SECURITY SCHEMES FOR WIRELESS SENSOR NETWORKS WITH MOBILE SINK

A Dissertation

by

AMAR ADNAN RASHEED

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2010

Major Subject: Computer Science

SECURITY SCHEMES FOR WIRELESS SENSOR NETWORKS WITH MOBILE SINK

A Dissertation

by

AMAR ADNAN RASHEED

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Rabi N. Mahapatra
Committee Members,	Eun Jung Kim
	Dezhen Song
	Deepa Kundur
Head of Department,	Valerie E. Taylor

May 2010

Major Subject: Computer Science

ABSTRACT

Security Schemes for Wireless Sensor Networks with Mobile Sink. (May 2010)

Amar Adnan Rasheed, B.S., University of Baghdad;

M.S., Northeastern Illinois University

Chair of Advisory Committee: Dr. Rabi N. Mahapatra

Mobile sinks are vital in many wireless sensor applications for efficient data collection, data querying, and localized sensor reprogramming. Mobile sinks prolong the lifetime of a sensor network. However, when sensor networks with mobile sinks are deployed in a hostile environment, security became a critical issue. They become exposed to varieties of malicious attacks. Thus, anti threats schemes and security services, such as mobile sink's authentication and pairwise key establishment, are essential components for the secure operation of such networks.

Due to the sensors, limited resources designing efficient security schemes with low communication overhead to secure communication links between sensors and MS (Mobile Sink) is not a trivial task. In addition to the sensors limited resources, sink mobility required frequent exchange of cryptography information between the sensors and MS each time the MS updates its location which imposes extra communication overhead on the sensors.

In this dissertation, we consider a number of security schemes for WSN (wireless sensor network) with MS. The schemes offer high network's resiliency and low communication overhead against nodes capture, MS replication and wormhole attacks.

We propose two schemes based on the polynomial pool scheme for tolerating nodes capture: the probabilistic generation key pre-distribution scheme combined with polynomial pool scheme, and the Q-composite generation key scheme combined with polynomial pool scheme. The schemes ensure low communication overhead and high resiliency.

For anti MS replication attack scheme, we propose the multiple polynomial pools scheme that provide much higher resiliency to MS replication attack as compared to the single polynomial pool approach.

Furthermore, to improve the network resiliency against wormhole attack, two defensive mechanisms were developed according to the MS mobility type. In the first technique, MS uses controlled mobility. We investigate the problem of using a single authentication code by sensors network to verify the source of MS beacons, and then we develop a defensive approach that divide the sensor network into different authentication code's grids. In the second technique, random mobility is used by MS. We explore the use of different communication channels available in the sensor hardware combined with polynomial pool scheme.

To my parents

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisor Dr. Rabi N. Mahapatra for his continuous support and guidance throughout the course of my research. Without his help, this work would not be possible.

I also would like to thank my committee members, Dr. Eun Jung Kim, Dr. Dezhen Song, and Dr. Deepa Kundur, for spending their invaluable time reviewing my dissertation and for suggesting improvements.

Finally, thanks to my mother and father for their encouragement, patience and love.

TABLE OF CONTENTS

CHAPTER Page

LIST OF FIGURES

FIGURE Page

FIGURE Page

FIGURE Page

FIGURE Page

LIST OF TABLES

CHAPTER I

INTRODUCTION

Mobility is exploited in the field of wireless sensor network [1], [2], [3], [4] to circumvent multi-hop relaying and to reduce energy consumption [5], [6], [7], [8], [9] at nodes near the base station, and hence elongate the lifetime of the network. Mobile elements already exist in the deployment environment; a network node can be attached to these mobile elements for data collection [10], [11], [12], [13], [14], [15]. Otherwise, mobile elements are part of the network infrastructure itself and can be controlled by the network [16], [17], [18], [19], [20], [21]. There exist a number of sensor networks applications that use mobile sinks in their operations, such as data collections in hazardous environments, localize reprogramming, and military navigation. Due to the their operating nature, they often left unattended, hence prone to different kinds of malicious attacks such as the S*ybil* attacks [22], [23], [24], *clone* attacks [25], [26], *node replication* attacks [27], [28], [29], [30], [31], *mobile sink replication* attacks, and *wormhole* attacks. Thus, security services, (such as authentication and pairwise key establishment), and countermeasure attacks are vital.

In this dissertation, we examine two security challenges for sensor network with MS: one security challenge is to cultivate efficient security schemes with low communication overhead that use authentication and pairwise keys establishment between sensors

---

This dissertation follows the style *IEEE Transactions on Parallel and Distributed Systems*.

and MS to tolerate nodes capture and *mobile sink replication* attack. Since to establish secure links with the MS, frequent exchange of cryptography information between the sensors and MS are required each time the MS update its location which imposes extra communication overhead on the constrained resources sensors unlike sensor network with a fixed localized sink. Where after deployment, sensors and the sink exchange cryptography information only once to establish a securely connected network. The other challenge is to develop security techniques that are based on key pre-distribution schemes to provide network's resiliency against *wormhole* attack.

Throughout this dissertation, we propose a number of security schemes for wireless sensor network with MS that addresses the above security challenges and how our proposed security based key pre-distribution schemes furnish better network resiliency against nodes capture, *mobile sink replication*, and *wormhole* attacks compared to a number of existing schemes for sensor networks with fixed localized sinks.

Finally, we propose an energy-efficient hybrid data collection architecture [21] based on controllably mobile infrastructure for a class of applications in which sensor networks provide both low-priority and high-priority data. High-priority data require a data delivery scheme with low latency and high fidelity. Meanwhile low-priority data may tolerate high-latency data delivery.

A. SECURITY SCHEMES FOR TOLERATING NODES CAPTURE AND MOBILE SINK REPLICATION ATTACK

Security schemes that provide authentication and pairwise keys establishment between communicating nodes have been widely studied in general network environments. These security schemes were widely known as *general key agreement schemes,* they usually offer network tolerance to nodes capture. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The *trusted-server scheme* depends on a trusted server for key agreement between nodes. This type of scheme is not suitable for sensor networks because there is no trusted infra-structure in sensor networks. The *self-enforcing scheme* depends on asymmetric crypto-graphy, such as key agreement using public key certificates. However, limited computa-tion and energy resources of sensor nodes often make it undesirable to use public key algorithms. The third type of key agreement scheme is key pre-distribution [32], [33], [34], [35], [36], [37], [38] where key information is distributed among all sensor nodes prior to deployment.

The simplest key pre-distribution scheme is to use a global pre-shared among the MS and sensor nodes. This scheme offer very low network resiliency to nodes capture and *mobile sink replication* attack. Since the capture of a single sensor will lead an at-tacker to get hold of the pre-shared key and then be able to lunch a wide range network *mobile sink replication* attack. A more robust scheme against nodes capture had been proposed by Eschenauer and Gilgor [32], it called the probabilistic key pre-distribution scheme. The main idea was to let each sensor node randomly pick a set of keys from a

key pool before deployment so any two sensors have a certain probability of sharing at least one common key. Chan et al. [33], [34] further extended this idea and developed two key pre-distribution schemes: *Q*-composite key pre-distribution scheme and random pairwise keys scheme. The *Q*-composite key pre-distribution scheme also uses a key pool but requires two sensor nodes compute a pairwise key from at least *Q* pre-distributed keys they share. The random pairwise keys scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key. Both schemes improve the security over the basic probabilistic key pre-distribution scheme.

The main drawbacks in both the probabilistic key pre-distribution scheme and the *Q*-composite scheme are high communication overhead and as the number of compromised nodes increases, the fraction of affected pairwise keys increases quickly As a result, a small number of compromised nodes may affect a large fraction of pairwise keys and will then lead to a large scale *mobile sink replication* attack.

An enhanced scheme using the *t*-degree bivariate key polynomial was proposed by Liu and Ning [35]. They develop a general framework for pairwise key establishment using polynomial pool-based key pre-distribution protocol [38] and the probabilistic key distribution in [32], [34]. Their scheme provides higher network's resiliency to nodes capture compared to the global pre-shared key, the probabilistic key pre-distribution scheme [32], and the *Q*-composite scheme [34], it can only tolerate no more than *t* compromised nodes, where the value of *t* is limited by the memory available in sensor nodes. Therefore, we consider the *polynomial pool-based key pre-distribution scheme* as the

basic component in our proposed schemes for network resiliency and low communication overhead against nodes capture and *mobile sink replication* attack.

In this dissertation, we contemplate two security schemes for tolerating nodes capture: the *probabilistic generation key pre-distribution scheme combined with polynomial pool scheme,* and the *Q-composite generation key scheme combined with polynomial pool scheme* [39], [40]. These schemes enable a mobile sink to establish a secure data communication link with any sensor nodes on the fly and with low communication overhead. The two proposed schemes are based on the polynomial pool-based key pre-distribution scheme, the probabilistic generation key pre-distribution scheme, and the *Q*-composite scheme. The security analysis in this dissertation indicates that these two schemes assures, with high probability and low communication overhead, that any sensor node can establish a pairwise key with the mobile sink. Finally, we compare the two proposed key pre-distribution schemes with the *Q*-composite scheme, the probabilistic key pre-distribution scheme, and the polynomial pool-based scheme, our analytical results clearly show that our schemes perform better in terms of network resilience to nodes capture than existing schemes if used in wireless sensor network with mobile sink.

For the anti *mobile sink replication* attack scheme, we propose a scheme called the *three-tier security scheme.* In this new security framework [41], [42], A small fraction of pre-selected sensor nodes, called the *stationary access nodes*, act as authentication access points to the network and to trigger sensor nodes to transmit their aggregated data to mobile sinks. A mobile sink sends *data request* messages to sensor nodes via a *stationary access node*, these mobile sink *data request* messages will initiate the *statio-*

nary access node to trigger sensor nodes to transmit their data to the requested mobile sink. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. The mobile Polynomial pool used for authentication and keys setup between mobile sinks and *stationary access nodes*. The static polynomial pool is used for authentication and pairwise key establishment between sensor nodes and *stationary access nodes.*

B. ANTI WORMHOLE ATTACK SCHEMES

A wormhole attack is very difficult to detect, because it can be launched without compromising either the host or the integrity and authenticity of the communication network [43], [44], [45].

Y. Hu, A. Perrig, and D. Johnson describe a solution for the threat of a wormhole attack, based on geographical and temporal packet leashes. The use of geographical leashes assumes knowledge of the node location. The use of temporal leashes requires all nodes to have tightly synchronized clocks and demands computational power, which according to the authors, is beyond the capability of sensors [43]. S. Capkun, L. Buttyan, J. Hubaux in [44], and Y. Hu, A. Perrig and D. Johnson in [43] propose a defense against wormhole attacks based on measurement of the time of flight of a message in a challenge–reply scheme. Such a scheme assumes that sensors are able to execute time measurements of nanosecond precision and, hence, this scheme requires very accurate clocks at each sensor. In addition, distance estimates based on the time of flight are sensitive to distance-enlargement errors.

All the above anti-wormhole attack solutions were implemented on sensor networks with static nodes. In this study, we propose two techniques that are suitable only for sensor networks with MS using random or control mobility to collect sensors data. The first technique was based on wireless sensor network that use a mobile sink to collect data along a pre-determine path [46]. We propose an efficient security scheme, which divides the sink's data collection path into grids, sensors in each grid, uses secret keying information and collision-resistant hash functions to authenticate the source of beacons. Through probabilistic analysis and definitive simulation, the proposed scheme shows with 60% of the grids under wormhole attacks, the probability that a node reply to a malicious beacon is 0.1. The second technique was design for sensor network with MS that uses random mobility for data gathering [47]. The proposed technique uses the polynomial pool-based key pre-distribution scheme [35] and the multiple channels available on the sensor hardware. It allows the MS to establish a direct secure link with any sensor node and over a communication channel randomly selected from a set of *c* available channels. Through quantitative analyses, it is shown that even when 50% of a sensor node's neighbors are malicious devices, the provision of one extra available channel for communication with the mobile sink reduces the probability of a wormhole attack to almost zero.

C. AN ENERGY-EFFICIENT DATA COLLECTION SCHEME IN WSN WITH MS

Our approach exploits the design of a network that supports a hybrid data delivery scheme to enhance the network performance and reduces total network energy usage

[21]. In our system design two delivery schemes are deployed for purposes of comparison. The first is the traditional ad hoc approach to deliver high-priority data with high fidelity and low latency. The second presents a controllable infrastructure in the sensor field, which acts as low-priority data collection agent. Through simulations, we show that our proposed approach can provide substantial energy saving in this class of sensor application compared to the traditional multi-hop approach used alone.

CHAPTER II

KEY PRE-DISTRIBUTION SCHEMES FOR TOLERATING NODES CAPTURE IN SENSOR NETWORK WITH MS

In this chapter, we propose two key pre-distribution schemes for tolerating nodes capture in wireless sensor network with MS. In the predicating of our security schemes, we exploit the use of either the probabilistic generation key pre-distribution scheme [48] or the Q-composite scheme [34] in conjunction with the polynomial pool-based key pre-distribution scheme [35] to establish a secure link between a mobile sink and a sensor node and improve the network resilience to nodes captures. First, we propose a scheme that combines the polynomial pool-based key pre-distribution [35] with the probabilistic generation key pre-distribution scheme [48] to establish a pairwise key between mobile sink and any sensor node. Second, we develop a scheme that uses the Q-composite scheme in conjunction with polynomial pool-based scheme. Prior to network deployment, every sensor node is pre-loaded with polynomial shares of a randomly selected subset of s polynomials out of $|S_p|$ polynomials, called the *polynomial ring*. In addition, every sensor node is pre-loaded with a randomly selected subset of k ($k \leq s$) generation keys out of $|S_k|$ generation keys, called the *generation key ring.* The mobile sink is pre-loaded with a randomly selected subset of s polynomial out of $|S_p|$ and a large subset of m ($m >> k$) generation keys out of $|S_k|$. Having a large a number of generation key in the mobile sink ensure that both the mobile sink and a sensor node share at least one generation key with high probability. The two proposed schemes guarantee that any sensor

node can establish a pairwise key with a mobile sink with high probability and without sacrificing security. Security analyses indicate that the two schemes provide a higher probability for non-compromised sensors to establish a secure communication with the mobile sink than previous schemes [34], [35], [48].

The rest of this chapter is organized as follows. Section A presents related works. Section B gives an overview of the polynomial pool-based scheme. Sections C & D presents the two proposed key pre-distribution schemes. Section E concludes the chapter.

A. RELATED WORK

Eschenauer and Gligor [32] proposed the first key pre-distribution scheme for sensor networks, which we will call it the random key distribution scheme. In this scheme, a large pool of random keys is generated at the server prior to the network deployment. For each sensor node, the server randomly selects a subset of keys, called the key ring. Two sensor nodes that share at least one common key in their key rings are able to establish a secure link. Nodes that cannot establish a secure link directly might engage in a key path discovery scheme.

In the previous scheme, the capture of a node may lead to compromising a link between two non-captured nodes, since these two nodes may have use the same key to secure their communication. To reduce the fraction of compromised links between non-compromised nodes, a modification to the random key scheme, called the Q-composite scheme, is presented in [34]. The authors of this scheme proposed that in order for two

nodes to establish a secure communication link, they are required to share at least Q common keys in their key rings. The secret common key is the hash of the Q common keys.

Hussain, Kausar, and Masood [48] proposed a probabilistic generation key pre-distribution scheme based on the random key distribution for heterogeneous sensor networks. In a key generation process, instead of generating a large pool of random keys, a key pool is represented by a small number of generation keys. They assume the network consists of a small number of powerful nodes, called H-sensors, and a very large number of low-end sensors (L-sensors). The L-sensors have very limited computation, communication, energy supply, and storage capability; the H-sensors have more storage, computation, and storage capability. Prior to the network deployment, the setup server generates a pool of random generation key. By applying a hash algorithm on each generation key and publicly known seed value, key chains are generated. Every key chain has its unique ID. The total number of key chains forms complete key pool. The setup server assigns each L-sensor r random generation keys. From these random generation keys, $r \times N$ random keys can be calculated effectively. Each H-sensor is pre-loaded with M randomly selected generation keys, where $M >> r$.

Another type of general networks cryptographic algorithms is called the threshold cryptography. This scheme was first proposed in [49] and further investigated in [38]. Such a scheme, in which every sensor node is pre-loaded with coefficients of a symmetric bivariate polynomial evaluated at one of its variables using its ID value, The symmetry property of a polynomial allows every node to establish a pairwise key with

every neighbor node or any node in the network evaluated at their ID values. For an adversary to compromise a communication link between two non-compromised nodes, he/she must capture at least a certain number of sensors to reconstruct the bivariate polynomial from its shares stored in the nodes and break the system. For a polynomial of degree *t*, the scheme provides unconditional secrecy if no more than *t* sensors collude. Liu and Ning [35] developed a general framework for pairwise key establishment based on the polynomial-based key pre-distribution protocol [38] and the probabilistic key distribution in [32], [34]. Their scheme shows that when the fraction of captured nodes is less than 60%, it provides a significantly higher probability for non-compromised sensors to establish secure communication links than the previous methods. Moreover, unless the number of compromised nodes sharing a common polynomial exceeds a threshold.

B. OVERVIEW OF THE POLYNOMIAL POOL-BASED KEY PRE-DISTRIBUTION SCHEME

In this section, we briefly review the polynomial pool-based key pre-distribution scheme. The key setup server randomly generates bivariate *t*-degree polynomials with coefficients over a finite field $GF(\lambda)$, where λ is a prime number large enough to accommodate a cryptographic key. Such that the polynomials have the property of $f(x,y) = f(y,x)$.

$$f(x,y) = \sum_{0 \le i,j \le t} a_{ij} x^i y^j, \text{ where } a_{ij}=a_{ji.}$$

To identify the different polynomials, the setup server may assign each polynomial a unique id, namely ID. For every sensor node u, the setup server chooses a subset of n polynomials from the polynomial pool and assigns shares of these n polynomials to node u. For each polynomial share of $f_{ID}(x, y)$, pre-loaded in sensor node u, the setup server computes $f_{ID}(u, y)$. For any two sensor nodes, u and v, node u computes the key $f_{ID}(u,v)$ at each of its randomly assigned shared polynomials by evaluating $f_{ID}(u, y)$ at point v. Node v can compute its key $f_{ID}(v,u)$ by evaluating $f_{ID}(v, y)$ at point u. If the two nodes can successfully establish a common key, there is no need to start path key establishment. Otherwise, sensors start path key establishment, trying to establish a pairwise key with the help of other intermediate nodes.

C. PROBABILISTIC GENERATION KEY PRE-DISTRIBUTION SCHEME COMBINED WITH THE POLYNOMIAL POOL-BASED SCHEME

We assume a typical sensor network that has hundreds to several thousands of low-cost, power-constrained, limited-computation power and storage capability nodes. Sensor nodes conserve communication energy by aggregating the data in their internal buffer. The network has a high-end mobile sink. The mobile sink is more powerful than any sensor. It has more computation, communication, energy supply, and storage capability. It acts as an agent to collect sensor readings. Every sensor node is able to store up to 210 keys; however, a MS is capable of storing up to 1,200 keys.

The key establishment patterns for a secure link between a node and the MS falls into two categories: direct and indirect MS-sensor path key establishment. In direct key

establishment, the mobile sink and the sensor share at least a common bivariate polynomial and at least one common generation key. In MS-sensor path key establishment, MS and a sensor node *u* try to establish a pairwise key with the help of an intermediate node *i*. Node *i* must shares a pairwise key with both the MS and sensor node *u*. Node *i* randomly generates a new shared key that will be sent directly to MS and indirectly to node *u* over the secure path *i*—MS—*u*.

In this chapter, we are considering a large sensor network (>1,000 sensor nodes) with a communication range (>30 neighboring nodes within the communication range).

The basic idea of our scheme [39], [40] can be described as the combination of polynomial pool-based key pre-distribution [35] and the probabilistic generation key pre-distribution scheme [48]. The general framework of the proposed scheme consists of three phases:

*Polynomial and generation key subsets assignments***:** Initially, the setup server separately generates two pools, a pool of $|S_p|$ random bivariate polynomials, each with a unique id namely ID_p and of degree-*t*, and a pool of $|S_k|$ random generation keys each with a unique id namely ID_{gk}. Prior to network deployment, for every sensor node *u*, the setup server randomly picks a subset of *s* polynomials out of $|S_p|$ and assigns polynomial shares of these *s* polynomials to the sensor node. In addition, for every sensor node *u*, the setup server randomly selects a subset of *k* ($k \le s$) generation keys out of $|S_k|$ and assigns them to the sensor node *u*. From these *k* generation keys, $k \times C$ random keys can be calculated effectively, where *C* is the total number of keys generated independently via a

unique generation key g_i and publicly known seed S. By applying a keyed hash algorithm repeatedly [50], the n-th key using a generation key g_i, and a publicly known seed S is computed as:

$$K=Hash^{n}(S, g_i) \quad (2.1)$$

For the MS, the setup server picks randomly a subset of m ($m >> k$) generation keys out of $|S_k|$, and a subset of s polynomials out of $|S_p|$. Having a large number of generation keys in the mobile sink guarantee that MS can discover a single common generation key with a sensor with high probability. The MS can establish a pairwise data-communication key with any sensor node on the fly. If the MS and a sensor node share at least one generation key and a common bivariate polynomial, the two can establish a secure data-communication link directly. However, if the MS and the sensor node do not share sufficient bivariate polynomials, the MS and the sensor node start a MS-sensor path key discovery, trying to establish a pairwise data-communication key with the help of other nodes.

*Mobile sink-sensor direct key establishment***:** In the case of establishing a secure MS-sensor link dynamically between MS and any node u within its communication range. First, MS and a sensor u need to discover that both have the polynomial shares of a common polynomial. The MS broadcasts hello messages containing the MS id (ID_{ms}). Sensor node u within the MS range that heard the MS's hello message can compute its keys by evaluating each of its assigned polynomial shares $f_{ID}(u, y)$ at point ID_{ms}. The sensor node u sends one message for each computed s key containing the ID of the node and s client puzzles. One such client puzzle is the Merkle puzzle [51]. If the MS re-

sponds with the correct answer to at least one client puzzle, it is thus identified as having the same polynomial shares of a common polynomial. Second, after discovering a shared polynomial between MS and the sensor node *u*, the MS broadcast messages which contain a randomly generated number *n* where $[0 \leq n \leq C]$, if node *u* heard the MS message, then for each pre-loaded generation key, and a publicly known seed S, *u* can compute its n-th keys as in (1). For discovering that both *u* and the MS share at least a common generation key, node *u* uses the same method (Merkle puzzle [51]).

After the shared polynomial and the shared generation key discoveries, a new MS-sensor data-communication link key K_d is generated as the hash of the key evaluated from the shared polynomial and the key computed from the shared generation key. MS-sensor key-setup is not performed between the MS and any node if at least the two do not share a common generation key or do not have the polynomial shares of a common polynomial.

*Mobile sink-sensor path key discovery***:** This phase occur between a sensor node and the MS. If the MS fails to establish a MS-sensor secure link directly, then it must start the MS-sensor path key discovery phase. In this phase, MS needs to discover an intermediate node that share a common polynomial with MS and a common polynomial with the destination node. We consider that MS can find a common generation key with the destination node with high probability (0.99). To establish a MS-sensor pairwise key with a destination node Y, MS needs to find a secure MS-sensor path through some intermediate nodes along the path, which can establish secure MS-sensor pairwise keys directly with both the MS and the destination node Y. MS broadcasts a request message,

which includes two lists of polynomial IDs. One polynomial ID list is for the MS. The other list is for the destination node Y. For any two sensor nodes want to establish a common key, both must discover that they share at least a common polynomial only. If an intermediate node *v* receives this request message is able to establish a common key with both of MS and the destination node Y, it replies with a message that contains two encrypted copies of a randomly generated key K_c: one encrypted by the pairwise key with the MS; the other by the pairwise key with the destination node. Both MS and Y can get the new key K_c from this message. The new MS-sensor data-communication link key is the hash value of K_c and the key computed form the shared generation key between MS and node Y.

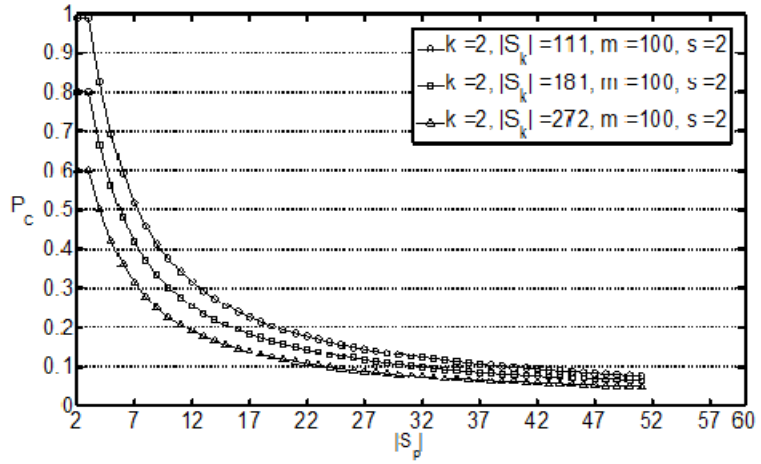
1. Security Analysis

Similar to the analysis in [35] and [48], the probability *p* that both the MS and a sensor node *u* share the same bivariate polynomial is the probability that the two can establish MS-sensor polynomial-based secure link directly, and can be estimated by

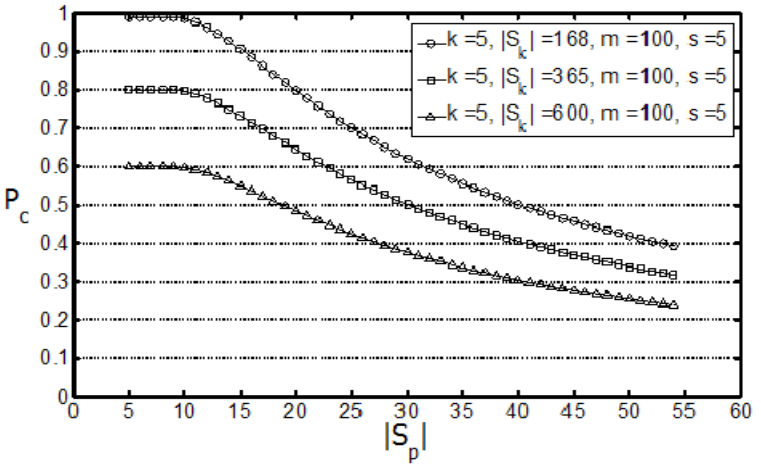
$$p = 1 - \frac{\binom{|S_p|}{2s} \cdot \binom{2s}{s}}{\binom{|S_p|}{s}^2} \tag{2.2}$$

The probability *q*, that both MS and a sensor node *u* have a common generation key in their generation keys rings is the probability that both MS and node *u* can establish a MS-sensor random key-based secure link, and can be computed as

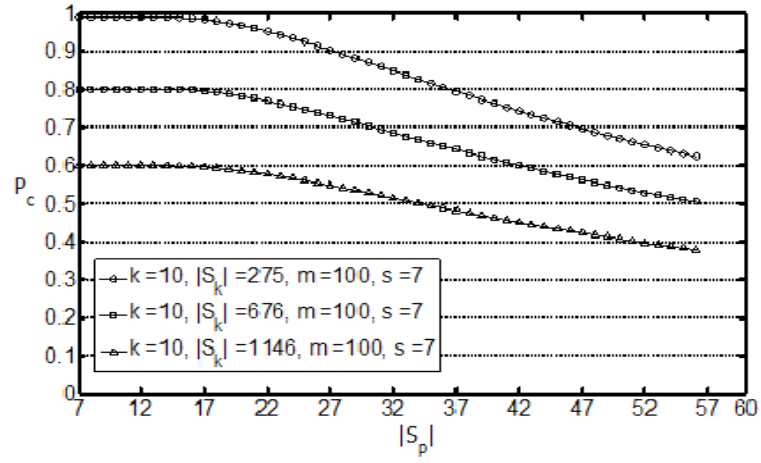
$$q = 1 - \frac{\binom{|S_k| - k}{m}}{\binom{|S_k|}{m}} \tag{2.3}$$



(a)



(b)



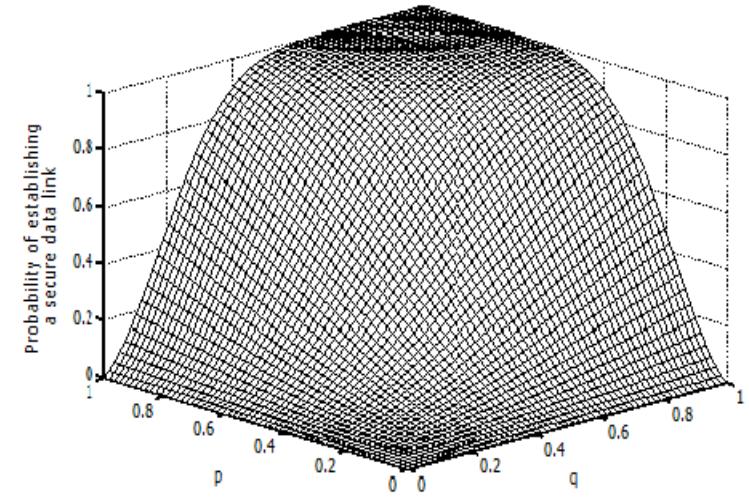
(c)

Fig. 1. The probability p_c that MS can establish a secure data link with any node vs. the size of the polynomial pool and combinations of k, $|S_k|$, and s

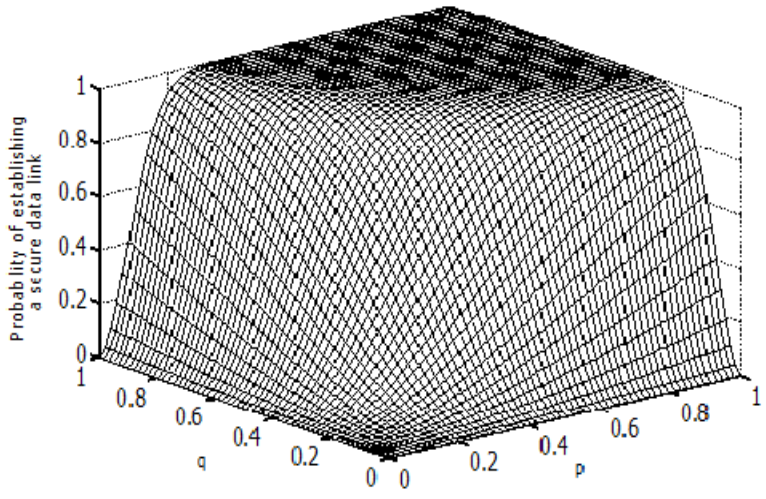
As described earlier, if a direct secure data-communication key K_d is generated as the hash of the polynomial-based key and the random key-based key, then the probability P_c that MS can establish a secure data-communication key K_d with any node is $P_c=pq$. Fig. [1(a), 1(b), and 1(c)] show the relationship between P_c and the combinations of k, $|S_k|$, s, and $|S_p|$. To predict that with high probability that MS shares at least a common generation key with any sensor node within its range, we assume MS to be pre-loaded with large number of generation keys ($m >> k$). However, MS is pre-loaded with the same number of bivariate polynomials as any sensor node in the network (s =2), the probability that both MS and any sensor node in its range have the same bivariate polynomials is low. It is easy to see that the closer s and $|S_p|$, the more likely that MS and a sensor node can establish a pairwise key.

Now we consider the probability that both MS and a sensor node can establish a data-communication key through MS-sensor direct establishment and MS-sensor path key discovery. Let d denote the average number of sensor nodes within the MS data communication range. If MS needs to establish a secure data-communication key directly or indirectly with any of the d nodes, for example node u, let us consider any of the remaining d-1 nodes. The probability that it shares a pairwise key with both MS and node u, is qp^2. Both MS and node u can establish a common data-communication key as long as one of the d-1 nodes can act as an intermediate node. Then the probability that MS and node u establishing a pairwise data-communication key (directly or indirectly) is $P_d=1-(1-pq)(1-p^2q^2)^d$. Fig. [2(a) and 2(b)], presents the relationship between P_d and the combinations of p, q and d. We investigate the security resilience of our proposed

scheme against node compromise attack. We assume an attacker randomly compromised x sensor nodes. For each compromised node, the attacker can obtain k generation keys. The probability that a given generation key is not chosen by a non-compromised node is



(a) $d = 10$



(b) $d = 60$

Fig. 2. The probability P_d of establishing a secure data link with MS vs. combinations of p, q and d

(1- $k/|S_k|$). If there are x compromised nodes, the probability that a given generation key is not compromised is (1- $k/|S_k|)^x$. The expected fraction of total generation keys compromised is thus

$$P_{kc} = 1 - \left(1 - \frac{k}{|S_k|}\right)^x \tag{2.4}$$

In the case of the captured bivariate polynomials of degree t, the attacker cannot determine the non-compromised polynomial-based key if he/she has captured no more than t sensors. Similar to the analysis in [35], let us assume the case where the number of compromised sensors $x > t$. The probability of any polynomial being chosen for a sensor node is ($s/|S_p|$), and the probability of this polynomial being chosen exactly j times among x sensor nodes is

$$P(j) = \binom{x}{j} \cdot \left(\frac{s}{|S_p|}\right)^j \cdot \left(1 - \frac{s}{|S_p|}\right)^{x-j} \tag{2.5}$$

Thus the probability of polynomial-based key being compromised between non-compromised sensors is

$$P_{pc} = 1 - \sum_{j=0}^{j=t} p(j) \tag{2.6}$$

From equations (2.4) and (2.6), the probability that a data communication link between MS and any non-compromised sensor node being compromised is

$$P_{pk} = \left(1 - \sum_{j=0}^{j=t} p(j)\right) \cdot \left(1 - \left(1 - \frac{k}{|S_k|}\right)^x\right) \tag{2.7}$$

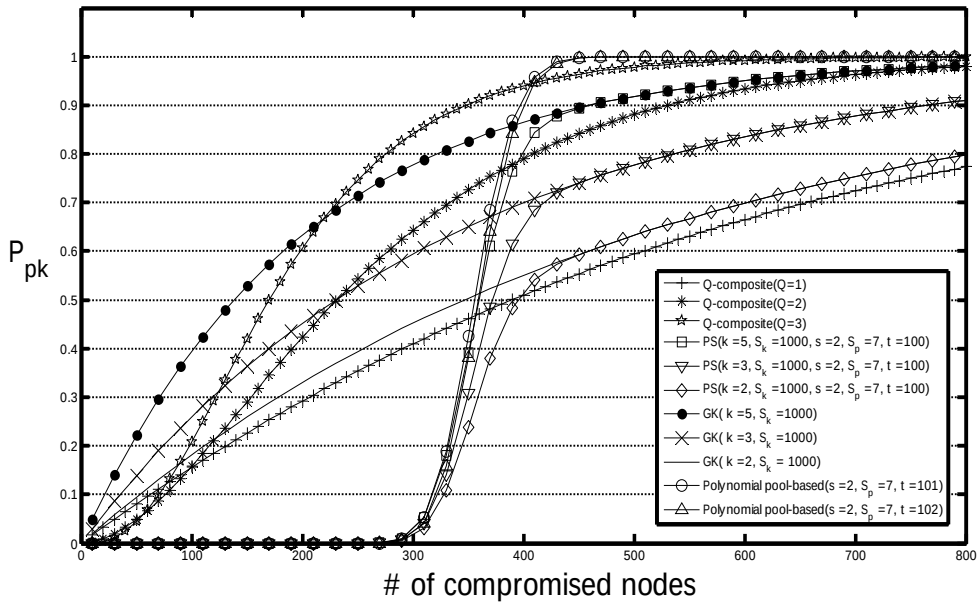
Similar to the scheme in [35], to improve the security of the polynomial-pool based scheme and prevent an attacker who has some knowledge of the polynomial dis-

tribution over the sensor nodes, that he/she can derived by compromising t+1 nodes . We assume each polynomial be used at most t+1 times. (We assume MS as one of the t+1 nodes). As a result, an attacker cannot recover a polynomial unless he/she captures all related nodes, including the mobile sink.

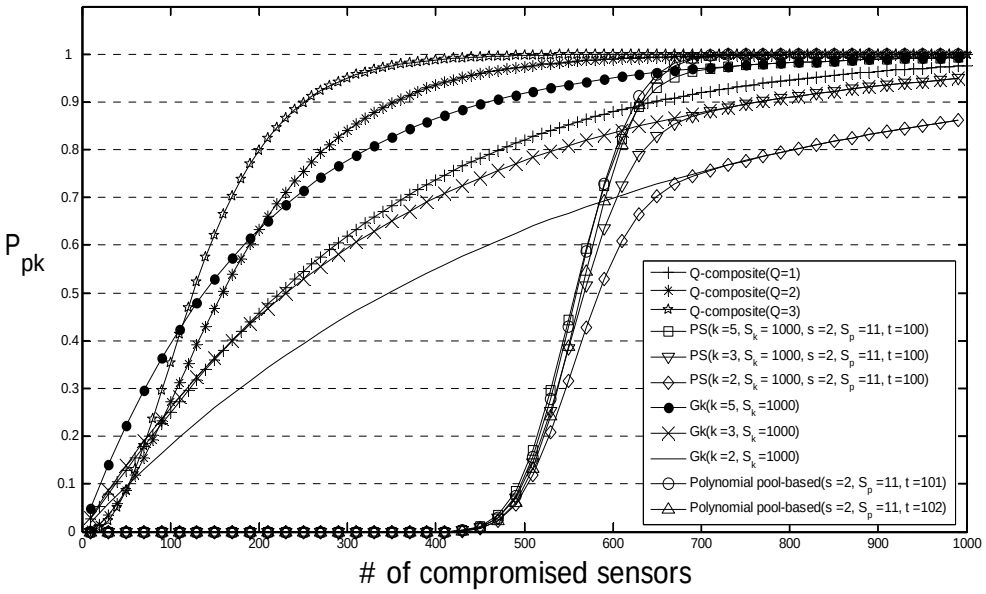
Now we compare the proposed scheme with the scheme in [48], the Q-composite [34], and the polynomial pool-based scheme [35]. We assume the same storage constrain for all schemes. Fig. [3(a) and 3(b)] show the fraction of compromised data links between non-compromised sensors and MS with q =0.99 and different p. These figures clearly show that using the proposed scheme in sensor networks with MS performs much better than the Q-composite scheme, the polynomial pool-based scheme, and the scheme in [48]. In the proposed scheme, each sensor node has to store k generation keys and s polynomials each of degree t. We assume that each generation key take the same storage overhead as the coefficients of a polynomial.

2. Communication Overhead

According to our pervious discussion, a mobile sink can establish a pairwise key and a common polynomial. If the MS and the sensor node i fails to establish a pairwise directly since the two don't share a common polynomial but share a common generation key. Then the MS and the sensor node i need to find at least one common neighbor that share a common polynomial with MS and a common polynomial with the sensor node i. In this section we investigate the smallest number of hops required by a sensor node to be securely connected to MS. Our analytical approach is similar to that given in [34], [52].



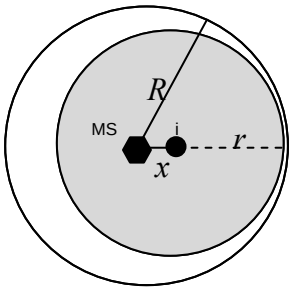
$p = 0.5, q = 0.99$



$p = 0.33, q = 0.99$

Fig. 3. Fraction of compromised data links between non-compromised sensors with different connectivity. PS and GK refer to our scheme and the probabilistic generation key pre-distribution scheme respectively. Assume MS and each sensor node has available storage for up to 600 keys, 210 keys respectively

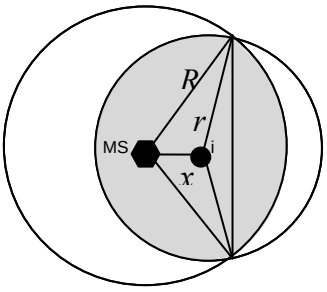
Let $p_h(x)$ be the probability that the smallest number of hops required to establish a pairwise key between a MS and a sensor node i is z. The probability $p_h(1)$ is obviously equal to p_c when the MS and the sensor node i can establish pairwise key directly. In the case where the MS and the sensor node i can't establish a pairwise key directly, the probability $p_h(2)$, the common neighbor connecting the MS and the sensor node i must be in the overlap area of the communication range of MS and the sensor node i, as shown in Fig. 4.



$$A_{overlap}(x) = \pi r^2$$

$0 \le x \le R - r$

(a)



$$A_{Overlap}(x) = \pi \cdot r^2 - r^2 \cos^{-1}\left(\frac{x^2 - r^2 + R^2 - x}{2xr}\right) - R^2 \cos^{-1}\left(\frac{x^2 - r^2 + R^2}{2xR}\right) - \frac{1}{2}\sqrt{(-x + r - R)(-x - r + R)(-x + r + R)(x + r + R)}$$

$R - r < x \le r$

(b)

Fig. 4. Overlap area $A_{\text{overlap}}(x)$ between MS and sensor node i

In our analysis, we assume that R, r represents the communication range of the MS and each sensor node respectively, where $R \geq r$. x is the distance between the MS and the sensor node i. The overlap area is

$$A_{overlap}(x) = \begin{cases} \pi \cdot r^2, & 0 \leq x \leq R - r \\ \pi \cdot r^2 - r^2 \cos^{-1}\left(\frac{x^2 - r^2 + R^2 - x}{2xr}\right) - R^2 \cos^{-1}\left(\frac{x^2 - r^2 + R^2}{2xR}\right) - & \\ \frac{1}{2}\sqrt{(-x + r - R)(-x - r + R)(-x + r + R)(x + r + R)}, & R - r < x \leq r \end{cases}$$

The total number of sensor nodes in the overlap area can be estimated as

$$N_{overlap}(x) = \frac{n}{\pi \cdot r^2} A_{overlap}(x) \tag{2.8}$$

where n is the number of sensor node within the communication range of a sensor.

The probability distribution function of the distance between the MS and a sensor node within communication range r is given by $F(x) = P(\text{distance} \leq x) = \pi x^2/\pi r^2$. The probability density function is thus

$$f(x) = \frac{\partial F(x)}{\partial x} = \frac{\partial [P(dis\ \tan\ ce \leq x)]}{\partial x} = \frac{\partial}{\partial x}\left[\frac{x^2}{r^2}\right] = \frac{2x}{r^2}$$

We then calculate the probability $p_h(2, x)$ that a MS and a sensor node i can't establish a pairwise key directly and there exist at least one common node in the overlap area that share a common polynomial with the MS and a common polynomial with the sensor node i to help establish a pairwise key between MS and the sensor node i. given the distance between MS and the sensor node i is x.

$p_h(2, x) = (1 - p_c)(1 - p_i(x))$, where $p_i(x)$ represent the probability that no common node in the overlap area is exist that share a common polynomial with MS and a common polynomial with the sensor node *i* given that MS and node *i* can't establish a pairwise key directly. By taking the average of $p_h(2, x)$ through all the possible values of *x,* the probability $p_h(2)$ can be calculated as:

$p_h(2)=p_{h,1}(2)+p_{h,2}(2)$, where $p_{h,1}(2)$, $p_{h,2}(2)$ are

$$p_{h,1}(2) = \int_0^{R-r} f(x) \cdot p(2,x) \quad dx, \quad 0 \le x \le R - r$$

$$= (1 - p_c) \cdot \left[1 - \int_0^{R-r} \frac{2x}{r^2} \cdot (p_{2,2})^{\pi \cdot r^2} dx \right]$$

$$p_{h,2}(2) = \int_{R-r}^{r} f(x) \cdot p(2,x) \quad dx, \quad R - r < x \le r$$

$$= (1 - p_c) \cdot \left[1 - \int_{R-r}^{r} \frac{2x}{r^2} \cdot (p_{2,2})^{a} dx \right],$$

where $a = \pi \cdot r^2 - r^2 \cos^{-1}\left(\frac{x^2 - r^2 + R^2 - x}{2xr}\right) - R^2 \cos^{-1}\left(\frac{x^2 - r^2 + R^2}{2xR}\right)$

$$- \frac{1}{2}\sqrt{(-x + r - R)(-x - r + R)(-x + r + R)(x + r + R)}$$

$$p_{2,2} = 1 - \frac{\binom{|S_p| - s}{s} \cdot \left[\binom{|S_p|}{s} - 2 \cdot \binom{|S_p| - s}{s} + \binom{|S_p| - 2s}{s} \right]}{\binom{|S_p|}{s}^2} \tag{2.9}$$

Fig. 5, Fig. 6 & Fig. 7 plots the values of $p_h(1)$ and $p_h(2)$. These figures clearly shows that MS can establish pairwise key with a sensor node with a probability equal to

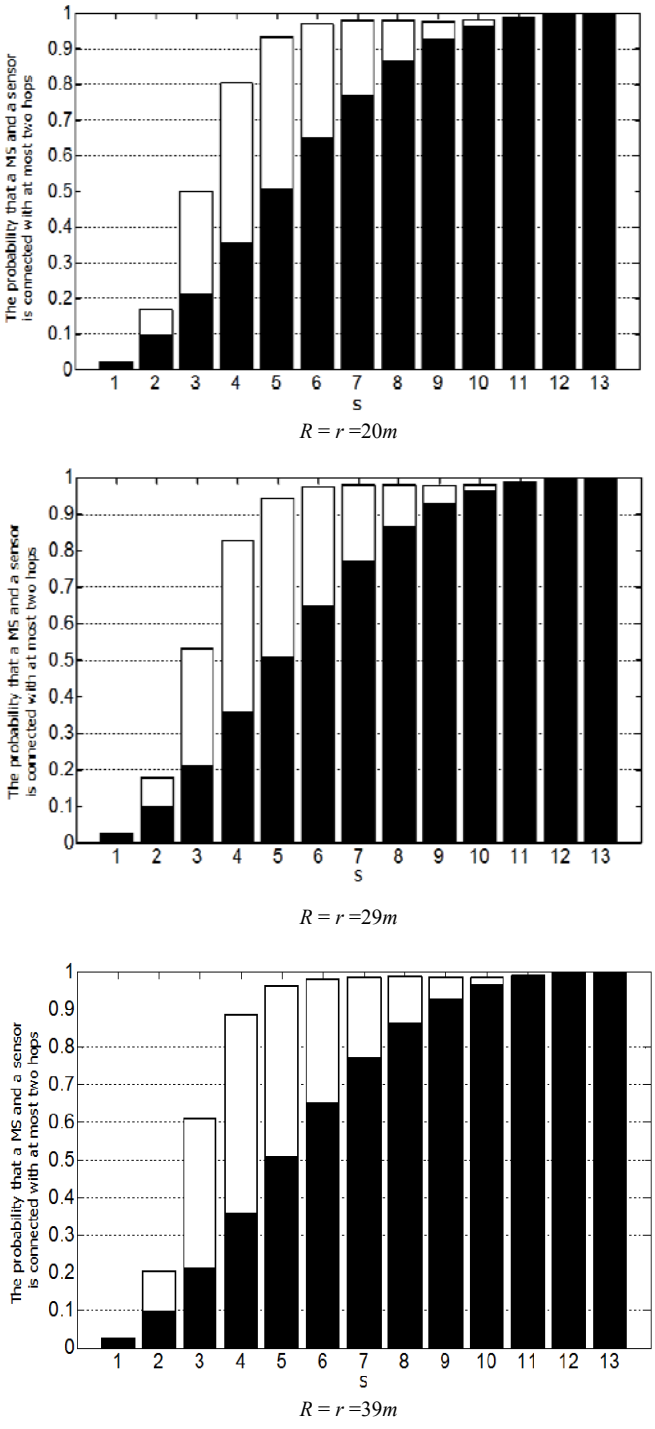
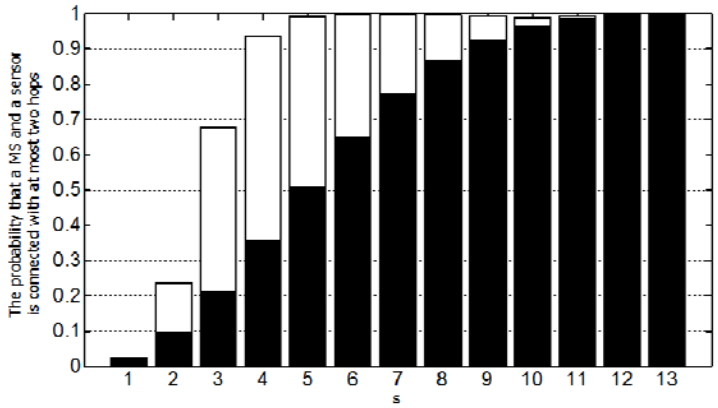
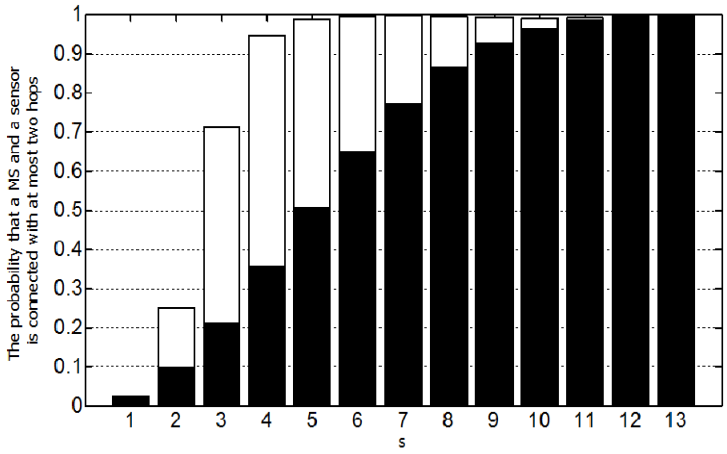


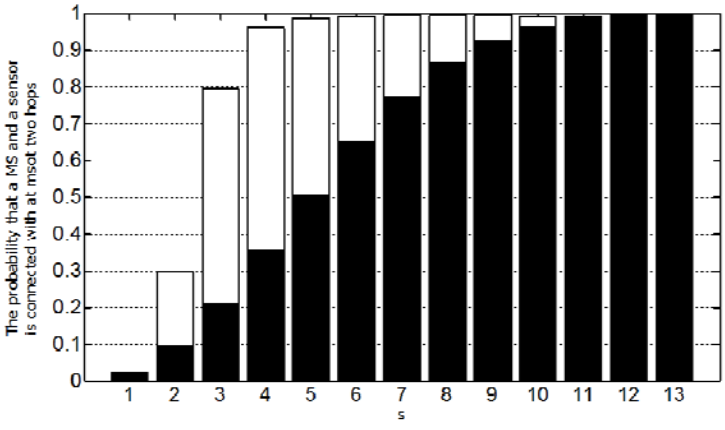
Fig. 5. The probability that a MS can establish a pairwise key with a sensor node with at most two hops with node density (n = 30), various mobile sink communication range (R) and a polynomial pool size ($|S_p|$ = 40)



$R = r = 20m$



$R = r = 29m$



$R = r = 39m$

Fig. 6. The probability that a MS can establish a pairwise key with a sensor node with at most two hops with node density (n = 60), various mobile sink communication range (R) and a polynomial pool size ($|S_p|$ = 40)

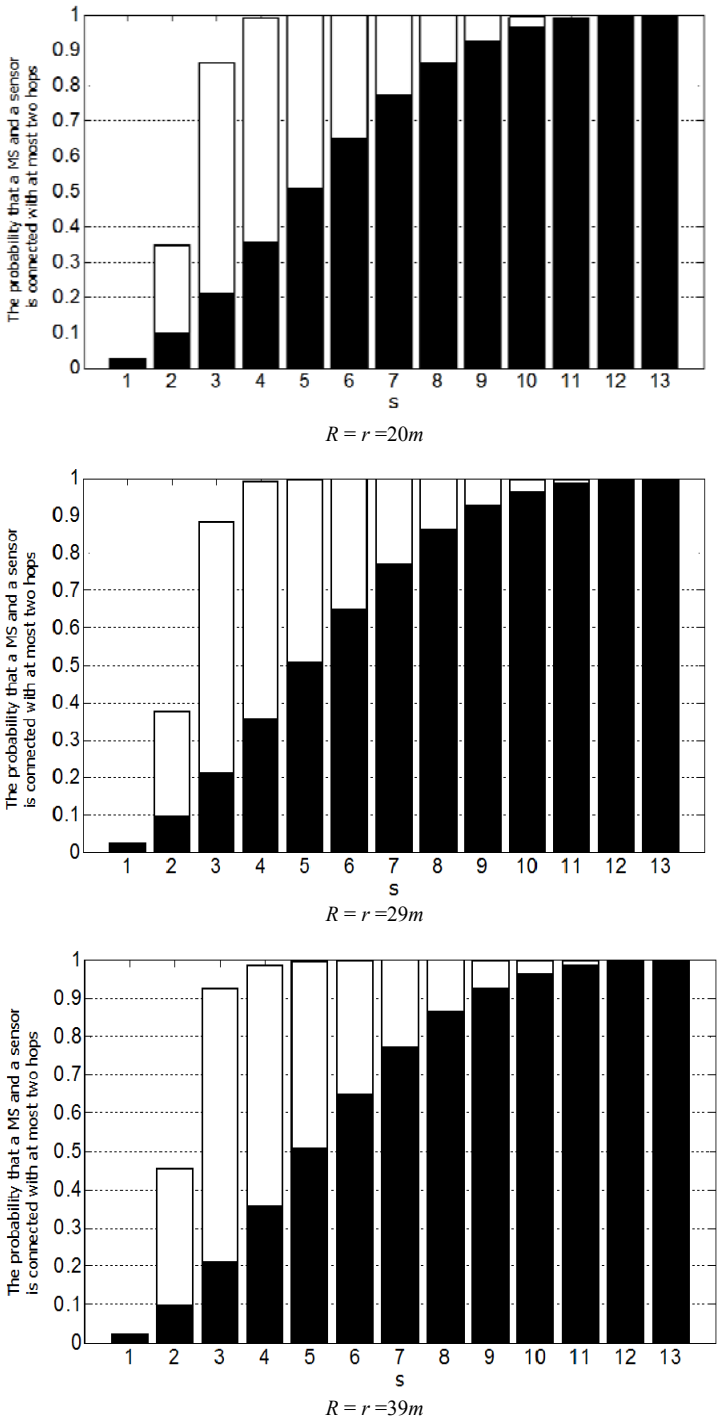


Fig. 7. The probability that a MS can establish a pairwise key with a sensor node with at most two hops with node density (n = 120), various mobile sink communication range (R) and a polynomial pool size ($|S_p|$ = 40)

unity, since $p_h(1)+p_h(2) \approx 1$ when s is large.

3. Memory Overhead

According to our scheme, each sensor node has to store k generation keys and s polynomials each of degree t. We assume that each generation key take the same storage overhead as the coefficients of a polynomial. Thus, the storage overhead is $(s\times(t+1)+k)\log \lambda$, where k in the range of 2 to 5.

D. Q-COMPOSITE GENERATION KEY SCHEME COMBINED WITH THE POLYNOMIAL POOL-BASED SCHEME

The operation of this scheme is similar to that of the previously proposed scheme, differing only in the amount of generation keys overlap that are used to establish secure communications instead of just one.

This scheme is based on the Q-composite scheme [34] and polynomial pool-based scheme [35] to establish pairwise keys. As it was describe in the previous section, a sensor node and MS can establish a pairwise key if the two share a single common generation key and a common polynomial in their key and polynomial rings. However, in this scheme, we increases the amount of generation keys overlap along with a common shared polynomial between MS and a sensor node that are required for key-setup. A Q common generation keys (Q > 1) and a common shared polynomial are needed, instead of just one generation key and one common polynomial. By increasing the amount of common generation keys, we increase the resilience of the network against nodes cap-

ture.

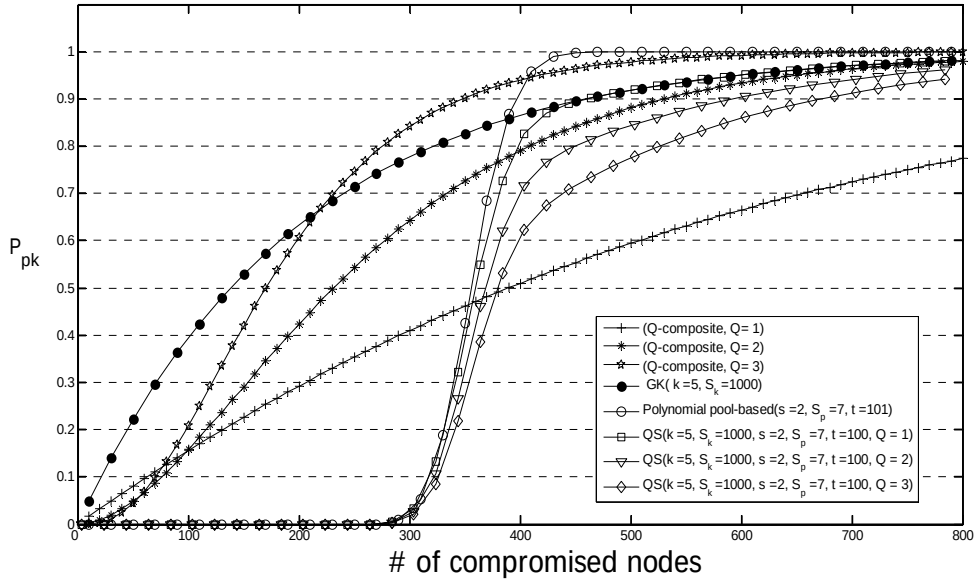
The proposed scheme is different from the Q-composite scheme. In the Q-composite scheme, to preserve a given probability of connection between two sensor nodes that share Q common keys to establish a secure link, it is necessary to reduce the size of the key pool. However, in our scheme the probability of connectivity is being preserved (q = 0.99), since the MS is initially pre-loaded with large number of generation keys ($m >> k$) and it is grantee to find at least Q common generation keys with a sensor node.

1. Security Analysis

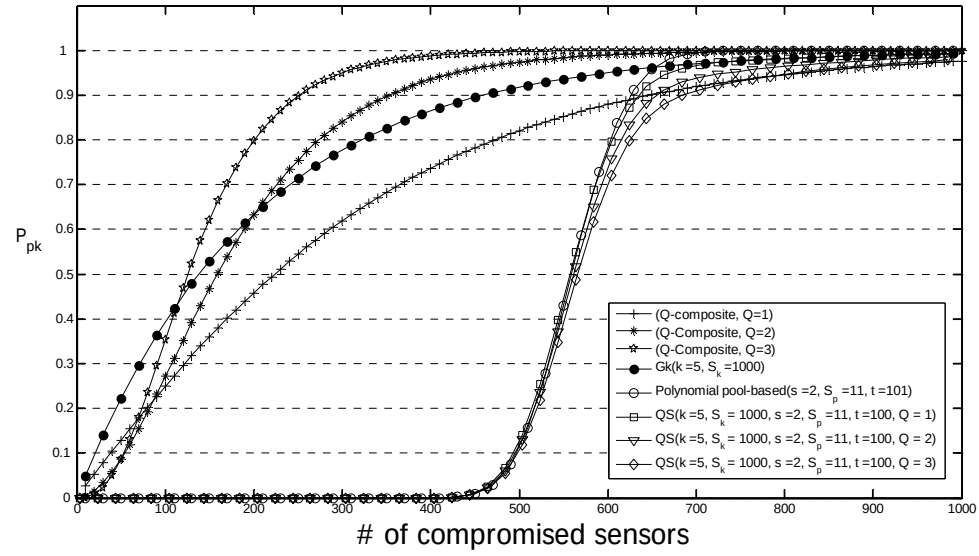
Similar to the security analysis that was described in section C, we drive the probability of a data communication link between MS and any non-compromised sensor node being compromised. This probability can be estimated by

$$P_{pk} = \left(1 - \sum_{j=0}^{j=t} p(j)\right) \cdot \left(1 - \left(1 - \frac{k}{|S_k|}\right)^x\right)^Q \tag{2.10}$$

We further compare the proposed scheme with the Q-composite scheme [34] and the polynomial pool-based scheme [35]. Fig. 8 shows that the proposed scheme performed butter in terms of network resilience to nodes capture compared to our previously proposed scheme (Q = 1), the Q-composite scheme and the polynomial pool-based scheme.



$p = 0.5$, $q = 0.99$



$p = 0.33$, $q = 0.99$

Fig. 8. Fraction of compromised data links between non-compromised sensors with different connectivity. QS and GK refer to our scheme and the probabilistic generation key pre-distribution scheme respectively

E. SUMMARY

In this chapter, we developed two key pre-distribution schemes for sensor network with mobile sink. The two proposed schemes are based on the polynomial pool-based scheme [35], the probabilistic generation key pre-distribution scheme [48], and the Q-composite scheme [34]. We show that both schemes have the threshold property, i.e., they remain perfectly secure up to the capture of a certain fraction of sensor nodes. Security analyses indicate that the proposed schemes provide a higher probability for non-compromised sensors to establish a secure communication with the mobile sink than previous schemes [35], [34], [48]. The schemes also provide both security and MS connectivity as the optimization criteria.

CHAPTER III

ANTI MOBILE SINK REPLICATION ATTACK SCHEMES

The problem of authentication and pairwise key establishment in sensor networks with MSs is still not solved in the face of *mobile sink replication* attacks. For the basic probabilistic [32] and *Q*-composite [34] key pre-distribution schemes, an attacker can easily obtain large number of keys by capturing a small fraction of the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink pre-loaded with some compromised keys to authenticate and then initiate data communication with any sensor node.

To address the above problem, we developed a general framework [41], [42] that permits the use of any pairwise key pre-distribution scheme as its basic component to provide authentication and pairwise key establishment between sensor nodes and MSs. To facilitate the study of a new security technique, we first cultivated a general three-tier security framework for authentication and pairwise key establishment based on the polynomial pool-based key pre-distribution scheme [35]. The proposed technique will substantially improve network resilience to *mobile sink replication* attacks compared with the single polynomial pool-based key pre-distribution approach [35], as an attacker would have to compromise many more sensor nodes to launch a successful *mobile sink-replication* attack. In the new security framework [41], [42], a small fraction of pre-selected sensors (see Fig. 9), called the *stationary access nodes*, act as authentication access points to the network and to trigger sensor nodes to transmit their aggregated data

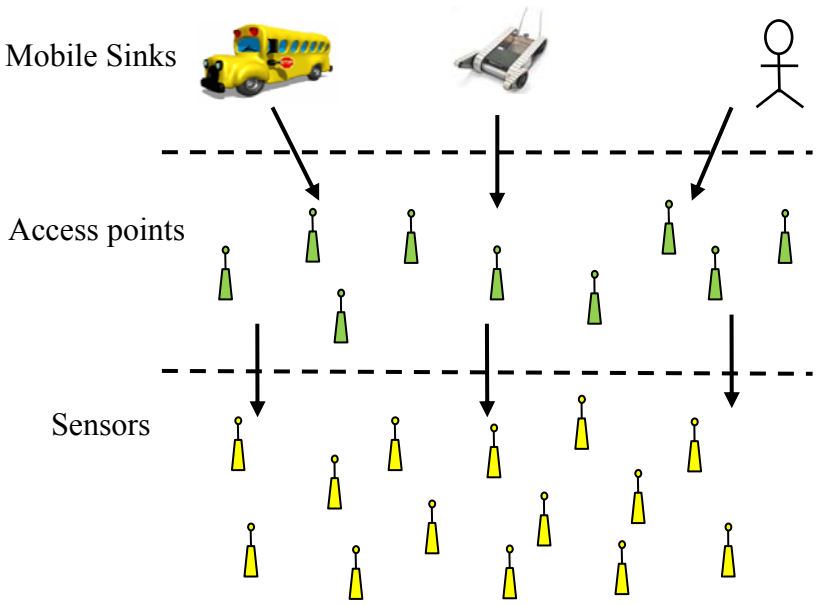


Fig. 9. The three-tier security scheme in WSN with mobile sinks

to mobile sinks. A mobile sink sends *data request* messages to sensor nodes via a *stationary access node*, these mobile sink's *data request* messages will initiate the *stationary access node* to trigger sensor nodes to transmit their data to the requested mobile sink. The scheme uses two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. The mobile Polynomial pool is used for authentication and keys setup between mobile sinks and *stationary access nodes*. From this pool, each mobile sink randomly selects a subset of K_m mobile polynomials out of $|M|$ mobile polynomials, and each *stationary access node* randomly selects a single mobile polynomial.

The static polynomial pool is used for authentication and pairwise key establishment between sensor nodes and *stationary access nodes*. From this pool, each sensor

node randomly selects a subset of K_s static polynomials out of $|S|$ static polynomials. Each *stationary access node* randomly selects a subset of K_s-1 static polynomials.

Using two separate key pools and have few sensor nodes that carry keys from the mobile key pool will made it more difficult for the attacker to launch a *mobile sink replication* attack on the sensor network by capturing only a few arbitrary sensor nodes. Rather, the attacker would also have to capture sensor nodes that carry keys from the mobile key pool. Keys from the mobile key pool are used mainly for mobile sink authentication and hence to gain access to the network for data gathering.

Although the above security approach makes the network more resilient to *mobile sink replication* attack compared with the single polynomial pool-based key predistribution scheme [35], it is still vulnerable to *stationary access nodes replication* attacks. In this type of attack, the attacker is able to launch a replication attack similar to the *mobile sink replication* attack. After a fraction of sensor nodes have been compromised by an adversary, captured static polynomials can be loaded into a replicated *stationary access node* that transmits recorded mobile sink's data request messages to trigger sensor nodes to send their aggregated data.

To make the three-tier security scheme more robust against *stationary access node replication* attack, we strengthen the authentication mechanism between the *stationary* access *nodes* and sensor nodes using *one-way hash chains* algorithm [53] in conjunction with the static polynomial pool-based scheme [35].

Our analytical results indicate that the new security technique makes the network more resilient to both *mobile sink replication attacks* and *stationary access nodes replic-*

ation attacks compared with the single polynomial pool-based approach.

This chapter is organized as follows: Section A presents our proposed scheme and its security performance against *mobile sink replication* attack [41], [42]. Section B shows the security analysis and the threat analysis for *stationary access nodes replication* attack for the enhanced three-tire scheme, and Section C draws conclusions.

A. THE THREE-TIER SECURITY SCHEME

In this work, we choose the Blundo scheme [38] to construct our approach. As we shall see, the Blundo scheme provides a clear security guarantee. Use of the Blundo scheme, therefore, greatly eases the presentation of our work and enables us to provide a clearer security analysis.

The Blundo scheme, when applied to ad hoc or sensor network usually involves the following steps.

- The base station (or a key setup server) chooses a random symmetric bivariate polynomial $f(x, y)$ of degree t with coefficients over a finite field $GF(q)$, where q is a prime number large enough to accommodate a symmetric key.

$$f(x,y) = \sum_{0 \le i,j \le t} a_{ij} x^i y^j \tag{3.1}$$

- The base station loads every sensor node u with $f(u, y)$, which is a polynomial obtained by evaluating $f(x, y)$ at $x = u$.

$$f(u,y) = \sum_{0 \le i,j \le t} a_{ij} u^i y^j \tag{3.2}$$

- If two nodes, u and v, want to set up a pairwise key, each evaluates the others' id in its own polynomial. The result $f(u, v) = f(v, u)$ serves as their pairwise key.

In the proposed scheme, we use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish authentication between mobile sinks and *stationary access nodes* that will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for sensor's data gathering. Polynomials from the static polynomial pool are used to ascertain authentication and keys setup between sensor nodes and *stationary access nodes* (see Fig. 10).

Prior to deployment, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. In our scheme, to improve the network resilience to *mobile sink replication* attack as compared to the single polynomial pool-based approach, we intend to minimize the probability of a mobile polynomial being compromised if R_c sensor nodes were captured. Since an adversary can use the captured mobile polynomial to launch a *mobile sink replication* attack, we achieve this by having a small fraction of sensor nodes randomly selected to carry a polynomial from the mobile polynomial pool. These pre-selected sensor nodes are called the *stationary access nodes*. They act as authentication access points for the network and trigger sensor nodes to tran-

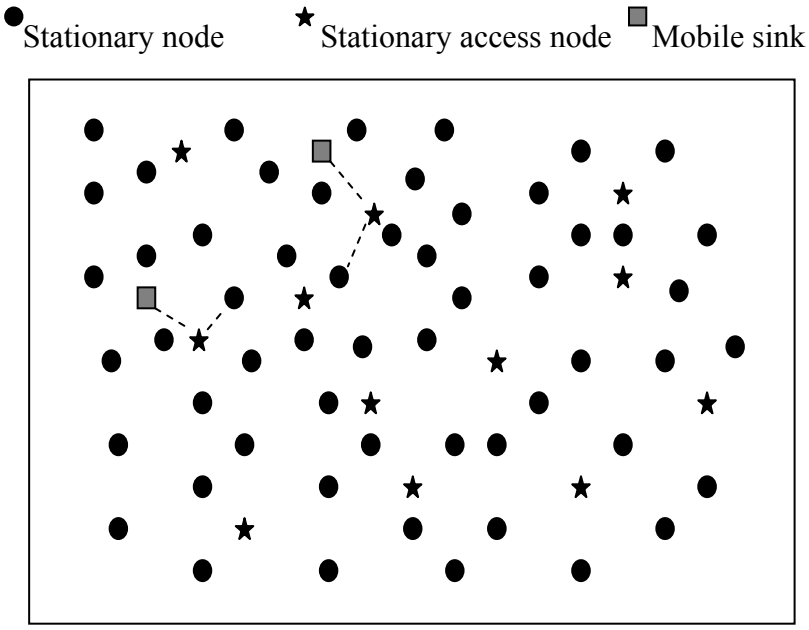


Fig. 10. Wireless sensor network with mobile sinks and sensor nodes using two separate key pools for key pre-distribution

smit their aggregated data to mobile sinks. A mobile sink sends *data request* messages to sensor nodes via a *stationary access node*. These mobile sink's *data request* messages will initiate the *stationary access node* to trigger sensor nodes to transmit their aggregated data to the requested sink. Each *stationary access node* may share a mobile polynomial with a mobile sink. All sensor nodes, including the *stationary access nodes*, randomly select a subset of polynomials from the static polynomial pool. The advantage of using separate pools is that mobile sink authentication is independent of the key distribution scheme used to connect the sensor network. We divide our scheme into two stages: static and mobile polynomial pre-distribution and key discovery between a mobile sink and a sensor node.

*Stage 1: Static and mobile polynomial pre-distribution***:** Stage 1 is performed before nodes are deployed. A mobile polynomial pool M of size $|M|$ and a static polynomial pool S of size $|S|$ are generated along with the polynomial identifiers. All mobile sinks and *stationary access nodes* are randomly given K_m and one polynomial ($K_m > 1$) from M. The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every *stationary access node*. This assures that a mobile node shares a common mobile polynomial with a *stationary access node* with high probability and reduces the number of compromised mobile polynomials when *stationary access nodes* are captured. All sensor nodes and the pre-selected *stationary access nodes* randomly pick a subset of K_s and K_s-1 polynomials from S. Fig. 11 shows key discovery between mobile node and stationary node.

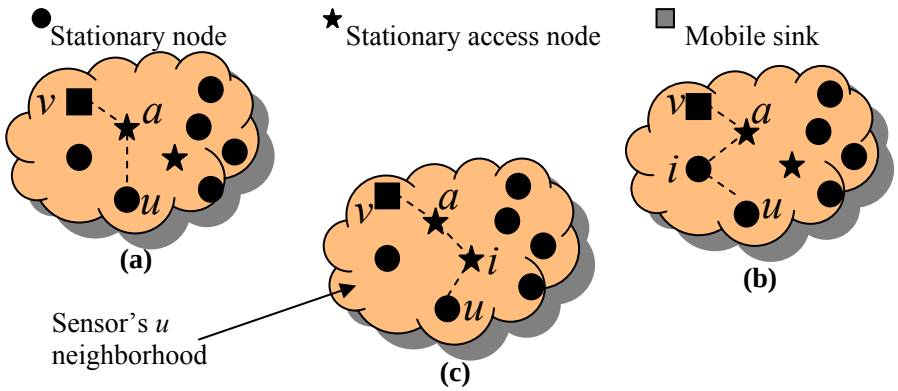


Fig. 11. (a) Direct key discovery, (b) Indirect key discovery through intermediate stationary node *i,* (c) Indirect key discovery through intermediate stationary access node *i*

*Stage 2: Key discovery between mobile node and stationary node***:** To establish a direct pairwise key between sensor node *u* and mobile sink *v*, a sensor node *u* needs to find a *stationary access node a* in its neighborhood, such that node *a* can establish pairwise keys with both mobile sink *v* and sensor node *u*. In other words, a *stationary access node* needs to establish pairwise keys with both a mobile sink and a sensor node. It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node. To discover a common mobile/static polynomial, a sensor node *i* may broadcast a list of polynomial IDs, or alternatively, an encryption list α , $E_{Kv}(\alpha), v = 1, \ldots |K_{si}|$, where K_v is a potential pairwise key the other node may have as suggested in [36], [37]. When a direct secure path is established between nodes *u* and *v*, mobile sink *v* sends the pairwise key K_c to node *a* in a message encrypted and authenticated with the shared pairwise key $K_{v,a}$ between *v* and *a*. If node *a* receives the above message and it shares a pairwise key with *u*, it sends the pairwise key K_c to node *u* in a message encrypted and authenticated with pairwise key $K_{a,u}$ between *a* and *u.*

If the direct key establishment fails, the mobile sink and the sensor node will have to establish a pairwise key with the help of other sensor nodes. To establish a pairwise key with mobile sink *v*, a sensor node *u* has to find a *stationary access node a* in its neighborhood such that node *a* can establish pairwise key with both node *u* and *v*. If node *a* established a pairwise key with node *v* only and not with *u*. Since the probability is high that *stationary access node a* can discover a common mobile polynomial with node *v*, sensor node *u* needs to find an intermediate sensor node *i* along the path *u*-*i*-*a*–*v*, such that intermediate node *i* can establish a direct pairwise key with node *a*.

1. Security analysis

We analyze the performance of the proposed scheme using two metrics: security and connectivity. For security, we present the probability of a mobile polynomial being compromised; hence an attacker can make use of the captured mobile polynomial to launch a *mobile sink replication* attack against the sensor network. In connectivity, we estimate the probability of a mobile sink establishing secure links with sensor nodes from any authentication access point in the network. Clearly, for a densely deployed network of *n* nodes, if a sensor node cannot find any s*tationary access node* in its neighborhood, it cannot connect securely to any mobile sink. Thus, we want to ensure that a sensor has at least one *stationary access node* in its neighborhood with a high probability of connectivity. A critical parameter is the number *m* of *stationary access nodes* in the network. For simplicity, we assume that sensor nodes are evenly deployed in the field. Let *c* be the average number of neighbor nodes for every sensor node before the deployment of *stationary access nodes*.

After the *stationary access nodes* are evenly deployed in the network, the probability that a sensor node cannot find any *stationary access node* in its neighborhood can be estimated by $(1-\frac{c}{n})^m$. The probability that a sensor node has at least one *stationary access node* in its neighborhood can be estimated by

$$P_{conn} = 1 - \left(1 - \frac{c}{n}\right)^m \tag{3.3}$$

In the dense sensor network, we can usually deploy a small fraction of sensor nodes that carry a mobile polynomial, such that any sensor node can find at least one *stationary ac-*

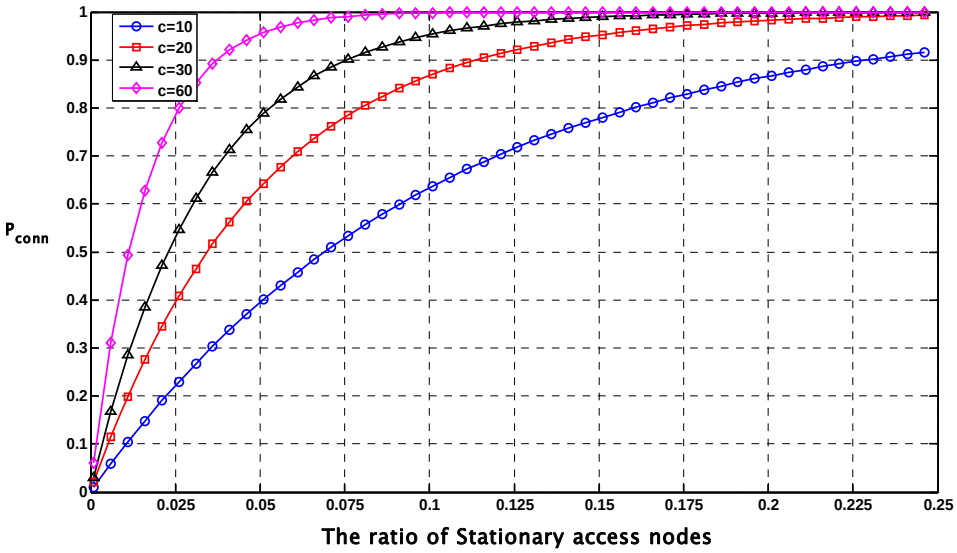


Fig. 12. The probability P_{conn} that a sensor has at least one stationary access node in its neighborhood vs. the ratio of stationary access nodes

cess node in its neighborhood with high probability. For example, when c = 60, we need to have 8% of the sensor nodes deployed carrying a mobile polynomial to ensure that a node can find at least one *stationary access node* in its neighborhood with probability 0.99. Fig. 12 shows P_{conn} vs. the ratio of *stationary access nodes.*

The probability that a mobile sink and a *stationary access node* share a mobile polynomial—in other words, the probability P_m that mobile sink and *stationary access node* can establish a key directly—is expressed by

$$P_m = \frac{K_m}{|M|} \tag{3.4}$$

The probability P_s that two sensor nodes share a common static polynomial the probability that the two sensors can establish a secure link directly can be estimated in equation (3.5).

$$P_s = 1 - \frac{\binom{|S|}{2K_s} \cdot \binom{2K_s}{K_s}}{\binom{|S|}{K_s}^2} \tag{3.5}$$

The probability P_{sa}, that a sensor node and a *stationary access node* sharing a common static polynomial—the probability that the two nodes can establish a pairwise key directly—is estimated by

$$P_{sa} = 1 - \frac{\binom{|S|}{2K_s - 1} \cdot \binom{2K_s - 1}{K_s - 1}}{\binom{|S|}{K_s} \cdot \binom{|S|}{K_s - 1}} \tag{3.6}$$

The probability P_a, that two *stationary access nodes* sharing a common static/mobile polynomial, can be estimated by

$$P_a = 1 - \frac{(|M| - 1)\binom{|S|}{2 \cdot (K_s - 1)} \cdot \binom{2 \cdot (K_s - 1)}{K_s - 1}}{|M| \cdot \binom{|S|}{K_s - 1}^2} \tag{3.7}$$

Fig. 13 show the relationship between the probability P_{sa} and the combination of $|S|$ and K_s, respectively. Fig. 14 shows the probability P_a with various combinations of $|S|$, K_s and $|M|$.

All figures clearly show that the closer $|S|$ and K_s are, the more likely two sensor nodes can establish a pairwise key directly.

Now let us consider the probability that a mobile sink v can establish a pairwise key with a sensor node u through direct or indirect key discovery. Let d denote the average number of stationary neighbors that static node u can contact. Let g denote the average number of stationary access nodes node u has in its neighborhood, through which u can contact a mobile node v. Considering any of these g *stationary access nodes*, the

probability that it shares a mobile polynomial with the sink v and share a static polynomial with the node u is $P_{sa}P_m$.

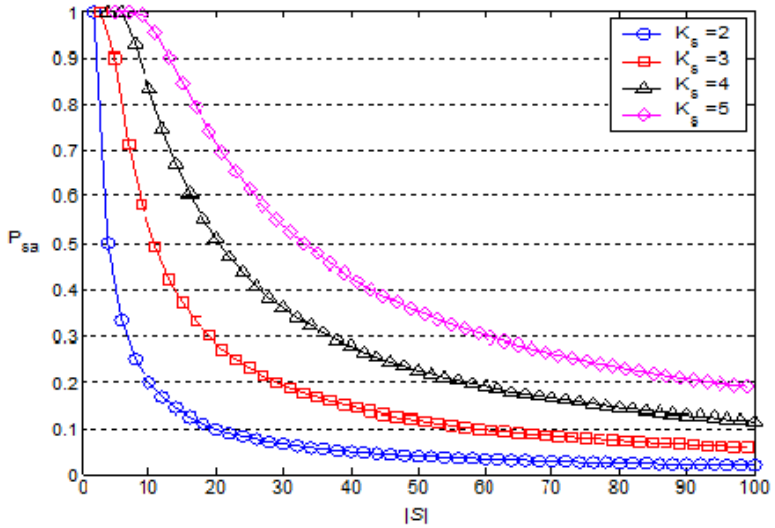


Fig. 13. The probability P_{sa} that a sensor and stationary access node share a static polynomial vs. the size $|S|$

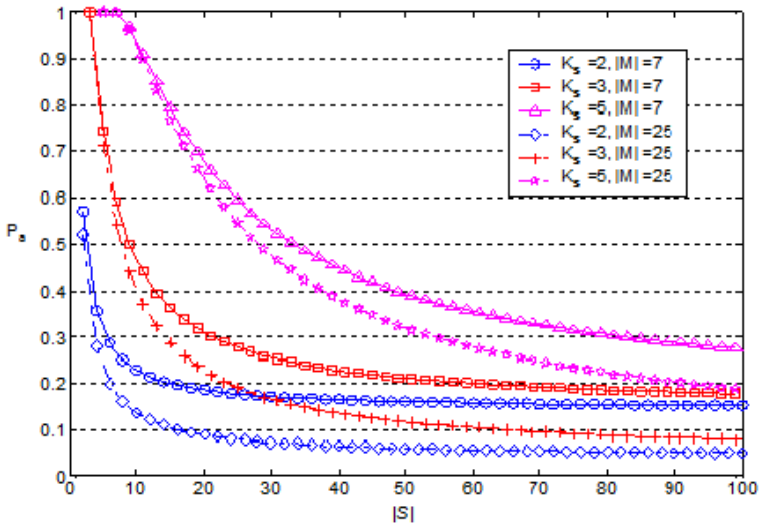


Fig. 14. The probability P_a , that two sensors share a static or a mobile polynomial vs. the size $|S|$

The probability that mobile sink v cannot establish a pairwise key directly with node u can be estimated by $(1- P_{sa}P_m)^g$. Considering that any of node u neighbors acts as an intermediate node, the probability that node u cannot establish a pairwise key indirectly with mobile sink v is $(1- P_mP_{sa}P_s)^{g.d}$. In the case that any stationary access neighbors of node u acts as an intermediate node, the probability that node u cannot establish a pairwise key indirectly with sink v is $(1- P_mP_aP_{sa})^{g(g-1)}$. The probability P_d of a mobile sink and a sensor node establishing a pairwise key (directly or indirectly) can be estimated by

$$P_d = 1- (1- P_{sa}P_m)^g \cdot (1- P_mP_{sa}P_s)^{g.d} \cdot (1- P_mP_aP_{sa})^{g(g-1)} .$$

Fig. 15 and Fig. 16 show the relationship between P_d vs. d and the combinations of g and P_m respectively.

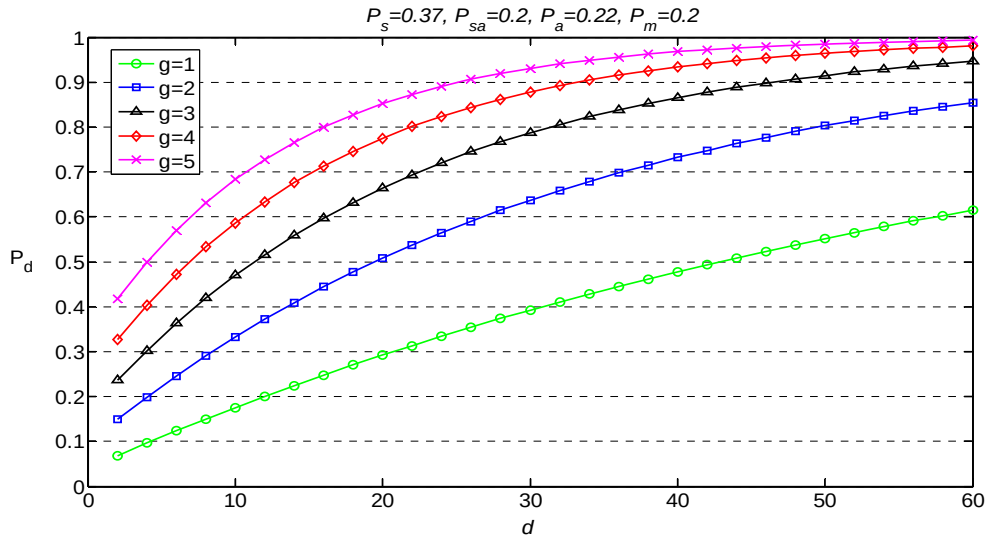
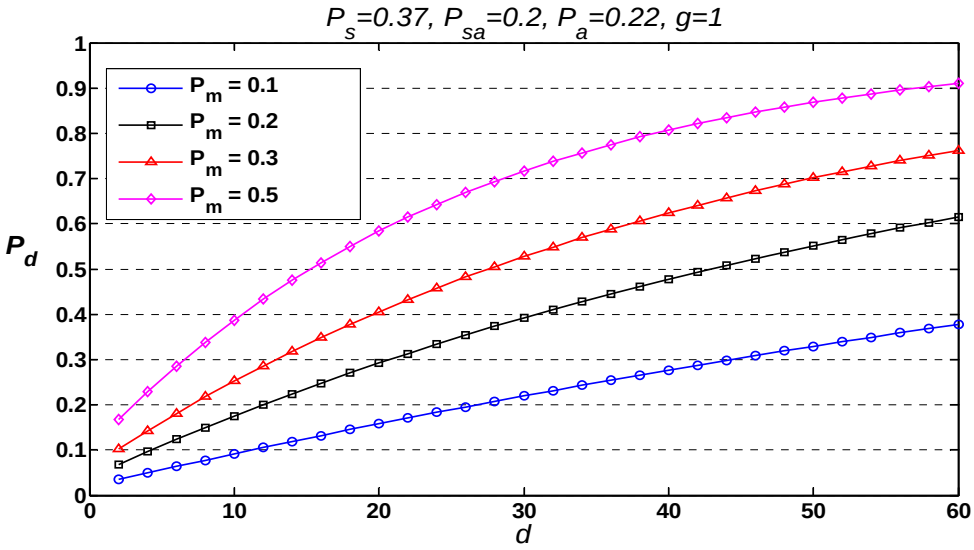
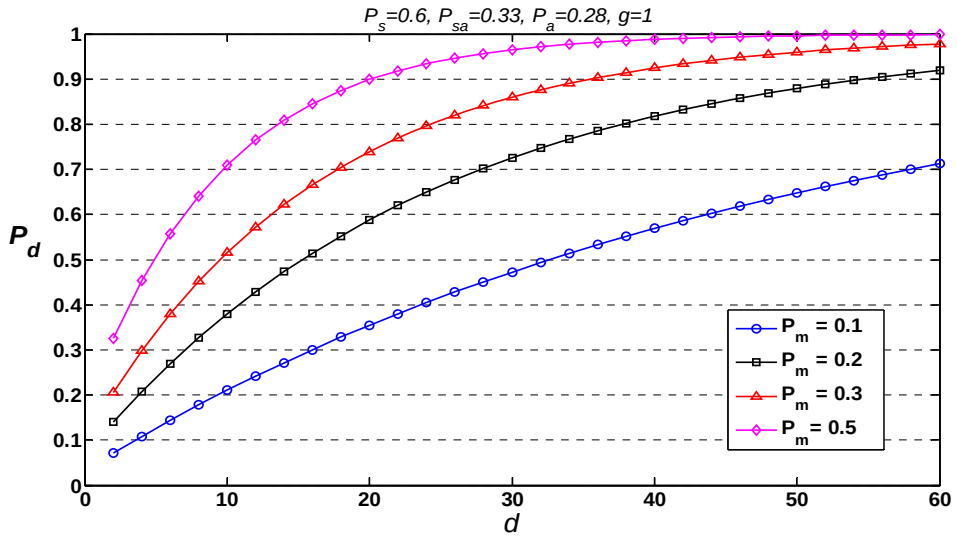


Fig. 15. The probability P_d of a mobile sink establishing a pairwise key with a sensor node vs. the number of sensor neighbors d



(a)



(b)

Fig. 16. The probability P_d of a mobile sink establishing a pairwise key with a sensor node

2. Threat analysis

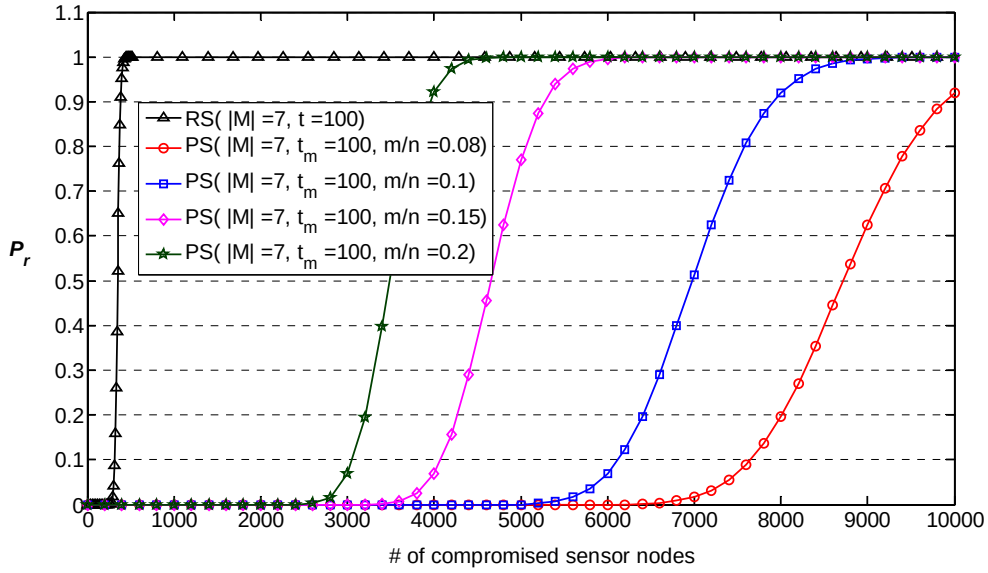
In this section, we analyze the security performance of the proposed scheme against *mobile sink replication* attack. As stated in the previous section, in order for an attacker to

launch a *mobile sink replication* attack on the network, the adversary has to compromise at least one polynomial from the mobile polynomial pool. To achieve this, the adversary must capture at least a specific number of *stationary access nodes* that hold the same mobile polynomial.

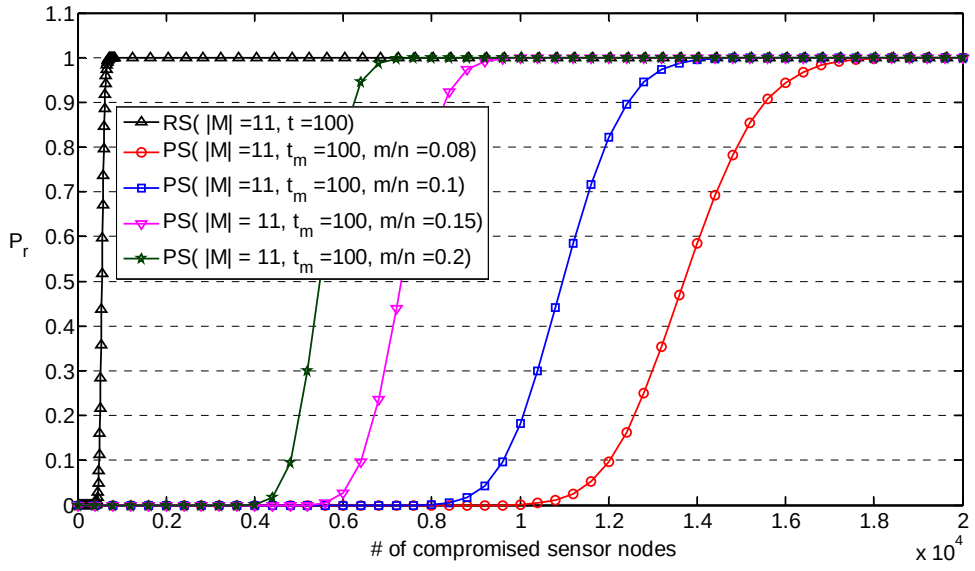
As we described earlier, a small number *of m stationary access nodes* are randomly being picked out of *n* sensor nodes in the network. Every *stationary access node* is assigned a mobile polynomial that may be randomly chosen from the mobile polynomial pool. It follows from the security analysis of the Blundo scheme, that for any polynomial *w* in the mobile polynomial pool of degree t_m, an attacker cannot recover polynomial *w*, if no more than t_m *stationary access nodes* that had chosen *w* are captured by the attacker. If more than t_m *stationary access nodes* with *w* as their mobile polynomial are captured by the attacker, then the attacker can recover the mobile polynomial *w*, and hence be able to launch a *mobile sink replication* attack against the sensor network. We assume an attacker randomly captures R_c sensor nodes, $R_c > t_m$. Consider any polynomial *w* in the mobile polynomial pool. The probability of *w* being chosen for a *stationary access node* is $\frac{1}{|M|}$, the probability that any captured node is a *stationary access node* is $\frac{m}{n}$, and the probability that this polynomial being chosen exactly by *x stationary access nodes* among R_c captured nodes is

$$P(x) = \binom{R_c}{x} \cdot \left(\frac{1}{|M|} \times \frac{m}{n}\right)^x \cdot \left(1 - \frac{1}{|M|} \times \frac{m}{n}\right)^{R_c - x} \tag{3.8}$$

Thus, the probability that any polynomial from the mobile polynomial pool being recovered by an attacker is $P_r = 1 - \sum_{x=0}^{t_m} P(x)$. Fig. 17 shows the probability P_r



(a)



(b)

Fig. 17. The probability P_r that any polynomial from the mobile polynomial pool is being recovered

when two separate polynomial pools are used for mobile sink and sensor nodes and compares it with the case of a single polynomial pool approach being used for both sensor nodes and mobile sinks. The figure clearly shows that an attacker must capture many more sensor nodes in this scheme than in the single polynomial pool approach.

B. THE ENHANCED THREE-TIER SECURITY SCHEME

As described in the previous section, the three-tier security scheme provides better network resilience against *mobile sink replication* attack compared with the single polynomial pool approach. This scheme delivers the same security performance as the single polynomial pool approach when network is being under a *stationary access node replication* attack. In both schemes, for any sensor node *u* that need to authenticate and establish a pairwise key with a *stationary access node A*, the two nodes must share at least a common polynomial in their polynomial rings. To perform a *stationary access node replication* attack on a network, the adversary needs to compromise at least a single polynomial from the static pool. This can be obtained easily by capturing arbitrary sensor nodes in the network. Then the adversary can make use of this compromised polynomial by a replicated stationary access node to enable insecure access to the network. When successful access to the network has been obtained through the compromised static polynomial, the replicated stationary access node transmits recorded mobile sink data request messages. Then sensor nodes that have the compromised polynomial in their rings will insecurely authenticate and establish a pairwise key with the replicated node and hence deliver their data to the replicated node.

In this section, we remedy the security performance of the proposed scheme in the case of *stationary access node replication* attack. We use *a one-way hash chain* [53] algorithm in conjunction with the polynomial pool scheme. In addition to the static polynomial, a pool of randomly generated passwords is used to enhance authentication between sensor nodes and *stationary access nodes*.

In the enhanced security scheme, each sensor node, such as u, is pre-loaded with a subset of K_s polynomials randomly chosen from the static pool |S|. In addition to the K_s preloaded static polynomials, node u randomly picks a subset of *Gs* passwords form the password pool $|W|$. Then for each of the *Gs* password Pw_i that was randomly chosen by node u, its rth hash value, $H^r(Pw_i)$ is loaded into node u. Each password is blinded with the use of a *collision-resistant hash function* such as MD5 [54]. Due to the collision-resistant property, it is computationally infeasible for an attacker to find a value Pw_x, such that $H(Pw_y) = H(Pw_x)$, $Pw_x \neq Pw_y$. For s*tationary access nodes,* each is pre-loaded with K_s-1 static polynomials and *Ga* hash values ($H^{r-1}(Pw_i)$) for the randomly chosen passwords from the pool $|W|$.

To establish authentication between a sensor node and a *stationary access node* in the enhanced scheme, the two must share a common static polynomial. Also, they need to discover at least a single access node verification of $H(H^{r-1}(Pw_i)) = H^r(Pw_i)$ for which both the sensor node and the *stationary access node* had the same password Pw_i randomly chosen from the pool $|W|$. In the access node verification, to verify the authentcy of a *stationary access node*, the sensor node performs a single hash operation on the hash value that sent from the stationary access node.

1. Security analysis

Similar to the security analysis presented in section A, we evaluate the performance of the enhanced three-tier security scheme in terms of connectivity. We estimated the probability P_{conn} that a sensor node has at least one *stationary access node* in its neighborhood, verified by $H(H^{r-1}(Pw_i)) = H^r(Pw_i)$, where $H^{r-1}(Pw_i)$ and $H^r(Pw_i)$ are the preloaded hash values of Pw_i in each of the *stationary access node* and the sensor node, respectively. Thus,

$$P_{conn} = 1 - \left(1 - p \times \frac{c}{n}\right)^m \tag{3.9}$$

where p is the probability that a *stationary access node* and a sensor share at least a common chosen password for access node verification.

$$p = 1 - \frac{\binom{|W|}{Gs+Ga} \cdot \binom{Gs+Ga}{Gs}}{\binom{|W|}{Gs} \cdot \binom{|W|}{Ga}} \tag{3.10}$$

For different node densities c =10, c =20, c =60, and c = 120, Fig. 18 and Fig. 19 shows the probability P_{conn} vs. the ratio of *stationary access nodes* and the probability p. All figures clearly indicate that for a given *stationary access node* ratio of α, and a node density c, the probability of connectivity increases as p increases.

We also estimated the probability P_g (Fig. 20) of a mobile sink being connected directly or indirectly to a sensor node via a *stationary access node* that share with sensor node at least a common static polynomial and a common chosen password Pw_i for which the node is able to verify the access node by ($H(H^{r-1}(Pw_i)) = H^r(Pw_i)$). To drive the

probability P_g, we use a similar analysis to the estimation of the probability P_d except that no sensor neighbor can act as intermediate node, thus P_g can be estimated in (3.11).

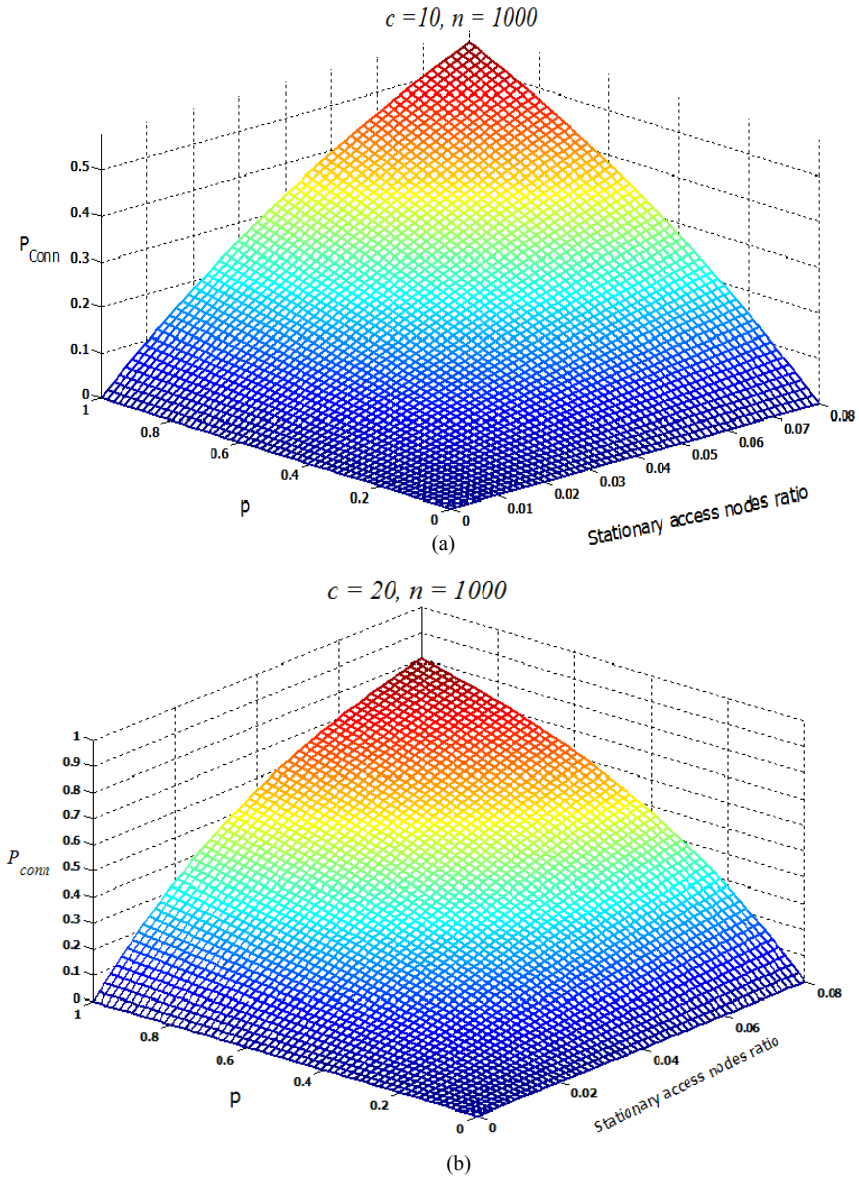
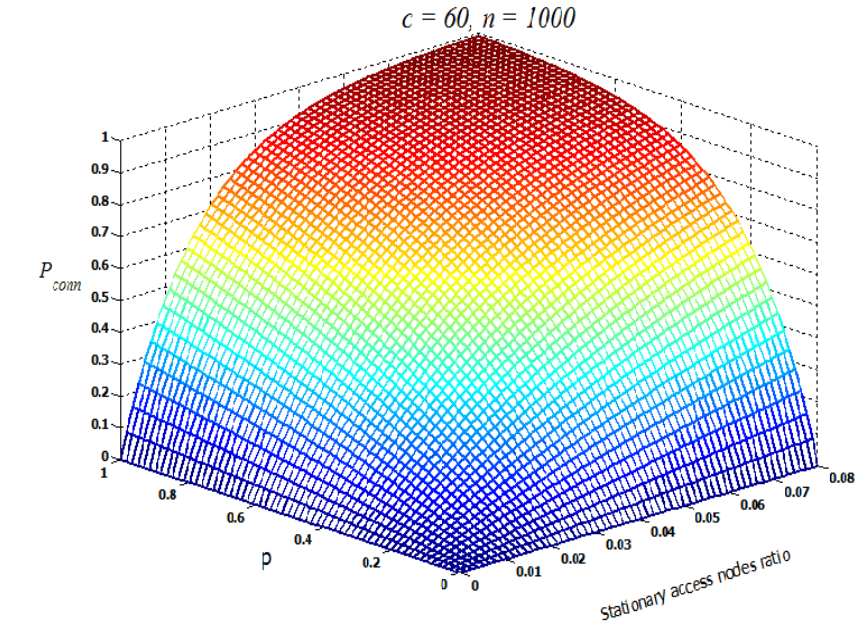
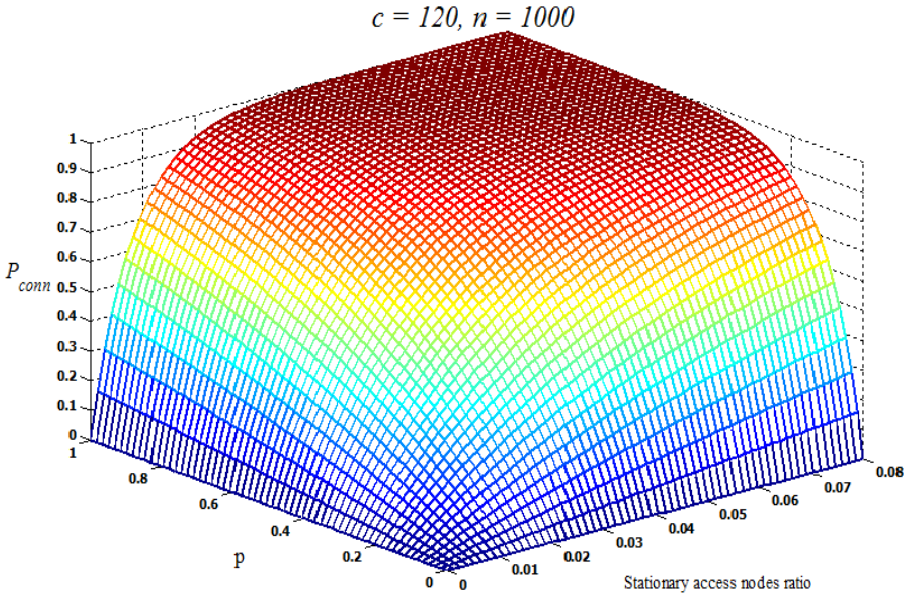


Fig. 18. The probability P_{conn} for various node density vs. the ratio of stationary access nodes and the probability p that a sensor and a stationary access node share at least a common chosen password (c = 10 and c = 20)

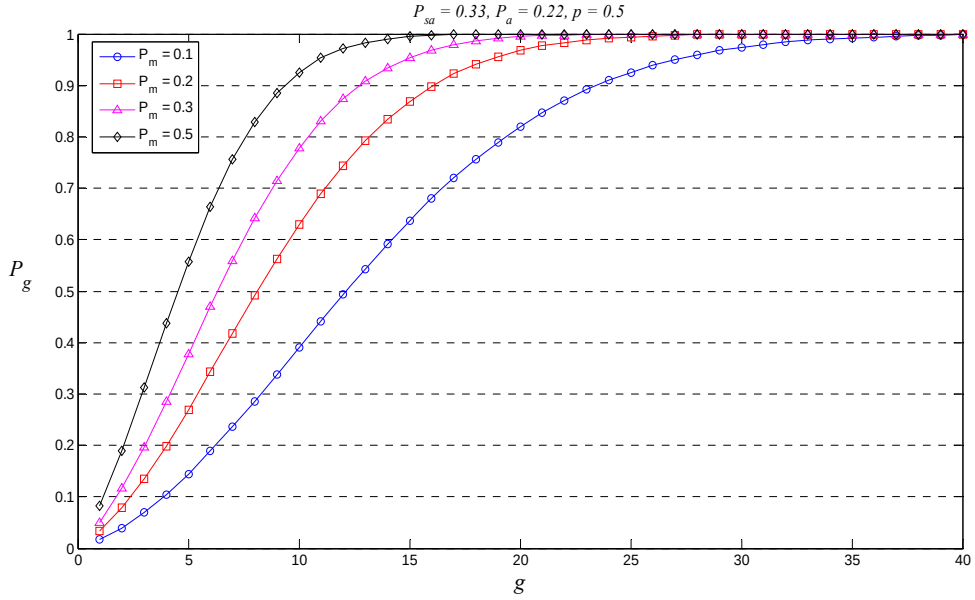


(a)

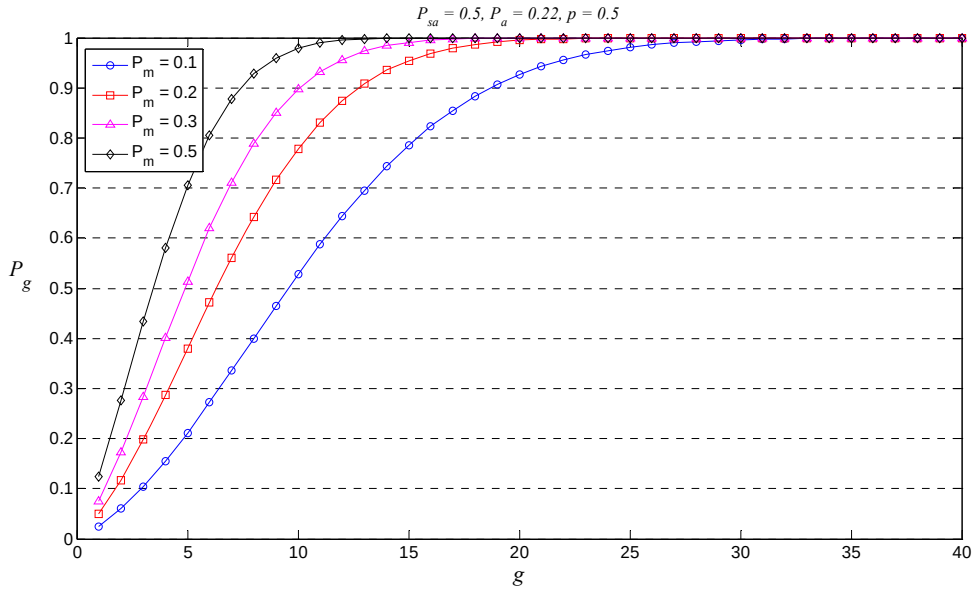


(b)

Fig. 19. The probability P_{conn} for various node density vs. the ratio of stationary access nodes and the probability p that a sensor and a stationary access node share at least a common chosen password (c = 60 and c = 120)



(a)



(b)

Fig. 20. The probability P_g under given probabilities of P_{sa}, P_a, P_m, and p vs. the average number of *stationary access nodes* g in a sensor neighborhood

$$P_g = 1 - (1 - pP_{sa}P_m)^g \cdot (1 - pP_mP_aP_{sa})^{g(g-1)} \qquad (3.11)$$

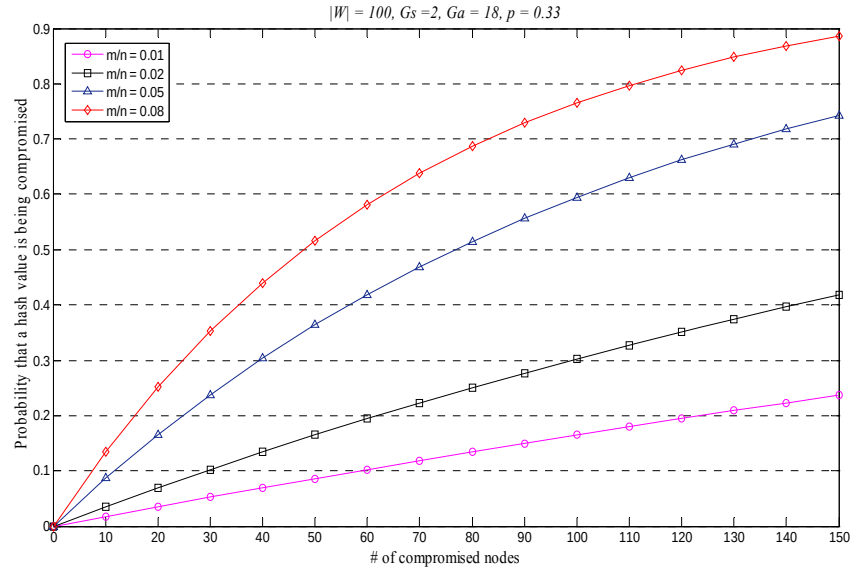
2. Threat analysis

In the *stationary access node replication* attack, the adversary needs to capture at least one polynomial from the static pool and at least one hash value $H^{r-1}(\ )$ of a chosen password. To analyze the security performance of the enhanced three-tier scheme, we estimated the probability P_{hp} of non-compromised sensor node being under a *stationary access node replication* attack when x number of nodes is being captured. In order to calculate the probability P_{hp} for a non-compromised sensor node that's had a hash value $H^r(Pw_i)$ in its hash value ring and static polynomial y in its static polynomial ring, we required to obtain the probabilities of both that $H^{r-1}(Pw_i)$ and polynomial y are being compromised when x nodes is captured.

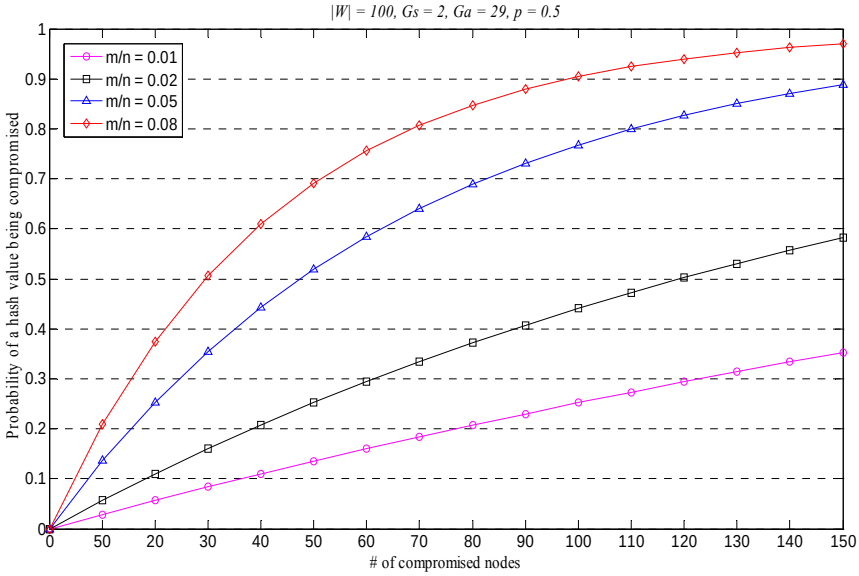
The probability P_h that a given hash value is not chosen by a non-compromised *stationary access node* is $1-\frac{Ga}{|W|}\times\frac{m}{n}$. If there are x compromised nodes, the probability that a given hash value $H^{r-1}(Pw_i)$ is not captured is $(1-\frac{Ga}{|W|}\times\frac{m}{n})^x$. The probability of the hash value being captured is thus

$$P_h = 1 - \left(1 - \frac{Ga}{|W|} \times \frac{m}{n}\right)^x \tag{3.12}$$

Fig. 21 shows the probability of a hash value $H^{r-1}(\ )$ being compromised vs. the number of captured nodes. From these figures we observed that, the probability P_h increases dramatically as we increase the ratio of stationary access nodes $\frac{m}{n}$ from 1% to



(a)



(b)

Fig. 21. The probability P_h of hash value being compromised vs. the number of compromised nodes under different stationary access nodes ratio $\frac{m}{n}$

8%. In the case of the captured static polynomial y of degree t, the attacker cannot determine the non-compromised static polynomial-based key if he/she has captured no

more than *t* nodes. Similar to the analysis in [35], let us assume the case where the number of compromised sensors $x > t$. The probability of any polynomial being chosen for a sensor node is $\frac{K_s}{|S|}$, and the probability of this polynomial being chosen exactly *j* times among *x* nodes is

$$P(j) = \binom{x}{j} \cdot \left(\frac{K_s}{|S|}\right)^j \cdot \left(1 - \frac{K_s}{|S|}\right)^{x-j} \tag{3.13}$$

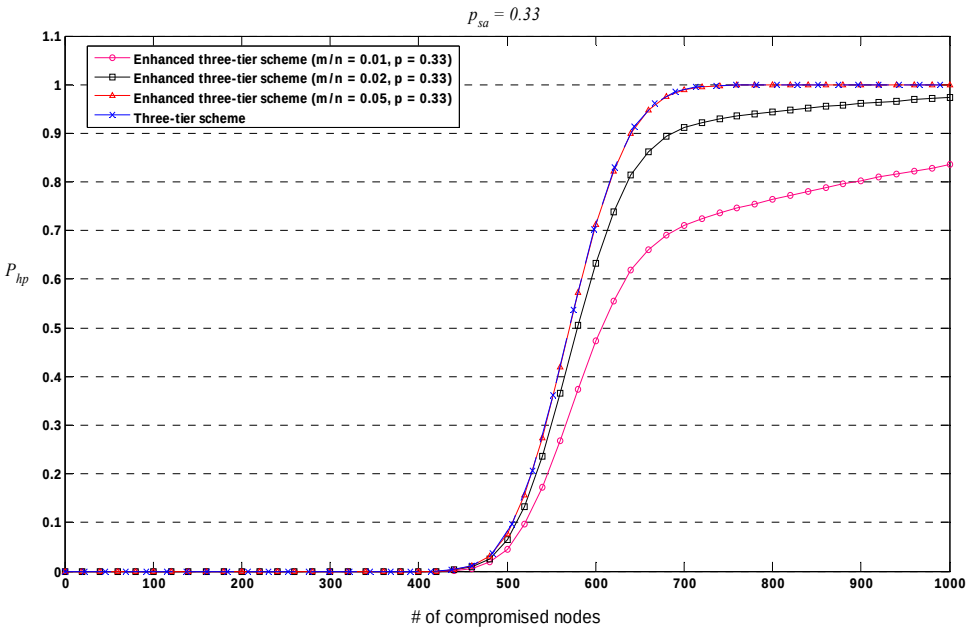
Thus the probability of polynomial *y* being compromised is

$$P_p = 1 - \sum_{j=0}^{j=t} p(j) \tag{3.14}$$

From equations (3.12) and (3.14) the probability P_{hp} that a non-compromised sensor node is under a *stationary access node replication* attack is thus can be estimated by

$$P_{hp} = \left(1 - \sum_{j=0}^{j=t} p(j)\right) \times \left(1 - \left(1 - \frac{Ga}{|W|} \times \frac{m}{n}\right)^x\right) \tag{3.15}$$

Fig. 22 and Fig. 23 show the probability P_{hp} of non-compromised sensor node being under a *stationary access node replication* attack. The figures clearly indicate that for low fraction of *stationary access node* ($\frac{m}{n} = 0.01$, $\frac{m}{n} = 0.02$) the enhanced three-tier security scheme has a butter security performance in terms of network resilience to *stationary access node replication* attack as compared to the previously proposed three-tier scheme. For *stationary access node* ratio greater than 2%, both versions of the three-tier Security scheme have similar resiliency against *stationary access node replication* attack



(a)

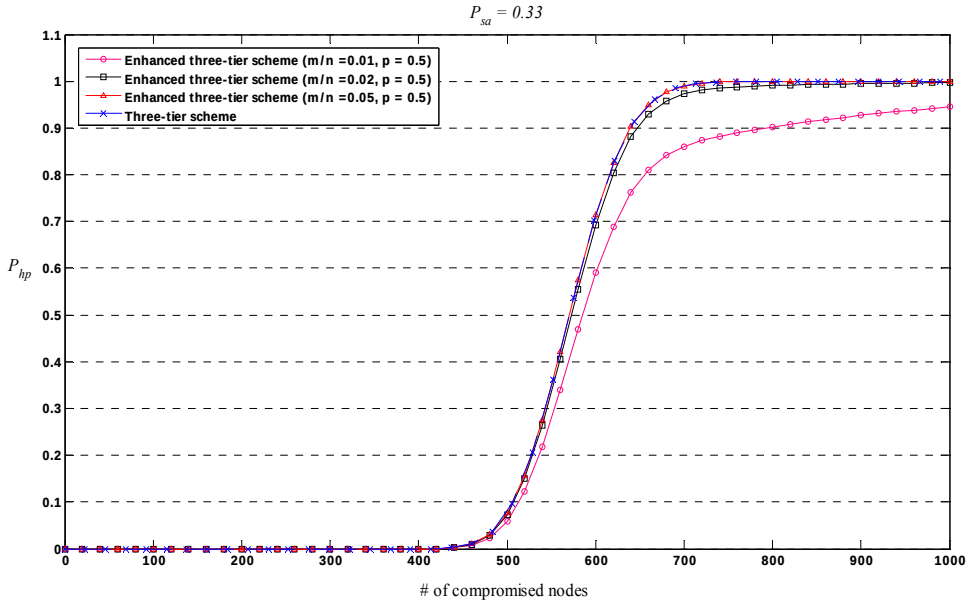
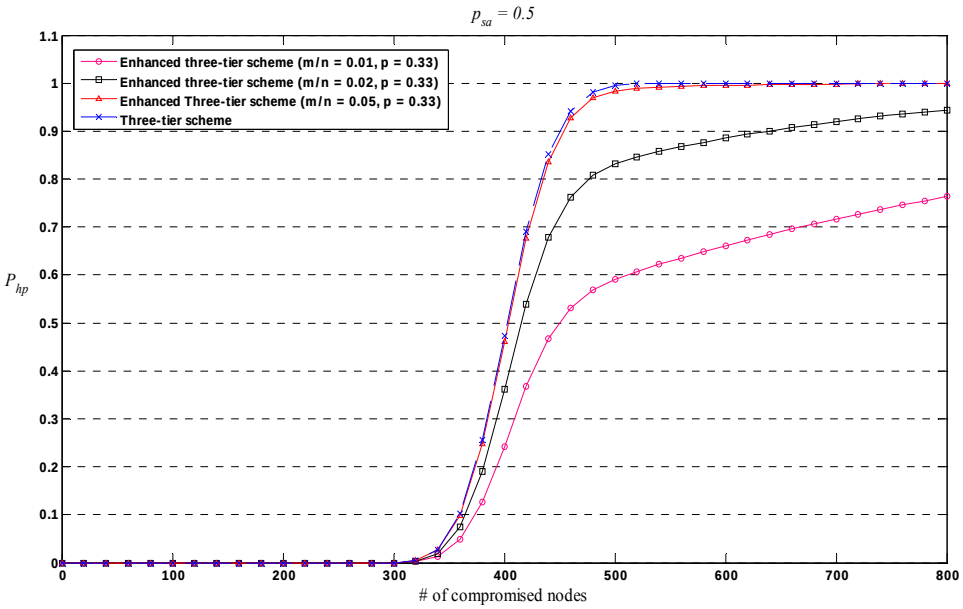
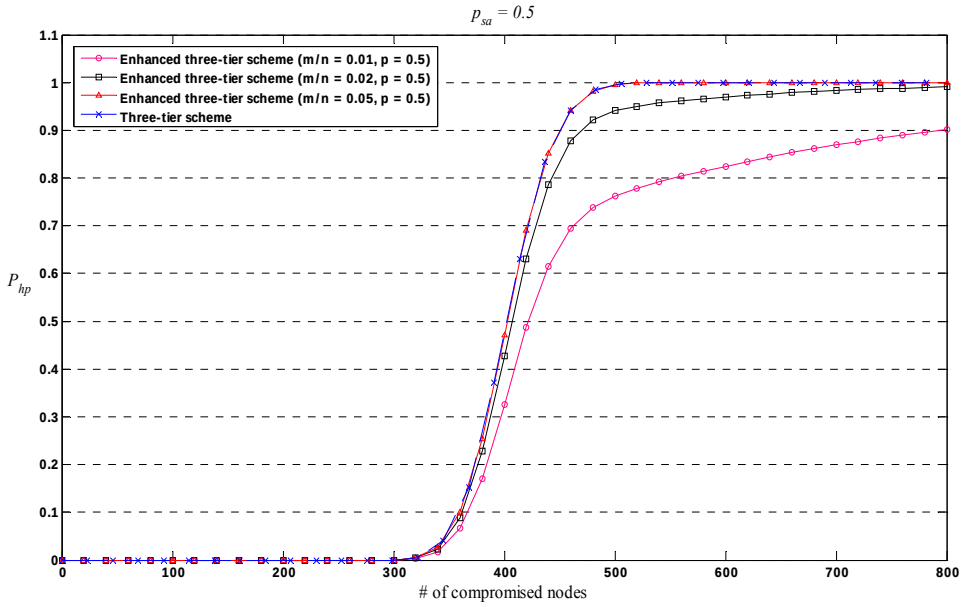


Fig. 22. The probability P_{hp} *o*f a non-compromised sensor node being under a stationary access node replication attack (P_{sa} = 0.33)



(a)



(b)

Fig. 23. The probability P_{hp} *o*f a non-compromised sensor node being under a stationary access node replication attack (P_{sa} = 0.5)

C. SUMMARY

In this chapter, we proposed a general three-tier security framework for authentication and pairwise key establishment between mobile sinks and sensor nodes. The proposed scheme is based on the polynomial pool-based key pre-distribution scheme, it substantially improve network resilience to *mobile sink replication* attacks compared with the single polynomial pool-based key pre-distribution approach [35]. In this scheme, a small fraction of pre-selected sensor nodes, called the *stationary access nodes,* acts as authentication access points to the sensor network, the scheme uses separate polynomial pools: The mobile polynomial pool and the static polynomial pool. The mobile polynomial pool is used for authentication and keys setup between mobile sinks and *stationary access nodes.* The static polynomial pool is used for authentication and pairwise key establishment between sensor nodes and *stationary access nodes.* Mobile sinks use the *stationary access nodes* to establish secure communications links with sensor nodes. Using two separate key pools and having few *stationary access nodes* carrying polynomial from the mobile pool in the network made harder for an attacker to gather sensors data by deploying a replicated mobile sink. Analysis indicates that with 10% of the sensor nodes in the network carrying a polynomial from the mobile pool, for any mobile polynomial to be recovered, the attacker would have to capture 20.8 times more nodes as compared to the single polynomial pool approach. We further improve the security performance of the proposed scheme against *stationary access node replication* attack by strengthen the authentication mechanism between *stationary* access *nodes* and sensor nodes.

CHAPTER IV

ANTI WORMHOLE ATTACK SCHEMES IN SENSOR NETWORKS WITH A CONTROL MOBILTY-SINK

The use of mobile sinks in WSN introduces a new security challenge. Fig. 24(a) shows a wireless sensor network with one mobile sink and a base station. Sensor nodes store the generated data in their buffers. The mobile sink traverses the network using random walk, periodically transmitting beacon signals. Sensor nodes that hear the mobile sink's beacon transmission begin transferring their aggregated data to the mobile sink. Since the mobile sink's beacon signal received by sensor nodes is not authenticated, an adversary can attack the network by placing a malicious mobile sink. As shown in Fig. 24(b), the malicious mobile sink begins transmitting beacon signals. Nodes that hear the malici-

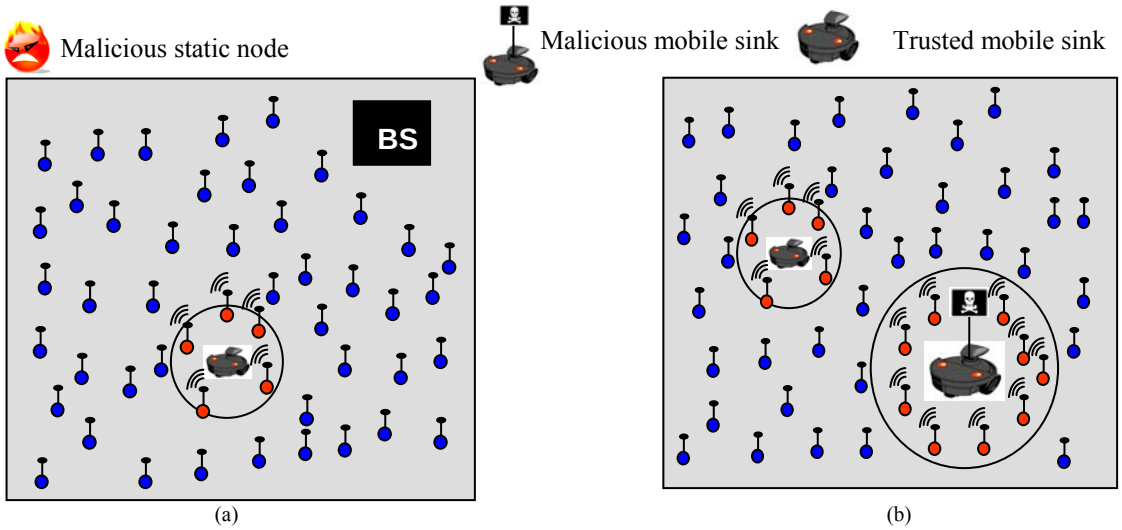


Fig. 24. (a) sensor network with a mobile sink. The mobile sink traversing the network randomly to collect sensors data. (b) Wireless sensor network with a malicious MS

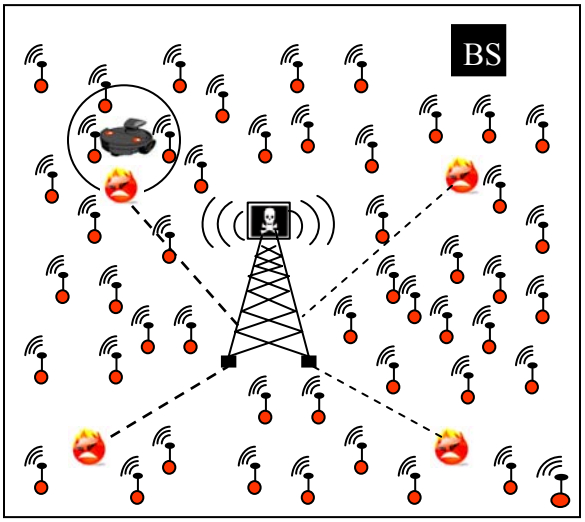


Fig. 25. Wormhole-HELLO flood attack

ous beacon sink will transmit their aggregated data to the malicious sink. The attacker can also launch a wormhole-HELLO flood attack by placing multiple malicious nodes capable of short-range communications and one with a powerful transmission range. When a short-range malicious node hears the mobile sink beacon, it tunnels the beacon signal over a secret communication channel to a high-range malicious node, which broadcasts the mobile sink beacon signal over the entire network, causing nodes that are not within the mobile sink's communication range to transmit their aggregated data, as shown in Fig. 25. Fig. 26 illustrates a different type of attack on a network that uses a controlled mobile sink to collect data. The mobile sink uses a deterministic communication path to collect sensor data from nodes that rely on the mobile sink's communication path. An attacker can launch a wormhole-sinkhole attack by having a number of static

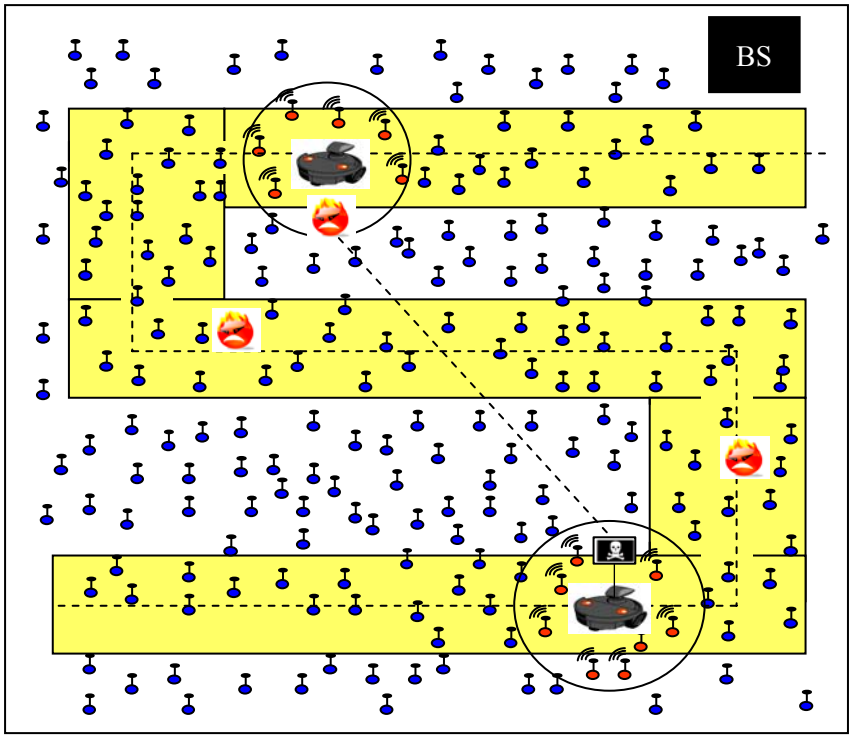


Fig. 26. Wormhole-Sinkhole attack

malicious nodes placed within the trusted mobile sink's communication path and one malicious mobile sink that moves along the trusted communication path. When a static malicious node hears the trusted sink's beacon signal, it tunnels the beacon message through a secret channel to a malicious mobile sink. The malicious mobile sink replays the beacon signal on different part of the network, causing nodes to transmit their aggregated data to the malicious mobile sink.

Another type of a wormhole attack is shown in Fig. 27. The attacker places a malicious node within the trusted mobile sink's communication path. The trusted sink moves along the communication path transmitting beacon signals. When it visits an attacker node, the attacker node records the trusted mobile sink's beacon and replays it ba-

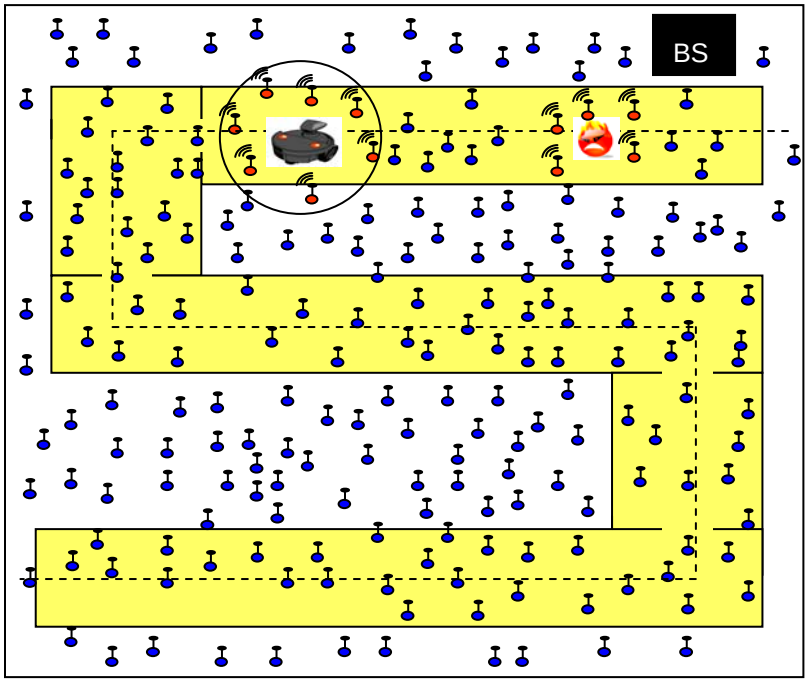


Fig. 27. Wormhole attack

ck at a different time. This will cause nodes within the attacker's communication range to transmit their aggregated data to the malicious node.

This chapter proposes a novel countermeasure attack for sensor networks with controlled mobility. The proposed security mechanism does not apply to sensor networks that use a mobile sink with random walk to gather sensors data. Since sensors are hardware- and power-limited, we consider computationally efficient methods, such as the use of an efficient hash function, to prevent attacks on the network. The proposed security mechanism uses a collision-resistant hash function, such as MD5 [54], to authenticate the source of the beacon signal before sensor nodes are allowed to transmit

their aggregated data to the trusted mobile sink. Our defense method is able to eliminate or minimize the effect of the threat models discussed earlier.

The rest of the chapter is organized as follows. Section A describe the network architecture. Section B presents the anti-threat system model. Section C presents the threat analysis. Section D & E show security performance and simulation evaluation for the proposed technique. Section F concludes the chapter and points out some future research direction.

A. NETWORK AND SECURITY MECHANISM

1. Node and network assumption

We assume regular stationary sensor nodes are constrained in resources, and the mobile sink moves along a fixed path to gather sensor data. We assume that every sensor node has space to store several hundred bytes of keying information. Sensor nodes are not synchronized. A mobile sink can be as powerful as a laptop-class device or a PDA. Mobile sink and sensor nodes have the same communication range R. The mobile sink's communication path (see Fig. 28) is divided into $\frac{L}{x}$ grids or cells, where L is the length of mobile sink's communication path and x is the cell length. In our system model, we assume $R > x$. A base station is located in a fixed and secure location. We assume that the base station and the mobile sink cannot be compromised.

2. Key establishing and hash values distribution schemes

A sensor node encrypts its data using a pre-loaded individual key shared with the base station. The base station generates a master key K_m , from which it derives an indi-

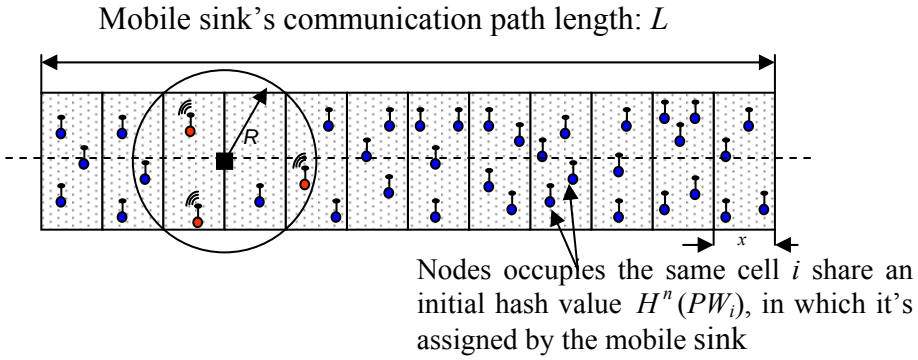


Fig. 28. Key distribution scheme

vidual key for every node u as $K_u = G_{Km}(u)$, where G is a pseudo-random function [55]. Sensor nodes send their encrypted messages to the mobile sink. Since the mobile sink does not carry individual key information for each sensor, it cannot decrypt sensors messages. The mobile sink carries the sensor's encrypted message to the base station. Hence, given an encrypted sensor message $[\{m\}K_u , u]$, u is the node ID, and $\{m\}_k$ denotes the encryption of message m with key k, the base station can compute its pairwise key with a sensor whenever needed, without having to store any pairwise keys.

Initially, the base station dispatches the mobile sink to distribute initial hash values information among sensor nodes. To prevent a malicious node from injecting false hash values information into the network during the hash values distribution phase, we

require sensors to authenticate the source of the beacons using *collision-resistant hash functions*.

We use the following scheme based on *efficient one-way hash chains* [53] to provide the mobile sink's beacon authentication [56], [57]. The mobile sink is pre-loaded with a global password PW_G and a table containing a unique password PW_j for each cell j in the mobile sink's communication path. As shown in Fig. 28, in a sensor network with a communication path of length L and cell of length x, the mobile sink is pre-loaded with L/x unique passwords. Passwords are blinded with the use of a *collision-resistant hash function* such as MD5 [54]. Due to the collision-resistant property, it is computationally infeasible for an attacker to find a value PW_x, such that $H(PW_y) = H(PW_x)$, $PW_x \neq PW_y$. The hash sequence generated for sensors in cell j uses the following equation:

$$H^0 = PW_j \, , H^i = H(H^{i-1}) \, , \quad i = 1, 2, \ldots n$$

with n being a large number and H^0 never revealed to any sensor in cell j. Each sensor node is pre-loaded with a hash value $H^n(PW_G)$. During the key distribution phase, the mobile sink moves along a deterministic path transmitting beacon messages which contain hash value information. For example, when the mobile sink is within cell j, it transmits a beacon message with the following format:

$$(H^{n-1}(PW_G)) \,||\, (H^n(PW_j)),$$

Initially, sensor nodes in cell j only know the hash value $H^n(PW_G)$. The mobile sink includes $H^{n-1}(PW_G)$ and the corresponding initial hash value for nodes within cell j. Every sensor node in cell j that receives the mobile sink's beacon can authenticate the source of

the beacon transmission if $H(H^{n-1}(PW_G))=H^n(PW_G)$. After verification, sensors in cell j replace $H^n(PW_G)$ with $H^{n-1}(PW_G)$ in their memory and each node is assigned the same initial hash value $H^n(PW_j)$.

B. PROPOSED SECURITY SCHEME

Since the proposed security mechanism prevents sensor nodes from sending their aggregated data to a malicious beacon node, we consider mobile sink's beacon authentication. Since sensors are constrained in both computational power and energy resources, we do not consider asymmetric key cryptography solutions. In addition, we do not consider symmetric key cryptography. Since the compromise of a single node makes the entire network susceptible to attacks, the proposed scheme is based on *efficient one-way hash chains* [53] in which sensors must verify the source of the beacon message before they are able to transmit their data to the beaconing node (mobile sink).

We introduce the following terminologies, which will be used to describe the proposed security scheme:

- *Service Time:* A mobile sink arriving at cell j transmits beacon messages for duration of T_s second. Each beacon transmission includes the hash value $(H^{n-i}(PW_j),i)$. With i, represent the i^{th} hash value published in cell j during the i^{th} visit. All communication cells have the same *service time* T_s, which can be calculated as follows.

  $T_s = 2x/v$, where x represent the cell length and v is the mobile sink speed.

- *Communication Time:* T_c, is the time interval in which a sensor node s in cell j can directly communicate with the mobile sink and is able to authenticate its beacon transmission. T_c is an important metric in the proposed scheme, as it controls the number of sensors that will be under attack.

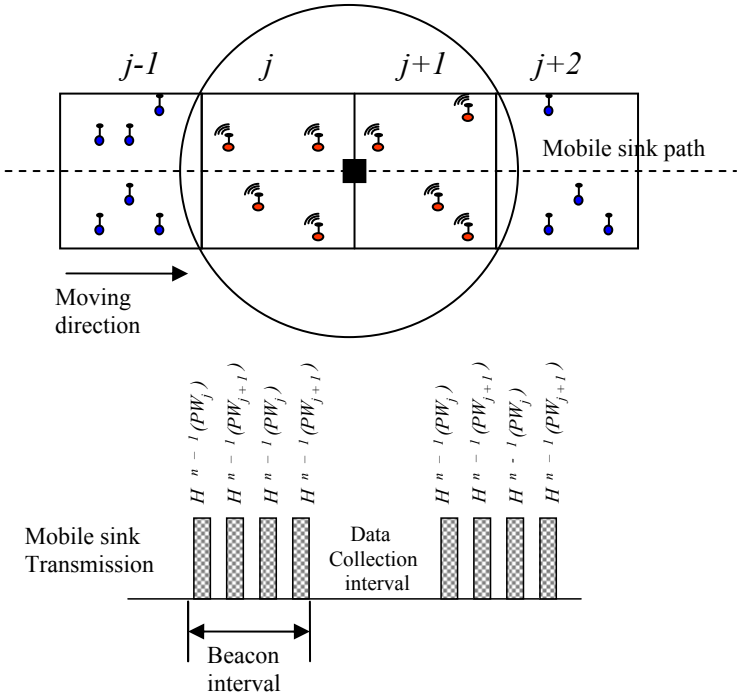


Fig. 29. The proposed security mechanism

Fig. 29 illustrates the proposed security mechanism. At the end of the hash values distribution scheme, sensor nodes in cells j and $j+1$ have initial hash values $H^n(PW_j)$ and $H^n(PW_{j+1})$, respectively. With n here being a large number, nodes will exhaust their energy before reaching n; therefore, it represent the number of times the mobile sink vis-

its a cell, such as j, during the lifetime of the network. We assume that the mobile sink is capable of estimating its (x, y) location, which will use it to determine in which communication's cell it's located. As described in section A, the mobile sink is pre-loaded with a table containing a unique password PW_j for each cell j in the mobile sink's communication path and an index i, which represents the current unpublished hash value in cell j during the i^{th} visit.

Assume the mobile sink in Fig. 29 visit cell $j+1$ the first time. Initially, sensor nodes in cell $j+1$ only know the hash value $H^n(PWj+1)$. During the cell's service time, the mobile sink includes $(H^{n-1}(PW_{j+1}),i)$ in its beacon transmission, with index $i = 1$ (first hash value published in cell $j+1$ during the first visit). Every sensor that hears the first beacon can authenticate the mobile sink's beacon only if $H(H^{n-1}(PW_{j+1})) = H^n(PW_{j+1})$. After verification of the first beacon message, sensor nodes in cell $j+1$ starts a timer with T_c sec (communication time), in which when it is expire, sensors ends their data communication with the mobile sink by replacing $H^n(PW_{j+1})$ with $H^{n-1}(PW_{j+1})$ in their memory. Since $H(\,)$ is a one-way hash function, when a sensor s replaces his hash value $H^n(PW_{j+1})$ with $H^n\text{-}1(PW_{j+1})$, it cannot authenticate the mobile sink beacons because $H(H_{n-1}(PW_{j+1})) \neq H^{n-1}(PW_{j+1})$. This hash value replacement method allows sensor nodes to perform only one hash operation in the reception of mobile sink's beacons during subsequent visits. As shown in Fig. 28 the mobile sink serves cells j and $j+1$ simultaneously. Since the service time for two adjacent cells (cells j and $j+1$), overlap, the mobile sink alternatively includes $H^{n-1}(PW_j)$ and $H^{n-1}(PW_{j+1})$ in its beacon transmission, and gather sensor data from both cells. The sensor *communication time* controls the scheme

security level. With $T_c = \frac{T_s}{2}$, our anti-threats mechanism eliminates all of the WSN attacks, and with an acceptable data throughput. As the s*ensor communication time,* increases, the proposed scheme trade security performance with higher data throughput.

C. SYSTEM MODEL

We consider a WSN as consisting of *N* static sensor nodes and one mobile sink. Sensor nodes are independently and uniformly distributed over a planar surface with area A_{net}. Sensor nodes have a communication time of T_c. The network is homogeneous, in that all sensors are identical. Thus each node has the same amount of energy and uses the same communication range *R*. The mobile sink has a communication range *R*, and it traverses the network using a deterministic path with a speed *v*. To validate the proposed security scheme, we consider the wormhole attack as the threat model. An attacker places a malicious beaconing node within the trusted mobile sink's path. The malicious node replays beacon message originating from the trusted mobile sink, which make sensor nodes believe that the trusted sink is still in proximity, then sensor nodes start their data transmission.

The mobile sink's communication path is divided into equal grids of size $x \times y$, and we assume that the path has the following properties,

- The set of points on the path is topologically path-connected, meaning that every point on the path is reachable from every other point by moving along the path.

- The path can be approximated by a straight line over distances of the order of the communication range of a sensor. In other words, the radius of curvature at each point on the path is large compared the communication path.
- Each grid has a service time T_s.

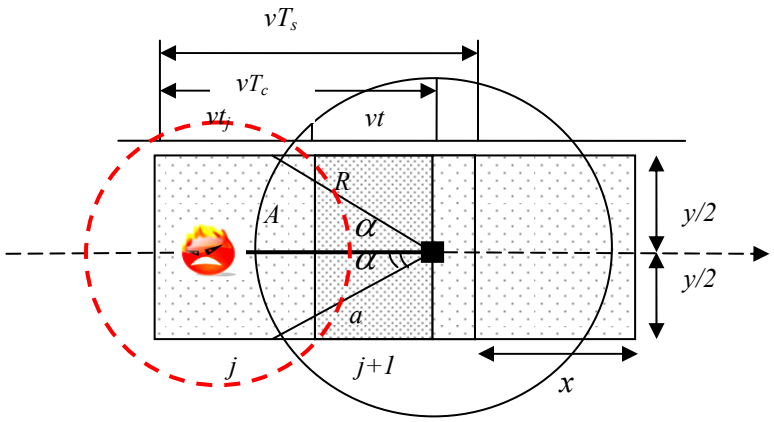


Fig. 30. System model

In a time interval of length t_j (see Fig. 30), the mobile sink moves a distance vt_j along cell j transmitting beacon messages. Nodes within the mobile sink range that were previously unable to authenticate the mobile sink's beacon transmission can now verify the source of the beacons with the potential to transmit data. During the time interval t_j, the probability is equal to zero (P_j=0), that at least one sensor node in cell j is under a wormhole attack. Since sensor nodes remain within the mobile sink's range, the reception of replayed beacons messages triggers sensor nodes to send their data which can be received by the trusted mobile sink.

In the time interval of length *t*, the mobile sink moves a distance *vt* away from cell *j*. Some sensor nodes that were previously within range now out of range, making them vulnerable to wormhole attack.

$$\alpha = sin^{-1} \frac{\sqrt{R^2 - y^2/4}}{R}$$

$$A = y/2\sqrt{R^2 - y^2/4} + (\pi - 2\alpha)R \tag{4.1}$$

$$a = vty \tag{4.2}$$

The network nodes can be modeled as random Poisson points [58]. In each cell, *n* nodes were placed randomly in the interval *T*, where *T* is the sensor communication time. We consider the time interval *t* to be the attack interval, in which a sensor node in cell *j* might be under a wormhole attack. The probability that *k* nodes in cell *j* will lie in the attack interval *t*:

$$p\{k \text{ in } t\} = \frac{(\lambda t)^k}{k!} e^{-\lambda t}, \tag{4.3}$$

where $\lambda = \frac{n}{T}$, with $T = \frac{x}{v}$ and

$$n = \left(xy - \left(y/2\sqrt{R^2 - y^2/4} + (\pi - 2\alpha)R - vty\right)\right)\rho$$

With $\rho = N/A_{net}$ (node density), where

P_j = (the probability that at least one node in cell *j* lie in the attack interval *t*), and

P_j = 1 - (the probability that no nodes in cell *j* lie in the attack interval *t*).

$$P_j = 1 - p\{0 \text{ in t}\} \tag{4.4}$$

$$P_j = 1 - e^{-\lambda t} \tag{4.5}$$

$$P_j = 1 - e^{-\frac{[xy - \left(y/2\sqrt{R^2 - y^2/4} + (\pi - 2\alpha)R - vty \right)]\rho}{T} t} \quad (4.6)$$

Equation (4.6) represents the probability P_j, that at least one sensor node in cell j is under attack. The probability q, in which at least one sensor node under attack is derived as follows:

We consider two cells under attack (j, i), with attack intervals (t_a, t_b), respectively. Since the two intervals (t_a, t_b) are independent and do not overlap. The probability z{k_a in t_a, k_b in t_b}, that k_a and k_b sensor nodes lie in the intervals (t_a, t_b) respectively [58] is expressed as:

$$\text{z } \{k_a \text{ in } t_a, k_b \text{ in } t_b\} = e^{-\lambda t_a} \frac{(\lambda t_a)^{k_a}}{k_a!} e^{-\lambda t_b} \frac{(\lambda t_b)^{k_b}}{k_b!} \quad (4.7)$$

q = (the probability of at least one node lying in the attack interval (t_a or t_b)).

$$q = 1 - \text{z } \{0 \text{ in } t_a, 0 \text{ in } t_b\} \quad (4.8)$$

$$q = 1 - e^{-\lambda t_a} e^{-\lambda t_b} \quad (4.9)$$

And since all communication cells have the same attack interval t ($t_a \equiv t_b \equiv t$).

$$q = 1 - e^{-2\lambda t} \quad (4.10)$$

By generalization, equation (4.10) for ℓ cells under wormhole attack intervals.

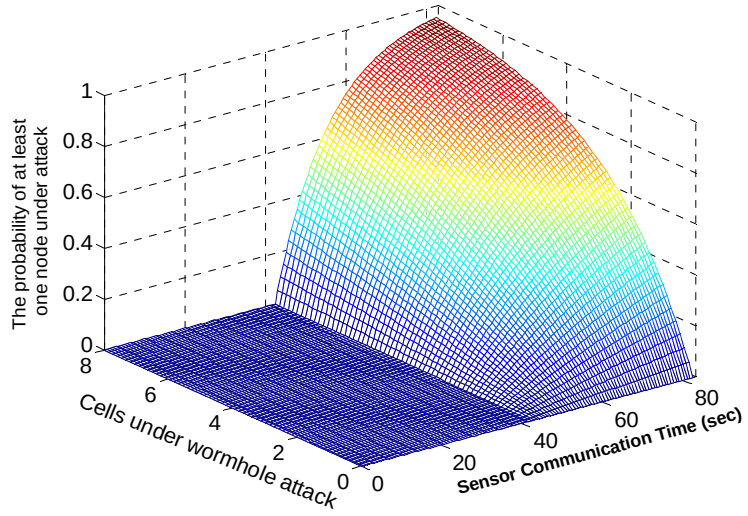
$$q = 1 - e^{-\ell \lambda t} \quad (4.11)$$

D. THREAT ANALYSIS

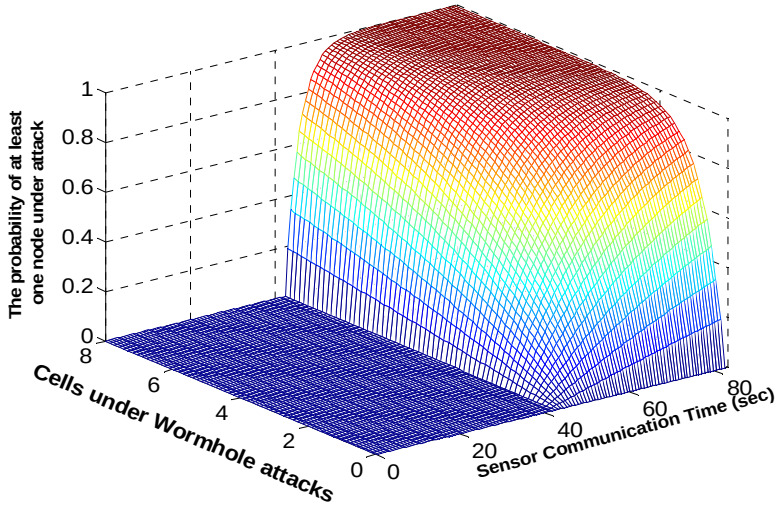
In this section we show that the proposed security scheme is resilient to several types of attacks, such as the wormhole attack [43], [44], [45] and compromised sensors. Our scheme is a trade-off between security performance and lower data collection rate.

Most of the threat models presented in this chapter are based on wormhole attack. In this section, we analyze the wormhole attack, and we show how the proposed scheme is resistant to such type of attack. A malicious beaconing node placed within grid *j* replays the trusted mobile sink beacon messages to gather sensor data. Our scheme eliminates or limits the effect of a wormhole attack into one communication grid *j*. The communication path is divided into grids. Sensor nodes within each grid have a unique hash value which it is used to authenticate the source of the beacon message. As sensor nodes are assigned a communication time $T_c = \frac{T_s}{2}$, the proposed security scheme prevents wormhole attack, and with $T_c > \frac{T_s}{2}$, the scheme offers enhanced security strength at the expense of higher data collection rate. We computed the probability *q* of at least one sensor node under wormhole attack. We consider a WSN with at most eight independent wormhole attacks (ℓ malicious beacon nodes placed within the trusted communication path). In Fig. 31(a), Fig. 31(b), and Fig. 32, we show the probability *q* for $\ell \in$ [0, 8] wormhole attacks, sensor communication time $t \in$ [0, T_s= 80 sec], and with node densities {50, 200, 1400}. From Fig. 31 and Fig. 32, we observe that the probability *q* increases rapidly as we increase the WSN node density from 50 nodes in Fig. 31(a) to 1400 nodes in Fig. 32. In addition, with ℓ cells under attacks, increasing the sensor

communication time T_c increases the probability q, since more sensor nodes will lie outside the trusted sink's range and become under wormhole attack.



(a)



(b)

Fig. 31. Probability q, that at least one sensor node under wormhole attack for different node densities. (a) 50 nodes. (b) 200 nodes

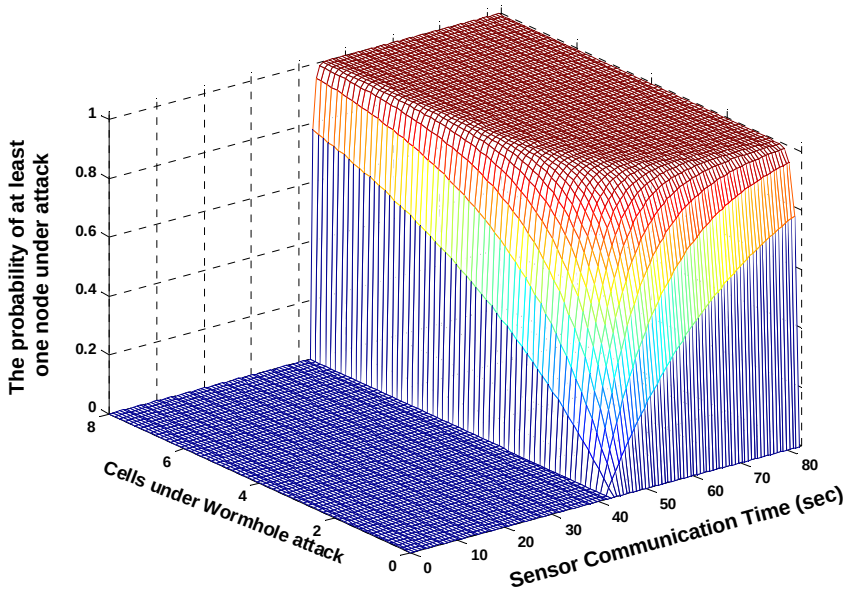


Fig. 32. The probability q for a WSN with 1400 nodes

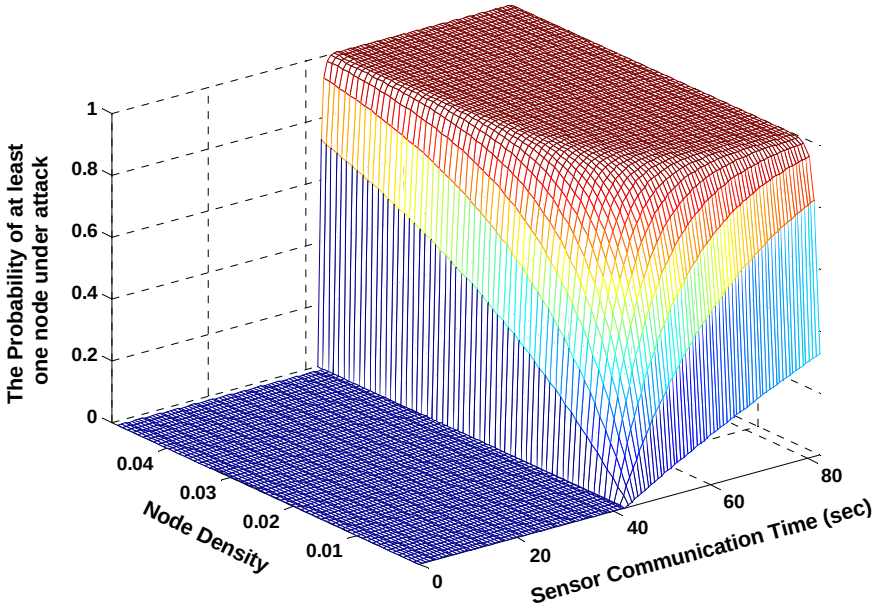


Fig 33. The probability q under various node density and sensor communication time

Fig. 33 shows the probability q for various node densities. The probability q increases exponentially with node density. Fig. 34 shows the wormhole attack p.d.f for various sensor communication time.

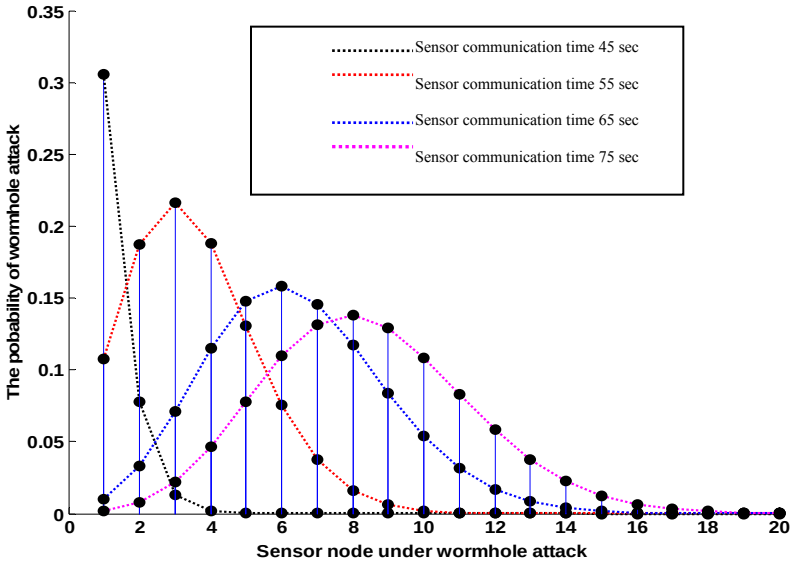


Fig. 34. The wormhole attack probability density function for various sensor communication time

E. PERFORMANCE EVALUATION

We randomly distribution 400 sensors within 2000×2000 m^2 rectangular area. Initially, the base station dispatches a mobile sink, it moves at a constant speed 50cm/sec along a deterministic data collection path transmitting beacon messages, which divide the data collection path into equal grids of size 20m×40m according to the distribution of sensor's initial hash values. After the distribution of the sensor's initial hash values, the mo-

bile sink travels along the data communication path sending beacon messages to sensors that lies within it range (mobile sink communication range R = 30m). A sensor node that hears the data request beacon message, first, it verifies the source of the beacon message before it sends its aggregated data to the beaconing node. We investigated the impact of wormhole attacks on the proposed security scheme. We evaluated the proposed security scheme with 1, 4, 8, and 16 malicious beacon nodes that were deployed within the trusted sink's data collection path. The malicious nodes were distributed among different data collection grid. Fig. 35 shows the effect of sensor communication time $T_c > \frac{T_s}{2}$ on the overall network data transfer rate. Data transfer rate increases as the sensor communication increases, since the mobile sink takes longer to collect sensors data. The figure also show that as the number of grids under attack increases, the overall network data collection rate increases.

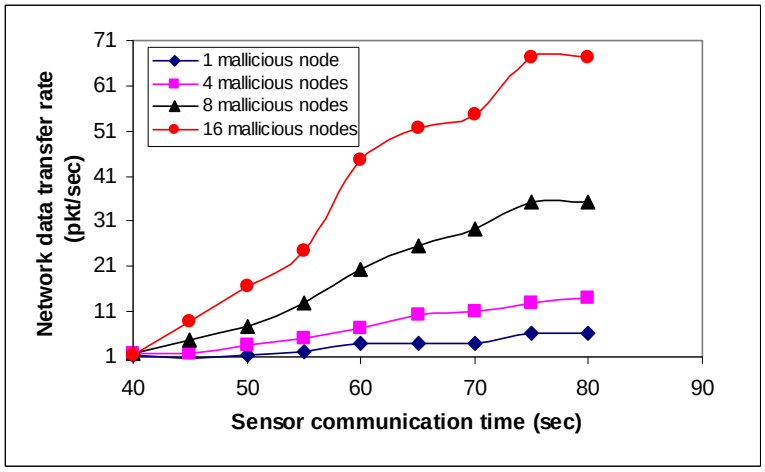


Fig. 35. The data transfer ratio with 1, 4, 8, and 16 malicious nodes and various sensor communication time

Fig. 36 shows the aggregated adversary data ratio: the ratio of the number of data packets transmitted when sensors hear a replayed beacon message to the total number of data packets transmitted. For sensor communication time $T_c > \frac{T_s}{2}$, this ratio increases as the sensor communication interval increases. Since sensors will take longer before they can update their hash values, replayed beacon messages transmitted from an attacker node can still be verified by the sensors even thought they are outside the trusted mobile sink range. We examine the aggregated adversary ratio under 1, 4, 8, and 16 attacker nodes.

We studied the influence of wormhole attacks on the total network energy consumption. For various number of grids, which are under wormhole attacks, as shown in Fig. 37, we determined the total network energy consumption for two sensor communication times (40 sec and 70 sec).

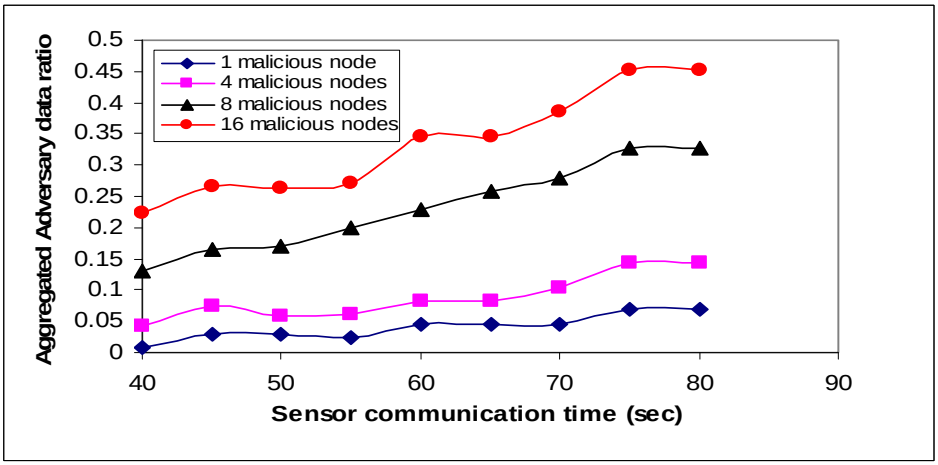


Fig. 36. The adversary data ratio with 1, 4, 8, and 16 malicious nodes and various sensor communication time

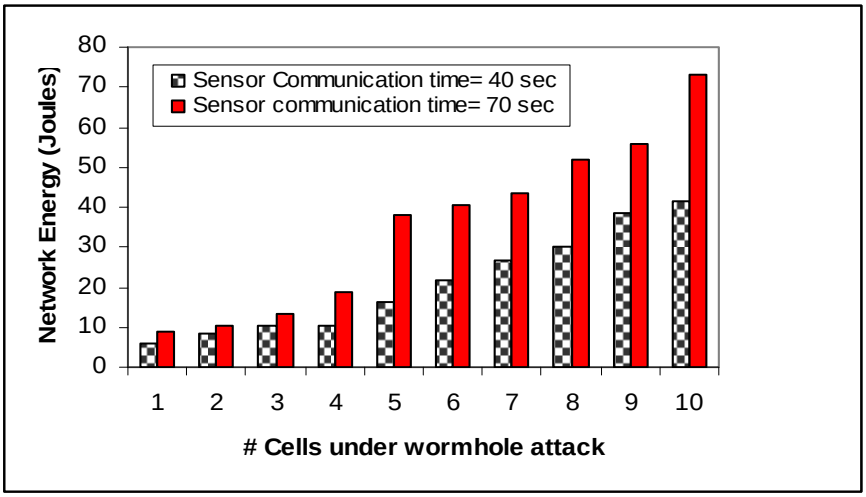


Fig. 37. Network energy with various number of cells under attack

F. SUMMARY

In this chapter, we identified new security challenges of using mobile sink for efficient data collection. A malicious beaconing node with a high transmission power replays the trusted mobile sink's data request message over the entire network causing large data loss. An adversary may easily bring down or even take over the sensor network by placing a malicious mobile node, which moves along the trusted sink's pre-determined path. In this chapter, we propose a robust security scheme, which allows a sensor to authenticate the data request message to ensure reliable data collection. Through definitive simulations and analysis, we show that our security scheme is robust against severe wireless sensor network attacks, such as wormhole attacks and HELLO flood attacks. We present a threat analysis and determine the probability that at least a single node is under wormhole attack.

CHAPTER V

ANTI WORMHOLE ATTACK SCHEME IN SENSOR NETWORK WITH A RANDOM MOBILITY-SINK

As described in the previous chapter, we proposed a security scheme against *wormhole* attack for WSN with MS which use control mobility to gather sensor data. In this chapter, a new technique is proposed, which allows a sink with random mobility to establish a secure link with any sensor node on the fly and to defend against threats posed by wormhole attacks and collusion of malicious nodes. The proposed technique has been tested using the polynomial pool–based key pre-distribution scheme [35], in addition to comparison with the scheme proposed by S. Hussain, F. Kausar, and A. Massod [48], which will be referred as the random generation key scheme, because the two schemes provide minimal communication overhead for sensors to establish pairwise keys with the MS compared to other existing schemes [32], [34]. Multiple communication channels available on the sensor hardware are used to depict the feature of resiliency against wormhole attack and node collusion.

It is assumed that every sensor node's hardware including the MS has *c* available communication channels. Prior to network deployment, every sensor node is pre-loaded with polynomial shares of a randomly selected subset of polynomials, called the *polynomial ring*. After every sensor node is randomly assigned a subset of polynomials, the base station dispatches the MS to gather sensor data; it randomly picks a subset of polynomials and assigns them to the MS. All the sensors and the MS use a pre-selected

common channel termed the *discovery channel.* A sensor node uses the *discovery channel* to detect whether it is within proximity of the MS. It uses this channel to establish both a common encryption key and a secure channel with the MS to transfer its encrypted data. The MS can establish a pairwise key with any sensor node on the fly. For every sensor node *u*, which wants to communicate securely with the MS, the two must first establish a common key. Second, the MS randomly picks a secure channel from a set of *c* available channels and assigns it to the sensor node *u;* the node *u* uses this secret channel for a specified period of T_s seconds to transfer its encrypted data to the MS. Through probabilistic analyses, it has been shown that even when 50% of a sensor node's neighbors are malicious devices, the provision of with a single extra channel for communication with the MS brings down the probability of a wormhole attack to nearly zero.

The rest of the chapter is organized as follows. Section A describes the sensor-network architecture. Section B introduces the proposed technique. Section C discusses the threat analysis. Section D presents the performance evaluation. Section E concludes the study.

A. SENSOR NETWORK ARCHITECTURE

A typical sensor network that has hundred to several thousand low-cost, power-constrained nodes with limited computational power and storage capability has been considered. Each sensor has *c* available channels and is capable of dynamically switching between them. Nodes conserve energy by aggregating the data in their internal

buffer. The network has a high-end MS. The MS is more powerful than any sensor. It has enhanced capability for computation, communication, energy supply, and storage, and it cannot be compromised. It acts as an agent to collect sensor reading. The MS dynamically assigns a communication channel from a set of *c* available channels to any sensor node on the fly.

The key-establishment patterns between any two nodes or between a node (e.g. node *i*) and the MS falls into two categories: direct key establishment (e.g. both the MS and a sensor node *i* share at least a common bivariate polynomial); indirect path key establishment (e.g. MS and node *i* execute the path key establishment through an intermediate node *j*, which shares a common polynomial with both the MS and the sensor node *i*, and the MS generates a new shared key that will be sent to *i* over the secure path MS—*j*—*i*.

In this article, a sensor network, with sensor nodes numbering more than 1000 and nodes within the MS's communication range exceeding 30 nodes, has been considered.

B. THE PROPOSED TECHNIQUE

A new technique is herein proposed to minimize the threats posed by wormhole attacks. This technique relies on the assumption that any physical device has only one radio. It is also assumed that a radio is incapable of simultaneously sending or receiving on more than one channel.

After network deployment, every sensor node is pre-loaded with polynomial shares of a randomly selected subset of polynomials. The base station dispatches the MS

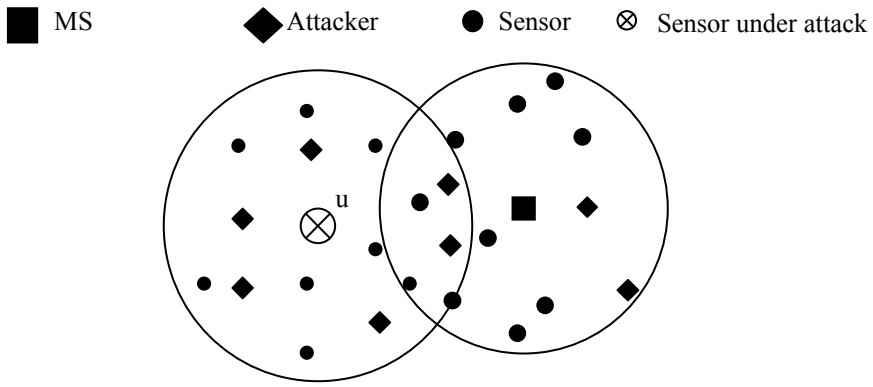


Fig. 38. Sensor node under wormhole attack in WSN with random mobility-sink node

to gather sensor data securely. The MS is loaded with its randomly selected subset of polynomials.

Initially, all sensor nodes including the MS have their radios tuned to a pre-selected common channel, called the *discovery channel*. The MS traverses the network that transmits beacon messages over the *discovery channel*; the beacon message contains the MS ID. Sensors that are in proximity of the MS can hear the MS beacons. Each sensor will engage its polynomial pool-based key scheme [35] to establish a pairwise key with the MS through either direct key establishment or by the path-key discovery. For every sensor node u that lies within the MS range (see Fig. 38) and establishes a common key k with MS, the MS picks a channel f_i, from a set of c available channels $\{f_1, f_2, f_3, \ldots, f_{c-1}, f_c\}$. The MS then sends the message $\{f_i\}_k$ over the *discovery channel* to sensor node u. The sensor node u receives the encrypted message, decrypts it using the shared key k, and tunes its radio to the specific channel for a period of T_s seconds. Node

u uses this secret channel f_i to transmit encrypted data messages $\{data\}_k$ to the MS. After T_s seconds, the sensor node u switches back its radio to the discovery channel. It is assumed that the distribution of the different channels over the sensor nodes follows a uniform distribution. From the randomly assigned list of channels, the MS picks a channel f_j and switches its radio from the discovery channel to f_j for a specified period of t_s sec, where $t_s << T_s$. The MS transmits a stream of data-pull beacon messages over the channel f_j and listens to it. Sensor nodes that are in the proximity of the MS's range and have their radios tuned in to f_j hear the MS transmission and reply back by sending their encrypted data messages to the MS. If no sensor nodes in the range of the MS have their radios tuned in to this channel, the MS deletes this channel from the list of assigned channels. After time t_s, the MS tunes its radio back to the discovery channel and transmits a burst of beacons that contains its ID, so that sensor nodes that were not in the MS's range before and now are within range will be able to establish a secure communication link with the MS. Similarly, the process is repeated with every channel chosen by the MS from the list of assigned channels. It is, however, assumed that all the assigned channels are chosen equally from the list.

C. THREAT ANALYSIS

To mount a wormhole attack [43], an adversary initially establishes a direct link between two points in the network. The attacker's link is referred to as the wormhole link. Once the wormhole link is established, the attacker eavesdrops on the messages at one end of

the link, referred as the origin point, tunnels them through the wormhole link and replays them at the other end, referred as the destination point.

In sensor networks with MS, the use of a single channel for communication between sensor nodes and MS makes the probability of a wormhole attack approximately unity. An attacker that is in the proximity of the MS can easily record the MS messages, tunnel them through an established wormhole link, and replay them at the other end of the link. Thus, using channel diversity for secure communication helps minimize this threat. In this work, a wormhole attack launched by a single malicious node using the discovery channel is not considered a continuous threat because the attacked node will use the wormhole link to switch its communication channel from the discovery channel to a channel assigned by the MS, which will prevent any further attacks from the malicious node. A successful wormhole attack will be accomplished when a sensor node begins sending its encrypted data messages although it is not within the MS range. Two malicious nodes need to collude to launch a successful wormhole attack. One of the two malicious nodes must have its radio tuned in to the discovery channel and the other to any other available channel.

As a concrete example, consider a sensor node *u* that has *m* legitimate neighbors and *n* malicious nodes within its communication range. The sensor *u*'s radio has *c* available communication channels. Suppose that out of the *c* available channels, a subset of *r* channels is chosen by the *n* malicious nodes to launch a wormhole attack. Each of the *r* channels is assumed to be equally chosen by *g* malicious nodes, where $g=\frac{n}{r}$.

Now, suppose that a nodes from u neighbors are located within the MS range, where $a \le g$, the probability p_a of a successful wormhole attack is

$$p_a = \sum_{i=2}^{i=\ell} p_i\,(attack\ \ with\ \ i\text{-}wormhole links),$$

where $\ell = a$ if $a \le r$; otherwise, $\ell = r$.

$$p_a = \sum_{i=2}^{i=\ell} p\,(attack \mid i\text{-}wormhole\ links)\, q(i\text{-}wormhole\ links) \tag{5.1}$$

q(*i-wormhole links*) is the probability of having i wormhole links, each with a different channel being randomly selected among the r channels.

$$q(i\text{-}wormhole\ \ \ links) = \frac{\binom{r}{i}\left\{\binom{i\times g}{a} + \sum_{j=1}^{j=i-1}(-1)^j \binom{i}{i-j}\cdot\binom{(i-j)g}{a}\right\}}{\binom{d}{a}}$$

where $d = m+n$; then,

$$p_a = \sum_{i=2}^{i=\ell} \frac{i}{c} \times \left\{ \frac{\binom{r}{i}\left\{\binom{i\times g}{a} + \sum_{j=1}^{j=i-1}(-1)^j \binom{i}{i-j}\cdot\binom{(i-j)g}{a}\right\}}{\binom{d}{a}} \right\}$$

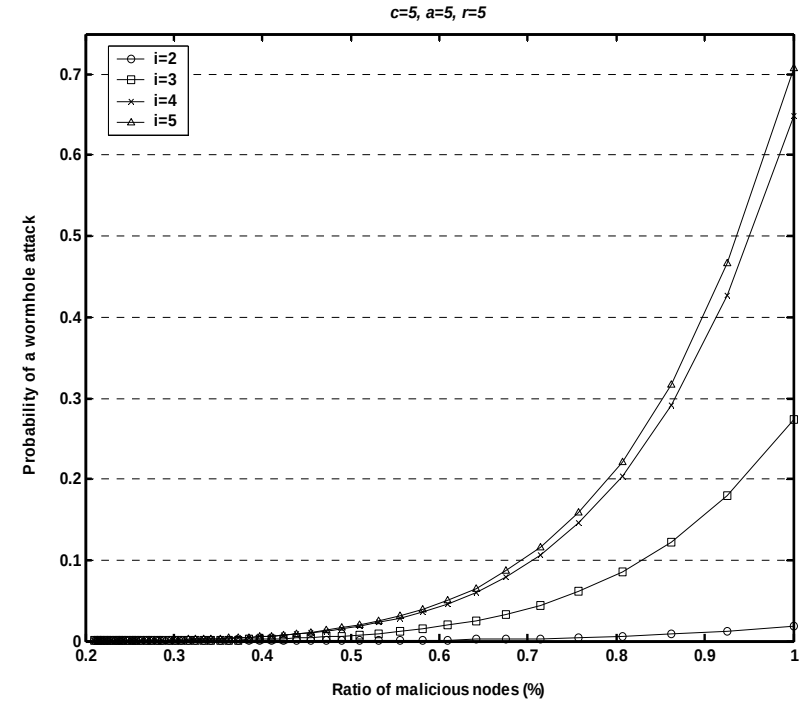
D. PERFORMANCE EVALUATION

Fig. 39 [(a) & (b)] shows the probability p_a of a sensor u with varied number of wormhole links and different malicious node ratios [0.2, 1] when 5 of the sensor *u's* neighbors became within the MS range. In Fig. 39(a), the probability p_a has been

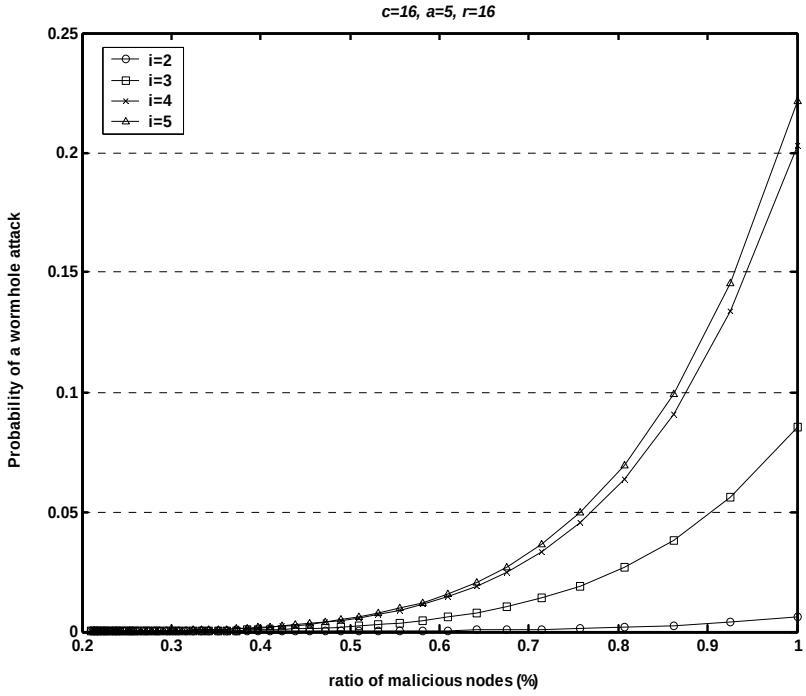
calculated with 5 communication channels available for u and each of its malicious neighbors. Similarly, in Fig. 39(b), p_a is calculated with 15 communication channels available for u and each of its neighboring nodes. The figures show that for a given number of wormhole links, a set of c channels available for sensor u, and a subset of r channels available for each of u's malicious neighbors, the probability of a wormhole attack increases exponentially with the malicious node ratio. The figures also show that as the number of channels available to sensor u increases, the probability p_a decreases.

Fig. 40 shows the probability p_a for a sensor u with 20 legitimate nodes, 40 malicious nodes within its communication range, and varying number of channels available to the malicious nodes. For a given number of r channels available to the malicious nodes, as the number of sensor u's available channels increases, the probability p_a decreases exponentially. Fig. 41 shows the probability p_a with $c = 2$ and different numbers of neighbors of a sensor being within the MS range.

The security resilience of the proposed technique against attacks caused by node collusion is investigated. An attacker randomly compromised of x sensor nodes is assumed. In the case of the captured bivariate polynomials of degree t, the attacker cannot determine the non-compromised polynomial-based key if he/she has captured no more than t sensors.



(a)



(b)

Fig. 39. The probability of a successful wormhole attack vs. the malicious node ratio with varied number of wormhole links

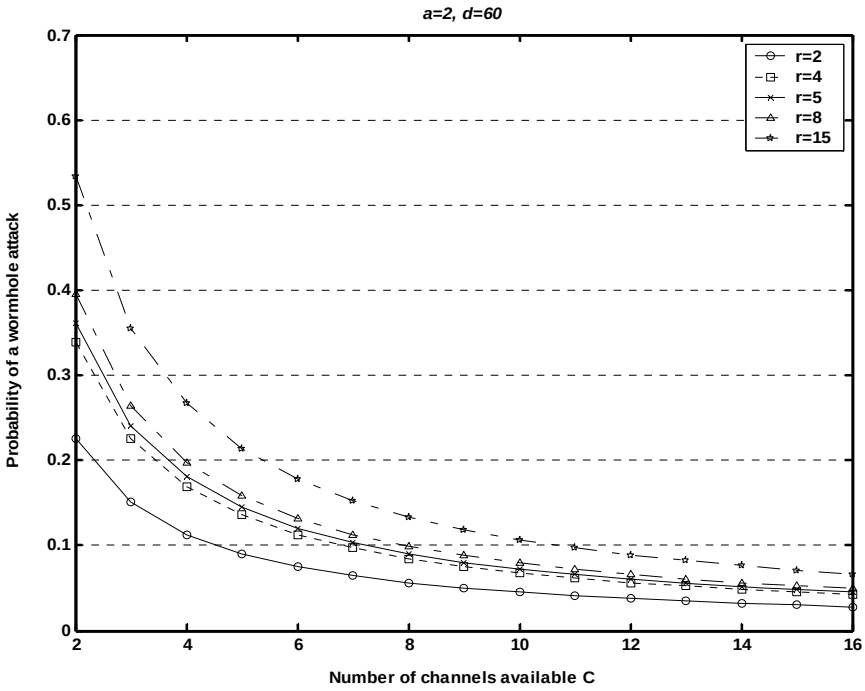


Fig. 40. The probability of successful wormhole attack

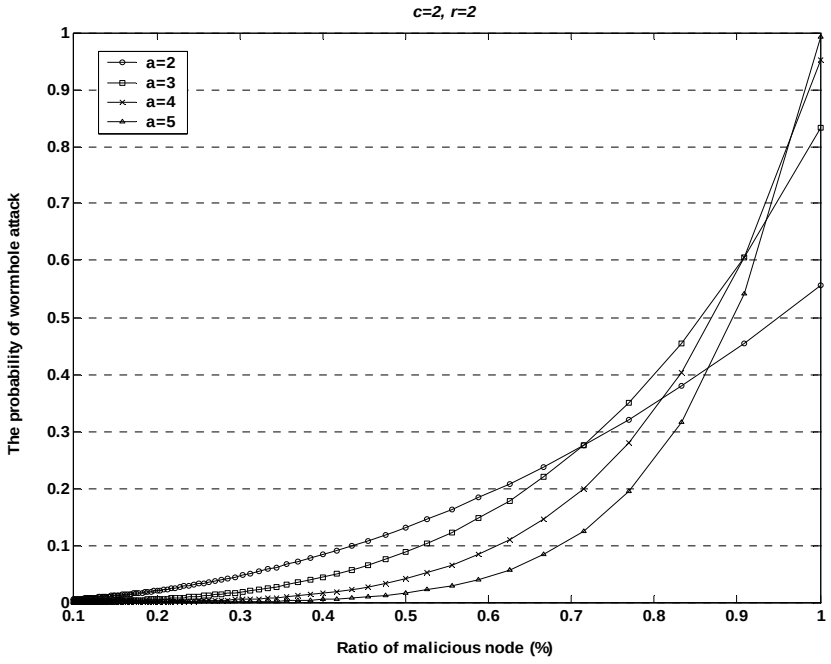


Fig. 41. The probability of a wormhole attack with c =2 and with various number of neighbors for a sensor being under attack

Now, let us assume the case where the number of compromised sensors $x > t$. The probability of any polynomial being chosen for a sensor node is $\frac{s'}{s}$, and the probability of this polynomial being chosen exactly j times among the x compromised sensor nodes is represented by D. Liu, P. Ning, and R. Li [35].

$$q(j) = \binom{x}{j}\left(\frac{s'}{s}\right)^{j}\left(1-\frac{s'}{s}\right)^{x-j} \tag{5.2}$$

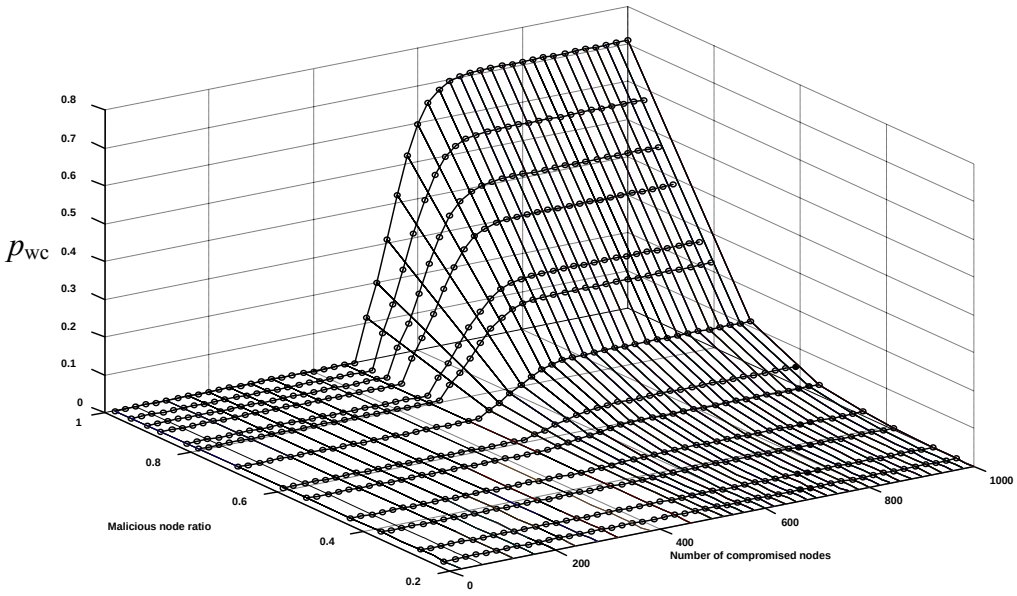
Thus, the probability of a polynomial-based key being compromised between non-compromised sensors is.

$$P_{pc} = 1 - \sum_{j=0}^{j=t} q(j) \tag{5.3}$$

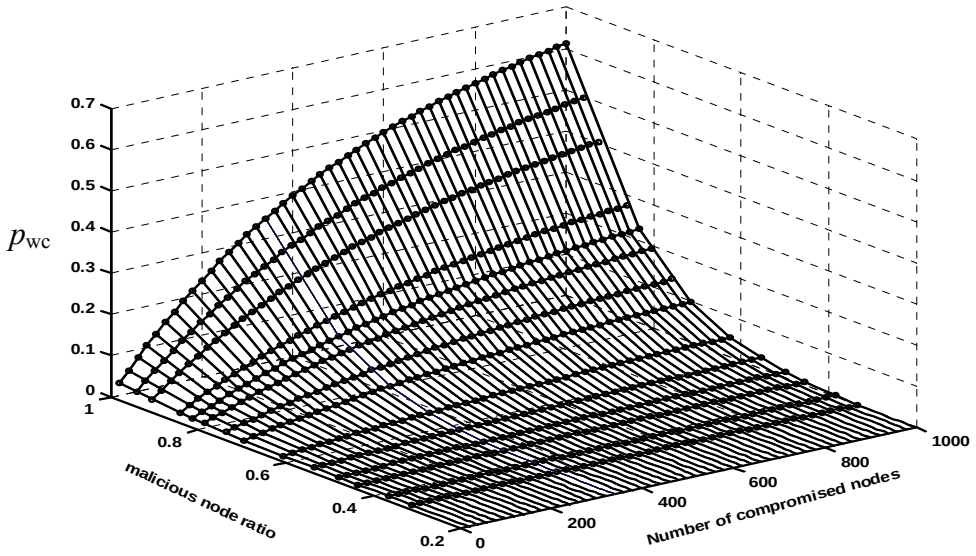
The probability that a data-communication link between the MS and any uncompromised sensor being compromised and it is under wormhole attacks.

$$p_{wc} = p_a \times \left(1 - \sum_{j=0}^{j=t} q(j)\right) \tag{5.4}$$

Now, the proposed technique is compared with its use in the scheme described by S. Hussain, F. Kausar, and A. Massod [48]. Fig. 42(a) shows the probability p_{wc} that a data-communication link between a MS and any uncompromised sensor being compromised and it being under a wormhole attack when using the polynomial pool–based scheme, Fig. 42(b) shows the probability p_{wc} when using the random generation key scheme Fig. 42 [(a) & (b)] clearly shows that the proposed technique when used in



(a)



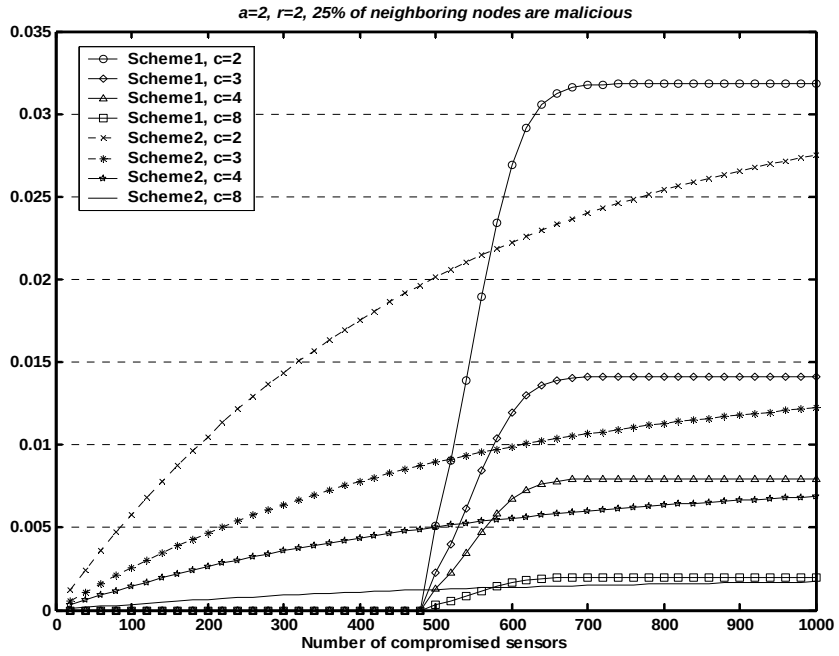
(b)

Fig. 42. The probability that a data-communication link between MS and uncompromised sensor is being compromised and it's under a wormhole attack when using either the polynomial pool-based key pre-distribution scheme as in (a) or the random generation key scheme as in (b)

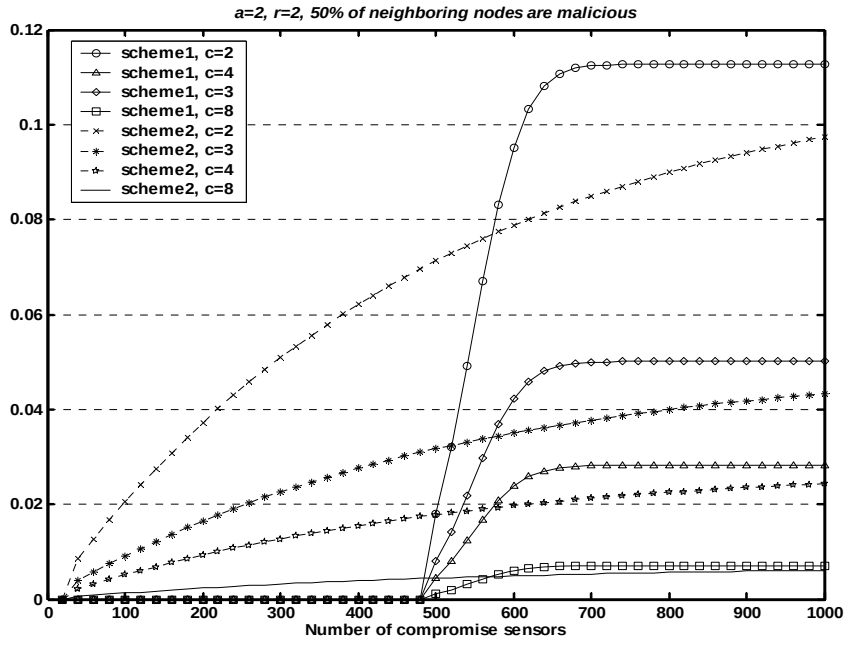
conjunction with the polynomial pool–based scheme performs much better than when it is used with the random generation key scheme .Furthermore, the threats posed by a wormhole attack used in combination with eavesdropping are herein investigated. In this type of attack, the adversary launches wormhole attacks on a sensor node that has *n* of its neighboring nodes as malicious devices; these malicious nodes can easily coordinate an eavesdropping attack on the sensor node with the help of the wormhole. For a sensor node with a set of *c* channels available for communication with the MS and *n* malicious neighboring nodes, where each malicious node is capable of tuning its radio to a channel randomly chosen from its set of *r* available channels, the probability p_{d} that the sensor node can be under eavesdropping attack is $\frac{r}{c}$. It is assumed that an adversary has captured *x* sensor nodes; for an uncompromised sensor node that is under wormhole attack and has *n* of its neighbors as malicious and eavesdroppers, the probability that at least one of the sensor's malicious neighbors is able to recover data messages sent over the wormhole to the MS is

$$p_r = p_{wc} \times \frac{r}{c} \tag{5.5}$$

Fig. 43 [(a), (b)] and Fig. 44 shows the relationship p_r and the number of compromised sensor nodes using the proposed technique in combination with the polynomial pool–based key pre-distribution scheme [35] and the random generation key scheme, which are referred to as scheme 1 and scheme 2, respectively.



(a)



(b)

Fig. 43. The probability P_r vs. number of compromised sensors using the proposed technique in conjunction with either the polynomial pool-based key pre-distribution scheme or the random generation key scheme which we refer to scheme 1 and scheme 2 respectively (25% in (a) and 50% in (b) of neighboring nodes are malicious)

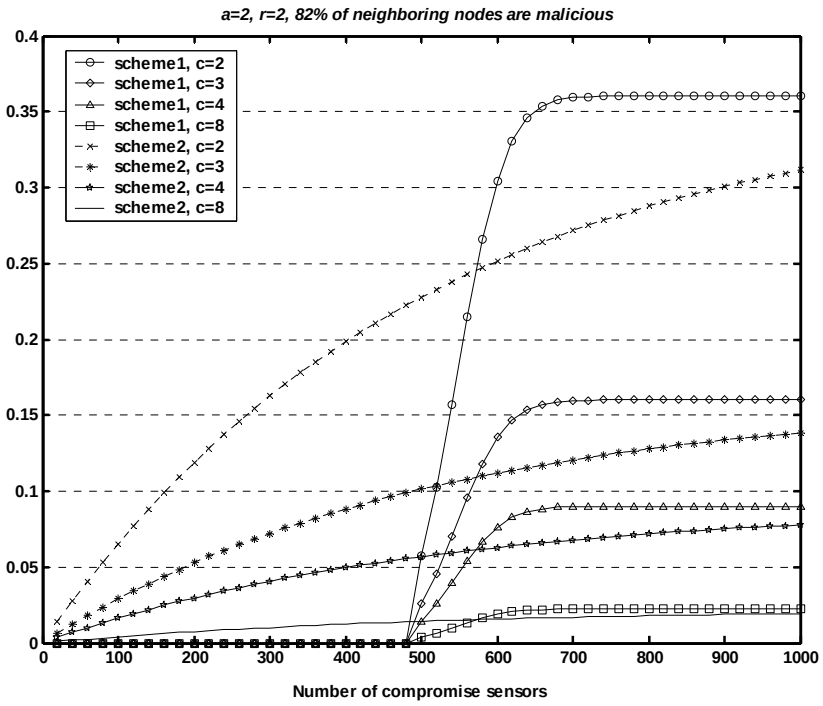


Fig. 44. The probability P_r v.s. number of compromised sensors using the proposed technique in conjunction with either the polynomial pool-based key pre-distribution scheme or the random generation key scheme which we refer to scheme 1 and scheme 2 respectively (82% of neighboring nodes are malicious)

E. SUMMARY

In this chapter, a security scheme for WSN with a MS is presented, which improves the resilience of the network against wormhole attacks and node collusion. In addition, the proposed scheme illustrates the threshold property: when the number of compromised sensors is less than the threshold, the probability that any uncompromised sensor being compromised is close to zero. The proposed scheme uses the polynomial pool-based key pre-distribution scheme [35] and the multiple channels available on the sensor hardware. It allows the MS to establish a direct secure link with any sensor node and over a

communication channel randomly selected from a set of c available channels. Through quantitative analysis, it has been shown that this technique functions very well in terms of resilience to wormhole and eavesdropping devices. The results show that with $c = 5$, $a = 5$, $r = 5$, and 50% of a sensor node's neighbors being malicious nodes, the probability of a wormhole attack is approximately zero for varying numbers of wormhole links.

CHAPTER VI

AN ENERGY-EFFICIENT DATA COLLECTION SCHEME IN SENSOR NETWORK WITH MS

In this chapter we investigate the employment of the traditional multi-hop approach in a multi-events monitoring sensor network. Such a network may exist for studying active volcanoes to collect seismic, temperature data, infrasonic signals, and detection of big eruptions. Data from the active volcanoes site is sensed and periodically reported to the base station. These sensor measurements can tolerate high latency, as geologists analyze data and draw conclusions with which to predict future eruptions. They do not require real time action. Meanwhile the detection of big eruption triggers sensor nodes to record the occurrence of the event to the base station with low latency and high data fidelity. The network uses this sensor reading to activate the alarm system. For this class of sensor application the network provides sensor readings with varied delivery delay constraints. We further explore the drawbacks on network performance and total network energy usage of using the traditional multi-hop scheme to route sensor readings. In our implementation, we consider two types of sensor reading: high-priority data (detection of big eruption) requiring low latency and high fidelity, and low-priority data (seismic, infrasonic signals and temperature) with high latency and low fidelity. One of the major energy expenditures in this type of sensor network is in communicating the low-priority sensor reading from the sensors to a base station. Usually, these reading are observed from the environment periodically (for example a low-priority packet might be generated

by a sensor node every 2 sec) and relayed to a base station using ad hoc multi-hop routes in the sensor network. A drawback with this approach, however, is that the sensor nodes closer to the base station relay high-priority and low-priority sensor readings from all the nodes in the network. Thus, nodes closest to the base station drain their batteries faster than those in the remaining network, which will lead to non-uniform depletion of energy in the sensor network. Once the nodes that are within direct communication with the base station have exhausted their energy, the network is disconnected. Another problem is the additional energy expenditure inherent in the multi-hop scheme to relay low-priority data to the base station in a multi-events network. Since low-priority data can tolerate high latency, we propose a new hybrid data delivery scheme which maintains the same delivery delay for high-priority data as the multi-hop approach and trades latency for energy in the case of low-priority data delivery. Our scheme will optimize the network performance and reduce the total network energy usage compared with the traditional ad hoc approach.

Our goal is to optimize the energy consumption at nodes near the base station and maximize the lifetime of the remaining nodes by minimizing the energy spent for relaying low-priority data to the base station. We implemented a dual communication sensor network with a mobile node. Mobile entities exist in the environment, and a data aggregation node with a finite amount of resources can be attached to these mobile entities for low-priority data collection. In our work, the mobile node is part of the network infrastructure itself and can be controlled by the network as required. A mobile node moving through the network deployment region can collect low-priority data from the

static nodes over a single hop radio link as and when the mobile node is within radio range of the static nodes. This reduces multi-hop relaying of low-priority data and reduces energy consumption at nodes closer to the base station. This arrangement may increase the latency of low-priority data, but it is acceptable. The mobile node periodically visits the base station to drop off the collected low-priority data. To ensure low latency and high fidelity, high-priority data are relayed over multi-hop routes to the base station. Low-priority data and high-priority data propagate over the network over two separate communication channels to minimize packet collision and hence improve the network throughput. The proposed approach shows how a significant advantage in network lifetime can be gained if some of the energy spent in relaying low-priority data can be saved.

This chapter is organized as follows: Section A summarizes related work. Section B explains the methodologies used in our approach to improve network performance and reduce energy consumption. Section C clarifies the communication protocol used by the mobile node to collect and transfer low-priority data to the base station. Section G presents the system evaluation of two large, dense networks using a dual-communication hybrid data delivery scheme and the traditional ad hoc network approach. Finally, section H concludes the chapter.

A. RELATED WORKS

Exploiting mobility in the domain of wireless sensor networks to maximize sensor network lifetime [59], [60], [61], [62], [63] by reducing the communication energy dictated

by the sensor has received much attention recently. Mobility can be generally classified into three categories: random, predictable [64], and controlled. Assuming all nodes are mobile, random mobility ameliorates the network data capacity [65]. Mobile entities with random motion were also considered for communication in [10] and [11], in which the mobile entities were designated zebras in [10] and whales in [11]. Exploiting mobile entities with random motion has been also studied in [66], where these randomly moving entities act as data mules to carry data from sensor to access point. Mules are assumed to be capable of short-range wireless communication and can exchange data as they pass by sensors and access points. Mules collect data from the sensors, store them in a buffer, and later on drop off the collected data as it pass by an access point. In all cases of random mobility, however, the unpredictable arrival time of the mobile entity at the sensor node may lead to excessive data caching at the sensor node and result in buffer overflows.

Predictable mobility was introduced in [67] in which a bus acts as mobile observer in wide area sensor network. The mobile observer follows a periodic schedule of movement. Static sensor nodes were placed near the bus trajectory in which all static nodes have direct communication links with mobile node. A sensor node learns the bus's arrival time, wakes up, and starts its data transfer with the mobile node. The drawback of this predictable mobility is that all sensor nodes must be in direct communication with the mobile node. This will not be practical in random sensor network such as those deployed for battlefield surveillance and wildfire observation, in which the presence of obstacles in the network environment prevents the mobile node from ensuring a direct

communication with all static nodes. With controlled mobility, in which sensor nodes have a limited mobility range [17], they can modify their locations to come within direct communication of a mobile node having a long mobility range.

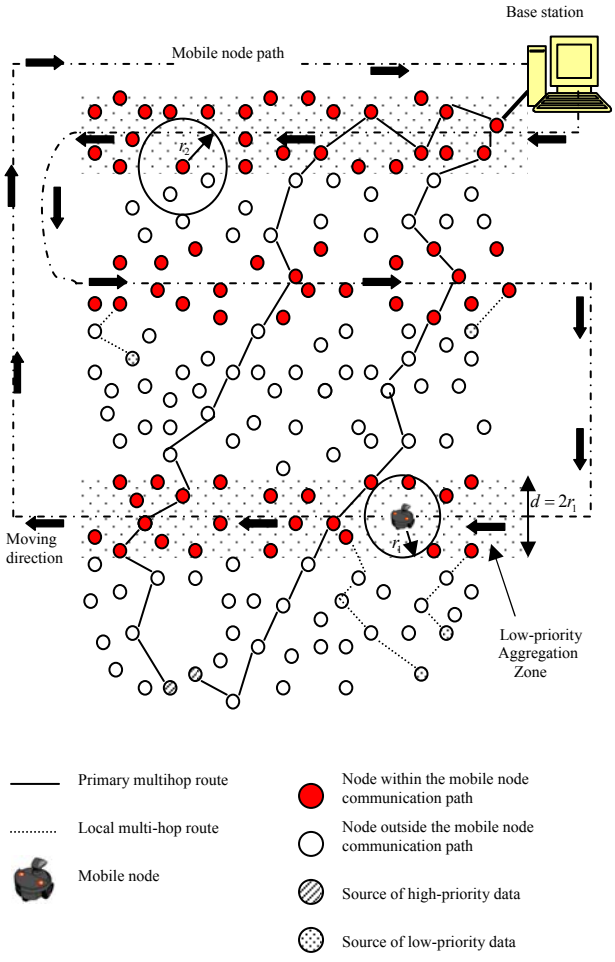


Fig. 45. The sensor network with one mobile node

B. NETWORK WITH MOBILE NODE

Our sensor network architecture is illustrated in Fig. 45. The network is used for monitoring and recording several types of events. Events are classified into two different cate-

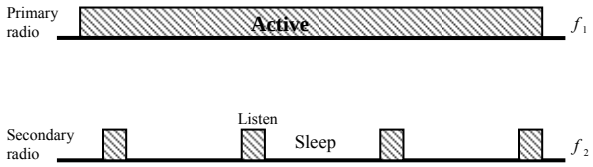


Fig. 46. The sensor node primary and secondary radios

gories, high-priority events and low-priority events. The occurrence of a high-priority event triggers the sensor node to generate a high-priority data packet; a low-priority event, a low-priority data packet.

The network consists of static sensor nodes, a base station, and a mobile node. Sensor nodes are capable of sensing different types of events; they support dual communication but have limited buffer size for data aggregation. Each sensor node is equipped with two radios: primary and secondary. They operate at two separate frequency bands, f_1 and f_2, and have duty cycles 100% and 2%, respectively, as shown in Fig. 46. The two radios provide a transmission range of r_2. Static-to-static communication is established via the primary radio, where a static sensor node relays a data packet (low and high priority) to another static node. Static-to-mobile communication is performed via the secondary radio, where a sensor node transfers its aggregated low-priority data to the mobile node. High-priority data is transmitted over a primary multi-hop route, which connects a source node to the base station. However low-priority data is transmitted over

a local multi-hop route, which connects a source node to node that is within direct communication of the mobile node. The mobile node acts as a low-priority data collection node with massive storage capability, rechargeable energy source, and it has no sensing functionality. The mobile node communicates directly with the static sensor via a single radio at a frequency band f_2, and furnishes a communication range of r_1. It periodically sends a stream of beacon packets. Nodes in the mobile node communication path receiving a beacon start contending for the channel to transfer their aggregated data to the mobile node. Controlled mobility is being used in our system architecture, in which the mobile node moves repeatedly along a deterministic route to collect low-priority data from static sensor over a single-hop radio link. The mobile node visits the base station periodically to offload its collected data. As shown in Fig. 45, a source node sends its high-priority data packet to the base station over a primary multi-hop route. However, a source node with a low-priority data packet relays its data to the nearest static node that is within a single-hop radio link of the mobile node. Sensor nodes in the mobile node communication path buffer the low-priority data received from nodes, which are not in the mobile node communication path, and avoid further relaying of the data. This scheme reduces the total number of hops required to transmit a low-priority data packet from the source to the base station, and hence minimize packet collisions, increase spatial reuse, improve network throughput, and reduce the total network energy usage.

C. COMMUNICATION PROTOCOLS BETWEEN SENSOR NODES AND THE MOBILE NODE

This section describes the communication protocols developed to facilitate the data transfer process in three phases as shown in Fig. 47 and discussed in detail below. The mobile node transmits three distinct types of beacon packets.

a. Beacon formation packet: Each beacon packet contains the mobile node MAC address. The mobile node periodically broadcasts a stream of beacon formation packets during the formation phase in order to form the low-priority data aggregation zone.

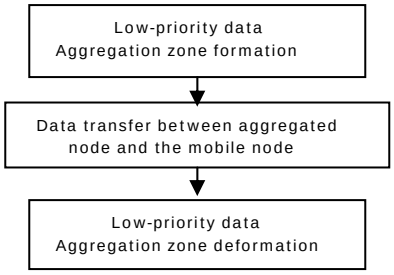


Fig. 47. The three phases used during the mobile node communication protocol

b. Beacon Deformation packet: it contains the mobile node MAC address and the remaining time for the next data transfer duration. To deconstruct a low-priority data aggregation zone, the mobile node periodically sends these beacon packets during the deformation phase.

c. Beacon data pull packet: it includes information similar to the beacon deformation packet. The mobile node uses this type of beacon packet to collect low-

priority data that were aggregated in nodes, which lies within the mobile node communication path.

D. FORMATION OF THE LOW-PRIORITY DATA AGGREGATION ZONE

The first phase is forming the low-priority aggregation zone in the network. It is a construction phase, and essential information required for subsequent phases is collected in this phase. In addition, it lasts for the duration of single path traversal by the mobile node. This training phase may be repeated at any time to adapt to network dynamic (such as node addition, deletion, construction of new data aggregation zone). The scheme used for forming the low-priority data aggregation zone is described below.

As mentioned earlier, the mobile node traverses the network over a fixed path (see Fig. 45). In the first path traversal, the mobile node moves along the path, broadcasting beacon formation packets periodically in band f_2. Nodes lying within the mobile node communication path receive the beacon formation packet and become data-aggregated nodes for relay of low-priority data, and, at the same time, they continue relaying high-priority data. In order to guarantee that nodes near the mobile node M moving path receive at least one beacon, the listen interval of the node secondary radio listen interval's T_{RX} as shown in Fig. 48 needs to be at least as long as the transmit time of a beacon plus the inter-beacon interval T_B. To ensure that the mobile node M produce a continuous low-priority data aggregation zone, it periodically transmits a stream of beacon formation packets during the beacon duration T_f every T_t seconds. Table I shows the protocol parameters used in the design.

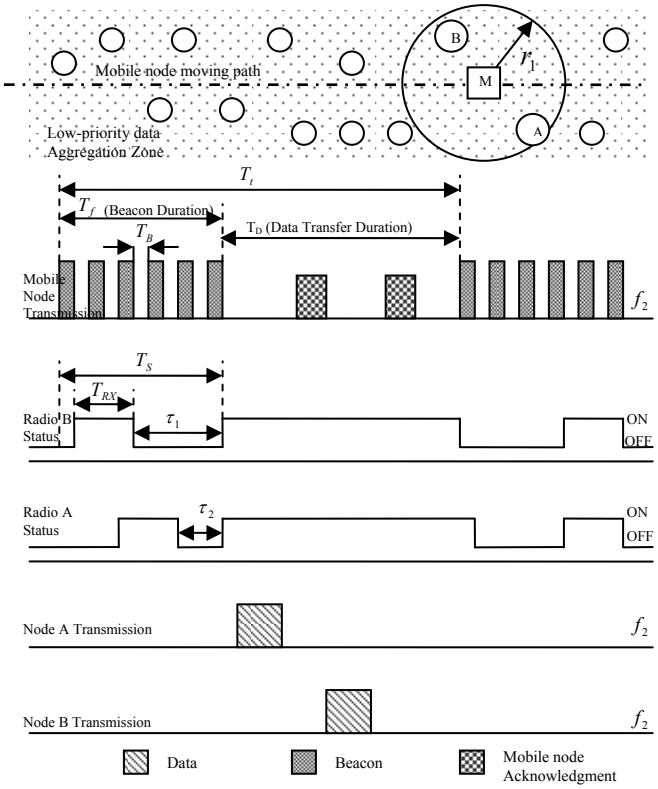


Fig. 48. Data transfer process between nodes that's lies in the low-priority data aggregation zone and the mobile node

TABLE 1: PROTOCOL PARAMETER VALUES

Radio Parameters	Values
Mobile Radio Interval (T_t)	250 ms
Beacon Duration (T_f)	100 ms
Data Transfer Duration (T_D)	150 ms
Beacon Interval (T_B)	1 ms
Sensor Node Radio Interval (T_S)	100 ms
Sensor Node Listen Duration (T_{RX})	2 ms
Data Rate	2.4 Kbps
Transmission Power	14.88 mW
Receiving Power	12.50 mW
Idle Power	12.36 mW

E. DATA TRANSFER BETWEEN AGGREGATED NODE AND MOBILE NODE

Once the aggregation zone is established, nodes lying in the mobile node communication path store forwarded low-priority data in their internal buffer and avoid further relaying to reduce the energy consumed by hop communication and minimize packet collisions, since fewer packets are relayed to the base station over the ad-hoc multi-hop route. As illustrated in Fig. 48, the mobile node M moves along the network periodically broadcasting a stream of the beacon data pull packets. Nodes within the low-priority data-aggregation zone that hear the node M broadcast, such as nodes A and B, indicate the arrival of the low-priority data collection node. When Nodes B and A receive at least one beacon, they use information included in the beacon packet to set their timers eto τ_1 and τ_2, respectively, where τ_1 and τ_2 are time remaining in the next data transfer interval. Since nodes A and B use their secondary radios, operating at a duty cycle of 2%, to communicate with the mobile node, the aggregated nodis unable to transfer a large amount of data to the mobile node during the data transfer duration. Moreover, since less data are being transferred each time in a node having direct contact with the mobile node, nodes will endure a fast buffer overflow and excessive data drop. In our approach, nodes turn their secondary radios on during the entire data transfer duration to increase the data transfer rate, and at the end of the data transfer duration they switch back to normal operation. During the data transfer duration nodes, such as A and B, contend for the channel to transfer their aggregated data to the mobile node. If the mobile node receives a data packet successfully, it replays back by sending an acknowledgment to the

source node, which verified to the source node that the connection is active and the data was reliably delivered.

F. DEFORMATION OF THE LOW-PRIORITY DATA AGGREGATION ZONE

During this phase, the mobile node transmits a train of beacon deformation packets along its moving path. Nodes near the mobile node communication path receive at least one beacon packet and become a non-aggregated node for low-priority data, and, at the same time, transfer any stored data that have not been previously transferred to the mobile node. In this phase, nodes lying in the deconstructing path will no longer be within the mobile node path. In order to minimize data loss, we increase the data transfer rate during this phase by decreasing the mobile node speed to its minimum value.

G. PERFORMANCE EVALUATION

This section describes the simulation setup used in the process of system development. Our scheme was implemented using the ns-2 network simulator. We analyzed the proposed scheme through extensive simulations. Two sensor networks with node densities of 256 and 356 were considered in our evaluation. In both networks, sensor nodes had a fixed buffer size and were uniformly distributed over a field of 450×450 m^2 square area. First, we considered the static multi-hop network where all data (low-priority and high-priority) is relayed over a multi-hop topology. Second, we considered the same networks deployment with a mobile node where all data with high-priority is relayed over a multi-hop route, and data with low-priority are locally relayed to aggregated nodes, which

store the data in their internal buffer until the arrival of the mobile node. We used the following performance metrics in our evaluation.

- Low-priority delivery success ratio*:* The ratio of the total number of low-priority packets successfully received by the sink node to the total number of generated packets.
- High-priority delivery success ratio. The ratio of total number of high-priority packets successfully received by the sink to the total number of generated packets.

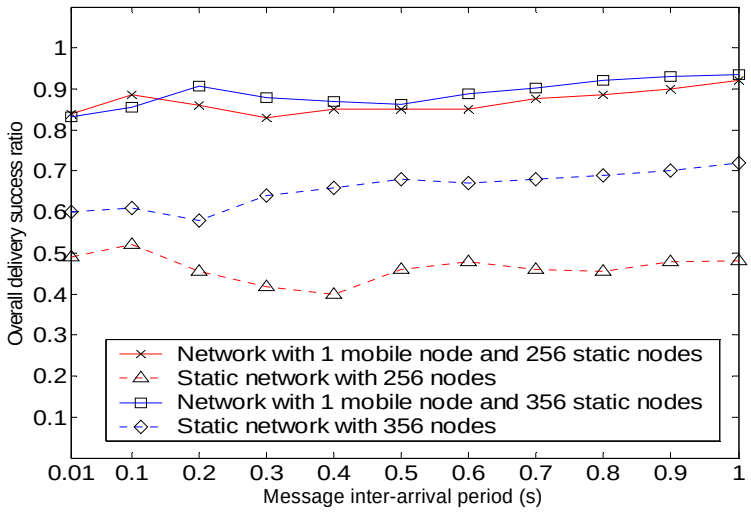


Fig. 49. Overall delivery success ratio under various traffic loads

- Total network energy reduction percentage. The total percentage of energy reduction.

The above performance metrics were determined under different traffic loads. We changed the traffic load by varying the message inter-arrival period. If the message inter-arrival period is 0.2 s, a message is generated every 0.2 s by the source node. In this experiment, the message inter-arrival period varied from 0.01 s to 1 s. Under various traffic loads, the proposed system achieved a higher overall delivery ratio than the static multi-hop network for the two densities, as shown in Fig. 49. For the highest traffic load with a low-priority message generated every 0.01 s, our approach attained a higher overall delivery ratio compared with the multi-hop approach. Fig. 50 shows how a network with a mobile node acting as a low-priority data collection node improves the low-priority delivery ratio. Because low-priority data are locally relayed to the nearest aggregated node, then further transferred to the mobile node to avoid hop communication at

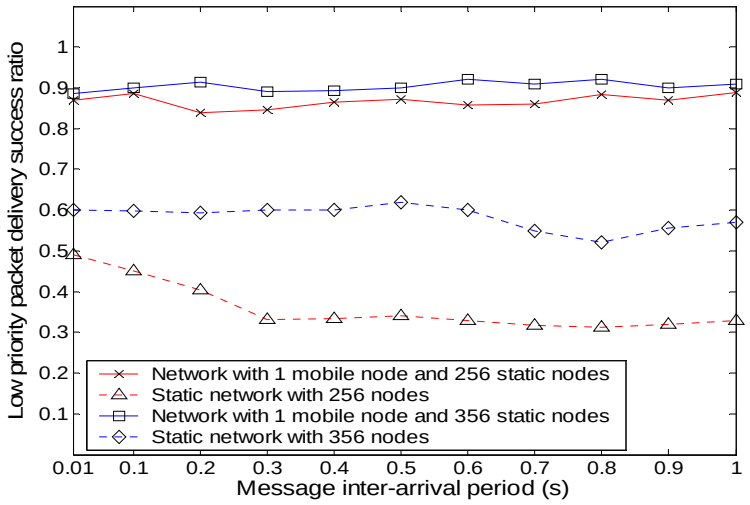


Fig. 50. Low-priority data delivery success ratio for various traffic loads

the time the mobile node contact the aggregated node. This method reduces the number of hop communications, decreases packet collisions, and, hence, ameliorates the low-priority delivery success ratio. For the high-priority delivery success ratio (see Fig. 51), our design and the static multi-hop method obtains about the same delivery ratio since high-priority data are send over multi-hop routes in both approaches to ensure low latency and high data fidelity.

Fig. 52 shows the total network energy reduction percentage between the two schemes under varied traffic loads. At the highest traffic load, the proposed design achieves total energy reduction of about 85% and 65% for densities 256 and 360, respectively. For low traffic loads, we obtain an energy reduction of 25% and 30% for densities 256 and 360, respectively. In the proposed approach energy reduction occurs by reducing the total number of hop communication required to relayed low-priority packets.

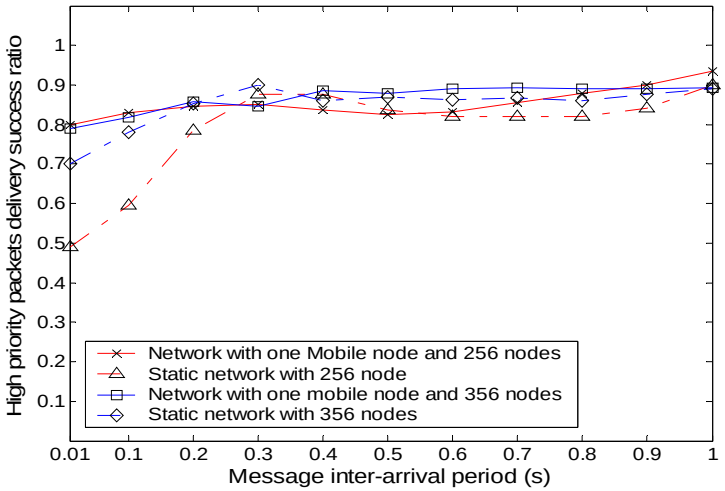


Fig. 51. High-priority delivery success ratio for various traffic loads

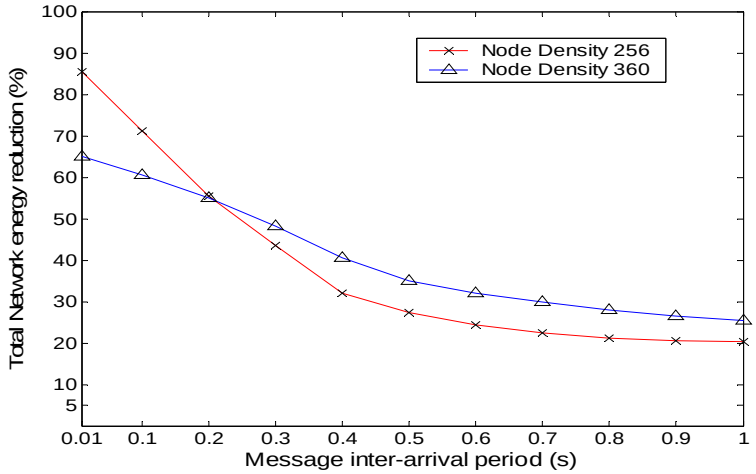


Fig. 52. Total network energy reduction (%) under various traffic loads

For the proposed scheme we also studied the effect of the sensor node buffer size on the low-priority delivery ratio for node density 256. Low-priority data and high-priority data were generated at a fixed message inter-arrival period 0.4 sec. The mobile traversing the sensor field at constant speed 10 m/sec to collect low-priority data from nodes that are lying in the mobile node communication path. As shown in Fig. 53 when the sensor node buffer size is small (10 data packets) the low-priority delivery ratio is less than 0.1, since the small buffer size may causes excessive data dropped which will degrade the low-priority delivery ratio. As the buffer size increases the delivery ratio increases to about 0.88 at 100.

To further visualize the relaying overhead, we plotted the total average number of low-priority packets transmitted under different traffic loads for density 256 in Fig. 54. Low-priority packets transmitted in the network with the mobile node required fewer hop communications than the network without the mobile node. In the network with one

mobile node and 256 static nodes, 63% of the average transmitted packets required at least four communication hops to reach the base station. In the network without the mobile node, however, about 11% of the average transmitted packets are delivered to the base station using at least four communication hops. buffer size is small (10 data packets) the low-priority delivery ratio is less than 0.1, since the small buffer size may causes excessive data dropped which will degrade the low-priority delivery ratio. As the buffer size increases the delivery ratio increases to about 0.88 at 100.

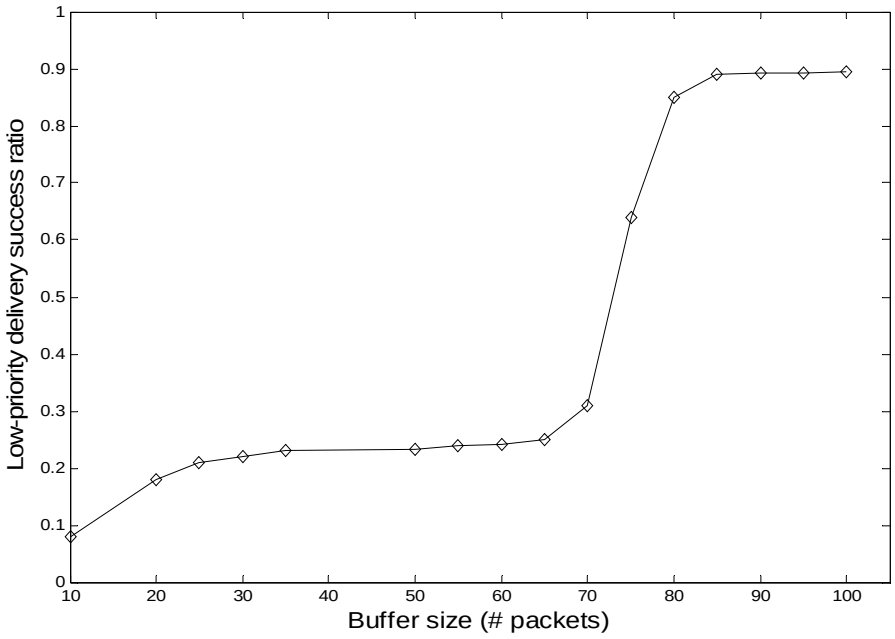


Fig. 53. The effect of the sensor node buffer size on the low-priority delivery ratio at fixed traffic load

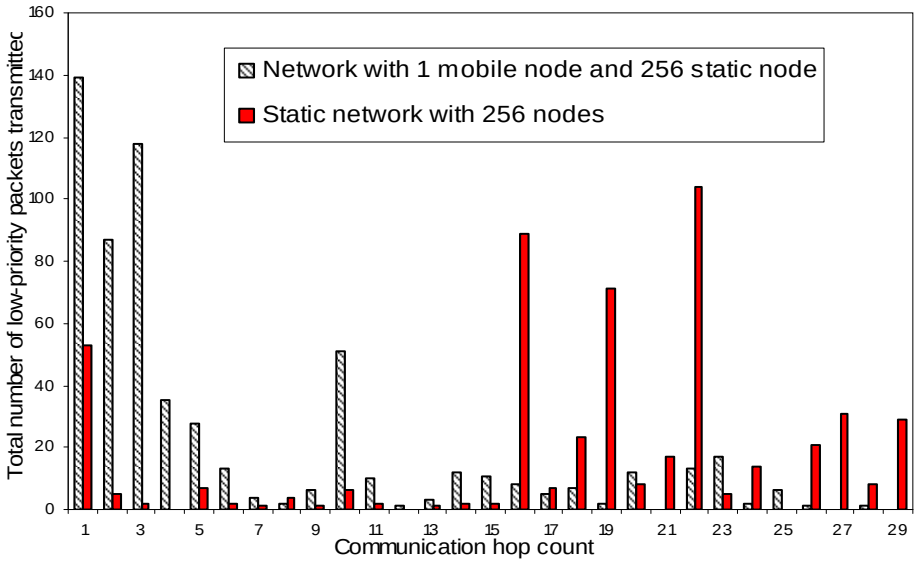


Fig. 54. Relaying overhead for the two low-priority data gathering approaches with node density 256

H. SUMMARY

In this chapter, we explored the possibility of using a mobile device for data transfer in sensor networks that provide low-priority data with high-latency and extreme high-fidelity data with low-latency. The motivation was to save energy in the embedded sensor node and increase the useful service life of a deployed system. The key intuition was that using a mobile node to collect low-priority data that were aggregated in nodes, which lies within the mobile node communication path. Our system establishes shorter low-priority data routes, reducing the data-relaying overhead. The simulation result shows that the proposed system improves the network delivery success ratio and reduces the total network energy consumption by about 88% during high traffic load and about 25% during low traffic.

CHAPTER VII

CONCLUSION AND FUTURE WORKS

Countermeasure attack schemes and security services such as sink authentication and pairwise key establishment are important in many sensor networks applications. In this dissertation, we examine two security challenges for wireless sensor network with MS: First, is to cultivate efficient security schemes with low communication overhead that use authentication and pairwise key establishment between sensor nodes and MS to tolerate nodes capture and *mobile sink replication* attack. Sink mobility imposes extra communication overhead on these constrained resource sensor nodes to establish secure links with the MS. This extra communication overhead are obtained because of the frequent exchange of cryptography keying information between the sensors and MS each time the MS update its location unlike sensor network with a fixed localized sink. Where after deployment, sensors and the sink exchange cryptography keying information only once to establish a securely connected network. The other challenge is to develop security techniques that are based on key pre-distribution schemes to provide network's resiliency against *wormhole* attack.

A. CONTRIBUTIONS

- We identified several drawbacks in both the probabilistic key pre-distribution scheme and the *Q*-composite scheme if used in a WSN with MS. Both schemes have high communication overhead and also as the number of compromised

nodes increases, the fraction of affected pairwise keys increases quickly As a result, a small number of compromised nodes may affect a large fraction of pairwise keys and will then lead to a large scale *mobile sink replication* attack. We proposed two schemes that are based on the polynomial pool scheme, the probabilistic generation key pre-distribution scheme, and the Q-composite scheme. The schemes uses a common polynomial and Q common generation keys to establish a secure pairwise key between MS and the sensor node, where $Q \geq 1$. Our security analysis indicate that these schemes assure, with high probability and low communication overhead, that any sensor node can establish a secure a link with MS. Furthermore, our analytical results clearly show that our schemes perform better in terms of network resilience to nodes capture than exiting schemes if used in WSN with MS.

- We investigate the problem of using a single key pool in existing key pre-distribution schemes for pairwise key establishment and authentication between sensors and mobile sink. For example, in the basic probabilistic and the Q-composite key pre-distribution schemes, an attacker can easily gain control to the network by deploying a replicated mobile sink preloaded with some compromised keys. We propose a three-tier general framework that permit the use of any pairwise key pre-distribution scheme as its basic component. The new framework require two separate key pools, one for the mobile sink to access the network, and one for pairwise key establishment between sensors. To further reduce the damages caused by stationary access node replication attack, we strengthen the

authentication mechanism between the sensor and the stationary access node in the proposed scheme. To facilities our study we choose the polynomial pool scheme as the basic component in our scheme. Through detailed analysis and with 10% of the sensor nodes in the network carrying a polynomial from the mobile pool, for a mobile polynomial to be recovered in order to lunch a mobile sink replication attack, the attacker would have to capture 21% times more nodes as compared with the single polynomial pool approach.

- We identified the problem of using one channel for communication and single authentication code by sensor nodes to verify the source of the MS beacon message, where an adversary can record the MS beacon transmission in one part of the network, tunnels the recorded message over low-latency channel and replays them at a different part of the same network. In this dissertation, we propose an efficient security scheme to tolerate *wormhole* attack, which divides the sink's data collection path into unique authentication grids, sensors in each grid, uses secret keying information and collision-resistant hash functions to authenticate the source of beacons. Through probabilistic analysis and definitive simulation, the proposed scheme shows with 60% of the grids under wormhole attacks, the probability that a node reply to a malicious beacon is 0.1. Furthermore we propose a scheme that involves leveraging channels diversity and the polynomial pool-based key pre-distribution scheme to tolerate *wormhole attack*. It allows the MS to establish a direct secure link with any sensor node and over a communication channel randomly selected from a set of *c* available channels. Through quan-

titative analyses, it is shown that even when 50% of a sensor node's neighbors are malicious devices, the provision of one extra available channel for communication with the mobile sink reduces the probability of a wormhole attack to almost zero.

- We propose an energy-efficient hybrid data collection architecture [21] based on controllably mobile infrastructure for a class of applications in which sensor networks provide both low-priority and high-priority data. High-priority data require a data delivery scheme with low latency and high fidelity. Meanwhile low-priority data may tolerate high-latency data delivery. The simulation result shows that the proposed system improves the network delivery success ratio and reduces the total network energy consumption by about 88% during high traffic load and about 25% during low traffic.

B. FUTURE WORKS

We developed a number of key pre-distribution schemes to tolerate nodes capture and node replication attack. The proposed schemes provide high resiliency when the number of captured nodes are less than a threshold value, however as the number of captured nodes exceed this threshold value, the network resiliency against nodes capture and node replication attacks dramatically decreases. It will be interesting to design key pre-distribution schemes that are capable of dynamically increasing the network resiliency when the number of nodes captured reaches a critical value. One technique that can be taken is to enables a wireless sensor network with mobile sink to dynamically update its

resiliency is to allow sensor nodes and with the help of the MS to dynamically re-keying when the number of compromised keys approaches captious value. The other approach is eliminate the threats impose by captured keys by revoking.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *The International Journal of Computer and Telecommunications Networking Computer Networks,* vol. 38, no. 4, pp. 393-422, March 2002.

[2] G.J. Pottie, and W.J. Kaiser, "Wireless integrated network sensors," *Communication of the ACM*, vol. 43, no. 5, pp. 51-58, May 2000.

[3] T. Gao, D. Greenspan, M. Welesh, R. R. Juang, and A. Alm, "Vital signs monitoring and patient tracking over a wireless network," *The 27th Annual International Conference of IEEE EMBS,* pp. 102-105, September 2005.

[4] L. Gu, D. Jia, P. Vicaire, T. Yan, L. Luo, A. Tirumala, Q. Cao, T. He, J. A. Stankovic, T. Abdelzaher, and B. H. Krogh, "Lightweight detection and classification for wireless sensor networks in realistic environments," *The 3rd ACM Conference on Embedded Networked Sensor Systems,* pp. 205-217, November 2005.

[5] Z. Vincze, D. Vass, R. Vida, A. Vidacs, and A. Telcs, "Adaptive sink mobility in event-driven muti-hop wireless sensor networks," *Proc. of the 1st International Conference on Integrated Internet Ad Hoc and Sensor Networks* (*InterSense'06*), vol. 138, no. 13, pp. 1-10, 2006.

[6] I. Chatzigiannakis, A. Kinalis, and S. Nikoletseas, "Sink mobility protocol for data collection in wireless sensor networks," *Proc. of the 4th ACM International Workshop on Mobility Management and Wireless Access* (*MOBIWAC'06*), pp. 52-59, 2006.

[7] S. Basagni, A. Carosi, E. Melachrinoudis, C. Petrioli, and Z. M. Wang, "Protocols and model for sink mobility in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 10, no. 4, pp. 28-30, 2006.

[8] S. Basagni, A. Carosi, E. Melachrinoudis, and Z. M. Wang, "Controlled sink mobility for prolonging wireless sensor networks lifetime," *Wireless Networks*, vol. 14, no. 6, pp. 831- 858, Dec. 2008.

[9] W. Wang, V. Srinivasan, and Kee-Chaing Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," *Proc. of the 11th Annual International Conference on Mobile Computing and Networking,* pp. 270-283, 2005.

[10] T. Small and Z. Haas, "The shared wireless infostation model-a new ad hoc networking paradigm (or where there is a whale, there is a way)," *Proc. of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (*MobiHoc'03*), pp. 233-244, 2003.

[11] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet," *Proc. of the 10th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS),* pp. 96-107, 2002.

[12] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," *Proc. of the 2nd Int'l. Workshop Information Processing in Sensor Networks (IPSN'03),* pp. 129-145, 2003.

[13] D. Puccinelli, M. Brennan, and M. Heanggi, "Reactive sink mobility in wireless sensor networks," *Proc. of the 1st International Workshop on Mobile Opportunistic Networking* (*MobiSys'07*), pp. 25-32, 2007.

[14] G. Xing, T. Wang, W. Jia, and M. Li, "Rendezvous design algorithms for wireless sensor networks with a mobile sink base station," *Proc. of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing,* (*MobiHoc'08*), pp. 231-240, 2008.

[15] L. Cheng, Y. Chen, C. Chen, and J. Ma, "Query-based data collection in wireless sensor networks with mobile sinks," *Proc. of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly,* pp. 1157-1162, 2009.

[16] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin," Intelligent fluid infrastructure for embedded networks," *Proc. of the 2nd Int'l. Conf. on Mobile Systems, Applications, and Services (MobiSys),* pp. 111-124, 2004.

[17] W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile ad hoc networks," *Proc. of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (*MobiHoc*), pp. 187-198, 2004.

[18] J. Luo and J.-P. Hubaux, "Joint mobility and routing for lifetime elongation in wireless sensor networks," *Proc. of the 24th Annual Conf. IEEE Comm. Soc. (InfoCom),* pp. 1735-1746, 2005.

[19] S. Jain, R.C. Shah, W. Brunette, G. Borriello and S. Roy, "Exploiting mobility for energy efficient data collection in wireless sensor networks," *Mobile Networks and Applications,* vol. 11, no. 3, pp. 327-339, 2006.

[20] A. Somasundara, A. Kansal, D. Jea, D. Estrin, and M. Srivastava, "Controllably mobile infrastructure for low energy embedded networks," *IEEE Transactions on Mobile Computing,* vol. 5, no. 8, pp. 958-973, August 2006.

[21] © [2007] IEEE. Reprinted, with permission, from [*The 3rd IEEE Int'l. Conf. Intelligent Sensors, Sensor Networks and Information Processing* (*ISSNIP '07*), An energy-efficient hybrid data collection scheme in wireless sensor networks, A. Rasheed and R. N. Mahapatra].

[22] J. R. Douceur, "The Sybil attack," *Proc. of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'01)*, pp. 251–260, 2002.

[23] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis & defenses," *Proc. of the ACM IPSN'04*, pp. 259–268, 2004.

[24] M. Demirbas and Y. Song, "An rssi-based scheme for Sybil attack detection in wireless sensor networks," *The 1st Workshop on Advanced Experimental Activities on Wireless Networks and Systems (EXPONWIRELESS 2006)*, pp. 564–570, 2006.

[25] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Real-world physical attacks on wireless sensor networks," *Proc. of the 3rd International Conference on Security in Pervasive Computing (SPC'06)*, pp. 104–118, 2006.

[26] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," *Proc. of the IEEE InfoCom*, pp. 1917–1928, 2005.

[27] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Requirements and open issues in distributed detection of node identity replicas in WSN," *Proc. of the 2006 IEEE International Conference on Systems, Man, and Cybernetics (SMC'06), Special Session on Wireless Sensor Networks*, pp. 1468-1473, 2006.

[28] B. Parno, A. Perrig, and V. D. Gligor, "Distributed detection of node replication attacks in sensor networks," *Proc. of the 2005 IEEE Symposium on Security and Privacy* (*S&P'05*), pp. 49–63, 2005.

[29] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," *Proc. of the 8th ACM International Symposium on Mobile ad hoc Networking and Computing* (*MobiHoc'07*), pp. 80-89, 2007.

[30] B. Zhu, V. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," *IEEE Computer Security Applications Conference* (*ACSAC'07*), pp. 257–267, 2007.

[31] Y. Sei and S. Honiden, "Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks," *The 4th Annual International Wireless Internet Conference* (*WICON'08*), pp. 1-8, 2008.

[32] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proc. of the ACM Conference Computer Communication Security* (*CCS'02*), pp. 41-47, 2002.

[33] H. Chan, A. Perrig, and D. Song, "Key distribution techniques for sensor networks," *Wireless Sensor Networks,* C. S. Raghavendra, K. M. Sivalingam, T. Znati, Norwell, MA: Kluwer Academic, pp. 277-303, 2004.

[34] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," *Proc. of the 2003 IEEE Symposium on Security and Privacy,* pp. 197-213, 2003.

[35] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *The 10th ACM Conference on Computers and Communication Security* (*CCS 03*). pp. 52-61, Oct 2003.

[36] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks," *Proc. of the 1st ACM Workshop on Security of ad hoc and Sensor Networks,* pp. 72-88, 2003.

[37] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanisms for large-scale distributed sensor networks," *The 10th ACM conference on Computers and Communication Security* (*CCS 03*), pp. 62-72, Oct 2003.

[38] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," *Advances in Cryptology – CRYPTO '92, LNCS 740,* pp. 471-486, 1993.

[39] © [2008] IEEE. Reprinted, with permission, from [*The 27th IEEE International Performance, Computing and Communication Conference* (*IPCCC '08*), An efficient key distribution scheme for establishing pairwise keys with a mobile sink in distributed sensor networks, A. Rasheed and R. N. Mahapatra].

[40] © [2010] IEEE. Reprinted, with permission, from [*IEEE Transactions on Parallel and Distributed Systems*, An efficient key distribution scheme for establishing pairwise keys with a mobile sink in distributed sensor networks, A. Rasheed and R. N. Mahapatra].

[41] A. Rasheed and R. N. Mahapatra, **"**A key pre-distribution scheme for heterogeneous sensor networks," *The 5th International Wireless Communications and Mobile Computing Conference* (*IWCMC'09*), pp. 263-268, 2009.

[42] A. Rasheed and R. N. Mahapatra, **"**The three-tier security scheme for wireless sensor with mobile sink," *IEEE Transactions on Parallel and Distributed Systems,* submitted for publication, 2010.

[43] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," *Proc. of the Infocom*'03. pp. 1976-1986, April 2003.

[44] S. Capkun, L. Buttyan, J. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," *Proc. of the 1st ACM Workshop on Security of ad hoc and Sensor Networks*, pp. 21-32, October 2003.

[45] P. Papadimitratos and Z. J. Haas, “Secure routing for mobile ad hoc networks,” *Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),* pp. 1-13, January 2002.

[46] © [2008] IEEE. Reprinted, with permission, from [*Network Computing and Applications* (*NCA’08*) *7th IEEE International Symposium*, Secure data collection scheme in wireless sensor network with mobile sink, A. Rasheed and R. N. Mahapatra].

[47] © [2009] IEEE. Reprinted, with permission, from [*The 28th IEEE International Performance, Computing and Communication Conference* (*IPCCC’09*), Mobile sink using multiple channels to defend against wormhole attacks in wireless sensor networks, A. Rasheed and R. N. Mahapatra].

[48] S. Hussain, F. Kausar, and A. Massod, "An efficient key distribution scheme for heterogeneous sensor networks," *International Conference on Wireless Communications and Mobile Computing* (*IWCMC’09*), pp. 388-392, 2007.

[49] R. Blom, “Non-public key distribution,” In *Advances in Cryptology-CRYPTO’82,* D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. New York: Plenum Publishing, pp. 231-236, 1982.

[50] K. Ren, K. Zeng, and W. Lou, “A new approach for random key pre-distribution in large-scale wireless sensor networks,” *Wireless Communication and Mobile Computing*, vol. 6, no. 3, pp. 307-318, 2006.

[51] R. Merkle, “Secure communication over insecure channels,” *Communication of the ACM,* vol. 22, no. 4, pp. 294-299, April 1978.

[52] W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, “A pairwise key predistribution scheme for wireless sensor networks,” *ACM Transactions on Information and System Security,* vol. 8, no. 2, pp 228-258, May 2005.

[53] L. Lamport, “Password authentication with insecure communication,” *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, November 1981.

[54] R. Rivest, “The MD5 message-digest algorithm,” *RFC 1321*, http://tools.ietf.org/html/rfc1321, April 1992.

[55] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *Journal of ACM,* vol. 33, no. 4, pp. 792-807, 1986.

[56] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Network,* vol. 1, no. 1, pp. 175-192, July 2003.

[57] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. Tygar, "SPINS: Security protocols for sensor networks," *Proc. of the 7th Annual International Conference on Mobile Computing and Networking* (*MobiCom*), pp. 189-199, 2001.

[58] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. Columbus, OH.: McGraw Hill, pp. 116-119, 2002.

[59] K. Fodor and A. Vidacs, "Efficient routing to mobile sinks in wireless sensor networks," *Proc. of the 3rd International Conference on Wireless Internet,* pp. 1-10, 2007.

[60] W. Wang, V. Srinivasan, Kee-Chaing Chua, "Extending the lifetime of wireless sensor networks through mobile relays," *IEEE/ACM Transactions on Networking* (*TON*), vol. 16, no. 5, pp. 1108-1120, Oct. 2008.

[61] G. Shi, M. Liao, M. Ma, and Y. Shu, "Exploiting sink movement for energy-efficient load-balancing in wireless sensor networks," *Proc. of the 1st ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing,* pp. 39-44, 2008.

[62] L. Galluccio, A. Leonardi, G. Morabito, and S. Palazzo, "A trade-off between energy consumption reduction and responsiveness in information delivery for delay-tolerant sensor networks with mobile sink," *Proc. of the 2006 International Conference on Wireless Communications and Mobile Computing,* pp. 563-568, 2006.

[63] Z. Vincze and R. Vida, "Multi-hop wireless sensor networks with mobile sink," *Proc. of the 2005 ACM Conference on Emerging Network Experiment and Technology,* pp. 302-303, 2005.

[64] B. Kusy, H. Lee, M. Wicke, N. Milosavljevic, and L. Guibas, "Predictive Qos routing to mobile sinks in wireless sensor networks," *Proc. of the 2009 International Conference on Information Processing in Sensor Networks,* pp. 109-120, 2009.

[65] M. Grossglauser and D.N.C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Networking (TON),* vol. 10, no. 4, pp. 477-486, Aug. 2002.

[66] S. Jain, R.C. Shah, W. Brunette, G. Borriello and S. Roy, "Exploiting mobility for energy efficient data collection in wireless sensor networks," *Mobile Networks and Applications,* vol. 11, no. 3, pp. 327-339, April 2006.

[67] A. Chakrabarti, A. Sabharwal and B. Aazhang, "Communication power optimization in a sensor network with a path-constrained mobile observer," *ACM Transactions on Sensor Networks (TOSN),* vol. 2, no. 3, pp. 297-324, 2006.

VITA

Amar Adnan Rasheed received his Bachelor of Science degree in electronic and communication systems from Baghdad University in May 1999, and a Master of Science degree in computer science from Northeastern Illinois University in December 2004. From 2006 to 2010 he worked as a Teaching Assistant in the Department of Computer Science and Engineering at Texas A&M University and received his Doctor of Philosophy degree in May 2010. His research interests include wireless sensor networks, mobile ad hoc network, energy-efficient data collection schemes, cryptography algorithms, and key pre-distribution schemes for sensor networks. Mr. Rasheed may be reached at amar_rasheed@tamu.edu

Name:	Amar Adnan Rasheed
Address:	Department of Computer Science and Engineering Texas A&M University H.R. Bright Building, room # 516 College Station, TX 77843-3112
Email Address:	amar_rasheed@tamu.edu
Education:	B.S., Electronic and Communication Systems Engineering, Baghdad University, 1999 M.S., Computer Science, Northeastern Illinois University, 2004 Ph.D., Computer Science, Texas A&M University, 2010