A Secure Routing Scheme for Mobile Wireless Sensor Networks

Yuji Watanabe and Tong Tran Nhat Linh

Graduate School of Natural Sciences, Nagoya City University,
1 Yamanohata, Mizuho-cho, Mizuho-ku, Nagoya 467-8501 Japan
(Tel : 81-52-872-5037; Fax : 81-52-872-5037)
(yuji@nsc.nagoya-cu.ac.jp)

Abstract: Frequency-hopping (FH) is a well-known spread-spectrum method of transmitting radio signals by hopping frequency channels along a predefined hopping sequence known to both transmitter and receiver. Although FH is resistant to jamming by external malicious nodes which have no knowledge of the sequence, it is of no effect against at tacks by internal compromised nodes which know the sequence. In this paper, we propose a secure creation scheme of the hopping sequence for mobile wireless sensor networks. The proposed scheme is based on the idea of a statistical en-route filtering (SEF). SEF exploits collective decision-making by multiple detecting nodes in the de nse deployment of large sensor networks. We evaluate the performance of our scheme thorough simulations.

Keywords: Mobile wireless sensor networks, Frequency-hopping, Hopping sequence, Statistical en-route filtering**.**

I. INTRODUCTION

Wireless sensor networks (WSNs) have lately drawn considerable attention because of the popularization of sensors that are smaller, cheaper, and intelligent [1]. These sensors are equipped with one or more sensors, a processor, memory and a power supply. They can also communicate with each other to form network with wireless interfaces. WSNs have many applications such as environment monitoring and target tracking. A type of WSN is a mobile wireless sensor network where sensor nodes have the ability to move such as robots. For example, researches on mobile WSNs are Robomote [2], Emulab [3] and ZebraNet [4]. Challenges in mobile WSNs include deployment, localization, self-organization, navigation, coverage, and energy maintenance. A difference between static and mobile WSNs is routing, that is, dynamic routing is used in a mobile WSN unlike a static WSN using fixed routing or flooding.

The issue of security in WSNs must be addressed because WSNs may be deployed in potentially adverse or hostile environment. Adversaries can inject jamming which may cause not only false alarms but also the depletion of the limited energy of sensor nodes. Frequency-hopping (FH) is a well-known spread-spectrum method of transmitting radio signals by rapidly changing the frequency channel, using a predefined hopping sequence known to both transmitter and receiver [5, 6]. Although FH is resistant to jamming by external malicious nodes which have no knowledge of the sequence, it is of no effect against attacks by internal compromised nodes which know the sequence. Since the computation and storage constraints of low-end sensor nodes make complex cryptography-based mechanisms for hopping sequence creation infeasible, it is necessary to create the sequence securely and simply.

In this paper, we propose a secure creation scheme of the hopping sequence for mobile wireless sensor networks. The proposed scheme is based on the idea of a statistical en-route filtering (SEF) [7]. In SEF, assuming that the same event can be detected by multiple nodes, forwarding nodes along the way to base station can statistically detect false reports en-route. SEF has achieved the early detection of false data reports with low computation and communication overhead. We evaluate the performance of our scheme thorough simulations.

The rest of the paper is organized as follows: In Section II, we describe the frequency-hopping and the statistical en-route filtering in detail. Section III presents our secure creation scheme of the hopping sequence for mobile wireless sensor networks. In Section IV, we evaluate the performance of our scheme thorough simulations. Section V concludes the paper.

II. RELATED WORKS

1. Frequency-hopping (FH) [5, 6]

FH is the periodic changing of the frequency channel of a transmitted radio signal according to a predefined hopping sequence (pattern) known to both transmitter and receiver. FH is highly resistant to narrowband interference and intercept compared with a fixed-frequency transmission. FH is actually used for IEEE 802.11-1997 and Bluetooth [8, 9].

In FH, hopping occurs over a frequency band which includes *M* frequency channels. Figure 1 illustrates the example of frequency-hopping sequence with 16 frequency channels. The time interval between hops is called the slot. The number of frequency channels for IEEE 802.11 and Bluetooth in the 2.4 GHz ISM frequency band is 14 and 79, respectively.

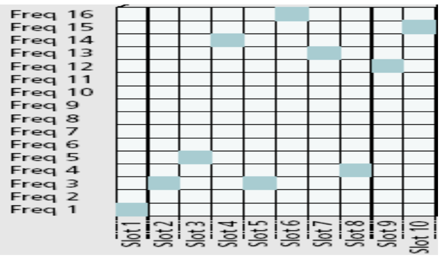

Fig.1. Example of frequency-hopping sequence

Normally the procedure of FH is as follows:

1. The transmitter sends a request via a predefined frequency channel.
2. The receiver sends a number, known as a seed.
3. The transmitter uses the seed as a variable in a predefined algorithm, which calculates the hopping sequence that must be used.
4. The transmitter sends a synchronization signal via the first frequency in the calculated sequence, thus acknowledging to the receiver it has correctly calculated the sequence.
5. The communication begins at the same point in time, and both the transmitter and the receiver change their frequencies along the sequence.

The sequence must be created securely and simply.

2. Statistical en-route filtering (SEF) [7]

SEF can probabilistically filter out false reports en-route. SEF exploits collective decision-making by multiple detecting nodes and collective false detection by multiple forwarding nodes in the dense deployment of large sensor networks.

SEF consists of three major components: 1) key assignment and report generation, 2) en-route filtering, and 3) base station verification. The process of key assignment and report generation is as follows:

1. The base station (sink) maintains a global key pool of *N* keys $\{K_i, 0 \le i \le N-1\}$, divided into *n* non-overlapping partitions. Each partition has *m* keys.
2. Before each sensor node is deployed, it stores randomly chosen *k* (*k* < *m*) keys from a randomly selected partition in the key pool.
3. When an event appears, multiple surrounding nodes can detect the event and a cluster head (center-of-stimulus node) is elected to generate the event report. Note that SEF assume that the same event can be detected by multiple nodes.
4. Each of the detecting nodes generates a keyed message authentication code (MAC) M_i using the event report (for example, the location, the time, and the type of event) and randomly selected K_i, one of its *k* stored keys.
5. The cluster head collects all the MACs from detecting nodes and attaches randomly chosen *T* MACs to the report. This set of multiple MACs acts as the proof that the report is legitimate.

In en-route filtering, when the cluster head forwards the event report with multiple MACs toward the base station, intermediate forwarding nodes verify the correctness of the MACs probabilistically and drop those with forged MACs en-route.

Due to the statistical nature of the detection mechanism, a few bogus reports with invalid MACs may escape en-route filtering and reach the base station. In base station verification, the base station further verifies the correctness of each MAC and eliminates false reports that elude en-route filtering.

III. PROPOSED SCHEME

We propose a secure creation scheme of the hopping sequence based on the SEF for mobile WSNs. The basic idea is to use multiple MACs generated by detecting nodes as a seed of the hopping sequence. In addition, although original SEF is applied for static WSNs, mobile WSNs require dynamic routing to search and find pathways to the base station. Therefore, in the proposed scheme, SEF is carried out in routing phase. Step 4 and 5 in the process of key assignment and report generation is changed as follows:

4'. Each of the detecting nodes generates a keyed MAC M_i using only the time of detection and randomly selected K_i. The total event report can be securely sent using FH after routing phase.

5'. The cluster head collects all the MACs from detecting nodes and attaches randomly chosen *T* MACs and the time of detection to RREQ

(Route Request) packet. The cluster head broadcasts RREQ packets to find route to the base station.

En-route filtering and base station verification, which function in the same way as original SEF, are carried out for the MACs in RREQ packets. After the base station verification, when the RREQ packet has valid MACs, the following process is additionally performed:

1. The base station sends RREP (Route Reply) packet back to the cluster head along the found route.
2. The cluster head and the intermediate forwarding nodes which can receive the RREP packet calculate the hopping sequence using the valid MACs as the seed in a predefined algorithm.
3. Both the transmitter and the receiver change their frequencies along the sequence, and the total event report is securely sent to the base station.

Figure 2 illustrates our secure creation scheme of the hopping sequence based on the SEF for mobile WSNs.

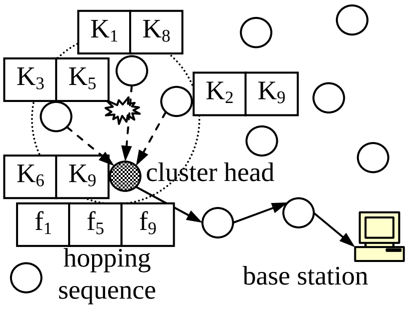

Fig.2. Secure creation scheme of the hopping sequen ce based on the SEF for mobile WSNs.

IV. SIMULATION RESULTS

We evaluate the performance of our scheme using network simulator NS2 [10]. We use a field size of 1000mX1000m, where 50 normal nodes and 1 malicious node are randomly located. Each node can move according to random waypoint model [11] with the speed randomly selected from 1m/s to 10m/s. In simulations, there are 5 event reports which must be sent to the base station by normal cluster heads. The speed of the packet is 4 packets per second, and the size of the packet is 512 bytes.

Like original SEF, we use a global key pool of 1000 keys, divided into 10 partitions, with 100 keys in each partition. Each node has 50 keys. Since the malicious node generates only incomplete multiple MACs using the time of false detection and its 50 stored keys, it send a forged event report to the base station along a invalid hopping sequence calculated by the incomplete MACs. As to the other simulation conditions, the maximum number of frequency channels is 14 like IEEE 802.11 in the 2.4 GHz ISM frequency band, and dynamic source routing (DSR) [12] is applied for mobile WSNs.

Figure 3 shows the packet delivery rate of event reports from normal cluster heads and the malicious node changing the number of frequency channels. The results of 1 channel correspond to the case without FH. When FH is not used, 97% packets of event reports from normal cluster heads can reach the base station, and 96% packets of the forged report from the malicious node can also reach. However, as the number of frequency channels increases, although the packet delivery rate from normal cluster heads slightly decreases, the delivery rate from the malicious node dramatically drops down. When the number of frequency channels is 14, only 13% packets of the forged report from the malicious node can reach.

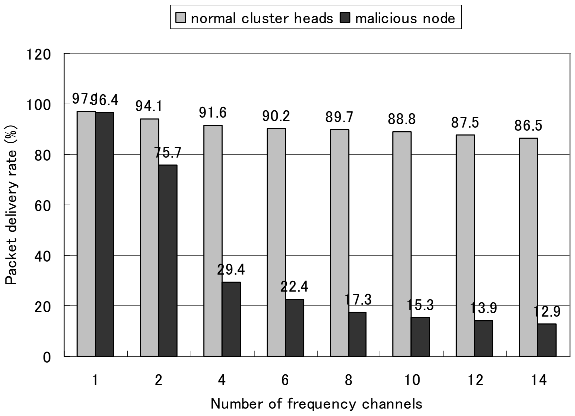

Fig.3. Simulation Results

V. CONCLUSION

This paper proposed a secure creation scheme of the hopping sequence for mobile wireless sensor networks based on the statistical en-route filtering. The effectiveness of our scheme is demonstrated thorough simulations.

REFERENCES

[1] Yick J, Mukherjee B, Ghosal D (2008), Wireless sensor network survey. Computer Networks 52:2292-2330

[2] Sibley GT, Rahimi MH, and Sukhatme GS (2002), Robomote: A Tiny Mobile Robot Platform for Large-Scale Ad-hoc Sensor Networks. Proceedings of the IEEE International Conference on Robotics and Automation. Washington DC

[3] Johnson D, Stack T, Fish R, Flickinger DM, Stoller L, Ricci R, Lepreau J (2006), Mobile Emulab: a robotic wireless and sensor network testbed. IEEE INFOCOM

[4] Zhang P, Sadler CM, Lyon SA, Martonosi M (2004), Hardware design experiences in ZebraNet. Proceedings of the SenSys'04, Baltimore, MD

[5] Torrieri D (2005), Principles of spread-spectrum communication systems. Boston: Springer

[6] Wikipedia, http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

[7] Ye F, Luo H, Lu S and Zhang L (2005), Statistical En-Route Filtering of Injected False Data in Sensor Networks. IEEE Journal on Selected Areas in Communications, 23(4):839-850

[8] IEEE 802.11, The Working Group Setting the Standards for WLANs, http://www.ieee802.org/11/

[9] Bluetooth.com, http://www.bluetooth.com/

[10] Ns2, http://www.isi.edu/nsnam/

[11] Camp T, Boleng J and Davies V (2002), A Survey of Mobility Models for Ad Hoc Network Research. Wireless Communications and Mobile Computing, 2(5):483-502

[12] Johnson DB, Maltz DA (1996), Dynamic source routing, in: T. Imielinski, H.F. Korth (Eds.), Ad Hoc Wireless Networks Mobile Computing 353