

Distributed Pairwise Key Establishment in Wireless Sensor Networks

Yi Cheng and Dharma P. Agrawal

OBR Center for Distributed and Mobile Computing, Department of ECECS
University of Cincinnati, Cincinnati, OH 45221
{chengyg, dpa}@ececs.uc.edu

Abstract - Security is a big challenge when wireless sensor networks are deployed in a hostile environment. Due to the computational and storage overheads, traditional asymmetric-key based security protocols are not suitable for the resource-constrained wireless sensors. Several symmetric-key distribution protocols have been proposed in literature to establish shared cryptographic keys between sensor nodes, but most of them only work for small-scale networks due to their linearly increased communication overhead and key storage overhead. Furthermore, existing protocols are not secure when the number of compromised nodes exceeds a threshold value. In this paper, we propose a new distributed pairwise key establishment method for large-scale wireless sensor networks. Compared with existing key distribution protocols, our scheme guarantees any two sensors to establish a pairwise key between them with low overheads. A high level network security also can be achieved in our scheme even a large number of sensors are compromised.

Keywords: Network security; Wireless sensor networks; Pairwise key establishment; Key distribution protocols

1. Introduction

Due to their easy-deployment, self-organization and fault-tolerance, wireless sensor networks (WSNs) facilitate large-scale, real-time data processing in various environments [1][2]. WSNs can be widely used to monitor military, environmental, safety-critical or domestic infrastructures and resources. Communication security is a big issue when WSNs are deployed in a hostile environment. Since wireless sensors are operated in the unattended mode, secret keys should be used to encrypt the exchanged data between communicating parties [4][5][6][10][11][12]. Considering the strict resource constraints of tiny sensors and the unpredictable network topology, key distribution and management is a big challenge when we design a wireless sensor network.

As we known, in traditional wired networks or cellular networks, most security protocols are based on asymmetric cryptography such as RSA or Elliptic Curve Cryptography (ECC), which are extremely complicate due to the high computational complexity, high energy

consumption and increased code storage requirements. Therefore, asymmetric-key cryptography is unsuitable for resource-constrained sensor networks. Furthermore, due to the unpredictable network topology and the lack of infrastructure support, trusted-server based key distribution protocols are not suitable for WSNs either. Research shows that key pre-distribution mechanism could be a practical method to solve the key distribution problem in WSNs [3][5]. The basic idea of key pre-distribution scheme is preloading some secret keys into sensor nodes before they are deployed. After the deployment, each sensor exchanges its stored key information with its one-hop neighbors. If two neighboring nodes share some common keys, they can use these keys to encrypt the communication data between them. Several key pre-distribution schemes have been proposed in literatures recently [3][7][8][9][13][14]. Briefly, existing schemes can be classified into three categories: random key pre-distribution schemes, polynomial-key pre-distribution schemes, and location based key pre-distribution schemes.

Random key pre-distribution schemes have no computational overhead, but the communication overhead is proportional to the total number of nodes in the network. There also exists a tradeoff between network connectivity and key storage overhead in this kind of schemes; more keys need to be pre-loaded into each sensor node if the higher network connectivity probability is desired.

Polynomial-key pre-distribution schemes have low communication overhead, but their computational overhead is relatively higher than the previous schemes. The main limitation of this kind of schemes is they can not provide sufficient security to against node capture attack. In other words, polynomial-key schemes only work well when the number of compromised nodes is less than a critical value; once the critical value is exceeded, the entire network could be crashed by the adversary.

Location based key pre-distribution schemes actually have the same procedures as the previous schemes; they just take advantage of the location information to improve the performance. By assuming sensors' expected location can be predicted before they are deployed, each sensor can store fewer keys to reach the same connectivity as the previous schemes. Considering that in most applications

sensor nodes are randomly dropped by a vehicle or airplane, it is impossible to predict each sensor's location before the deployment. Therefore, location based key pre-distribution schemes only can be applied for some specific situations, which narrows their contributions significantly.

To address the limitations of existing schemes, we propose a new distributed pairwise key establishment scheme (DPKE) for large-scale WSNs in this paper. Compared with previous schemes, DPKE can provide the complete connectivity of a network without the prior information of sensor's location; good network resilience also can be achieved in DPKE no matter how many sensors are captured by the adversary. Our performance analysis shows that DPKE has lower communication and storage overheads than previous schemes as well as the larger maximum supported network size.

The remainder of this paper is organized as follows. In the next section, we discuss and analyze some existing key pre-distribution protocols. Section 3 is a detailed description of our proposed distributed pairwise key establishment scheme. In Section 4, the performance evaluation of the proposed scheme and the comparisons with other protocols are presented. Section 5 is the conclusions of our work.

2. Related Work

Several key pre-distribution schemes have been proposed to establish pairwise key between sensors in the literature recently [3][7][8][9][13][14]. Also the basic idea of key pre-distribution scheme is quite simple; designing an applicable protocol is not just a trivial problem. Due to the resources constraints and the non-infrastructure support of WSNs, it is a real challenge to design a key pre-distribution scheme to achieve both communication security and network performance requirements.

The first significant progress was made by Eschenauer et al.; they proposed a random key pre-distribution scheme for WSNs in 2002 [3]. In their scheme, a randomly selected subset of symmetric keys from a large size key pool is assigned into each sensor before they are deployed. After the deployment, each sensor exchanges its stored keys with its neighbors. If two neighbors share a common key, they are secure linked. The shared common key would be used to encrypt the communication between them. In case two neighboring nodes have no common keys, they still can setup a pairwise path-key if they can find a common secure linked intermediate node between them; otherwise, the two nodes are considered as disconnected. According to the random graph theory, if the probability that any two nodes share at least one common key reaches a critical value, the whole network is almost sure to be a connected network.

Based on [3], Chan et al. [7] proposed a "q-composite" scheme to improve the network resilience against the node capture attack. Network resilience here is defined as how much fraction of the communication between non-compromised nodes could be compromised by an

adversary after some sensor nodes are captured or compromised, which is the main metric to evaluate the security property of the key pre-distribution schemes. Chan et al.'s scheme requires two nodes share at least q ($q \geq 2$) common keys to establish a secure link. They showed that as the value of q increases, the network resilience against node capture attack is improved when the total number of compromised nodes is small. In other words, an attacker needs to capture more sensors in [7] to compromise the same fraction of communication between non-captured nodes in [3].

Above two schemes are considered as random key pre-distribution schemes in this paper, as we mentioned in previous section, this kind of schemes have some limitations. First, they can not guarantee the connectivity of the entire network. A node will be isolated from the network if it has no shared key with its neighbors. Although increasing the number of pre-loaded keys in each sensor node could improve the connectivity, it also increases the key storage overhead and degrades the network resilience against node capture attack. Another weakness of these schemes is the communication overhead. In the network initialization phase, each node needs to exchange its key information with its neighbors, which involves lots of communication overhead and collisions. Meanwhile, the path-key establishment procedure is a complicated, energy-consuming operation, which not only lowers the security level of the established key, but also produces additional communication overhead in the network.

Blom proposed a mechanism in [5] to ensure any two members in a group to establish a pairwise key between them. First, a $(\lambda - 1) \times n$ matrix G and a $(\lambda - 1) \times (\lambda - 1)$ symmetric matrix D are constructed, where n is the group size and λ is the expected threshold to compromise the secret collusively. Then each member stores a row vector from matrix A , ($A = G^T D^T$) and a corresponding column vector from matrix G in its memory. According to the property of symmetric matrix, any two members can calculate a unique key between them by multiplying its pre-loaded row vector with its partner's column vector.

Actually, Blom's mechanism is a specific case of λ -degree bivariate polynomial key pre-distribution schemes which is proposed by Blundo et al. in [9]. Polynomial key schemes use a λ -degree bivariate symmetric polynomial $f(x, y)$ to generate a pairwise key between two communicating nodes. Before deployment, each node evaluates $f(x, y)$ at $x = i$, where i is the particular node's id. Suppose nodes a and b want to communicate after the deployment, node a stores $f(a, y)$ and node b stores $f(b, y)$. They exchange their node id first, then node a evaluates $f(a, y)$ at $y = b$, and node b

evaluates $f(b, y)$ at $y = a$. Since $f(x, y)$ is a bivariate symmetric polynomial, it is obviously that $f(a, b) = f(b, a)$. Therefore, nodes a and b can establish a unique pairwise key between them.

As we mention before, polynomial key pre-distribution schemes are secure only when no more than λ members are compromised in the network. Due to the property of λ -degree bivariate polynomial, if more than λ members are compromised, the adversary can derive all the coefficients of the polynomial. To improve the network resilience, Du et al. modified [5] and [9] slightly to make them more suitable for WSNs [14]. By separating a single key space into multiple key spaces, and using the random key pre-distribution procedure to select a space for each sensor node, Du's scheme has better network resilience than previous schemes, but it can not guarantee the connectivity of the entire network.

Based on the previous work, Liu et al. attempted to improve the network performance and resilience by taking advantage of sensors' expected locations information. Several location based pairwise keys establishment schemes have been proposed in [13][15][16]. Although location based schemes have better network resilience and performance than previous schemes, they are not applicable for most of the situations. As we known, usually wireless sensors are randomly dropped in an unattended area by a vehicle or airplane to track a particular object or monitor the entire area. It is impossible to predict each sensor's location before the deployment, therefore, location based key pre-distribution schemes only can be used for some specific applications.

To address the limitations of existing schemes, we propose a distributed pairwise key establishment scheme for large-scale WSNs in this paper. Compared with previous protocols, our scheme can achieve full network connectivity, low communication overhead and key storage overhead, as well as the good network resilience against node capture attack.

3. Our Proposed Distributed Pairwise Key Establishment Scheme (DPKE)

In this section, we present our proposed distributed pairwise key establishment scheme (DPKE) in detail. The sensor network we investigate in this paper is a large-scale, static and homogeneous network. Sensor nodes are tiny, low-cost wireless device without the tamper-resistant hardware support, which means all the information stored in a sensor's memory would be compromised if it is physically captured by an adversary. In addition, each sensor is battery-powered and only has limited radio transmission range, memory storage and data processing capacity. Sensor nodes are uniformly distributed in a two-dimensional area, their location can not be predicted before the deployment. Sink node has unlimited power, memory storage and data processing capacity, its radio

transmission range can cover all the sensors in the network.

In current existing key pre-distribution schemes, two communicating sensors either use one or some of their shared pre-loaded keys directly as their communication key [3][7], or compose a pairwise key by their pre-loaded secret shares [5][9][13][14][15][16]. Although this kind of mechanisms has low computational overhead, they could lead to a serious security threat in practice. If some sensors are captured after the deployment, an adversary may crack some or even all the communication keys in the network by those compromised keys or secret shares. This is called node capture attack in WSNs, which is the main threat that a key pre-distribution scheme needs to deal with.

In our proposed scheme, each pair of sensors can establish a unique pairwise key between them after the network initialization phase. The established pairwise keys are composed of two parts; the first part is the shared common keys pre-loaded in the communicating nodes, the second part is the random numbers generated by the two communicating parties in the network initialization phase. Since the communication pairwise keys in our scheme are distinct for each pair of communicating nodes, and can not be derived directly from the pre-loaded setup keys, an adversary can not crack the pairwise keys among non-captured sensors even some sensors are captured and their stored key information is compromised.

Two kinds of keys are involved in our approach: network setup keys and communication pairwise keys. Similarly as the previous schemes, network setup keys are pre-loaded into sensors before the deployment. Communication pairwise keys are the indeed keys used to encrypt the exchanged data between sensors, they are distinct each other and can not be derived from the network setup keys.

3.1. Procedure of DPKE

In DPKE, communication pairwise keys are established through two phases: setup keys pre-assignment phase and pairwise keys generation phase. We assume there is an off-line authority center called Key Distribution Server (*KDS*) in our network model, which is in charge of the initialization of the sensor nodes. Before deployment, each sensor is assigned a unique node id by *KDS*. *KDS* also generates a large size key pool P composed of more than 2^{20} distinct symmetric keys. For each sensor N_i , *KDS* randomly selects a secret key from P and stores it into N_i 's memory, this pre-loaded key is denoted as pk_{N_i-Sink} .

pk_{N_i-Sink} is the shared pairwise key between node N_i and the Sink node, and will be used to encrypt the exchanged data between node N_i and Sink node.

A. Setup Key Assignment Phase

Before sensor nodes are deployed, setup keys need to be pre-loaded into them in a certain way to ensure any two

nodes can find some common keys after the deployment. This procedure is the setup key assignment phase in our scheme. In this phase, for each sensor node, *KDS* randomly selects some keys from P and pre-loads them into the intended sensor's memory. In our scheme, those pre-loaded keys are called network setup keys. To ensure any two sensors share some pre-loaded setup keys after the deployment, we propose a simple but efficient setup key assignment method for WSNs, which is described as follows.

	kc_1	kc_2	kc_3	kc_4	kc_5	kc_6	..	kc_m
kr_1	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$	$k_{1,4}$	$k_{1,5}$	$k_{1,6}$..	$k_{1,m}$
kr_2	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$	$k_{2,4}$	$k_{2,5}$	$k_{2,6}$..	$k_{2,m}$
kr_3	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$	$k_{3,4}$	$k_{3,5}$	$k_{3,6}$..	$k_{3,m}$
kr_4	$k_{4,1}$	$k_{4,2}$	$k_{4,3}$	$k_{4,4}$	$k_{4,5}$	$k_{4,6}$..	$k_{4,m}$
kr_5	$k_{5,1}$	$k_{5,2}$	$k_{5,3}$	$k_{5,4}$	$k_{5,5}$	$k_{5,6}$..	$k_{5,m}$
kr_6	$k_{6,1}$	$k_{6,2}$	$k_{6,3}$	$k_{6,4}$	$k_{6,5}$	$k_{6,6}$..	$k_{6,m}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	..	⋮
kr_m	$k_{m,1}$	$k_{m,2}$	$k_{m,3}$	$k_{m,4}$	$k_{m,5}$	$k_{m,6}$..	$k_{m,m}$

Fig.1. An example of constructed setup key matrix K

Suppose there are n sensor nodes in our investigating network. First, *KDS* randomly selects n distinct keys from key pool P and uses them to construct a two-dimensional ($m \times m$) matrix K , where $m = \lfloor \sqrt{n} \rfloor$. Fig.1 illustrates an example of the constructed key matrix K . Each entry in matrix K is a symmetric key, and has a unique two-dimensional id denoted by $k_{i,j}$, ($i, j=1, 2, \dots, m$). For convenience, we use kr_i ($i=1, 2, \dots, m$) and kc_j ($j=1, 2, \dots, m$) to represent the i^{th} row and the j^{th} column of the key matrix K respectively.

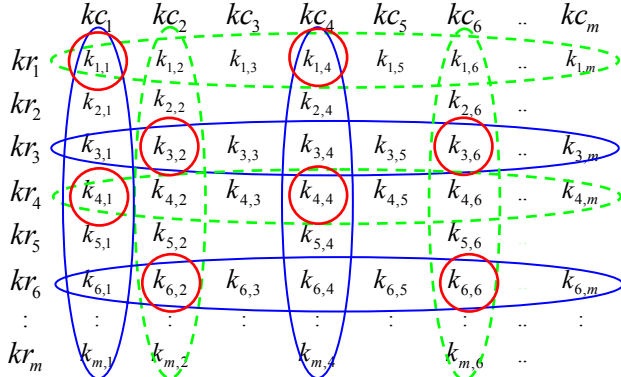


Fig.2. An example of network setup keys assignment

Before the deployment, for each sensor node *KDS* randomly selects t ($1 < t < m$) different rows and t different columns keys from matrix K , and pre-loads the selected keys and their corresponding indices into the intended sensor node's memory. Those pre-loaded keys are called network setup keys for each sensor node. Fig.2 shows the network setup keys pre-loaded in a sensor node when $t=2$. In this case, each sensor stores two rows and two columns keys in its memory. It is easy to see that any two sensors

share at least $2t^2$ common keys in their memories, therefore, our setup key assignment procedure can guarantee the connectivity between any two nodes in the network. Compared with existing key pre-distribution schemes, our approach is the first one to support the full network connectivity without the prior deployment information and no matter how the sensors are deployed, which is the one of the main contributions of our proposed scheme.

B. Pairwise Key Generation Phase

To secure the communication between two neighboring nodes, any sensor needs to generate a pairwise key with each of its one-hop neighbors after the deployment. In our proposed scheme, the pairwise key generation phase has three steps. First, node N_i randomly selects l ($1 \leq l \leq t$) rows and l columns from its stored setup keys; also, N_i generates a random nonce rn_i . Then, node N_i broadcasts a handshaking message including its node id N_i , the random nonce rn_i , and indices of it selected rows and columns to its one-hop neighbors. After two neighboring nodes exchanged the handshaking message, they can generate a pairwise key using their shared setup keys and the random nonce. To explain the procedure clearly, we use an example to illustrate how two communicating nodes generate a pairwise key between them.

Suppose nodes N_a and N_b are two neighboring sensors after the deployment. As shown in Fig.2, N_a has been pre-loaded the 1^{st} and 4^{th} columns, and the 3^{rd} and 6^{th} rows of key matrix K in its memory, N_b has the 2^{nd} and 6^{th} columns, and the 1^{st} and 4^{th} rows of key matrix K pre-loaded in its memory. To establish a pairwise key between them, first N_a generates a random nonce rn_a . Then, N_a broadcasts a handshaking message $\{N_a, kr_3, kr_6, kc_1, kc_4, rn_a\}$ to node N_b . Similarly, sensor node N_b generates a random nonce rn_b , and broadcasts $\{N_b, kr_1, kr_4, kc_2, kc_6, rn_b\}$ to node N_a . After exchanging their handshaking messages, node N_a obtains rn_b as well as its shared setup keys with N_b , $\langle k_{1,1}, k_{1,4}, k_{3,2}, k_{3,6}, k_{4,1}, k_{4,4}, k_{6,2}, k_{6,6} \rangle$, which are the intersections of the corresponding key rows and columns. Node N_b also can get rn_a and the shared setup keys with N_a at the same time. Now, nodes N_a and N_b can calculate a pairwise key between them by Equation (1):

$$pk_{N_a-N_b} = rn_a \oplus sk_{(N_a, N_b)} \oplus rn_b \quad (1)$$

In Equation (1), " \oplus " is the exclusive-or operator, $pk_{N_a-N_b}$ denotes the pairwise key between nodes N_a and N_b , rn_a and rn_b are two random nonce generated by N_a and N_b respectively, $sk_{(N_a, N_b)}$ are the shared common setup keys between N_a and N_b , they are $\langle k_{1,1}, k_{1,4}, k_{3,2}, k_{3,6}, k_{4,1}, k_{4,4}, k_{6,2}, k_{6,6} \rangle$ in this instance.

In our proposed DPKE scheme each sensor node stores t rows and t columns keys from the constructed matrix K . Since each pair of row and column has an intersection entry between them, any two sensors can find $2t^2$ common

keys after they exchanged the handshaking messages, which means, any two sensors within their radio transmission range can directly setup a secure link without the third node's participation. In other words, the path-key establishment phase of existing key pre-distribution schemes is eliminated in our approach, which not only reduces the communication overhead, but also increases the security level of the generated pairwise keys. On the other hand, since each generated pairwise key is distinct to others, DPKE improves the network resilience against node capture attack.

4. Security Analysis and Performance Evaluation

We analysis the security property and evaluate the performance of our proposed DPKE scheme in this section.

4.1. Security Analysis

A. Resistance Against Node Replication Attack

As we known, WSNs are commonly deployed in a hostile environment and operated on the unattended mode. Therefore, some sensors could be physically captured by an adversary during the operating period. Node replication attack is a serious threat for WSNs due to its non-infrastructure support architecture. In existing key pre-distribution schemes, especially in [3][7], the pairwise communication keys are directly selected from the pre-loaded keys. After the network initialization phase, if a sensor is captured and all its stored keys are compromised, the adversary may duplicates some malicious nodes and deploy them into the network to execute some attacks such as eavesdropping, Denial-of-Service (DoS), etc. In our proposed DPKE scheme, any pair of sensors has a unique pairwise key between them after network initialization phase, which can be used to authenticate the communicating parties mutually. Without the proper authentication, any stranger's packets will be just ignored. Consequently node replication attack can be totally prevented by our proposed scheme.

B. Resiliency Against Node Capture Attack

In WSNs environment, an adversary not only can get the critical data by eavesdropping or intercepting the radio mediums, but also can physically capture some sensors to compromise the secret information, such as communication keys, critical data and other valuable information. Node capture attack is the most serious threat in WSNs. In random key pre-distribution schemes, different pair of sensors may have the same pairwise keys during the network operating period. Since each sensor stores a subset of keys from a same key pool, if an adversary captured a certain number of sensors, a large portion of the key pool may be compromised by the adversary. In this case, the communication between non-

captured nodes could be cracked even they are not physically captured.

In [3], if each sensor stores 200 keys in its memory and the probability that any two nodes share at least one common key is 0.33, 50 nodes' capture could compromise 10% of the communication among the non-captured nodes. Although [7] claims it can improve the network resilience by requiring two nodes share at least q ($q > 1$) common keys to establish a secure link, it only works when the number of captured nodes is less than a critical value. As shown in Fig.3, when the number of captured nodes exceeds the critical value, the fraction of compromised communication among non-captured nodes increases even much faster than [3].

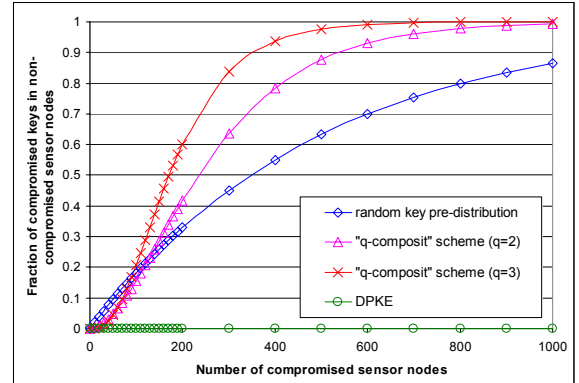


Fig.3. Fraction of compromised keys among non-captured nodes vs. number of captured nodes.

In DPKE, after the pairwise key generation phase, each pair of neighboring nodes have a unique pairwise key between them, hence any node's capture can not affect the secure communication between non-captured nodes. In other words, our approach can guarantee the communication security among non-captured nodes no matter how many sensors are captured by the adversary, which is one of the main contributions of our work. Fig.3 shows that above 30% of the communication between non-captured nodes are compromised in [3][7] when 200 nodes are captured; if the number of captured nodes increases to 500, more than 60% of the communication of the rest network will be compromised. Oppositely, no communication between non-captured nodes could be compromised in DPKE no matter how many sensors are captured by the adversary.

4.2. Performance Evaluation

A. Maximum Supported Network Size

Compared with random key pre-distribution schemes, DPKE can achieve the larger maximum supported network size. According to the description in Section 3, if each sensor stores $2tm$ setup keys in its memory, the maximum supported network size of DPKE is $(m!)^2 / (t!(m-t)!)^2$, where $(1 \leq t \leq m/2)$. It is much larger than the network size supported by the random key pre-distribution schemes.

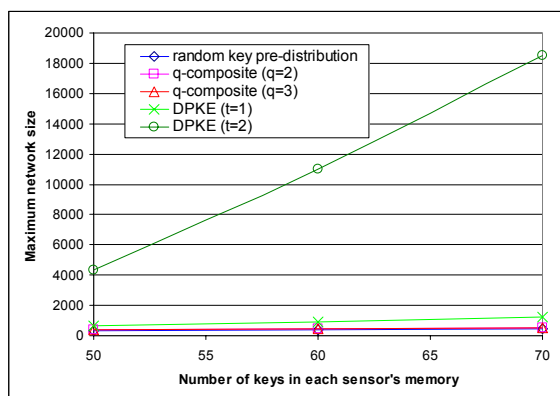


Fig.4. Maximum supported network size vs. number of keys in sensor's memory.

Fig.4 shows the difference between DPKE and random key schemes. For convenience, we use the same evaluation metrics in [7], where the probability of any two nodes can establish a secure link is 0.33, and the maximum compromise threshold is 0.1. It is easy to see that for random key schemes, the network size is linearly increased when the key ring size increases. In DPKE, the maximum supported network size is exponentially increased when the key ring size increases linearly, which means our proposed scheme has better scalability than random key pre-distribution schemes.

B. Network Connectivity

To monitor an area properly, connectivity of a sensor network should be guaranteed no matter how the sensors are deployed. Random key pre-distribution schemes can not guarantee any two sensors establish a pairwise key directly. To increase the network connectivity, intermediate nodes need to be involved in a path-key establishment procedure. Even that, based on the probability theory, some sensors or some portions of a network is still possibly isolated from the network if no path-keys can be established.

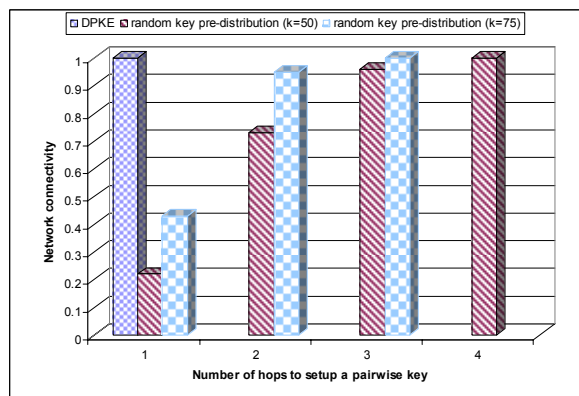


Fig.5. Network connectivity vs. number of hops to setup a pairwise key.

DPKE can guarantee a completed network connectivity since any two sensors can find common setup keys between them, which is the second contribution of our work. Fig.5 shows that DPKE can generate a connected

network with only one-hop neighbors' information exchanging. For random key pre-distribution schemes, two or three more hops neighbors need to be involved to setup an almost connected network, which not only reduce the security of the established pairwise key, but also produce more communication overhead in the network.

C. Communication Overhead

In random key pre-distribution schemes, to find the shared keys with its neighbors, each sensor exchanges all of its stored key information with its neighbors. For a large-scale network, each sensor stores many keys in its memory, this energy-consuming procedure produces additional traffic overload and collisions. In DPKE, only a random nonce and the indices of the corresponding key rows and key columns need to be broadcasted for each sensor, which extremely reduces the energy consumption and communication overhead in a network.

Furthermore, in random key pre-distribution schemes, if two neighbors can not setup a pairwise key directly, a complicated and time-consuming path-key establishment procedure is triggered, additional communication and memory storage overheads are produced in this procedure. DPKE guarantees any two nodes to establish a pairwise key directly; therefore, its communication overhead is much lower than the previous schemes.

5. Conclusion

In this paper, we proposed a distributed pairwise key establishment scheme (DPKE) for large-scale WSNs. Compared with the existing random key pre-distribution schemes, our proposed scheme has better resilience against node capture and replication attacks. Better network performance also can be achieved by DPKE in terms of network connectivity, communication overhead, key storage overhead and maximum supported network size.

Acknowledgement

This work has been supported by the Ohio Board of Regents Doctoral Enhancement Funds.

References

- [1] D. P. Agrawal and Q-A Zeng, "Introduction to Wireless and Mobile Systems," Brooks/Cole Publishing, Aug. 2003.
- [2] Neha Jain and Dharma P. Agrawal, "Current trends in wireless sensor network design," International Journal of Distributed Sensor Networks, Vol.1, issue 1, pp.101-122, 2005.
- [3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In *Proceedings of the 9th ACM conference on Computer and communications security*, November 2002.
- [4] David W. Carman, Peter S. Kruus, and Brian J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs Technical Report #00-010, September 2000.

- [5] R. Blom, "An optimal class of symmetric key generation systems," *Advances in Cryptology: Proceedings of EUROCRYPT 84* (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), Lecture Notes in Computer Science, Springer-Verlag, 209:335–338, 1985.
- [6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," In *Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001)*, July 2001.
- [7] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," In *IEEE Symposium on Security and Privacy*, pp. 197–213, Berkeley, California, May 11-14 2003.
- [8] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," In *ACM CCS 2003*, pp. 62–72, October 2003.
- [9] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," *Lecture Notes in Computer Science*, 740:471–486, 1993.
- [10] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pp. 483–492, 1999.
- [11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," In *First IEEE Int'l Workshop on Sensor Network Protocols and Applications*, May 2003.
- [12] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communication Magazine*, vol. 40, no. 8, pp. 102–116, Aug. 2002.
- [13] D. Liu and P. Ning, "Location-Based Pairwise Key Establishments for Relatively Static Sensor Networks," in *2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)*, October 31, 2003 George W. Johnson Center at George Mason University, Fairfax, VA, USA.
- [14] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, Washington DC, USA, October 27-31 2003, pp. 42–51.
- [15] D. Liu, P. Ning, W. Du, "Group-Based Key Pre-Distribution in Wireless Sensor Networks," in *Proceedings of 2005 ACM Workshop on Wireless Security (WiSe 2005)*, September 2005.
- [16] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks", in *ACM Transactions on Information and System Security (TISSEC)*, 2004.