ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Data Relay Against Hotspot-Locating Attack in Wireless Sensor Networks Using Mobile Elements

T.Uma Maheswari, K.Ravikumar, Dr.ArokyRaju

Graduate Student, Department of CSE, Rrase College of Engineering, Chennai, India.

Professor, Department of CSE, Rrase College of Engineering, Chennai, India.

Professor &Principal, Department of CSE,Rrase College of Engineering,Chennai,India.

ABSTRACT: In network traffic pattern due to a large volume of packets originating from a small area. Develop a realistic adversary model, assuming that the adversary can monitor the network traffic in multiple area. Introducing a novel attack called Hotspot-Locating where the adversary uses traffic analysis techniques to locate hotspots. The mobile nodes which change their location to better characterize the sensing area, or to forward data from the source nodes to the sink. Using low-cost disposable mobile relays to reduce the total energy consumption of data intensive WSNs. Due to the limited storage capacity of sensor nodes, most data must be transmitted to the base station for archiving and analysis. However, sensor nodes must operate on limited power supplies such as batteries or small solar panels.

KEYWORDS: Hotspot-Locating Attack, Adversary Models,Mobile Elements,Wireless Sensor Networks.

I. INTRODUCTION

A wireless sensor network (WSN) consists of a large number of sensing devices called sensor nodes. They are interconnected through wireless links to perform distributed sensing tasks. When a sensor node detects a soldier or an endangered animal, it reports the event to the data collector called the *Sink*.

This data transmission may occur via multi-hop transmission, where the sensor nodes act as routers. However, WSNs are usually deployed in open and large areas that are unattended and lack of protected physical boundary, which makes the networks vulnerable to security threats. The privacy threats can usually be classified into: *content privacy* and *contextual privacy*. For the content *privacy* threat, the adversary attempts to observe the content of the packets sent in the network to learn the sensed data and the identities and locations of the source nodes. This privacy threat can be countered by encrypting the packets' contents and using pseudonyms instead of the real identities.

II. RELATED WORK

In [2] author location privacy in wireless and wired networks has gained more and more attention. Different schemes have been developed to protect users' privacy in location tracking systems which determine the users'positions for location-based services. Location privacy in these schemes is content-oriented where location information is collected and protected as the users' private data. In [3] author Onion routing provides anonymous communication for the Internet by hiding the identities of the end users of a communication session. The proposed schemes conceal the nodes' network/MAC addresses in order to achieve anonymous communications for mobile ad hoc networks. However, these schemes employ different network and threat models from the ones suitable for the source location-privacy problem in sensor networks. In [4] author fake packet injection to preserve the location privacy of the *Sink*. The scheme makes it hard for an adversary to deduce the sink by making the directions of both incoming and outgoing traffic at each node uniformly distributed. Deng et al. propose a scheme for preserving the *Sink*'s location

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

privacy against traffic-rate analysis attacks. Each node has to send packets at a constant rate and the transmissions of the packets are randomly delayed to hide the traffic pattern and the parent-child relationship. In [5] author Wang et al present a privacy-aware parallel routing scheme to maximize the time of back tracing the packets to the source nodes. A weighted random stride routing that breaks the entire routing into strides is proposed. In [20],dynamically selected nodes in each route modify the packets to make back tracing packets to the source node difficult, but the adversary can trace the modified packets if there are only one or few transmissions.. In [6] author Shao et al. propose a statistically strong source privacy preserving scheme. The nodes send the real packets as soon stronger privacy protection than *routing-based* schemes because in addition to varying traffic routes, it can conceal the traffic analysis information. Our scheme also requires much less energy than *global-adversary-based* schemes.

III. PROPOSED ALGORITHM

A. *Design Consideration:*

Mobile Relay:

The network consists of mobile relay nodes along with static base station and data sources. Relay nodes do not transport data; instead, they move to different locations to decrease the transmission costs. We use the mobile relay approach in this work. Goldenberg et al. showed that an iterative mobility algorithm where each relay node moves to the midpoint of its neighbors converges on the optimal solution for a single routing path. However, they do not account for the cost of moving the relay nodes. In mobile nodes decide to move only when moving is beneficial, but the only position considered is the midpoint of neighbors.

Node Assumption:

Aim of the proposed algorithm is to use low-cost disposable mobile relays to reduce the total energy consumption of data intensive WSNs.

Every node has two local certificate repositories (LR1 and LR2) and stores acquired certificates in the repositories. All nodes share the same secure hash function Hash (), digital signature generation Sign () and verification SignVer () functions. Each node has its own public/private key pairs. Every node has an identifier (ID).

B. Description of proposed Algorithm:

Step 1: *Ciphertext-Policy, Attribute-Based Encryption:*

1) u $\longrightarrow$ v:$ID_u|pub_u$;

2) v $\longrightarrow$ u:$ID_v|pub_v$;

3) u: verify ID_v and derive r_v =Hash($ID_v|pub_v$);

v: verify ID_u and derive r_u =Hash($ID_u|pub_u$);

4) u $\longrightarrow$ v:бu = sign (IDu\ IDv, prv u);

5) v $\longrightarrow$ u:бv = sign (IDv\ IDu, prv v);

6) u: check sign ver (Idv\ Idu, бv, pubv) = 1;

v: check sign ver (Idu\ Idv, бu, pubu) = 1;

7) u: generate certv = rv\Idv\Idu\pubv\б'u and

Store certv in LR1 repository;

(б'u = sign (rv\IDv\Idu\pubu, prvu))

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

v: generate certu = ru\Idu\Idv\pubu\ϭ'v and

Store certu in LR1 repository;

(ϭ'v = sign (ru\IDu\Idv\pubu, prvv))

IV. PSEUDO CODE

```
INPUT:  nbits, previous_block
OUTPUT: random_data, previous_block'
Step 1: Find the previous block
        if (previous_block != Null)
        random_data = GenerateRandomData(nbits)
Step 2: Calculate random data
        if (nbits < 64)
        tocompare = random_data || 0^(64 - nbits)
Step 3: Find shortest path
        else
         tocompare = LeftMostBits(random_data, 64)
Step 4: Compare the block between leftmost
         if (tocompare == previous_block)
         return "catastrophic error"
Step 5:
        previous_block' = GenerateRandomData(64)
        return random_data
Step 6:
        End
```

V. SIMULATION RESULTS

In the Event-based simulator to evaluate the effectiveness of the *Hotspot-Locating* attack and the privacy protection of our scheme and *routing based* schemes. The nodes' radio transmission radius is 50 m, and the monitoring devices' overhearing radius is(ξ × 50) m. The network has one hotspot that is randomly located and fixed during each simulation run, and the number of source nodes in the hotspot is 30. It finds the random nodes to find shortest path and low cost.

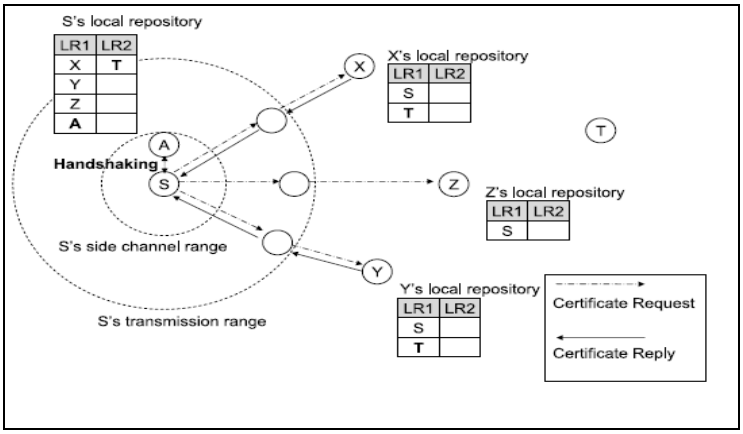

Fig.1. Example of Running Proposed Scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

VI. CONCLUSION AND FUTURE WORK

Mobile IP (MIP) has been proposed by the Internet Engineering Task Force (IETF) to provide global mobility in IP networks. It allows maintaining mobile terminals ongoing communications while moving through IP network. the MT movement is frequent, the MIP concept is not suitable and needs to be improved.

In order to reduce the signaling load for interregional networks, mobility dynamic location management approaches for MIP have been proposed.

Another alternative that reduce the signaling load in Mobile IP network is to use a multicast-based mobility approaches

The modules in the project are

- Mobile Terminal Module
- Foreign Agent Module
- Gateway Foreign Agent Module
- Mobile Server Module

An analytical model is proposed which evaluates the delay and the bandwidth of three mobility management approaches: MIP, DHMIP, and MHMIP. Our analysis gives a lower delay and bandwidth for MHMIP approach than DHMIP and MIP approaches.

In our future work, we will continue to implement a prototype of SEAKS and extend the scale of the experiments and to allow the emergence of other key management techniques to come up with highly efficient and secure key management scheme in terms of throughput, complexity, and authentication overhead.

REFERENCES

1. I. Akyildiz, W. Su, Y. Sankarasubramanian, and E. Cayirci, "Wireless sensor networks: a survey, computer networks", Computer Networks, vol. 38, pp. 393-422, 2002.
2. A. Arora, P. Dutta, S. Bapat, V. Kulathumani, and et al., "A line in the sand: A wireless sensor network for target detection, classification and tracking", Computer Networks, vol. 46, pp. 605-634, 2004.
3. WWWF-the conservation organization, http://www.panda.org/.
4. Star News, Panda poaching gang arrested, Shanghai Star Telegram,April 2003.
5. P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source location privacy in sensor network routing", Proc. of IEEE International Conference on Distributed Computing Systems (ICDCS'05),pp. 599-608, Columbus, Ohio, USA, 6-10 June 2005.
6. A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "Spins:security protocols for sensor networks", Wireless Networks, vol. 8,no. 5, pp. 521-534, 2002.
7. M. Shao, Y. Yang, S. Zhu and G. Cao, "Towards statistically strong source anonymity for sensor networks", Proc. of IEEE INFOCOM'08, pp. 51–59, Phoenix, Az, USA, April 2008.
8. Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks", Proc. of ACM WiSec, pp. 77–88, Alexandria, Virginia,USA, April 2008.
9. B. Hoh and M. Gruteser, "Protecting location privacy through path confusion", Proc. of IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks(SecureComm), pp. 194–205, Athens, Greece, September 5 -9, 2002.

BIOGRAPHY

Uma Maheswari is a post graduate student in the department of computer science engineering, rrase college of engineering, Anna University. She received Bachelor of Engineering degree (B.E) in 2011 from Anna University, Chennai, India. Her research interests are Cloud Computing,Database Management System etc.