International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.411-422
http://dx.doi.org/10.14257/ijsia.2016.10.2.35

A Hybrid Key Establishment Scheme for Wireless Sensor Networks

Jianmin Zhang[1], Qingmin Cui[1] , Rui Yang[2]

[1]*College of Computer, Henan Institute of Engineering*
Zhengzhou 451191, China
[2]*College of Science, Henan Institute of Engineering*
Zhengzhou 451191, China

Abstract

To establish pairwise keys for each pair of neighboring sensor nodes is a basic service, forming the basis other security services, such as authentication and encrypted in wireless sensor networks (WSNs). However, due to constrained energy, memory, and computational capabilities of sensor nodes to establish the pairwise key is challenging task. Here, a combination of polynomial pool-based and the probabilistic key predistribution scheme for WSN is presented. In the proposed scheme part of sensor nodes are pre-loaded polynomial shares, and the polynomial shares are used to compute the keys which make up a key pool. And the rest of sensor nodes are preloaded the keys selected from this key pool. The proposed scheme is analyzed based on connectivity, resistance against attacks, memory consumption and communication overhead. And the simulation results show that the proposed scheme performs better in terms of network resilience to node capture compared to the existing schemes.

Keywords*: Wireless sensor networks; Key predistribution; Security; Polynomial*

1. Introduction

Wireless sensor networks (WSNs) is composed a large number, battery-powered, limited memory and limited computational power sensor nodes distributed in a designed area without any fixed structure [1]. Each sensor node is a small device that consists of data processing, sensing, and short range radio communication units, and a battery. Typically, sensor nodes are employed to collect environmental information. This information is aggregated by transferring it to other sensor nodes wirelessly until it reaches a sink node. Usually, the sensor nodes are compromised of low-cost hardware components with constraints on battery life, memory size, and computation capabilities [2]. The application of WSNs range from civilian, like habit monitoring and health care, to military or security areas, such as battlefield surveillance, targeting and tracking systems[3,4]. Since sensor nodes may be located in hostile locations, particularly with military applications, security is an essential issue in these networks. WSN is subject to different types of security threats and attacks. These include capture of a sensor node, intentionally providing false information, impersonation, data modification, eavesdropping, etc. Therefore, security considerations, such as authentication and confidentiality must be undergone to ensure integrity of sensor node and proper functionality of the network. As an indispensable security component, key management is a core mechanism to secure WSNs. Key management can be defined as a set of process and mechanisms that support key establishment and maintenance of ongoing keying relationships between valid parties according to a security policy. Since sensor nodes in WSNs have constraints in their computational power and memory capability, it is not

ISSN: 1738-9976 IJSIA

feasible for WSNs to use traditional pairwise key establishment techniques such as public key cryptography and key distribution center (KDC) [5, 6].

A particular symmetric approach in WSNs is to use key pre-distribution with the sensor nodes, resulting in low cost key establishment. In this regard, various schemes have been proposed for key management in WSNs [7-23]. The choice of a key management protocol should consider factors such as processing overhead, resource consumption and connectivity. However, some of these goals are contradictory. For example, increasing network connectivity also increases the memory requirements of sensor nodes. Hence, some techniques that provide high connectivity also consume significant memory and processing power. Others use less memory but have low connectivity.

1.1 Contributions and Organizations

In this paper, we exploit the use of the probabilistic key predistribution scheme in conjunction with the polynomial pool key predistribution scheme to establish a secure link between sensor nodes and improve network resilience to node captures. Prior to network deployment, part of sensor nodes in WSNs are preloaded with polynomials shares of randomly selected subsets of r polynomials out of m polynomials. Then a new key poll is generated by using the preloaded polynomials shares in the first part of sensor nodes. And the rest of sensor nodes are preloaded with the generation keys in the key pool. This proposed scheme guarantee that the compromised sensor nodes in the later part of sensor nodes will not leak key information in the sensor nodes in the first part of sensor nodes.

The rest of the paper is organized as follows. The remainder of this section introduces a summary of the related works in the literature. Section 2 gives an overview of the polynomial- based key predistribution scheme. Section 3 presents our proposed scheme in detail. Section 4 given the detailed performance evaluation of the proposed protocol and comparisons with the previous scheme. Finally, some conclusions are given in Section 5.

1.2 Selected Related Work

Eschensuer and Gligor[7] were the first to propose a key predistribution scheme for WSNs . It also constitutes the foundation of the subsequent of key distribution schemes in WSNs. In this scheme, before deployment, a large key pool which contains many distinct keys with key identifier is randomly generated. And each sensor node is loaded with a predefined number of keys that constitute its key rings. Keys in the key rings are randomly picked form the key pool. After deployment in the networks, a pair of neighboring nodes may have shared common key to establish a secure connection. In the literature, this procedure of discovering of the common key between two sensor nodes is called shared key discovery. If there is no common key between two nodes, they have to establish a key through an intermediate sensor node which has common keys with both sensors, which is called path key establishment. Unfortunately, this scheme cannot provide sufficient security as the number of compromised increases. To improve the network resilience against the node capture attack, Chen et al. [8] generalized this scheme to the q-compromised scheme , in which two nodes can establish a secure communication link only if they share at least q (q>1) common keys. They showed that the network resilience against the node capture attach can be improved when number of compromised nodes is small.

Liu et al. proposed a new key predistribution scheme [9], which is combined the basic scheme in[7] with Blundo's polynomial-based key distribution scheme[10]. In this scheme, every sensor node is preloaded with coefficient of symmetric bivariate polynomial computed at one of its variables using its identification. The symmetry property of the polynomial allows two nodes to get their pairwise key respectively. This

scheme exhibits a nice threshold property, which means that when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is close to zero. A similar method was also developed by Du et al. [11], in which matrices are uses instead of polynomials. Later, these two schemes have been further explored in [12, 13, 14].

Liu et al. [15] proposed several schemes that use location information. The goal of such schemes was to save memory costs while maintaining a high level of security. Du et al[16] considered the priority of deployment packets in order to avoid unnecessary key assignments. In this scheme, they assume that the sensor nodes are deployed in groups of some sensor nodes over a rectangular area. In the key predistribution phase, the original key pool is divides into many smaller pools, each of which is associated to different group. These schemes can gain substantial improvement over exiting schemes that do not exploit deployment. This group-based deployment model was further deployed in[17, 18].

Camptepe and Yener [19] first applied combinatorial designs to key pre-distribution. They proposed two classed of combinatorial designs: symmetric-balanced incomplete block designs and generalized quadrangles. The points and blocks in the combinatorial designs are associated with the distinct key identifiers and nodes, respectively. Later, Sanchez et al. [20] made use of combinatorial design theory to the pre-distribution of multiple bivariate polynomial shares based on Blundo's [10] key pre-distribution. This scheme enable direct key establishment for a large number of nodes, independently of the physical connectivity properties of WSNs. Lee and Stinson[21,22,23] proposed a class of key pre-distribution schemes based on combinatorial designs. Their approaches improve the efficiency in direct-key and path-key establishments compared with the random key pre-distribution protocols.

2. Overview of the Polynomial-based Key Predistribution Scheme

In this section, we briefly review the polynomial-based key predistribution scheme proposed by Blundo et al.[10]， which is the basis of our new technique.

The key setup sever randomly generates a bivariate *t*-degree polynomials with coefficients $f(x,y)=\sum_{0\le i,j\le t} a_{ij}x^i y^j$, where $a_{ij}=a_{ji}$, over a finite field F_q, where q is a prime number large enough to accommodate a cryptographic key. The polynomials have the property $f(x, y)=f(y, x)$.

To identify the different sensor nodes, the setup sever many assign each sensor node a unique *ID*. For each sensor node *u*, the setup server computes a polynomial share of $f(u,y)$, and preloaded it into sensor node *u*. For any two sensor nodes *u* and *v*, node *u* can compute its key $f(u,v)$ by evaluating $f(u,y)$ at point *v* and node *v* can compute the same key $f(v, u)=f(u, v)$ by evaluating $f(v,y)$ at point *u*. Then the two sensor nodes *u* and *v* can establish a common key $f(u,v)$.

In this approach, each sensor node *i* needs to store a *t*-degree polynomial $f(i, x)$, which occupies $(t + 1)\log q$ storage space. To establish a pairwise key, both sensor nodes need to evaluate the polynomial at the ID of the other sensor ode. There is no communication overhead during the pairwise key establishment process. The advantage of this scheme is that any two neighbor nodes can establish a secret key using the same symmetric bivariate polynomial $f(x,y)$and there is no communication overhead during the pairwise key establishment process. The security proof in Blundo scheme [10] ensures that this scheme is unconditionally secure and *t*-collision resistant. In other words, the coalition of no more

than compromised sensor nodes knows nothing about the shared keys between any two non-compromised sensor nodes.

It is theoretically possible to use the general group key distribution protocol in [10] in sensor networks. However, the storage cost for a polynomial share is exponential in terms of the group size, making it prohibitive in sensor networks. In particular, it can only tolerate the collusion of no more than t compromised nodes, where the value of t is limited by the available memory space and the computation capability on sensor nodes. Indeed, the larger a sensor network is, the more likely an adversary compromises more than t sensor nodes and then the entire network. To have secure and practical key establishment techniques, the authors in [9] developed general framework for key predistribution based on the combination of the polynomial-based key predistribution and [10] and the key pool idea used in[8]. In this scheme, instead of randomly selecting keys from a large key pool and assigning them to sensor nodes, this method randomly choose polynomials from a polynomial pool and the key pool in [8] are replaced by the polynomial-pool and assign their polynomial shares to sensor nodes.

3. The Proposed Scheme

3.1 Preliminaries

In the proposed scheme part of sensor nodes in WSNs, which are called *P*-sensors in the paper, are preloaded with polynomials shares as in [9]. Then a new key poll is generated by using the preloaded polynomials shares in the *P*-sensors. And the rest of sensor nodes, which are called *B*-sensor in the paper, are preloaded with the generation keys in the key pool as in[7].

Moreover, we list the all the notations used in rest of the paper in Table 1.

Table 1. Summery of Notations

Notation	Description
n	The number of sensors in the WSN
ID_u	Identity of sensor node u.
p	The percentage of the *P*-sensors in the WSN
m	The polynomial pool size
t	The degree of a polynomial in our scheme
Id_p	Identity of polynomial p
r	The number of polynomial in each *P*-Sensor
s	The number of keys in each *B*-Sensor
H	Secure hash function H:$\{0,1\}^*$--> $\{0,1\}^{160}$
||	Concatenation operation

3.2 Key Predistribution Scheme

The goal of the scheme is to allow sensor nodes to find a common secret key identity after deployment. Our scheme consists of three phases: Initialization Phase, Direct Key Establishment Path and Path Key Establish Establishment Phase. The last phase is exactly as that of the basic scheme[7], so we will not discuss it here.

Initialization Phase This phase is done offline by a Key Distributions Servers (KDS) before deploying the sensor nodes in a target field. It consists of the following steps:

Step 1 (*Polynomial Share Predistribution in P-Sensor*). The KDS generates a large pool of bivariate *t*-degree polynomials over the finite field F_q and each polynomial has a unique *Id*. For a each *P*-sensor *u*, the KDS randomly picks a subset of polynomials $f(x,y)$ and compute the shares of these polynomials to node *u*. The shares of these polynomials are the coefficients b^i of y^i of $f(u,y)$. Here we denotes $f(u,y)$ as a univariate *t*-degree polynomials. Then the KDS assigns the polynomial *Id*, the shares of polynomial b^i and the exponent *i* of their corresponding variable y^i.

Step 2 (*Key Pool Generation for B-sensors*): For each shares in *P*-sensor *u*, the KDS compute $K=H(b_i||i||ID_u)$ as the key in the key pool. With all *P*-sensor, the KDS generates a key pool. And each key in the key pool is identified by a 3-tuple (Id_p, i, ID_u).

Step 3 (*Key Predistribution in B-sensors*). For each *B*- node, the KDS randomly picks a subset keys from the key pool and loads these keys and their corresponding identity to it.

An example of key pool generation is illustrated in Figure 1.

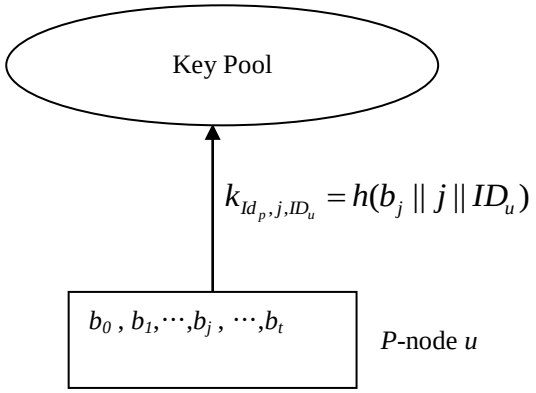


Figure 1. A Sample Key Pool Generation

Direct Key Establishment Phase This phase takes place during wireless sensor networks initialization in the operation environment where every node discovery its neighbors in wireless communication range with which it can establish a key. To discovery whether two neighbor nodes can establish a common key, the *P*-sensor disclose a list of *Id* of the polynomial and its ID and the all *B*-node disclose a list *ID* of the preload keys to its neighbors.

Assuming that sensor *u* and sensor *v* are neighbors, According the type of sensor node *u* and sensor node *v*, the pairwise key between these sensor nodes can be computed as following method. There are three cases needed to be considered.

Case 1: Both sensor nude *u* and sensor *v* are *P*-sensor. In this case, in this case these two sensor node can compute their pairwise keys as in [9].

Case 2: Both sensor node *u* and sensor *v* are *B*-sensors. In this case, in this case these two sensor node can compute their pairwise keys as in [7].

Case 3: One of the two nodes is *P*-sensor and another is *B*-sensors. Without loss of generality, here we suppose node *u* is a *P*-sensor and node *v* is a *B*-sensor. If the identification of one key *K* in sensor node *v* is (Id_p, i, ID_u) and the identification of one polynomial in sensor *u* is Id_p ,the sensor node *u* can compute the communication key $K_{uv}=h(b_i||i||ID_u)$. And the sensor node *v* can use the *K* as the communication key. It is obviously that the *K* in the sensor node *v* is $h(b_i||i||ID_u)$.

4. Performance Analysis

In this section, we evaluate the proposed scheme. The evaluation metrics includes the storage and communication overhead of every sensor node, the network connectivity and the security of the scheme.

4.1 Overhead

Memory Overhead: According to our scheme, during the initialization phase each *B*-sensor needs to store *s* keys over F_q. In addition, each node needs to store the ID of the keys Assume the ID of sensor nodes are chosen from a finite field F_q.Thus, the overall storage overhead of each *B*-sensor is $s(\log q + \log q')$ bits. For each *P*-sensor, the memory overheads is $(r(t+1)\log q + \log q')$.

Communication Overhead: In the shared key discover phase each *B*-sensor needs to disclose of a list of *s* index of keys to its neighbor nodes. And each *P*-sensor needs to disclose of a list *r* index of polynomial to its neighbor nodes.

4.2. Local Connectivity

Local connectivity is the probability of two neighbor sensor nodes establishing communication key directly. It is an important metric to evaluate a key predistribution scheme. To achieve a desired global connectivity, the probability of direct key establishment must be higher than a certain threshold value.

Let $A_1(u, v)$ be the event that sensor node *u* and *v* are both *P*-nodes, $A_2(u, v)$ be the event that sensor node *u* and *v* are both *B*-node, and $A_3(u, v)$ be the event that one of node in sensor node *u* and *v* is *P*-node and another is *B*-node. Then the probabilities of these events are as follows.

$$P(A_1(u,v)) = p^2 \tag{1}$$

$$P(A_2(u,v)) = (1-p)^2 \tag{2}$$

$$P(A_3(u,v)) = 2p(1-p) \tag{3}$$

Let $B(u,v)$ be the event that sensor node *u* and *v* can establish pairwise key directly, then we have

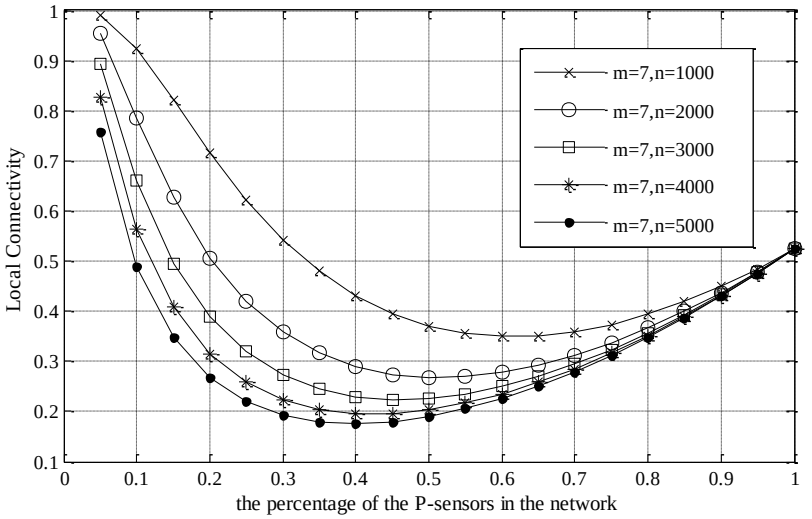
$$\Pr(B(u,v) \mid A_1(u,v)) = 1 - \frac{\binom{m}{r}\binom{m-r}{r}}{\binom{m}{r}\binom{m}{r}} = 1 - \frac{((m-r)!)^2}{m!(m-2r)!} \tag{4}$$

$$P(B(u,v) \mid A_2(u,v)) = 1 - \frac{\binom{pnt-s}{s}\binom{pnt}{s}}{\binom{pnt}{s}\binom{pnt}{s}} = 1 - \frac{((pnt-s)!)^2}{(pnt)!(pnt-2s)!} \tag{5}$$

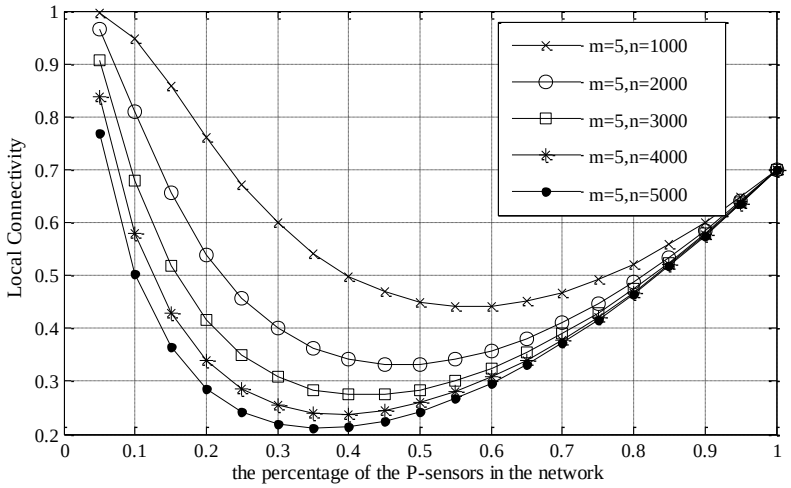
$$P(B(u,v) \mid A_3(u,v)) = 1 - \frac{\binom{m}{r}\binom{pnt - rpnt/m}{s}}{\binom{m}{r}\binom{pnt}{s}} == 1 - \frac{(pnt - rpnt/m)!(pnt - s)!}{(pnt - rpnt/m - s)!(pnt)!} \tag{6}$$

As the events A_1, A_2 and A_3 are mutually exclusive and $A_1+A_2 + A_3 = \Omega$, here Ω is the probability space, we have

$$\Pr(B(u,v)) = \sum_{i=1}^{3} P(A_i(u,v))P(B(u,v) \mid A_i(u,v)) = p^2\left(1 - \frac{((m-r)!)^2}{m!(m-2r)!}\right)$$
$$+ (1-p)^2\left(1 - \frac{((pnt-s)!)^2}{(pnt)!(pnt-2s)!}\right) + 2p(1-p)\left(\frac{(pnt - rpnt/m)!(pnt-s)!}{(pnt - rpnt/m - s)!(pnt)!}\right) \tag{7}$$



(a)



(b)

Figure 2. The Local Connectivity Versus the Percentage of the *P*-sensors in the Network and the Combination of *m* and *n* given *r*=2,*t*=100,*s*=200

Figure. 2 indicates the relationship between the local network connectivity and the combination *m*, *n*, *r*, *t*, *s* and *p*. It is nodded that in a given situation the local network connectivity will decrease with the percentage of the *P*-sensors in the WSN increasing at first and then the local network connectivity will increase as with the percentage of the *P*-sensors in the WSN increasing.

4.2. Security Analysis

In this subsection, we first study the resiliency of the proposed scheme against sensor capture through probability analysis. Then we compare our scheme with some existing schemes by calculating the fraction of compromised communication among non-compromised nodes.

Because the working environments of sensor networks usually are hostile, it's easy for sensor nodes will be captured and revealed information. Adversaries could get all the pairwise keys in compromised nodes therefore they could break a number of secure links. Node capture attack is one of the most serious threats in wireless sensor networks. An adversary may physically capture sensor nodes and compromise the stored secret information since sensor nodes are not tamer resistant due to their low cost. We assume that if a sensor node is captured all the information in the sensor node will be disclosed by the adversary. And we also assume that the adversary has no knowledge about the sensor nodes before the node has been compromised. The resilience of the scheme is measured as the fractions of total network communication that are compromised when *x* sensor nodes are captured [7].

Resilience against Nodes Capture In this section, we calculate the fraction of compromised network communication that is the disclosed communication among non-compromised sensor nodes. To compute this fraction, we calculate the probabilities of compromising the shared keys between any two non-compromised sensor nodes after *x* sensor nodes have been compromised.

Suppose *K* be the communication key used by two non-compromised sensor node *u* and *v*. For simplicity, we call the communication *K* between two *P*-sensors polynomial-based key, which is calculated by the polynomial and key-pool-based key in other cases. Let D_1 represents the event the communication *K* is a polynomial-based key, D_2 be the key-pool-based key. Let E_1 represents the joint event that the key is a polynomial-based key and the key has been compromised and Let E_2 represents the joint event that the key is a key-pool-based key and the key has been compromised. We use the notation $K \in D_1$ to represent that "Key *K* was a polynomial-based key and $K \in D_2$ to represent that "Key *K* was a key-pool-based generation key". When *x* nodes have been compromised, the probability of the communication key *K* been compromised is:

$$P(K_{compromised} \mid C_x) = P((E_1 \cup E_2) \mid C_x) \tag{8}$$

As the event E_1 and E_2 are mutually exclusive, we have

$$P(K_{compromised} \mid C_x) = P(E_1 \mid C_x) + P(E_2 \mid C_x) \tag{9}$$

Since the event $K \in D_1$ is dependent of the event C_x and (D_1 is compromised) and the event $K \in E_2$ is dependent of the event C_x and (D_2 is compromised), we have

$$P(K_{compromised} \mid C_x) = P(E_1 \mid C_x) + P(E_2 \mid C_x)$$
$$= \frac{P((K \in D_1) \cap (D_1 \text{ is compromised}) \cap C_x)}{P(C_x)} + \frac{P((K \in D_2) \cap (D_2 \text{ is compromised}) \cap C_x)}{P(C_x)}$$
$$= P(K \in D_1)P(D_1 \text{ is compromised} \mid C_x) + P(K \in D_2)P(D_2 \text{ is compromised} \mid C_x) \tag{10}$$

Then we have

$$P(K \in D_1) = P(A_1(u,v)) = p^2 \tag{11}$$

$$P(K \in D_2) = P(A_2(u,v) \cup A_3(u,v)) = P(A_2(u,v)) + P(A_3(u,v))$$
$$= (1-p)^2 + 2p(1-p) = 1 - p^2 \tag{12}$$

Because of the one-way computation property of the hash function, an adversary can't get any polynomial information from a compromised B-sensor. As the sensor nodes are captured randomly, there are xp P-sensors in the x compromised sensors. Similar to the analysis in [9] and [7], we have

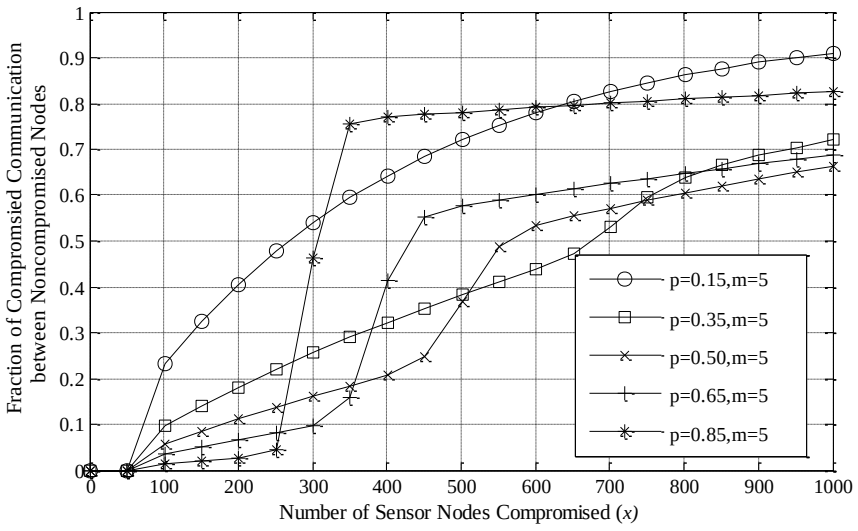
$$P(D_1 \text{ is compromised} \mid C_x) = 1 - \sum_{i=0}^{t} \binom{px}{i} \left(\frac{r}{m}\right)^i \left(1 - \frac{r}{m}\right)^{px} \tag{13}$$

$$P(D_2 \text{ is compromised} \mid C_x) = 1 - \left(1 - \frac{s}{pnt}\right)^x \tag{14}$$

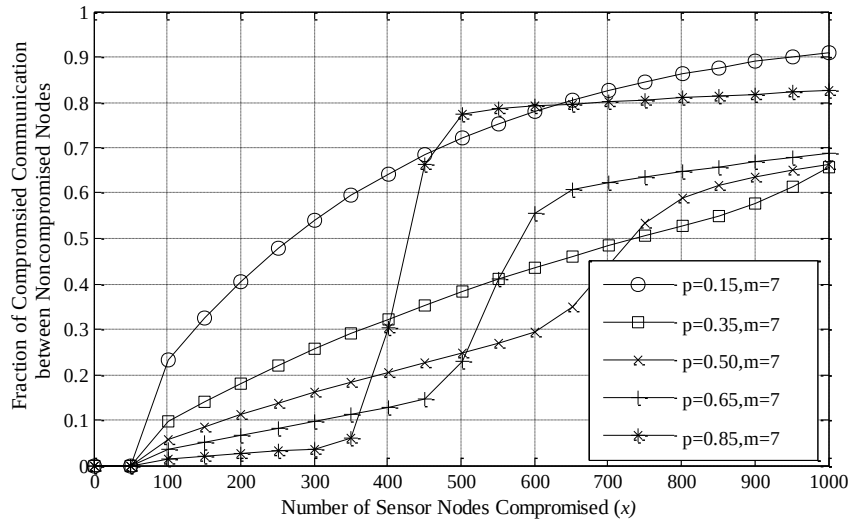
From (9)(10)(11)(12)(13), the probability of a data-communication link between two non-compromised sensor being compromised is :

$$P(K_{compromised} \mid C_x) = p^2 \left(1 - \sum_{i=0}^{t} \binom{px}{i} \left(\frac{r}{m}\right)^i \left(1 - \frac{r}{m}\right)^{px}\right) + (1-p^2)\left(1 - \left(1 - \frac{s}{pnt}\right)^x\right) \tag{15}$$

The relationship between the fraction of compromised links for non-compromised nodes and the number of compromised nodes is presented in Figure 3.



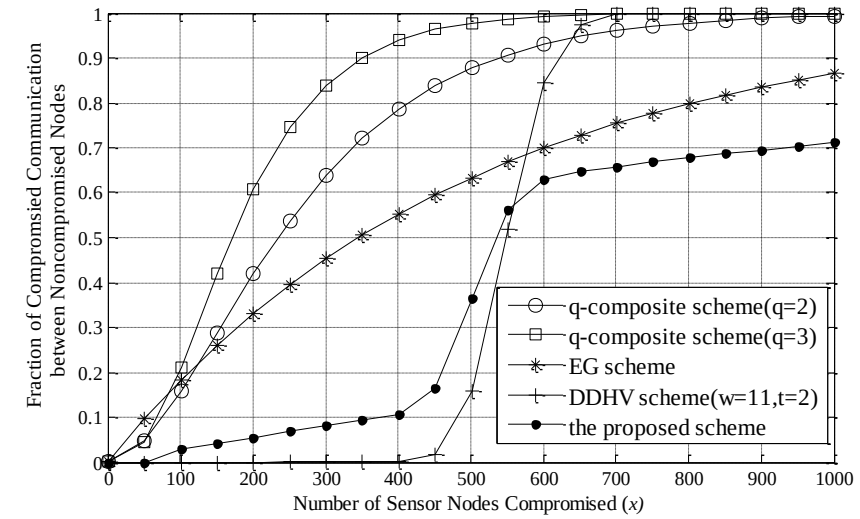
(a)



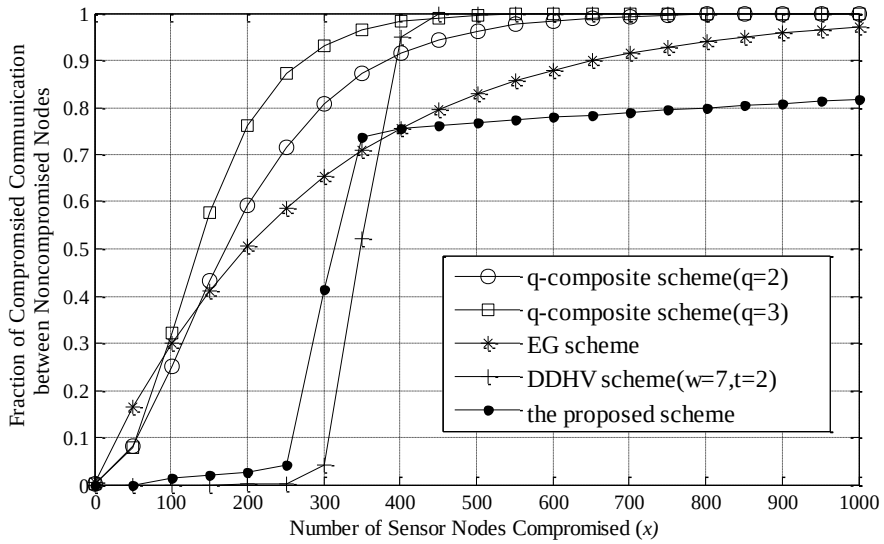
(b)

Figure3. Fraction of Compromised Link between Non-compromised Nodes with different connectivity, after an adversary has compromised x random nodes given r=2,t=100,s=200,n=5000

Comparison with Previous Schemes To evaluate our work, in this subsection we compare the security of our scheme with that of the related previous works. Here, we compare our scheme with EG scheme [7], q-composite scheme (for q=2,3) [8], and DDHV scheme[9] . In the following analysis, we use the same amount of the storage per node for a fair comparison. In the all schemes, we assume that each sensor node is capa ble of holding 200 cryptographic keys in its memory. The local network connectivity probability is taken as 0.33 and 0.5 with suitable values of the parameters for the different schemes.



(a)



(b)

Figure. 3. Fraction of Compromised Link between Non-compromised Nodes, after an Adversary has Compromised x Random Nodes. The Local Network Connectivity is 0.33 in (a) and 0.5 in (b) Respectively

Figure.3 compares the fraction of links compromised between non-compromised sensors given the same local connectivity P_L, t and storage overhead. We can see that our scheme significantly better than the other two schemes. For example, in the Fig. 3(a), when there has 600 sensor nodes compromised, there will be 70.0% of links compromised between non-compromised sensors in EG scheme, 97.8% in q-composite (q=2), 87.7% in q-composite (q=3) , and 84.5% is DDHV scheme, while there will only be 63.1% in our scheme.

5. Conclusion

In this paper, a new key predistribution approach based on the combination of polynomial and key pool technology was proposed and numerically evaluated. In the proposed, the part of compromised sensor nodes will not disclosed any key information of

other sensor nodes and these two parts of sensor nodes can establish key directly. The effectiveness of the proposed algorithms has been demonstrated through analysis and comparisons with the existing schemes.

References

[1] K. Romer K, F. Mattern F, "The design space of wireless sensor networks", IEEE Wireless Communications, vol.11, no.6, **(2004)** , pp.54-61,
[2] P.Rawat P, K.D.Singh, H.Chaouchi, "Wireless sensor networks: a survey on recent developments and potential synergies", The Journal of Supercomputing,vol.68, no.1, **(2014)**,pp.1-48.
[3] K.Padmavathi, K.S.Reddy, "Wireless Sensor Networks Application of Wellness Determination for elderly people", International Journal of Research in Computer Engineering & Electronics, vol.3, no.4, **(2014)**.
[4] D. Puccinelli, M.Haenggi, "Wireless sensor networks: applications and challenges of ubiquitous sensing", Circuits and Systems Magazine, IEEE1, vol.5, no.3, **(2005)**, pp. 19-3.
[5] C.Y.Chen, H.C.Chao, "A survey of key distribution in wireless sensor networks", Security and Communication Networks, vol.7, no.12, **(2014)**, pp. 2495-2508.
[6] L.Si, Z.Ji, Z.Wang, "The application of symmetric key cryptographic algorithms in wireless sensor networks", Physics Procedia, vol.25, **(2012)**, pp.552-559.
[7] L. Eschenaure and V.D. Gligor, "A key-management scheme for distributed sensor networks". in Proc. of the 9the ACM Conference on Computer and Communications, , Nov. **(2002),** pp.41-47
[8] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", in Proc. of 2003 IEEE Symposium on Security and Privac, May **(2003)**, pp.197-213
[9] D. Liu, P. Ning and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks", ACM Transactions on Information and System Security, vol.8, no.1,**(2005)**, pp. 41-77.
[10] W. Du, J. Deng, Y.S. Han, P.Varshney, J. Katz and A. Khalili, "A Pairwise Key Predistribution Schemes for Sensor Networks", ACM Transactions on Information and System Security,vol.8, no. 2,**(2005)**, pp.228-258.
[11] W.Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution schemes for sensor networks networks". ACM Transactions on Information and System Security, vol.8. no2, **(2005)**, pp.228-258
[12] A. Rasheed and R. N. Mahapatra, "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks", IEEE Transactions on Parallel and Distributed Systems,vol.22, no.1,**(2011)**, pp 176-184.
[13] F. Delgosha and F. Fekri, "A multivariate key-establishment scheme for wireless sensor networks", IEEE Transactions on Wireless Communications, vol.8, no.4, **(2009)**, pp.1814-1824.
[14] H. Dai and H. Xu, "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", IEEE Sensors Journal, vol.10, no.8, **(2011)** , pp1399-1409.
[15] W. Du, J., Y. S.Han and P.Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge", IEEE Transactions Dependable Secure Compute, vol.3, no.1,**(2006)**, pp.62-77.
[16] B. Zhou, S. Li, Q. Li, X. Sun and X. Wang, "An Efficient and Scalable Pairwise Key Pre-distribution Scheme for Sensor Networks Using Deployment Knowledge", Computer Communications, vol.32, no.1, **(2009)**, pp.124-13.
[17] T. Kwon, J. Lee and J. Song, "Location-based pairwise key predistribution for wireless sensor networks", IEEE Transactions on Wireless Communications, vol.8, no.1, **(2009)**, pp.5436-5442.
[18] Claude Castelluccia, Angelo Spognardi, "Rok: A robust key pre-distribution protocol for multi-phase wireless sensor networks", in Proc. of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, pp.351-360, **(2007).**
[19] C. Blundo, A. D. Santis, A. Herzberg. S. Jutten, U. Vaccaro, and M. Yung. "Perfectly secure key distribution for dynamic conference", Information and Computation, vol.1, **(1995)**, pp.1-23
[20] S.A Campete and B.Yener, "Combintorial design of key distrbution mechanisms for wirless sensor networks", in Proc of Computer Security, pp.293-308, **(2004)**.
[21] J.Lee and D.K. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks, " in Proc. of IEEE Wireless Communication Network Conference, pp.1200-1205,**(2005)**.
[22] J.Lee and D.K. Stinson, "Deterministic key pre-distribution schemes for distributed sensor networks", in Proc. of the 11th Int'l Workshop, pp.293-307, **(2005)**.
[23] D.Sanchez and H.Baldus, "A deterministic pairwise key predistribution scheme for mobile sensor networks", in Proc. of the 1st Int's Conf. on Security and Privace for Emergin Area in Communications Networks, pp.277-288,**(2005)** .

