WILEY
Publishers Since 1807

JOHN WILEY & SONS, LTD., THE ATRIUM, SOUTHERN GATE, CHICHESTER P019 8SQ, UK

*** PROOF OF YOUR ARTICLE ATTACHED, PLEASE READ CAREFULLY ***

After receipt of your corrections your article will be published initially within the online version of the journal.

PLEASE NOTE THAT THE PROMPT RETURN OF YOUR PROOF CORRECTIONS WILL ENSURE THAT THERE ARE NO UNNECESSARY DELAYS IN THE PUBLICATION OF YOUR ARTICLE

☐ **READ PROOFS CAREFULLY**

ONCE PUBLISHED ONLINE OR IN PRINT IT IS NOT POSSIBLE TO MAKE ANY FURTHER CORRECTIONS TO YOUR ARTICLE

- This will be your only chance to correct your proof
- Please note that the volume and page numbers shown on the proofs are for position only

☐ **ANSWER ALL QUERIES ON PROOFS** (Queries are attached as the last page of your proof.)

- List all corrections and send back via e-mail to the production contact as detailed in the covering e-mail, or mark all corrections directly on the proofs and send the scanned copy via e-mail. Please do not send corrections by fax or post

☐ **CHECK FIGURES AND TABLES CAREFULLY**

- Check sizes, numbering, and orientation of figures
- All images in the PDF are downsampled (reduced to lower resolution and file size) to facilitate Internet delivery. These images will appear at higher resolution and sharpness in the printed article
- Review figure legends to ensure that they are complete
- Check all tables. Review layout, titles, and footnotes

☐ **COMPLETE COPYRIGHT TRANSFER AGREEMENT (CTA) if you have not already signed one**

- Please send a scanned signed copy with your proofs by e-mail. **Your article cannot be published unless we have received the signed CTA**

☐ **OFFPRINTS**

- 25 complimentary offprints of your article will be dispatched on publication. Please ensure that the correspondence address on your proofs is correct for dispatch of the offprints. If your delivery address has changed, please inform the production contact for the journal – details in the covering e-mail. Please allow six weeks for delivery.

Additional reprint and journal issue purchases

- Should you wish to purchase a minimum of 100 copies of your article, please visit http://www3.interscience.wiley.com/aboutus/contact_reprint_sales.html
- To acquire the PDF file of your article or to purchase reprints in smaller quantities, please visit http://www3.interscience.wiley.com/aboutus/ppv-articleselect.html. Restrictions apply to the use of reprints and PDF files – if you have a specific query, please contact permreq@wiley.co.uk. Corresponding authors are invited to inform their co-authors of the reprint options available
- To purchase a copy of the issue in which your article appears, please contact cs-journals@wiley.co.uk upon publication, quoting the article and volume/issue details
- Please note that regardless of the form in which they are acquired, reprints should not be resold, nor further disseminated in electronic or print form, nor deployed in part or in whole in any marketing, promotional or educational contexts without authorization from Wiley. Permissions requests should be directed to mailto: permreq@wiley.co.uk

WILEY AUTHOR DISCOUNT CLUB

We would like to show our appreciation to you, a highly valued contributor to Wiley's publications, by offering a **unique 25% discount** off the published price of any of our books*.

All you need to do is apply for the **Wiley Author Discount Card** by completing the attached form and returning it to us at the following address:

The Database Group (Author Club)
John Wiley & Sons Ltd
The Atrium
Southern Gate
Chichester
PO19 8SQ
UK

Alternatively, you can **register online** at www.wileyeurope.com/go/authordiscount
Please pass on details of this offer to any co-authors or fellow contributors.

After registering you will receive your Wiley Author Discount Card with a special promotion code, which you will need to quote whenever you order books direct from us.

The quickest way to order your books from us is via our European website at:

http://www.wileyeurope.com

Key benefits to using the site and ordering online include:

- Real-time SECURE on-line ordering
- Easy catalogue browsing
- Dedicated Author resource centre
- Opportunity to sign up for subject-orientated e-mail alerts

Alternatively, you can order direct through Customer Services at:
cs-books@wiley.co.uk, or call +44 (0)1243 843294, fax +44 (0)1243 843303

So take advantage of this great offer and return your completed form today.

Yours sincerely,

Verity Leaver
Group Marketing Manager
author@wiley.co.uk

*TERMS AND CONDITIONS

This offer is exclusive to Wiley Authors, Editors, Contributors and Editorial Board Members in acquiring books for their personal use. There must be no resale through any channel. The offer is subject to stock availability and cannot be applied retrospectively. This entitlement cannot be used in conjunction with any other special offer. Wiley reserves the right to amend the terms of the offer at any time.

REGISTRATION FORM
For Wiley Author Club Discount Card

To enjoy your 25% discount, tell us your areas of interest and you will receive relevant catalogues or leaflets from which to select your books. Please indicate your specific subject areas below.

Accounting [ ]
- Public [ ]
- Corporate [ ]

Chemistry [ ]
- Analytical [ ]
- Industrial/Safety [ ]
- Organic [ ]
- Inorganic [ ]
- Polymer [ ]
- Spectroscopy [ ]

Encyclopedia/Reference [ ]
- Business/Finance [ ]
- Life Sciences [ ]
- Medical Sciences [ ]
- Physical Sciences [ ]
- Technology [ ]

Earth & Environmental Science [ ]

Hospitality [ ]

Genetics [ ]
- Bioinformatics/ Computational Biology [ ]
- Proteomics [ ]
- Genomics [ ]
- Gene Mapping [ ]
- Clinical Genetics [ ]

Medical Science [ ]
- Cardiovascular [ ]
- Diabetes [ ]
- Endocrinology [ ]
- Imaging [ ]
- Obstetrics/Gynaecology [ ]
- Oncology [ ]
- Pharmacology [ ]
- Psychiatry [ ]

Non-Profit [ ]

Architecture [ ]

Business/Management [ ]

Computer Science [ ]
- Database/Data Warehouse [ ]
- Internet Business [ ]
- Networking [ ]
- Programming/Software Development [ ]
- Object Technology [ ]

Engineering [ ]
- Civil [ ]
- Communications Technology [ ]
- Electronic [ ]
- Environmental [ ]
- Industrial [ ]
- Mechanical [ ]

Finance/Investing [ ]
- Economics [ ]
- Institutional [ ]
- Personal Finance [ ]

Life Science [ ]

Landscape Architecture [ ]

Mathematics Statistics [ ]

Manufacturing [ ]

Materials Science [ ]

Psychology [ ]
- Clinical [ ]
- Forensic [ ]
- Social & Personality [ ]
- Health & Sport [ ]
- Cognitive [ ]
- Organizational [ ]
- Developmental & Special Ed [ ]
- Child Welfare [ ]
- Self-Help [ ]

Physics/Physical Science [ ]

Please complete the next page /

I confirm that I am (*delete where not applicable):

a **Wiley** Book Author/Editor/Contributor* of the following book(s):
ISBN:
ISBN:

a **Wiley** Journal Editor/Contributor/Editorial Board Member* of the following journal(s):

SIGNATURE: …… Date: ……

PLEASE COMPLETE THE FOLLOWING DETAILS IN BLOCK CAPITALS:

TITLE: (e.g. Mr, Mrs, Dr) …… FULL NAME: ……

JOB TITLE (or Occupation): ……

DEPARTMENT: ……

COMPANY/INSTITUTION: ……

ADDRESS: ……

……

TOWN/CITY: ……

COUNTY/STATE: ……

COUNTRY: ……

POSTCODE/ZIP CODE: ……

DAYTIME TEL: ……

FAX: ……

E-MAIL: ……

YOUR PERSONAL DATA
We, John Wiley & Sons Ltd, will use the information you have provided to fulfil your request. In addition, we would like to:

1. Use your information to keep you informed by post of titles and offers of interest to you and available from us or other Wiley Group companies worldwide, and may supply your details to members of the Wiley Group for this purpose.
   [ ] Please tick the box if you do **NOT** wish to receive this information

2. Share your information with other carefully selected companies so that they may contact you by post with details of titles and offers that may be of interest to you.
   [ ] Please tick the box if you do **NOT** wish to receive this information.

E-MAIL ALERTING SERVICE
We also offer an alerting service to our author base via e-mail, with regular special offers and competitions. If you **DO** wish to receive these, please opt in by ticking the box [ ].

If, at any time, you wish to stop receiving information, please contact the Database Group (databasegroup@wiley.co.uk) at John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, PO19 8SQ, UK.

TERMS & CONDITIONS
This offer is exclusive to Wiley Authors, Editors, Contributors and Editorial Board Members in acquiring books for their personal use. There should be no resale through any channel. The offer is subject to stock availability and may not be applied retrospectively. This entitlement cannot be used in conjunction with any other special offer. Wiley reserves the right to vary the terms of the offer at any time.

PLEASE RETURN THIS FORM TO:
Database Group (Author Club), John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, PO19 8SQ, UK author@wiley.co.uk
Fax: +44 (0)1243 770154

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2008; **1**:1–14
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.89

An efficient scheme for removing compromised sensor nodes from wireless sensor networks‡

Yong Wang[1*,†], Byrav Ramamurthy[2], Xukai Zou[3] and Yuyan Xue[2]Q2

[1]*Calient Networks, 215 Pacific Oaks Road, Apt 109, Goleta, C.A. 93117, U.S.A.*Q3
[2]*Computer Science and Engineering Department, University of Nebraska Lincoln, Lincoln, N.E., U.S.A.*
[3]*Department of Computer and Information Science, Indiana University-Purdue Univesity Indianpolis, Indianapolis, I.N. 46202, U.S.A.*

Summary

The goal of key management is to establish the required keys between sensor nodes which exchange data. A Key management protocol includes two aspects: key distribution and key revocation. Key distribution has been extensively studied in the context of sensor networks. However, key revocation has received relatively little attention. In this paper, we first review and summarize the current key revocation schemes for sensor networks. Then, we present an efficient scheme, KeyRev, for removing compromised sensor nodes from a wireless sensor network (WSN). Unlike most proposed key revocation schemes focusing on removing the compromised keys on the sensor nodes, the KeyRev scheme uses key update techniques to obsolesce the keys owned by the compromised sensor nodes and thus remove the nodes from the network. We analyze the security of the KeyRev scheme and evaluate its performance against another centralized key revocation scheme and a distributed key revocation scheme. Our analyses show that the KeyRev scheme is secure in spite of not removing the pre-distributed key materials at compromised sensor nodes. Simulation results also indicate that the KeyRev scheme is scalable and performs very well compared with other key revocation schemes in WSNs. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: wireless sensor network; key management; centralized key revocation scheme; distributed key revocation scheme

1. Introduction

Wireless Sensor Networks (WSNs) are used in many applications in military, ecological and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs for these applications [1]. Among all security issues in WSNs, key management is one of core mechanisms to ensure the security of applications and network services in WSNs.

*Correspondence to: Yong Wang, Calient Networks, 215 Pacific Oaks Road, Apt 109, Goleta, California, USA, 93117.
†E-mail: yongwang91@gmail.com
‡An earlier version of this paper appeared in the Proceedings of the IEEE International Conference on Communications (ICC), 2007.

Copyright © 2008 John Wiley & Sons, Ltd.

UNCORRECTED PROOFS

The goal of key management is to establish the required keys between sensor nodes which exchange data. A key management protocol includes two aspects: key distribution and key revocation. Key distribution refers to the task of distributing secret keys to sensor nodes to provide communication secrecy and authenticity. Key revocation refers to the task of securely removing keys which are known to be compromised. Key distribution has been exclusively studied under the constraints on computation and power consumption in sensor networks [2–4]. However, key revocation has received relatively little attention.

Since sensor nodes might be deployed in hostile or insecure environments, sensor nodes can be tampered or compromised by an adversary. Once a sensor node is compromised, the attacker is capable of stealing the key materials contained within that node and starts various of attacks [1]. The security of sensor nodes must be considered. In case a sensor node is known to be captured or compromised, the sensor node must be removed securely from the network. The problem of sensor node removal is usually reduced to that of key revocation [4,5]. By revoking all of the keys belonging to a known compromised sensor node, the node can be removed from the network.

Most of the proposed key management schemes depend on some key materials being pre-distributed in the sensor nodes. These pre-distributed key materials usually include an initial key shared by all sensor nodes [2], a pairwise key shared between the base station and the sensor node [3], or a key ring consisting of certain number of keys to be used in the future [3,4]. The keys for secure communication, for example, *pairwise keys* [3], *path keys* [3], and *cluster keys* [2] used by sensor nodes are set-up based on those pre-distributed materials in the bootstrap stage. When a sensor node is compromised, the keys set up on the fly and the pre-distributed materials must be revoked.

A revocation attack is a specific attack in which an adversary uses the node revocation protocol to selectively revoke uncompromised sensors from the network. Revocation attacks must be considered in designing a revocation scheme. Since compromised sensor nodes may act as an adversary's surrogates within a revocation protocol and subvert the execution of the revocation protocol [5], the resistance to compromised sensors must be evaluated in a revocation protocol. Further, after compromised sensors are removed from the network, new sensors might be re-deployed to replace those compromised sensors. The node addition problem must be considered. The node addition problem is usually reduced to the key distribution problem. In this paper, we focus on the key revocation issues.

A few schemes [3–5] have been proposed to address the key revocation problem in WSNs. However, these schemes incur various difficulties when used in sensor networks. For example, the centralized key revocation scheme proposed in Reference [3] requires a signature key distributed in the non-revoked sensor nodes. However, the signature key can only be distributed by unicasting which causes severe performance issues in large scale sensor networks. The distributed key revocation schemes proposed in References [4,5] are faster. However, they are also more complex than the centralized key revocation schemes. Further, the distributed key revocation schemes proposed in References [4,5] are based on some strong assumptions such as each node knowing its neighboring nodes before the sensor network is deployed. These assumptions are hard to satisfy. Thus, designing a new efficient scheme of removing compromised sensor nodes from WSNs is highly desirable.

In this paper, we present an efficient scheme, KeyRev, to remove compromised sensor nodes. The KeyRev scheme was first proposed in Reference [6]. This paper is a significant improvement of the previous paper. In Reference [6], we focused on centralized key revocation schemes. We compared the KeyRev scheme with another centralized key revocation scheme, EsRev scheme, and demonstrated that the KeyRev scheme has a better performance than the EsRev scheme. However, compared to centralized key revocation schemes, distributed key revocation schemes usually perform better using local communication and reducing global broadcast messages. Thus, it is essential to understand the performance of the KeyRev scheme by comparing it with a distributed key revocation scheme. In this paper, we review and summarize the distributed key revocation scheme proposed in References [4,5]. We also analyze and evaluate for the first time the distributed key revocation scheme in WSNs. Our analyses and simulation results reveal that the centralized key revocation scheme, which had been believed inefficient before, can also attain high efficiency in sensor networks.

Unlike most proposed key revocation schemes focusing on removing the compromised keys at compromised sensor nodes, the KeyRev scheme uses key update techniques to obsolesce the keys owned by the compromised sensor nodes and thus remove the nodes from the network. The KeyRev scheme

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

depends on a unique key shared by all nodes in the network and the unique key is distributed to the network using an efficient group communication scheme [7]. In addition, the proposed scheme does not depend on any specific key distribution schemes and thus, the KeyRev scheme can be extended for implementation with other key distribution schemes, for example, the schemes proposed in Reference [5,8].

The KeyRev scheme is a centralized key revocation scheme. However, unlike other centralized key revocation schemes [3,4] which try to remove the keys shared with the compromised sensor nodes, there are really no keys to be removed from the sensor nodes in the KeyRev scheme. The sensor node removal problem is reduced to a key update problem in this paper. In the remainder of this paper, without specific explanation, the KeyRev scheme is also called a key revocation scheme.

Our contributions in this paper include the following:

(1) We present a novel scheme of removing compromised sensor nodes from WSNs utilizing key update techniques.
(2) We analyze and evaluate the performance of the distributed key revocation scheme in WSNs for the first time.
(3) Simulation results reveal that the centralized key revocation scheme can also attain high efficiency in WSNs.

Our analyses and simulation results show that the proposed scheme, KeyRev, is secure and efficient in computation, communication, and storage usage. Simulation results also indicate that the KeyRev scheme is scalable and performs very well compared with other revocation schemes.

The remainder of this paper is organized as follows: Section 2 discusses the related work. Section 3 presents our proposed key revocation scheme. The security and performance analyses are presented in Section 4, and the simulation experiments and results in Section 5. Section 6 concludes the paper.

2. Related Work

As discussed before, key management includes two aspects: key distribution and key revocation. Many key distribution schemes have been proposed in sensor networks. According to the network structure, the schemes can be divided into centralized key distribution schemes [9] and distributed key distribution schemes [3,10]. According to the probability of key sharing between a pair of sensor nodes, the key distribution schemes can be classified into deterministic approaches [2,8] and probabilistic approaches [3,10]. An investigation of key distribution schemes for WSNs can be found in References [1,11]. In this paper, we focus on the key revocation problem.

Key revocation refers to the task of securely removing keys which are known to be compromised. To detect a compromised sensor, intrusion detection techniques are employed. Intrusion detection is out of the scope of this paper. We assume that there are some methods [12–14] for a base station to detect a compromised sensor node. Another issue which must be considered is reconfiguration. The topology of the WSN needs to be rebuilt after the compromised sensors are removed. Sensors might be re-deployed to replace those compromised sensors. The rest of the section reviews several known key revocation schemes in WSNs.

Recent work conducted on key revocation for WSNs include [3–6,15] and no other schemes have been reported to date. These key revocation schemes can be divided into two categories: the centralized key revocation schemes [3,6,15] and the distributed key revocation schemes [4,5]. We discuss these in turn below.

2.1. Centralized Key Revocation Scheme

In centralized key revocation scheme, a centralized authority (base station) is used to revoke compromised sensors [3]. Eschenauer and Gligor presented a key management scheme for WSNs in Reference [3]. This scheme, which is called the basic random key scheme in this paper, is a centralized key revocation scheme. Before describing the key revocation scheme, we first introduce the key distribution scheme which will be used later to demonstrate how to revoke the compromised key materials in our scheme.

The key distribution scheme consists of three phases: key pre-distribution, shared-key discovery, and path key establishment.

In the key pre-distribution phase, each sensor is equipped with a *key ring* held in the memory. The key ring consists of k keys which are randomly drawn from a large pool of P keys. The association information of the key identifiers in the key ring and sensor identifier are also stored at the base station. Further, the authors assumed that each sensor i shares a pairwise key K^{ci} with the base station.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

In the shared key discovery phase, each sensor discovers its neighbors within wireless communication range with which it shares keys. Two methods to accomplish this are suggested in Reference [3]. The simplest method for each node is to broadcast[Q4] a list of identifiers of the keys in its key ring in plain text allowing neighboring nodes to check whether they share a key. However, an adversary may observe the key-sharing patterns among sensors in this way. The second method uses the challenge-response technique to hide key-sharing patterns among nodes from an adversary. For every key K_i on a key ring, each node could broadcast a list $\langle \alpha, E_{K_i}(\alpha) \rangle$, $i = 1, \ldots, k$ where α is a challenge. The decryption of $E_{K_i}(\alpha)$ with the proper key by a recipient would reveal the challenge and establish a shared key with the broadcasting node.

Finally, in the path-key establishment phase, a path-key is assigned between sensor nodes which are within wireless communication range but do not share a key at the end of the second phase.

If a node is compromised, the base station can send a message to all other sensors to revoke the compromised node's key ring. The revocation scheme in Reference [3] can be divided into three phases: signature key distribution, key revocation, and link reconfiguration.

In the signature key distribution phase, the base station generates a signature key K_e and unicasts it to each node by encrypting it with a pairwise key K^{ci} shared by the base station with the ith sensor node.

In the key revocation phase, the base station broadcasts a single message containing a list of key identifiers for the key ring to be revoked signed by the signature key. Each sensor verifiers the signature of the key revocation message, locates those identifiers in its key ring, and removes the corresponding keys.

Once the keys are removed from the key rings, some links may disappear, and the affected nodes need to reconfigure those links by restarting the shared-key discovery, and possibly the path-key establishment, phases.

The key revocation scheme, referred to as EsRev scheme, requires n unicast messages and one broadcast message. In a large scale sensor network, distributing the signature key might be a problem. Pre-distributing the signature key might be possible; however, once the signature key is compromised, the adversary could use the signature key to duplicate the revocation messages from the base station.

Zhang *et al*. proposed a location-based revocation scheme utilizing multiple revocation messages in Reference [15]. When the revocation area is large or complicated, the revocation area can be divided into sub-areas. For each sub-area, a revocation message is sent to a certain node within that area using GPSR protocol [16], and then the revocation message is multicasted to the remaining sub-area. The revocation message includes the identifier of the sensor nodes to be revoked and the scope of the revocation area. On receiving the message, for each node, if it has received the message before or is outside of the revocation area, the message is dropped. If the sensor node is within the revocation area indicated by the revocation message, the sensor node records the identifier of the revoked sensor node, and rebroadcast the message to its neighboring nodes. The revocation scheme, referred to as the GPSRRev scheme, is also a centralized key revocation scheme.

2.2. Distributed Key Revocation Scheme

In a distributed key revocation scheme, no centralized authority is used. Chan *et al*. proposed a distributed key revocation scheme for sensor networks in Reference [4] and further investigated this scheme in Reference [5]. In this distributed key revocation scheme, a vote is cast and collected among sensor nodes. If the vote tally against a sensor node exceeds a specified threshold, the sensor node will be revoked. Chan's scheme depends on the secret sharing scheme proposed in Reference [17]. The distributed key revocation scheme is described below.

The revocation timeline is divided into sessions. Each sensor has at most s_{total} revocation sessions against any target nodes (compromised nodes). Before the sensor network is deployed, the setup server generates a t degree random polynomial $q_{A_s}(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ for each session s on sensor node A. For each node B of A's participants (a participant of A is a sensor which shares a key with node A), the setup server loads the revocation vote $(q_{B_s}(x_{AB_s}), x_{AB_s})$ from A against B on node A. This revocation vote is encrypted by a mask Mask_{AB_s} that B gives to A. That is, the pre-loaded data on A against B is $E_{\text{Mask}_{AB_s}}(q_{B_s}(x_{AB_s}), x_{AB_s})$. For each vote, the setup server also loads the $\log m$ authentication hash values for the Merkle tree with leaves $(q_{B_s}(x_{iB_s}), x_{iB_s})$ for each node i in B's participants (a total of m leaves). The root R_B of the Merkle tree is also loaded on A. Finally, the setup server loads $H^2 q_{B_s}$, which is the hash of the[Q4] revocation polynomial of B on A. This will allow non-local participants (a non-local participant of B is a sensor node which shares a key with B but multi-

UNCORRECTED PROOFS

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

hops (>1) away from B) to verify the authenticity of a revocation decision against B.

In the beginning of each session, the masks are exchanged among neighboring nodes. The purpose of the mask key is to ensure that each node is only able to revoke sensors within its immediate neighborhood.

Each revocation session is divided into three states: pending, active, and completed. The pending state indicates that no voting occurs in the current session. When the first vote of the session is cast and received by A, A changes its state to active. The active state lasts for exactly Δ_s time for each node, after which the node transitions to the completed state for this session, and starts the pending state for the next session.

When A votes against B during the revocation session s, it decrypts the vote using B's mask key Mask_{AB_s} and broadcasts $(q_{B_s}(x_{AB_s}), x_{AB_s})$ along with the $\log m$ Merkle authentication values. This is a local neighborhood broadcast. The broadcast only needs to go far enough to ensure complete dissemination in the neighborhood of B. The node receiving the vote verifies the authenticity of the vote using the Merkle authentication values. The node will disseminate the broadcast if the verification is successful. When A casts a vote on B, it will vote both in the current session and on the next session. Voting on the next session occurs immediately upon completion of the current session.

When A's state for the session has transited to completed state, it counts the number of votes it has received when it was in the active state. If A has at least t revocation votes, then A can use these t points to compute the random t-degree polynomial q_{B_s} using the secret sharing scheme in Reference [17]. From this, A computes the hash of the polynomial, Hq_{B_s}. This value is then broadcasted through the entire network. All participants of B receiving this value can verify it by computing the hash of the received value. If the verification is successful, the keys shared with B will be revoked.

Note that Chan's scheme, referred to as DistRev scheme, is built on some simplifying assumptions; for example, each node knows its neighboring nodes before deployment. It is hard to satisfy these requirements.

Compared with the centralized key revocation schemes, the distributed key revocation schemes are faster because they require local broadcast and avoid a single point of failure. However, the distributed key revocation schemes are also more complex than the centralized key revocation schemes and, hence, more prone to design error since compromised sensor nodes can participate in the revocation protocol and attempt to block or circumvent it. In addition, it is also possible to compromise enough nodes to sabotage the distributed key revocation scheme. For more detailed information about the distributed key revocation scheme, please refer to References [4,5].

In the remainder of this paper, we present an efficient scheme, KeyRev, to remove compromised sensor nodes from WSNs. We use the following notation in the remainder of this paper:

- A, B are principals such as communicating nodes.
- $K_{A,B}$ denotes the secret pairwise key shared between A and B.
- M_K is the encryption of message M with key K.
- $\text{MAC}(K, M)$ denotes the computation of the message authentication code (MAC) of message M with key K.
- $M_1|M_2$ denotes the concatenation of messages M_1 and M_2.
- $A \longrightarrow B$ denotes that A unicasts a message to B.

3. KeyRev: An Efficient Scheme of Removing Compromised Sensors From WSNs

Unlike most of the proposed key revocation schemes focusing on removing the compromised keys, our scheme, KeyRev, uses key update techniques to obsolesce the keys owned by the compromised sensor nodes and thus remove the nodes from the network. The KeyRev scheme does not depend on a specified key distribution scheme. Without loss of generality, we assume that the basic random key distribution scheme [3] is used.

3.1. Assumptions of Our Protocol

We assume that the base station is secure and well protected. The sensor nodes are not tamper-resistant and thus can be compromised. If a sensor node is compromised, the attacker is capable of stealing all the key materials contained within that node. We also assume that all the sensor nodes are within reach of the base station. Next, we provide an overview of our scheme.

3.2. Overview

The basic random key distribution scheme establishes two kinds of keys among sensor nodes: the *pairwise keys* and the *path keys*. When a sensor node is

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

compromised, the compromised keys must be revoked so that the compromised keys will not be chosen again as the new secret keys. Instead of using the pairwise keys and the path keys directly for the communication secrecy and authenticity, we propose two kinds of keys for secure communication in the sensor network: the *encryption key* and the *message authentication code* (*MAC*) *key*. The encryption key and the MAC key are generated by a pseudo-random function which is bound to the pairwise key or the path key, and a *session key* distributed regularly by the base station to all the sensor nodes in the network. When the session key is updated, the encryption key and the MAC key are also changed. A sensor node always uses the latest encryption key and MAC key to encrypt and sign the outgoing messages or decrypt and verify the incoming messages. If there is a session key distribution scheme in which the compromised sensors cannot recover the new session key when they are revoked, these revoked sensors will be removed from the network because they cannot derive the new encryption and MAC keys on the next session. Although an adversary may retain the pairwise and path keys, the adversary cannot figure out the encryption keys and the MAC keys because of the pseudo-random function used. Thus, the key revocation problem is reduced to the session key update problem.

In the remainder of this section, we first introduce the KeyRev scheme assuming an effective session key distribution scheme is used, and then we discuss the session key distribution scheme, followed by broadcast authentication problem.

3.3. KeyRev Scheme

The lifetime of a WSN is partitioned into time intervals called *sessions*. The duration of sessions can be fixed or dynamic depending on the applications. The base station is responsible for distributing *session keys* to the sensor nodes. We use K_j to denote the jth session key where $j \in \{1, 2, \ldots, m\}$ and m is the number of sessions.

We assume that each sensor is uniquely identified by an ID number i, where $i \in \{1, \ldots, n\}$ and n is the largest ID number. Each sensor maintains a list: *node revocation list* (*NRL*). A *node revocation list* includes all the sensor identifiers which have been revoked in the network. The revocation list is empty initially and will be populated as the time goes by. The revocation list is checked for any incoming and outgoing messages to ensure that only valid sensors are members of the network. We also assume that the pairwise keys and the path keys have been set up by the basic random key distribution scheme.

We propose two kinds of keys for secure communication in the sensor network: the *encryption key* K_{encr} and the *message authentication code* (*MAC*) *key* K_{mac}. For any message transmitted in the network, authentication, confidentiality, and integration are required. Let A and B be two entities in a WSN, the complete message A sends to B is

$$A \longrightarrow B : \{M|T_s\}_{K_{\text{encr}}}, \text{MAC}(K_{\text{mac}}, \{M|T_s\}_{K_{\text{encr}}})$$

where M is the message, T_s is the timestamp when sending the message, and MAC(K, R) denotes the computation of the message authentication code of message R with key K.

Let K_j be the current session key and $K_{A,B}$ represent the pairwise key or path key shared between the sensor nodes A and B. The encryption and the MAC key used in session j can be generated as follows:

$$K_{\text{encr}} = F(\text{MAC}(K_{A,B}, K_j) \quad (1)$$

$$K_{\text{mac}} = F(\text{MAC}(K_{A,B}, K_j) \quad (2)$$

where $F(K, x)$ is a pseudo-random function and x is an integer 1 or 2 for generating K_{encr} or K_{mac}, respectively.

The security of the communication between A and B is ensured by the encryption key K_{encr} and the MAC key K_{mac}. Both of them are bound to the session key and will be updated when the session key is updated. Any message that A sends to B is encrypted by the encryption key K_{encr} and signed by the MAC key K_{mac}. For any message that B receives from A, B always verifies the message first and then decrypts it. Further, a sensor node always uses the encryption and MAC key corresponding to the current session key to encrypt and sign the outgoing messages or decrypt and verify the incoming messages.

If there is a method to stop the compromised sensors from obtaining the new session keys and thus stop them from deriving K_{encr} and K_{mac}, then the compromised sensors can no longer decrypt new messages and authenticate themselves. For example, if A is compromised and A cannot recover the new session key, then A cannot derive the new encryption key and the MAC key while B can. Due to the lack of the proper keys to encrypt and sign the messages, A cannot send any valid messages to B from that time. Therefore, the sensor node A is removed from the network.

Next, we introduce the session key distribution scheme used in the KeyRev scheme.

UNCORRECTED PROOFS

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

3.4. Session Key Distribution Scheme

To make the KeyRev scheme work, the session key distribution scheme must satisfy the following criteria:

(1) The compromised sensors should not be able to obtain the new session keys.
(2) The sensor network is time synchronized so that the current keys can be identified.

Criterion 2 is easily satisfied. For criterion 1, we derive a simple session key distribution scheme based on the personal key share distribution scheme in Reference [7]. The session key distribution scheme can be divided into three phases, *viz.*, setup, broadcast, and session key recovery.

(1) Setup: The setup server randomly picks m $2t$-degree masking polynomial, $h_j(x) = h_{j,0} + h_{j,1}x + \cdots + h_{j,2t}x^{2t}$, $j \in \{1, 2, \ldots, m\}$, over a finite field F_q where q is a sufficiently large prime number. For each sensor node A_i, the setup server loads the personal secrets, $\{h_1(i), h_2(i), \ldots, h_m(i)\}$, to the node A. The setup server also loads the polynomial, $h_j(x)$, to the base station. For each session key K_j, the setup server randomly picks a t-degree polynomial $p_j(x)$ and constructs $q_j(x) = K_j - p_j(x)$.
(2) Broadcast: Given a set of revoked group members, $R = \{r_1, r_2, \ldots, r_w\}$, $w \leq t$ in session j, the base station distributes the shares of t-degree polynomial $p_j(x)$ and $q_j(x)$ to non-revoked sensors via the following broadcast message:

$$B = \{R\} \cup \{P_j(x) = g_j(x)p_j(x) + h_j(x)\}$$
$$\cup\{Q_j(x) = g_j(x)q_j(x) + h_j(x)\}$$

where the revocation polynomial $g_j(x)$ is constructed as $g_j(x) = (x - r_1)(x - r_2)\ldots(x - r_w)$.
(3) Session key recovery: If any non-revoked sensor node A_i receives such a broadcast message, it evaluates the polynomial $P_j(x)$ and $Q_j(x)$ at point i and gets $P_j(i) = g_j(i)p_j(i) + h_j(i)$ and $Q_j(i) = g_j(i)q_j(i) + h_j(i)$. Because A_i knows $h_j(i)$ and $g_j(i) \neq 0$, it can compute $p_j(i) = \frac{P_j(i) - h_j(i)}{g_j(i)}$ and $q_j(i) = \frac{Q_j(i) - h_j(i)}{g_j(i)}$. A_i finally can compute the new session key $K_j = p_j(i) + q_j(i)$.

The revoked sensors cannot recover $p_j(i)$ and $q_j(i)$ because $g_j(i) = 0$ and thus cannot recover the new session key. Without obtaining the new session key, the revoked sensors cannot derive the encryption key K_{encr} and the MAC key K_{mac} and thus cannot decrypt new messages and authenticate themselves to other sensor nodes in the network. The compromised sensor nodes can thus be removed.

To demonstrate the session key distribution process, an example is given below. We consider three sensors with ID numbers 1, 2, and 3, respectively. We assume sensor 2 is compromised in session 5 and will be revoked in session 6. In the setup phase, the setup server picks the masking polynomial $h_6(x) = 1 + x^8$ for session 6 and each sensor receives a secret $h_6(1) = 2$, $h_6(2) = 257$, and $h_6(3) = 6562$, respectively. Let $K_6 = 101$, $p_6(x) = 1 + x^4$ and thus we have $q_6(x) = 100 - x^4$ and $g_6(x) = x - 2$. In session 6, the base station broadcasts a message:

$$B = \{2\} \cup \{P_6(x) = (x - 2)(1 + x^4) + 1 + x^8\}$$
$$\cup\{Q_6(x) = (x - 2)(100 - x^4) + 1 + x^8\}$$

When sensor 1 receives the message, sensor 1 calculates: $P_6(1) = 0$, $Q_6(1) = -97$ and thus $p_6(1) = 2$ and $q_6(1) = 99$. Sensor 1 computes the session key $K_6 = p_6(1) + q_6(1) = 101$; Similarly, sensor 3 calculates: $P_6(3) = 6644$, $Q_6(3) = 6581$ and thus $p_6(3) = 82$ and $q_6(3) = 19$. Sensor 3 can also compute the session key $K_6 = p_6(3) + q_6(3) = 101$. However, sensor 2 cannot calculate $p_6(2)$ and $q_6(2)$ because $g_6(2) = 0$ and thus sensor 2 cannot derive the new session key.

3.5. Broadcast Authentication

A missing link in the above scheme is how a base station broadcasts authenticated messages. In the absence of authentication of broadcast messages, an adversary can impersonate a base station and start a revocation attack. μTESLA [18] and its extensions [19,20] have been proposed to provide such services for sensor networks. We assume that a proper broadcast authentication scheme such as μTESLA is used with the KeyRev scheme. Note that to use μTESLA protocol, the sensor network should be loosely time synchronized to meet the requirements [21].

To add new nodes to the sensor network, pre-distributed key materials required by the basic random key distribution scheme and the broadcast authentication scheme must be loaded on the sensor nodes. In addition, the setup server must also load the personal secrets, $\{h_j(i)\}_{j=1,\ldots,m}$, required by the

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

session key distribution scheme, to each added sensor node.

4. Security and Performance Analysis

In this section we first discuss the security of the protocol. Then, we analyze the computation, the communication costs, and the storage requirements of the KeyRev protocol.

4.1. Security Analysis

Our proposed scheme, KeyRev, satisfies the following properties:

Property 1. The session key distribution process is secure.

The session key is distributed using the personal key distribution scheme [7]. To restore the session key, it requires some personal secret to be pre-distributed among the sensor nodes. Outsiders cannot recover the session key without the pre-distributed secret. Further, as we show in Section 3.4, the revoked sensors cannot recover the new session keys either. Thus, the session key distribution process is secure.

Property 2. The KeyRev scheme is secure in spite of the non-removal of the pre-distributed key materials at a compromised sensor node.

Although, due to the non-removal of the pre-distributed key materials, the compromised sensor may retain the pairwise keys, the adversaries cannot figure out the encryption key K_{encr} and the MAC key K_{mac} if the session key is updated. In the worst case, an adversary might use a chosen plaintext attack to crack the session key; however, the attack itself is also time consuming. As long as the duration of sessions is less than the session key cracking time, the proposed key revocation scheme is secure.

Property 3. The KeyRev scheme is immune to revocation attack assuming the base station is secure.

The KeyRev scheme depends on the base station to distribute and update the session key. Broadcast authentication schemes such as μTESLA [22] can be used to protect the authenticity of the broadcast messages. To start the revocation attack, an adversary must impersonate the base station. However, since the base station is the only one which can broadcast authenticated messages using μTESLA protocol, the compromised sensor nodes cannot be used to start the revocation attack. Thus, the KeyRev scheme is immune to revocation attack if the base station is secure.

4.2. Performance Analysis

4.2.1. Computation cost

To[Q5] restore the session key, each sensor node must evaluate the polynomial $P_j(x)$ and $Q_j(x)$ at point i. The polynomial evaluation is fast and thus the session key recovery is efficient in computation.

4.2.2. Communication cost

The performance of the KeyRev scheme depends mainly on the session key updating process. The session key can be updated in one round using broadcasting. The maximum size of the broadcast message in bits is decided by S

$$S = (5t + 2) \log q$$

Let B indicate the transmission rate of the base station, L be the maximum range between the base station and the sensor nodes. The session key distribution time can be calculated as

$$t_s = \frac{S}{B} + \frac{L}{3 \times 10^8}$$

Compared with the transmission time, the propagation delay is very small. Thus, we can approximately estimate the session key distribution time as

$$t_s \approx \frac{(5t + 2) \log q}{B}$$

4.2.3. Storage requirement

To restore the session key, each sensor node needs to be loaded with m personal secrets. Since the encryption key and the message authentication code key can be set up on the fly, the extra storage units to implement the KeyRev scheme is $m \log q$.

4.2.4. Sessions and session duration time

The lifetime of the WSN is partitioned into m sessions. m can be estimated based on the battery power and average energy consumption on the sensor nodes. Let T_{int} denote the duration of each time interval and T_{atta}

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

denote the session key cracking time required by an adversary to start a plaintext attack, we have

$$T_{\text{int}} < T_{\text{atta}}$$

Further, the distribution of a session key in each interval requires that the broadcast message is authenticated. If μTesla is used for session key broadcast authentication scheme, T_{int} must also be suitable for running a μTesla instance on a sensor node.

In addition, the duration of each session can be fixed or dynamic according to the applications. In a low compromised environment, the duration of each session can be set longer to reduce the communication overhead caused by session key distribution process. In case a compromised sensor node is detected, the session key will be updated immediately and it does not need to wait for the next session.

Overall, the KeyRev scheme is efficient in consideration of the computation load, the communication cost, and the storage space.

4.3. Comparison

The KeyRev scheme is a centralized key revocation scheme. It depends on an efficient session key distribution scheme which can be done in one round using a broadcast message (Section 3.4). Compared with the EsRev scheme, in case a sensor node is compromised, the EsRev scheme requires two rounds of communications: distributing a signature key to the non-revoked sensors, followed by broadcasting a message containing a list of revoked key identifiers. Since the signature key is distributed to the network using unicasting, the EsRev scheme may cause heavy traffic in large scale sensor networks. Note that there is no need of the unicasting and the session key can be updated in one round using broadcasting, the KeyRev scheme is much better than the EsRev scheme.

By dividing the revocation field into sub-areas and using multiple revocation messages, the GPSRRev scheme performs better than the EsRev scheme. However, additional information, such as location of the sensor nodes, must be used. Further, the multicast of the revocation message in the sub-area is implemented using message flooding and it is still time and energy consuming. The KeyRev scheme is more efficient than the GPSRRev scheme since it uses broadcast instead of multicast.

The distributed key revocation scheme, DistRev, has been regarded to be faster than the centralized key revocation schemes due to the fact that it requires only broadcast messages of a few hops that reach the local destinations [5]. However, it is not true for the KeyRev scheme. In case a sensor node is compromised and revoked successfully from the network, the DistRev scheme requires four rounds of communications:

(1) Neighboring nodes exchange the masks to decrypt the votes for the current revocation sessions at the connection time.
(2) At least t sensor nodes cast their votes against the target node (compromised node) in the current session.
(3) The voting nodes also cast their votes against the target node in the next session.
(4) If a sensor node receives at least t revocation votes, a hash value containing the compromised sensor node information needs to be broadcasted through the entire network.

Although the first three rounds of the communications are local broadcast, the last one involves a broadcast through the entire network. The broadcast message can either be flooded from the sensor node which receives t revocation votes or be forwarded to the base station and broadcasted to the network by the base station. Either way, the KeyRev scheme is much better than the DistRev scheme since it requires only one broadcast and no local communication is required. Further, the DistRev scheme is also built on some simplifying assumptions, for example, each node knows its neighboring nodes before deployment, which are hard to satisfy in many sensor network applications.

Table I compares the four revocation schemes discussed in the paper, where n is the number of sensor nodes in the network, d is the number of sub-areas in the GPSRRev scheme, and t is the number of votes which a sensor node has to collect to revoke a compromised node in the DistRev scheme. We consider

Table I. Comparison of the key revocation schemes in wireless sensor networks.[Q6]

	Scheme	Rnds	Unicast	Broadcast	Local broadcast	Scalability
I	EsRev	2	n	1	0	Low
I	GPSRRev	1	d	0	d	Medium
I	KeyRev	1	0	1	0	Good
II	DistRev	4	0	1	$2 \times t$	Good

Category I denotes centralized key revocation schemes and category II denotes distributed key revocation schemes.
Note that the GPSRRev scheme requires the location information of the compromised sensor nodes.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

the situation when a single node is compromised and revoked successfully from the network.

The comparison in Table I shows that the KeyRev scheme is better than other schemes in reducing the communication overhead caused by the revocation protocol. Note that the KeyRev scheme requires a session key to be distributed to the network during each session. The duration of the session time could be set and adjusted dynamically according to the application to reduce the background traffic in the sensor network.

5. Simulation and Results

5.1. Experimental Setting

The performance of the KeyRev scheme was evaluated in SENSIM [23], a component-based discrete-event simulator for sensor networks. Each sensor node in SENSIM consists of six components, i.e., app, net, mac, phy, event generator, and battery. In the physical component, the free space propagation model is used. In the mac component, all the packets sent to MAC layer are guaranteed to be received at the receivers. Thus, no packet collisions are considered and the performance evaluated in the simulation are under ideal conditions.

We consider two sensor network experimental settings: a small-scale sensor network with 100 nodes uniformly dispersed in a field with dimension 100 m × 100 m and a large-scale sensor network with 1000 nodes uniformly dispersed in a field with dimension 2000 m × 2000 m. In both the networks, we set the base station at the center of the field and we assume that all the sensor nodes are within reach of the base station.

We compare the KeyRev scheme with the centralized key revocation schemes, the EsRev scheme and the GPSRRev scheme. The sensor field in the GPSRRev scheme is divided into four areas as shown in Figure 1. The revocation message is sent to a sensor node in each sub-area. Then, the revocation message is multicasted to the remaining sub-area.

The evaluation metrics include the key revocation time t_v and the average energy consumption e_v per node to revoke a compromised sensor in the network. The key revocation time is the time duration from when the key revocation protocol starts until all the uncompromised sensor nodes receive the key revocation message.

We consider the KeyRev scheme operating on a finite field F_q, where q is a 56-bit integer. The polynomial

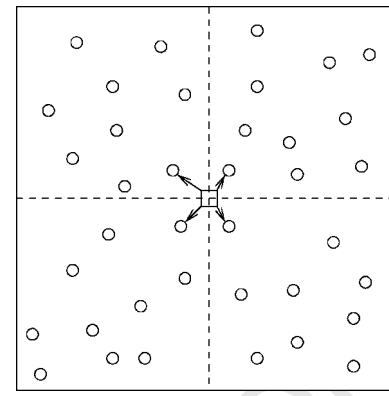

Fig. 1. Illustration of the GPSR-based revocation scheme. The revocation message is sent to a sensor node in each sub-area. Then, the revocation message is multicasted to the remaining sub-area.

Table II. Characteristic data for the Mica2 sensor platform.

Field	Value
Effective data rate	19.2 kbps
Transmit power	36 mW
Receive power	14.4 mW
Idle power	14.4 mW
Sleep	0.015 mW
Transition power	28.8 mW
Transition time	800 μs

degree t in the KeyRev scheme is set to $t = 4$. We use the simulator parameters that represent the Mica2 Mote radio characteristics. These parameters are shown in Table II. For each experimental sensor network, we randomly select one sensor to be revoked and run the simulation ten times using the same revoked sensor node. The average value is measured.

5.2. KeyRev *versus* EsRev *versus* GPSRRev

Table III shows the key revocation time to revoke a compromised sensor node in the two networks. As the table shows, in the 100-node sensor network, the key revocation time by using the EsRev scheme and the

Table III. Key revocation time.

Scheme	100-node WSN Time (s)	1000-node WSN Time (s)
EsRev	49.63	496.06
GPSRRev	1.02	4.04
KeyRev	0.59	0.62

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

Table IV. Average energy consumption per node to revoke a compromised sensor.

Scheme	100-node WSN Energy (J)	1000-node WSN Energy (J)
EsRev	0.71	7.14
GPSRRev	0.19	0.29
KeyRev	0.01	0.01

GPSRRev scheme is about 83 times and 1.6 times that of the KeyRev scheme. In the 1000-node sensor network, the key revocation time by using the EsRev scheme and the GPSRRev scheme is 800 times and 6.5 times that of the KeyRev scheme. The KeyRev scheme is much better than the EsRev scheme and the GPSRRev scheme in the key revocation time.

Table IV shows the average energy consumption to revoke a compromised sensor in the 100-node and 1000-node sensor networks. As the table shows, in the 100-node sensor network, the average energy consumption to revoke a single node by using the EsRev scheme and the GPSRRev is about 71 times and 19 times that of the KeyRev scheme. In the 1000-node sensor network, the average energy consumption to revoke a single sensor by using the EsRev scheme and the GPSRRev is about 714 times and 29 times that of the KeyRev scheme. The KeyRev scheme is much better than the EsRev scheme and the GPSRRev scheme in the average energy consumption.

In both the experimental settings, the KeyRev scheme performs very well compared with the EsRev and GPSRRev scheme. Further, Tables III and IV also show that the key revocation time and the average energy consumption to revoke a single sensor node by using KeyRev scheme have only a slight difference between the 100-node and 1000-node sensor network, which indicates that the KeyRev scheme is scalable to large-scale sensor networks. However, due to the long key revocation delay caused by the EsRev scheme, the EsRev scheme is not scalable to large-scale sensor networks. The performance of the GPSRRev scheme is better than the EsRev scheme but not as good as the KeyRev scheme.

5.3. KeyRev *versus* DistRev

To evaluate the performance of the KeyRev scheme, we also compare the KeyRev scheme with the DistRev scheme. The metrics we evaluate include the key revocation time and the average energy consumption.

Table V. The number of nodes in the covered area.

L (max-hops)	1	2	3	4	5	6
100-node WSN	100	n/a	n/a	n/a	n/a	n/a
1000-node WSN	15	44	85	142	219	299

Note: All the sensor nodes in the 100-node sensor network are in the covered area when the max-hops is set to 1.

As we discussed in Section 2.2, each revocation session in the DistRev scheme consists of three states: pending, active, and completed. The critical part of the three states which decides the key revocation time is the active state. In the active state, a sensor node casts a vote and the vote is broadcasted locally among the neighboring nodes. Assume that the active state lasts for Δ_s time for each node and Δ_c is the maximum time that a message needs to completely propagate in a local neighborhood broadcast. We have $t_v > \Delta_s$ and $\Delta_s > 2\Delta_c$ since each sensor has to vote both in the current session and on the next session. Therefore, the key revocation time t_v of the DistRev scheme is at least twice that of Δ_c, $t_v > 2\Delta_c$. Similarly, let e_{Δ_s} be the energy consumption during the active state and e_{Δ_c} be the energy consumption consumed during the Δ_c period of time, We have $e_v > e_{\Delta_s}$, $e_{\Delta_s} > te_{\Delta_c}$ (to revoke a compromised sensor node, the sensor node must receive at least t revocation votes) and thus, $e_v > te_{\Delta_c}$.

The duration of Δ_c is decided by a maximum count L (max-hops) which the vote can be broadcasted to ensure complete dissemination in the neighborhood of a compromised sensor node (four-six hops can cover this area with high probability [3]). We test the Δ_c in the 100-node and 1000-node sensor networks. The sensor node casting the vote is set to the center of each testbed. Table V shows the number of sensor nodes in the coverage area when the max-hops changes.

In the 100-node sensor network, the simulation results show that $\Delta_c = 0.035$ s and $e_{\Delta_c} = 995$ nJ. Thus, we have $t_v > 0.070$ and $e_v > 995t$ nJ. Compared with the KeyRev scheme in the 100-node sensor network as shown in Tables III and IV, the DistRev scheme might be better than the KeyRev scheme but the performance of the KeyRev scheme is also very good in the 100-node sensor network.

Figure 2 shows the key revocation time of the DistRev scheme in the 1000-node sensor network when the max-hops changes. Note that the column value is not the real key revocation time t_v of the DistRev scheme but the value of the $2\Delta_c$. The actual key revocation time is $t_v > 2\Delta_c$. The dotted horizontal line shows

UNCORRECTED PROOFS

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

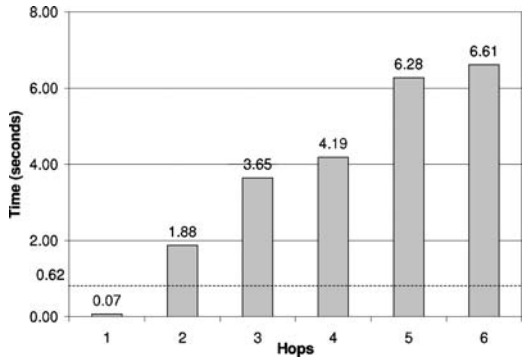

Fig. 2. Key revocation time in the 1000-node sensor network. The column value is not the real key revocation time t_v of the DistRev scheme but the value of the $2\Delta_c$.

the key revocation time of the KeyRev scheme in the 1000-node sensor network. From the figure, we can draw the conclusion that the KeyRev scheme is better than the DistRev scheme in terms of the key revocation time since the max-hops is definitely greater than one in the DistRev scheme to ensure full coverage of the neighboring nodes of the target node (compromised node).

Figure 3 shows the average energy consumption per node in the DistRev scheme in the 1000-node sensor network when the max-hops changes. The column value is also not the real average energy consumption e_v of the DistRev scheme but the value of $2e_{\Delta_c}$ (we set t to the minimum value $2, t = 2$). The actual average energy consumption is $e_v > te_{\Delta_c}$. The dotted horizontal line shows the average energy consumption of the KeyRev scheme in the 1000-node sensor network. The figure indicates that the KeyRev scheme is better than the

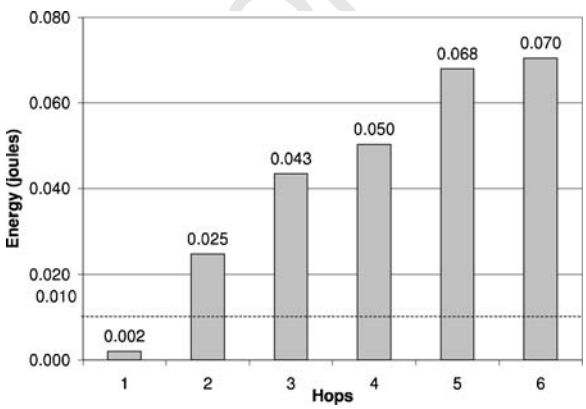

Fig. 3. Average energy consumption per node to revoke a compromised sensor in the 1000-node sensor network. The column value is also not the real average energy consumption e_v of the DistRev scheme but the value of $2e_{\Delta_c}$.

DistRev scheme even if we set the number of votes to revoke a sensor node to the minimum value of 2.

To ensure the neighborhood of the target node (compromised node) is fully covered, the max-hops cannot be set too small. Thus, our proposed scheme, KeyRev, is better than the DistRev scheme. From Figures 2 and 3, we can estimate the performance of the KeyRev scheme and the DistRev scheme. For example, if the max-hops is set to five, the key revocation time of the DistRev scheme is at least 10.1 times that of the KeyRev scheme and the average energy consumption of the DistRev scheme is at least 6.8 times that of the KeyRev scheme.

Overall, the KeyRev scheme is much better than the previously proposed centralized key revocation schemes, such as the EsRev scheme and the GPSRRev scheme. It is also superior to the distributed key revocation scheme, the DistRev scheme. The superior performance of the KeyRev protocol is due to the efficient session key distribution scheme presented in Section 3.4.

6. Conclusion and Future Work

In this paper, we proposed a key revocation scheme, KeyRev, for WSNs. Unlike most of the key revocation schemes proposed in the literature (such as References [3–5]) focusing on removing the compromised keys, our proposed scheme focuses on updating the session key and thus removing the compromised sensor nodes from the network.

Previous research on key revocation have concluded that the distributed key revocation schemes are faster than the centralized key revocation schemes. For example, Chan *et al.* in Reference [5] proposed and analyzed the security of the DistRev scheme. However, they did not evaluate its performance. In this paper, we evaluated and estimated the minimum value of the key revocation time and the average energy consumption of the DistRev scheme. To the best of our knowledge, this is also the first paper which evaluates the performance of a distributed key revocation protocol in a WSN. We found that our proposed centralized scheme, KeyRev, is much better than the distributed key revocation scheme proposed in Reference [5]. It goes counter to the conclusion in the paper [5] which claims that the distributed key revocation scheme has better performance than any centralized key revocation scheme.

As the simulation results show, the performance of the KeyRev scheme is much better than that of other

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

CORRECTED PROOFS

revocation schemes and the KeyRev scheme is also scalable to large-scale sensor networks. The KeyRev scheme depends on an effective session key distribution scheme in the network, which is currently based on the personal key share distribution scheme proposed in Reference [7]. However, the KeyRev scheme does not need to use the personal key share distribution scheme. The session key distribution and revocation scheme can be replaced by other secure group communication schemes [24]. Further investigation on different session key distribution schemes will be conducted in the future.

Further, the KeyRev scheme is a centralized revocation scheme and the base station is the single point of failure. A distributed key revocation scheme might be still attractive due to the avoidance of single points of failure. The integration of both centralized and distributed key revocation scheme merits is under further investigation. In addition, the proposed scheme assumes that all the sensor nodes are within the reach of the base station. In case sensor nodes might not be reached by the base station directly, the proposed scheme does not work properly. In this situation, multiple base stations can be deployed in the network to ensure that each sensor node can be reached by a base station [25].

Finally, the KeyRev scheme depends on a globally distributed session key in the network, which requires the sensor network to be synchronized. Since most broadcast authentication schemes, such as μTesla, require the synchronization of all sensor nodes in the network, it is not a problem if such broadcast authentication schemes are used. Our future work will extend the framework to scenarios where the sensor network is not synchronized.

Acknowledgements

This work is partially supported by NSF Grant No. CCR-0311577.

References

1. Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys and Tutorials* 2006; **8**(2): 2–23.
2. Zhu S, Setia S, Jajodia S. LEAP: efficient security mechanisms for large-scale distributed sensor networks. In *CCS '03: Proceedings of the 10th ACM conference on Computer and Communications Security*. ACM Press: New York, NY, USA, 2003; 62–72.[Q7]
3. Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM Press: New York, NY, USA, 2002; 41–47.
4. Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2003, 197–213.
5. Chan H, Gligor V, Perrig A, Muralidharan G. On the distribution and revocation of cryptographic keys in sensor networks. *IEEE Transactions on Dependable and Secure Computing* 2005; **2**(3): 233–247.
6. Wang Y, Ramamurthy B, Zou X. KeyRev: an efficient key revocation scheme for wireless sensor networks. In *ICC '07: Proceedings of IEEE International Conference on Communications*, Glasgow, Scotland, UK, June 2007, 1260–1265.
7. Liu D, Ning P, Sun K. Efficient self-healing group key distribution with revocation capability. In *CCS '03: Proceedings of the 10th ACM Conference on Computer and Communications Security*. ACM Press: New York, NY, USA, 2003; 231–240.
8. Cametepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. In *Proceedings of 9th European Symposium on Research Computer Security*, Sophia Antipolis, France, 2004, 346–358.
9. Pietro RD, Mancini LV, Law YW, Etalle S, Havinga PJM. LKHW: a directed diffusion-based secure multicast scheme for wireless sensor networks. In *ICPPW '03: Proceedings of the 32nd International Conference on Parallel Processing Workshops*. IEEE Computer Society Press, 2003; 397–406.[Q8]
10. Du W, Deng J, Han YS, Chen S, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge. In *Proceedings of IEEE INFOCOM*, 2004, 586–597.
11. Camtepe SA, Yener B. Key distribution mechanisms for wireless sensor networks: a survey. *Technical Report TR-05-07*, Computer Science Department at RPI, 2005.[Q7]
12. Zhu S, Setia S, Jajodia S, Ning P. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2004, 259–271.
13. Ye F, Luo H, Lu S, Zhang L. Statistical en-route filtering of injected false data in sensor networks. In *Proceedings of IEEE INFOCOM*, 2004, 839–850.
14. Wang G, Zhang W, Cao C, Porta TL. On supporting distributed collaboration in sensor networks. In *Proceedings of MILCOM*, 2003, 752–757.
15. Zhang W, Song H, Zhu S, Cao G. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *MobiHoc '05: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM Press: New York, NY, USA, 2005; 378–389.
16. Karp B, Kung HT. GPSR: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*. ACM Press: New York, NY, USA, 2000; 243–254.
17. Shamir A. How to share a secret. *Communications of the ACM* 1979; **22**(11): 612–613.
18. Przydatek B, Song D, Perrig A. SIA: secure information aggregation in sensor networks. In *SenSys '03: Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*. ACM Press: New York, NY, USA, 2003; 255–265.
19. Liu D, Ning P. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In *Proceedings of the 10th Annual Network and Distributed System Security Symposium*, San Diego, CA, USA, February 2003, 263–276.[Q7]

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

UNCORRECTED PROOFS

20. Liu D, Ning P. Multi-level μTESLA: broadcast authentication for distributed sensor networks. *Transactions on Embedded Computing System* 2004; **3**(4): 800–836.
21. Liu D, Ning P, Zhu S, Jajodia S. Practical broadcast authentication in sensor networks. In *MobiQuitous '05: Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, San Diego, CA, USA, July 2005, 118–129.
22. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD. SPINS: security protocols for sensor networks. *Wireless Networks* 2002; **8**(5): 521–534.
23. Wang Y, Ramamurthy B. SENSIM: SEnsor Network SIMulator (Version 0.1). August 2006. Available Online at: http://cse.unl.edu/∼ywang/sensim.htm
24. Zou X, Ramamurthy B, Magliveras SS. *Secure Group Communications Over Data Networks*. Springer, 2005.
25. Wang Y, Ramamurthy B, Xue Y. A key management protocol for wireless sensor networks with multiple base stations. In *ICC '08: Proceedings of IEEE International Conference on Communications*, Beijing, China, June 2008, 1625–1629.

UNCORRECTED PROOFS

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/sec

Author Query Form (SEC/89)

Special Instruction: Author please include responses to queries with your other corrections and return by e-mail.

Q1: Author: Please check the suitability of suggested short title.
Q2: Author: Please ensure that author names are in the order forename/surname.
Q3: Author: Please check the affiliations.
Q4: Author: Please check the change made.
Q5: Author: Please check the presentation of headings.
Q6: Author: Please check the presentation of table.
Q7: Author: Please check the presentation.
Q8: Author: Please provide publisher location.

UNCORRECTED PROOFS