route a packet towards the target region. Within a region, it uses a recursive geographic forwarding technique to disseminate the packet. The simulation results show that GEAR exhibits markedly longer network lifetime than non-energy-aware geographic routing algorithms.

In recent years, secure routing of WSNs has become a popular research focus. Several techniques were propositioned recently to address secure routing in wireless sensor networks, including the feedback information based secure routing protocol, the Location based secure routing protocol, the cryptographic algorithms based secure routing protocol and other routing protocols. In order to improve the Security of GEAR, this paper presents a SGEAR(Secure Geographic and Energy Aware Routing) secure routing protocol, a innovative pairwise key pre-distribution schemes to tackle the security for static sensor networks. These techniques are based on the observation that in static sensor networks, although it is difficult to accurately pinpoint sensors' positions, it is often possible to approximately determine their locations. For example, when we use trucks to deploy static sensors, we can normally place sensors within a certain distance (e.g.,100yards) from their target locations, though it is difficult to place the sensors in their expected locations precisely.

This paper emphases on the modeling and design of secure routing protocol to find a new research idea. By taking benefit of this observation, our techniques are efficient to defend bogus routing information, sybil attack and selective forwarding attacks.

II. GEAR Routing Protocol and Security Analysis of GEAR

Disseminating information to a geographic region is a very useful basic in many location-aware systems, and specifically sensor networks. An efficient way to disseminate the geographic query to a specified region is to leverage the location knowledge in the query and to route the query directly to the region instead of flooding it everywhere. GEAR is an improved algorithm of Directed diffusion. The latter is a data- centric protocol for sensor network applications. It accomplishes some level of energy savings by selecting empirically good paths, and by caching and processing data in-network. However, without proposed geographic routing support, there is initial and periodic interest and low rate data flooding throughout the network. GEAR protocol can compliment this work by effectively routing interest to the destination region, thus conserving more energy.

A. GEAR Routing Protocol Overview

GEAR algorithm practices energy aware and geographically informed neighbor selection heuristics to route a packet towards the target region. It uses a recursive geographic forwarding method to disseminate the packet, within a region. The main notion of GEAR is using the location information. The process of forwarding a packet to all the nodes in the target region involves two phases:

1. Forwarding the packets towards the target region:

There are two cases to contemplate:

(a) When a closer neighbor to the destination exists: GEAR chooses a next-hop node among all neighbors that are nearer to the destination.

(b) When all neighbors are further away: In this case, there is a hole. GEAR algorithm picks a next-hop node that reduces some cost value of this neighbor

2. Disseminating the packet within the region:

GEAR algorithm practicess a Recursive Geographic Forwarding algorithm to disseminate the packet within the region under most conditions. Recursive geographic forwarding sometimes does not terminate in some low density conditions and routes uselessly around an empty target region before the packet's hop-count surpasses some bound. In these cases, GEAR algorithm proposes to use restricted flooding.

B. Security Analysis of GEAR

The security threats of sensor network routing protocol comprise of bogus routing information, selective forwarding, Sinkhole attacks, Sybil attacks, Wormholes attacks, and HELLO flood attacks. The security defense capability of the GEAR routing protocol against the above attacks are examined below.

1. Bogus routing information

Since the path of the GEAR protocol establishing process from sink node makes use of greedy algorithm, GEAR routing protocol can't resist this attack. the attacker can forge their own positions and energy information, causing the routing to be not ideal.

2. Selective forwarding

As long as malicious nodes exist, there may be selective forwarding. Malicious nodes can discard the received packets. Most of the proposed routing protocol can not resist such attacks, GEAR routing is no exception

3. Sinkhole attacks

In a sinkhole attack, the adversary's intention is to lure almost all the traffic from a specific area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. This facilitates many prospects to tamper with the application data, thereby enabling many other attacks. Since the routing selection relate to location information in the GEAR routing protocol, the attacker need to declare their own position and thus the protocol is able to endure such an attack.

4. Sybil attacks

In a Sybil attack, a single node presents multiple identities to other nodes in the network. by using the Sybil attack an adversary can "be in more than one place at once" thus posing significant threat to GEAR routing protocols.

5. Wormholes attacks

Wormholes attacks involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. Since we can know whether the two nodes are neighbours through their location GEAR routing can defy the attack.

6. HELLO flood attacks

Many protocols necessitate nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. A laptop-class attacker could convince every node in the network that the adversary is its direct neighbor. In GEAR node neighbor relationship can be guessed through the location information thus defending it.

III. Secure Geographical and Energy Aware Routing protocol (SGEAR)

Given below is the description of SGEAR algorithm, which ensures that the sensor network is secure.

A. Location Pairwise Keys Based Safety Bootstrap Scheme

The security bootstrap refers to the process for a sensor network to form a network with solid security outer protection gradually from a pile of scattered nodes without safe passages protection through some shared knowledge and agreement. The core issue of secure bootstrap is the establishment of security key process. It is usually assumed that the key pre-distribution model completes almost all of the establishment of the security infrastructure before deployment. So only a simple protocol is used for consultations after the deployment process, thus making it suitable for the sensor network security guide.

A primary security service is the establishment of a symmetric, pairwise key shared between two sensors, which is the core of other security services such as encryption and authentication. Key pre-distribution model primarily contains the pre-shared key model and the random key pre-distribution model. SPINS uses a pre-shared key model. Its implementation is simple and has a high success rate but the drawback is the over-reliance on the base station and the inability to resist the DoS attack in multi-hop network environment.

B. Design of the SGEAR Security Routing Protocol

For the use of position information the node deployment needs a setup server. To predistribute pairwise keys the setup server randomly generates a bivariate t-degree polynomial f(x,y) over a finite field Fq where q is a prime number which is large enough to accommodate a cryptographic key, such that it has a property of f(x,y)=f(y,x). It is assumed that each sensor has a unique ID. For each sensor i, the setup server computes a polynomial share of f(x,y), f(i,y). For any two sensor nodes i and j, node i can compute the common key f(i,j) by evaluating f(i,y) at point j, and node j can compute the same key f(j,i) = f(i,j) by evaluating f(j,y) at point i.

In this approach, the target field is partitioned into small areas called cells, each of which is associated with a unique random bivariate polynomial. For simplicity, we assume the target field is a rectangle area that can be partitioned into equal-sized squares $\{C_{ir,ic}\}_{ir=0,1,...,R-1, ic=0,1,...,C-1}$, each of which is a cell with the coordinate (i_r, i_c) denoting row i_r and column i_c. For convenience, we use s = R ×C to denote the total number of cells. The setup server randomly generates s bivariate t-degree polynomials $\{f_{ir,ic}(x,y)\}_{ir=0,1,...,R-1, ic=0,1,...,C-1}$, and assigns $f_{ir,ic}(x,y)$ to cell $C_{ir,ic}$. For each sensor, the setup server first determines its home cell, in which the sensor is expected to locate. It then discovers four cells adjacent to the sensor's home cell. Conclusively, the setup server distributes to the sensor its home cell coordinate and the polynomial shares of the polynomials for its home cell and the four selected cells. For example, in Figure 1, sensor u is expected to be deployed in cell $C_{2,2}$. Obviously, cell $C_{2,2}$ is its home cell, and cell $C_{1,2}$, $C_{2,1}$, $C_{2,3}$ and $C_{3,2}$ are the four cells adjacent to its home cell. Thus, the setup server gives this sensor the coordinate (2,2) and the polynomial shares $f_{2,2}(u,y), f_{1,2}(u,y), f_{2,1}(u,y), f_{2,3}(u,y), f_{3,2}(u,y)$.The key idea of the SGEAR secure routing protocol is a combination location-based pairwise keys bootstrap scheme and location-based routing protocol GEAR, and using the multi-path makes the protocol can resist more routing attack type.

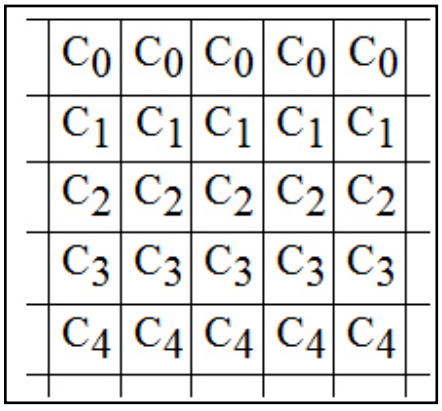

Fig. 1 : Partition of a target field

1. Notation

We use the ensuing notation to describe the security protocols and cryptographic operations in this paper.

a) A, B are principals, such as communicating nodes pos_A

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

denotes Position information of the node A

b) $M1 \mid M2$ denotes the concatenation of messages and maintain order

c) K_{AB} denotes the secret (symmetric) key which is shared between A and B

d) $\{M\}K_{AB}$ is the encryption of message M with the symmetric key shared by A and B

e) $\{M\}(K_{AB}, IV)$ denotes the encryption of message M, with key K_{AB}, and the initialization vector IV which is used in encryption modes such as cipher-block chaining (CBC), output feedback mode (OFB), or counter mode (CTR).

2. Adjacent Nodes Exchange Position and Energy Information

In GEAR routing protocol, each node is awre of their location and residual energy information. A simple exchange mechanism enables the node to obtain the location and energy information of its neighbor node. To ensure the security of the message the nodes need share keys.

Direct Key Establishment. If two sensors want to setup a pairwise key after deployment,they identification of a shared bivariate polynomial is necessary. If at least one such polynomial could be found, a common pairwise key can be established directly using the basic polynomial- based key pre-distribution

Indirect Key Establishment. If two neighbor sensors u and v do not share a pre-distributed pairwise key after deployment, an intermediate neighbor sensor may be found that shares pairwise keys with both of them to help establish a session key. Basically, either of these two sensors may broadcast a request message with their IDs. After establishing a pairwise key between adjacent nodes, the location and energy information of the neighbor nodes could be obtained through a simple exchange mechanism.

IV. Performance Analysis of SGEAR Protocol

In this section, a detailed analysis of the security and the overheads of SGEAR is discussed..

A.Security Analysis The Sybil Attack

Location confirmation is an effective method to resist sybil attacks. A location pairwise keys bootstrap scheme based on the location and polynomial is used by the SGEAR security routing. Since the node authentication key is related to location, and the polynomial share in the node is related to node ID, a node which wants to declare multiple identities must have polynomial share of the location, to get through the authentication.

Bogus routing information. The nodes can not arbitrarily declare a false location since its location information is related to pairwise key inorder to get certified.

Selective Forwarding. Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over n paths whose nodes are completely disjoint are protected against selective forwarding attacks involving at most n compromised nodes and still offer some probabilistic protection when over n nodes are compromised. The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information

B. Overheads Analysis

Conclusively we examine the overheads of security mechanisms. Almost all the overheads will result from the extra transmissions required by the protocols. In Key pre- distribution stage, each sensor needs to store the coordinate of its home cell and the polynomial shares of five cells. The storage overhead for the coordinate of its home cell is trivial. Thus, each sensor has to allocate $5(t + 1)\log q$ memory space to store the secret. When there are compromised sensors, each non- compromised sensor also needs to store the IDs of the compromised sensors with which it shares at least one polynomial. However, for each of the 5 polynomials, a non-compromised sensor only needs to store up to t IDs; it can remove the corresponding polynomial share and all the related IDs if the number of compromised sensors with which it shares the polynomial exceeds t. To create a common key between two neighbor nodes, the communication overhead includes sending a request message and a reply message. To compute the common key with a given sensor, each sensor node needs to evaluate a t-degree polynomial. Thus, the computational cost in each sensor mainly comes from the evaluation of this polynomial, which requires t modular multiplication and t modular addition

V. Conclusion

The contribution of this paper is three-fold. Initially, we present the detailed security analysis of GEAR routing protocol for sensor networks. Then, we propose a new secure geographical routing protocol based on a location pairwise keys bootstrap scheme. Finally, we present a analysis of the security and the overheads of SGEAR, that elucidates those novel designs can obtain a higher security in the smaller system overhead. SGEAR is suitable for wireless sensor network.