INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 5 AUG 2015

A PRIVACY SECURE KEY PRE-DISTRIBUTION SCHEME FOR WIRELESS SENSOR NETWORKS

[1] **CHAGANTI.B.N.LAKSHMI, ASSO.PROFESSOR M.TECH[PH.D],**

[2] **T.ASHWINI,** PG Scholar in S E (CSE),

[1] ch.nagalakshmi08@gmai l.com, [2] thi.ashwini1991@gmail.com

[1,2] Mahaveer Institute of science & Technology, Hyderabad, R.R Dist, Telangana –India

***Abstract*—**To achieve security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent among sensor nodes. Keys for encryption and authentication purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is non-trivial. Many key agreement schemes used in general networks, such as Daffier-Hellman and public-key based schemes, are not suit-able for wireless sensor networks. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. To solve the key pre-distribution problem, two elegant key pre-distribution approaches have been proposed recently [11, 7].In this , i propose a new key pre-distribution scheme which substantially improves the resilience of the network com-pared to the existing schemes. Our scheme exhibits a nice thresh-old property: when the number of compromised nodes is less than the threshold, the probability that any nodes other than these com- promised nodes is affected is close to zero. This desirable property lowers the initial payoff of smaller scale network breaches to an adversary, and makes it necessary for the adversary to attack a sig-nificant proportion of the network. I also present an in depth analysis of our scheme in terms of network resilience and associated overhead.

I. Introduction

Recent advances in electronic and computer technologies have paved the way for the proliferation of wireless sensor networks (WSN). Sensor networks usually consist of a large number of ultra- small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communications. In typical application scenarios, sensor nodes are spread randomly over the terrain under scrutiny and collect sensor data. Examples of sensor network papers include Smart Dust [12] and WINS [1].Sensor networks are being deployed for a wide variety of applications [2], including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important, as they are prone to different types of malicious attacks. For example, an adversary can easily listen to the traffic, impersonate one of the network nodes, or intentionally provide misleading information to other nodes. To provide security, communication should be encrypted and authenticated. The open problem is how to bootstrap secure communications between sensor nodes, i.e. how to set up secret keys between communicating nodes? This problem is known as the key agreement problem, which has been widely studied in general network environments. There are three types of general key agreement schemes: trusted-serve scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes, e.g., Kerberos [15]. This type of scheme is not suitable for sensor networks because there is no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. However, limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Daffier Hellman key agreement [8] or RSA [18], as pointed out in [16]. The third type of key agreement scheme is key pre-distribution, where key information is distributed among all sensor nodes prior to deployment. If we know which nodes will be in the same neighborhood before deployment, keys can be decided a priori? However, most sensor network deployments are random; thus, such a priori knowledge does not exist. There exist a number of key pre-distribution schemes which do not rely on a priori deployment knowledge. A naive solution is to let all the nodes carry a master secret key. Any pair of nodes can use this global master secret key to achieve key agreement and obtain a new pair wise key. This scheme does not exhibit desirable network resilience: if one node is compromised, the security of the entire sensor network will be compromised. Some existing studies suggest storing the master key in tamper-resistant hardware to reduce the risk, but this increases the cost and energy consumption of each sensor. Furthermore, tamper-resistant hardware might not always be safe [3]. Another key pre-distribution scheme is to let

each sensor carry $N - 1$ secret pair wise keys, each of which is known only to this sensor and one of the other $N - 1$ sensors (assuming N is the total number of sensors). The resilience of this scheme is perfect because a compromised node does not affect the security of other nodes; however, this scheme is impractical for sensors with an extremely limited amount of memory because N could be large. Moreover, adding new nodes to a pre-existing sensor network is difficult because the existing nodes do not have the new nodes' keys. Very recently Schnauzer and Gligor proposed a random key pre-distribution scheme: before deployment, each sensor node receives a random subset of keys from a large key pool; to agree on a key for communication, two nodes find one common key within their subsets and use that key as their shared secret key [11]. Based on this scheme, Chan, Perrig, and Song proposed a q –composite random key pre-distribution scheme, which increases the security of key setup such that an attacker has to compromise many more nodes to achieve a high probability of compromising communication [7]? The difference between the q -composite scheme and the scheme in [11] is that q common keys ($q \geq 1$), instead of just a single one, are needed to establish secure communication between a pair of nodes. It is shown that by increasing the value of q network resilience against node capture is improved [7]

1.1 Main Contributions of Our Scheme

In this paper, i propose a new key pre-distribution scheme. The main contributions of this paper are as follows:

1. Substantially improved network resilience against node capture over existing schemes.
2. Pair wise keys that enable authentication.
3. Thorough theoretical analysis of security, and communication and computation overhead analysis.

Our scheme builds on Blom's key pre-distribution scheme [4] and combines the random key pre-distribution method with it. Our results show that the resilience of our scheme is substantially better than Blom's scheme as well as other random key pre-distribution schemes. In [4], Blom proposed a key pre-distribution scheme that allows Any pair of nodes to find a secret pairwise key between them.Compared to the $(N-1)$-pairwise-key pre-distribution scheme,Blom's scheme only uses $\lambda + 1$ memory spaces with λ much smaller than N . The tradeoff is that, unlike the $(N-1)$-pairwise-key scheme, Blom's scheme is not perfectly resilient against node capture. Instead it has the following λ secure property: as long as an adversary compromises less than or equal to λ nodes, uncompress-missed nodes are perfectly secure; when an adversary compromises more than λ nodes, all pairwise keys of the entire network are compromised. The threshold λ can be treated as a security parameter in that selection of a larger Λ leads to a more secure network. This threshold property of Blom's scheme is a desirable feature because an adversary needs to attack a significant fraction of the network in order to achieve high payoff. However, λ also determines the amount of memory to store key information, as increasing λ leads to higher memory usage.

The goal of our scheme is to increase network's resilience against node capture without using more memory. Blom's scheme uses one key space for all nodes to make sure that any pair can compute its pairwise key in this key space. Motivated by the random key pre-distribution schemes presented in [11, 7], i propose a new scheme using multiple key spaces: i first construct spaces using Blom's scheme, and each sensor node carries key information from τ ($2 \leq \tau < \omega$) randomly selected key spaces.According to Blom's scheme, if two nodes carry key information from a common space, they can compute their pairwise key from the information; when two nodes do not carry key information from a common space, they can conduct key agreement via other nodes which share pairwise keys with them. Our analysis has shown that using the same amount of memory, our new scheme is substantially more resilient than Blom's scheme and other key pre-distribution schemes.To further improve the resilience, i also develop a two-hop-neighbor key pre-distribution scheme. The idea is to let the direct neighbor forward the message from a sender, such that nodes that are two hops away from the sender can also receive the message. The nodes that are two hops away are known as two-hop neighbors.Treating two-hop neighbors as "direct" neighbors, the number of neighbors of each sender increases fourfold. The consequence is that the resilience threshold can be improved as well. Our results show that under certain conditions, the threshold can be improved to four times as much as that of our first scheme. The rest of the paper is organized as follows. Section 2 describes how our building block, the original Blom's method, works. Then i describe our key pre-distribution scheme in Section 3. Section 4 shows the resilience of our scheme against node capture. It also compares our scheme with existing key pre-distribution schemes. Section 5 presents the communication and computation overheads of our scheme. Section 6 describes our two-hop-neighbor key predistribution scheme. Finally, i provide some concluding remarks in Section 7.

1.2 Other Related Work

The Eschenauer-Gligor scheme [11] and the Chan-Perrig-Song scheme [7] have been reviewed earlier in this section. Detailed comparisons with these two schemes will be given in Section 4.Some other related work is discussed next. Du et al. proposed a method to improve the Eschenauer-Gligor scheme using a priori deployment knowledge [9]. This method canalso be used to further improve other random key pre-distribution schemes, such as the Chan-Perrig-Song scheme and the scheme presented in this paper. Blundo et al. proposed several schemes which allow any group of t parties to compute a common key while being secure against collusion between some of them [5]. These schemes focus on saving communication costs while memory constraints are not placedon group members. When t = 2 , one of these schemes is actually a special case of Blom's scheme [4]. A modified version of Blom's scheme will be reviewed in Section 2. Compared to Blom'sscheme, our scheme is more resilient and more memory-efficient.Perrig et al. proposed SPINS, a security architecture specifically designed for sensor networks [16]. In SPINS, each sensor node shares a secret key with the

base station. Two sensor nodes cannot directly establish a secret key. However, they can use the base station as a trusted third party to set up the secret key.

2. BACKGROUND: BLOM'S KEY

PRE-DISTRIBUTION SCHEME
Blom proposed a key pre-distribution method that allows any pair of nodes in a network to be able to find a pairwise secret key [4]. As long as no more than λ nodes are compromised, the network is perfectly secure (this is called the λ -secure property). I briefly describe how Blom's λ -secure key pre-distribution system works. Blom's scheme is not developed for sensor networks, so in the following description, i have made some slight modifications to the original scheme to make it suitable for sensor networks. During the pre-deployment phase, the base station first constructs a (λ+ 1) × N matrix G over a finite field GF (q) , where N is the size of the network. G is considered as public information; any sensor can know the contents of G , and even adversaries are allowed to know G . Then the base station creates a random (λ+1) × (λ+1) symmetric matrix D over GF (q), and computes an N × (λ+ 1) matrix A = (D G) T , where (D G) T is the transpose of D G Matrix D needs to be kept secret, and should not be disclosed to adversaries or any sensor node (although, as will be discussed later, one row of (D G) T will be disclosed to each sensor node). Because D is symmetric, it is easy to see: A G = (D G)T G=G T D T G = G T D G = (A G) T This means that A G is a symmetric matrix. If i let K = A G we know that K ij = K ji , where K ij is the element in K located in the I th row and j th column. I use K ij (or K ji) as the pairwise key between node I and node j . Fig. 1 illustrates how the pairwise key K ij = K ji is generated. To carry out the above computation, nodes I and j should be able to compute K ij and K ji , respectively. This can be easily achieved using the following key pre-distribution scheme, for k = 1 , .N
1. store the k th row of matrix A at node k , and
2. store the k th column of matrix G at node k 1 Therefore, when nodes I and j need to find the pairwise key between them, they first exchange their columns of G , and then they 1 I will show later that each sensor does not need to store the whole column, because each column can be generated from a seed can compute K ij and K ji , respectively, using their private rows of A . Because G is public information, its columns can be transmit- ted in plaintext. It has been proved in [4] that the above scheme is λ -secure if any λ + 1 columns of G are linearly independent. This λ -secure property guarantees that no nodes other than I and j can compute K ij or K ji if no more than λ nodes are compromised.

II. BACKGROUND: BLOM'S KEY PRE-DISTRIBUTION SCHEME

Blom proposed a key pre-distribution method that allows any pair of nodes in a network to be able to find a pairwise secret key [4]. As long as no more than λ nodes are compromised, the network is perfectly secure (this is called the λ -secure property). I briefly describe how Blom's Λ -secure key pre-distribution system works. Blom's scheme is not developed for sensor networks, so in the following description, i have made some slight modifications to the original scheme to make it suitable for sensor networks. During the pre-deployment phase, the base station first constructs a (λ+ 1) × N matrix G over a finite field GF (q) , where N is the size of the network. G is considered as public information; any sensor can know the contents of G , and even adversaries are allowed to know G . Then the base station creates a random (λ+1) × (λ +1) symmetric matrix D over GF (q) , and computes an N × (λ+ 1) matrix A = (D G) T , where (D G) T is the transpose of D G .Matrix D needs to be kept secret, and should not be disclosed to ad versaries or any sensor node (although, as will be discussed later, one row of (D G) T will be disclosed to each sensor node).

A. Probabilistic schemes

In probabilistic key management schemes, each two neighboring nodes can establish a secure link with some probability If two neighboring nodes cannot establish a secure link, they establish a secure path composed of successive secure links. Eschenauer and Gligor proposed in [2] the basic Random Key Pre-distribution scheme denoted by RKP. In this scheme, each node is pre-loaded with a key ring of *k* keys randomly selected from a large pool *S* of keys. After the deployment step, each node *i* exchanges with each of its neighbor *j* the list of key identifiers that it maintains. This allows node *j* to identify the keys that it shares with node *i*. If two neighbors share at least one key, they establish a secure link and compute their session secret key which is one of the common keys. Otherwise, they should determine a secure path which is composed by successive secure links. The values of the key ring size *k* and the key pool size $|S|$ are chosen in such a way that the intersection of two key rings is not empty with a high probability. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring.
Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised. Chan *et al.* proposed in [3] a protocol called Q-composite scheme that enhances the resilience of RKP. In this solution,twoneighboring nodes can establish a secure link only if they share at least *Q* keys. The pairwise session key is calculatedas the hash of all shared keys concatenated to each other:
$K_{i,j} = Hash(K_{s1} \_ K_{s2} \_ \ldots \_ K_{sq})$ where $K_{s1}, K_{s2}, \ldots K_{sq}$ are the $q\_$ shared keys between the two nodes *i* and *j* ($q\_ \geq Q$).This approach enhances the resilience against node captureattacks because the attacker needs more overlap keys to breaka secure link.

However, this approach degrades the networksecure connectivity coverage because neighboring nodes musthave at least Q common keys to establish a secure linkChan*et al.* proposed also in [3] a perfect secure pairwisekey pre-distribution scheme where they assign to each possiblelink between two nodes i and j a distinct key $K_{i,j}$. Prior todeployment, each node is pre-loaded with $P_c \times n$ keys, where$n$ is the network size and P_c is the desired secure coverageprobability. Since we use distinct keys to secure each pairwiselink, the resiliency against node capture is perfect and eachcaptured node does not reveal any information about externallinks. The main drawback of this scheme is the non scalabilitybecause the number of the stored keys depends linearly on thenetwork sizeDu *et al.* proposed in [4] an enhanced random scheme assumingthe node deployment knowledge. Nodes are organizedin regional groups to which are assigned different key pools,each node selects its keys from the corresponding key poolThe key pools are constructed in such a way that neighboringones share more keys than distant pools. This approach allowsto enhance the probability of sharing common keys as wellas the resilience against node capture attacks. However, theapplication of this scheme is restrictive if the deploymentknowledge is not possibleIn [6], Liu and Ning proposed a key management scheme inwhich nodes are pre-loaded with bivariate polynomials insteadof keys. A global pool of symmetric bivariate polynomials($f(x, y) = f(y, x)$) is generated off-line and each node I is pre-loaded with a subset of polynomials $f(i, y)$. If twoneighboring nodes share a common polynomial, the sessionkey is derived by computing the polynomial value at theneighbor identifier. This approach allows to compute distinctsecret keys which enhances the resilience against node capture.However, it requires more memory to store the polynomialsand induces more computational overhead.In [16], Blom proposed a λ-secure symmetric key generationsystem in which each node i stores a column i and a row i of size $(\lambda + 1)$ of two matrices G and $(DG)^T$respectively where : $D_{(\lambda+1)\times(\lambda+1)}$ is a symmetric matrix,$G_{(\lambda+1)\times n}$ is a public matrix and $(DG)^T$ is a secret matrix.The matrix of pairwise keys of a group of n nodes is then $K = (DG)^T G$. Yu and Guan [7] used the Blom's scheme for key pre-distribution in group-based WSNs. Nodes are deployed into a grid and to each group is assigned a distinct secret matrix. Using deployment knowledge, the potential number of neighboring nodes decreases which requires less memory. The application of this solution gives good results in the case of node deployment knowledge which is not always possible In [8], Ruj*et al.* propose a trade-based key management scheme denoted Trade-KP. Given a finite set X of v elements, an *Steiner trade* $t - (v, k)$ is defined to be two *disjoint* sets T_1 and T_2 of k-elements blocks of X such that each set of t elements from X occurs in precisely the same number of blocks of T_1 as those of T_2, and no set of t elements from X is repeated more than once in any of T_1 or T_2. An Steiner trade is said to be strong if any two blocks of T_1 and T_2 respectively intersects in at most two elements. Ruj*et al.* proposed a new trade construction: Having q a prime power and k $(4 \leq k < q)$, they construct T_1 and T_2 while the blocks of T_1 are represented by $t_{1i,j} = \{(x, (xi + j) \bmod q) : 0 \leq x < k\}$ where $0 \leq i, j < q$, and the blocks of T_2 are represented by $t_{2\,i,j} = \_(x, (x_2 + xi + j) \bmod q) : 0 \leq x < k \_$, where $0 \leq i, j < q$. Ruj*et al.* proved that the proposed construction results in a $2 - (qk, k)$ strong Steiner trade. They proposed then a mapping to key pre-distribution where they associate to each element a distinct key and to each block of T_1 and T_2 a key ring. The key ring size is then equal to k and the scalability of the scheme is equal to $2q_2$ After the deployment step, each two nodes can establish a direct secure link if they share exactly two common keys which are used to compute the pairwise session key. Based on the trade properties, authors prove that each pair of keysoccurs either in exactly two nodes from T_1 and T_2 respectively or none of the nodes.The main strength of the proposed scheme is the establishmentof unique secret pairwise keys between connected nodes.However, this does not ensure a perfect network resilience as we prove later. Indeed, the attacker may construct a part of the global set of keys and then compute pairwise secret keys used to secure external links where the compromised nodes are not involved. Moreover, the proposed scheme provides a low session key sharing probability which does not exceed 0.25 as we show later. *B. Deterministic schemes* Deterministic schemes ensure that each node is able to establish a pair-wise key with all its neighbors. Many solutions were proposed to guarantee determinism.A naive deterministic key pre-distribution scheme can be designed by assigning to each link (i,j) a distinct key $K_{i,j}$and pre-loading each node with $(n - 1)$ pairwise keys in which itis involved where n is the network size. It is obvious that this solution is not scalable for large WSNs. Choi *et al.* proposed in [17] an enhanced approach allowing to store only $(n+1)/2$ keys at each node. For that purpose, they propose to establish an order relation between node identifiers and propose a hash function based key establishment in order to store only half of the node symmetric keys while computing the other half at each node. This approach allows to reduce the required stored keys to the half of network size, however, it is obvious that this scheme remains non scalable enough.LEAP [9] make use of a common transitory key which is preloaded into all nodes prior to deployment of the WSN. The transitory key is used to generate pairwise session keys and is cleared from the memory of nodes by the end of a short time interval after their deployment.

LEAP is based on the assumption that a sensor node, after its deployment, is secure during a time $T_{min}$and cannot be compromised during this period of time. LEAP is then secure as far as this assumption is verified.In [10], C¸ amtepe and Yener proposed to use combinatorial design for key pre-distribution in WSN. They proposed a new deterministic key pre-distribution scheme based on Symmetric Balanced Incomplete Block Design (SBIBD). The proposed mapping from SBIBD to key pre-distribution allows to construct $m^2 + m + 1$ key rings from a key pool S of $m^2 + m + 1$ keys such that each key ring contains $k = m+1$ keys and each two key rings shares exactly one common key. The main strength of the C¸ amtepe scheme is the total

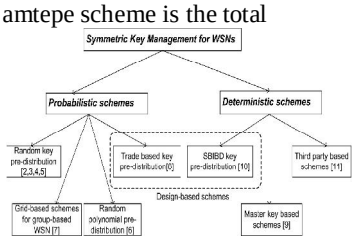

Fig. 1. Classification of symmetric key management schemes for WSNs

secure connectivity, indeed each two nodes share exactly one common key. However, the SBIBD scheme does not scale to very large networks. Indeed, using key rings of $m+1$ keys we can generate only $m^2 + m + 1$ key rings. SBIBD based key pre-distribution was also used in [18] to guarantee intra-region secure communications in grid group WSNs.

In this work, i seek to design a scalable key managementscheme which ensures a good secure coverage of large scalenetworks with a low key storage overhead. Basic schemesgiving a perfect network resilience [3] [17] achieve a networkscalability of $O(k)$ where k is the key ring size. The SBIBD[10] and the trade [8] based ones allow to achieve a networkscalability of $O(k^2)$. In this work, i propose new solutionsachieving a network scalability up to $O(k^4)$ when providinghigh secure connectivity coverage and good overall performances.For this purpose, i make use of the unital designtheory in order to pre-distribute keys. I propose in whatfollows a basic mapping from unitals to key pre-distributionas well as an enhanced unital based scheme which achieves agood trade-off between scalability and connectivity.

III. Unital Design for Key Pre-Distribution inWSNs

WSNs are highly resource constrained. In particular, theysuffer from reduced storage capacity. Therefore, it is essentialto design smart techniques to build blocks of keys that willbe embedded on the nodes to secure the network links.Nonetheless, in most existing solutions, the design of key rings(blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability, or degrade otherperformance metrics including secure connectivity and storageoverhead. This motivates the use of unital design theory thatallows a smart building of blocks with unique features thatallow to cope with the scalability and connectivity issues.

In what follows, i start by providing the definition andthe features of unital design theory. I explain then thebasic mapping from unital to key pre-distribution and evaluateits performance metrics. I propose finally an enhancedunital-based scheme which achieves a good trade-off between scalability and connectivity.

A. Background: Unital Design

In combinatorics, the design theory deals with the existenceand construction of systems of finite sets whose intersectionshave specified numerical properties. Formally, A t-design$(v,b,r,k,\lambda)$is defined as follows : Given a finite set$X$of$v$points (elements), i construct a family of$b$subsets of$X$, called blocks, such that each block has a size$k$, each$t$point is contained in$r$blocks and each$t$points are containedtogether in exactlyλblocks.

IV. A NewScalableUnital-BasedKeyPre-DistributionScheme forWSNs

In this section, i present a new unital-based key pre-distribution scheme for WSNs. In order to enhance the keysharing probability while maintaining high network scalability, i propose to build the unital design blocks and pre-load eachnode with a number of blocks picked in a selective way

.

A. Key Pre-distribution

Before the deployment step, i generate blocks ofmorderunital design, where each block corresponds to a key set. I pre-load then each node with completely disjointblockswheretis a protocol parameter thatwe will discuss later in thissection. In lemma 1, demonstrate the condition of existenceof suchcompletely disjoint blocks among the unitalblocks.In the basic approach each node is pre-loaded with only oneunital block and i proved that each two nodes share at mostone key. Contrary to this, pre-loading each two nodes withdisjoint unital blocks means that each two nodes share betweenzero andkeys since each two unitals blocks share at mostone element.

After the deployment step, each two neighbors exchangethe identifiers of their keys in order to determine the commonkeys. If two neighboring nodes share one or more keys,we propose to compute the pairwise secret key as the hashof all their common keys concatenated to each other. Theused hash function may beSHA-1[22] for instance. Thisapproach enhances the network resiliency since

the attackerhave to compromise more overlap keys to break a secure link.Otherwise, when neighbors do not share any key, they shouldfind a secure path composed of successive secure links.The major advantage of this approach is the improvementof the key sharing probability. As i will prove in nextsubsection, this approach allows to achieve a high secureconnectivity coverage since each node is pre-loaded withdisjoint blocks. Moreover, this approach gives good networkresiliencythrough the composite pairwise secret keys whichreinforces secure links. In addition, i show that our solutionmaintains a high network scalability compared to existing

V. PERFORMANCE COMPARISON

In this section, i compare the proposed unital-basedschemes to existing schemes regarding different criteria (irecall that metric definitions are given in table I).A. Network scalability at equal key ring size I compare in Figure 3 the scalability of the proposedunital based schemes against that of the SBIBD-KP and theTrade-KP ones. The network scalability of the t-UKP schemesis computed as the averagevalue between the maximumand the minimum scalability.

VI. CONCLUSION

I have presented a new pairwise key pre-distribution scheme for wireless sensor networks. Our scheme has a number of appealing properties. First, our scheme is scalable and flexible. For a network that uses 64-bit secret keys, our scheme allows up to N = 2 64 sensor nodes. These nodes do not need to be deployed at the same time; they can be added later, and still be able to establish secret keys with existing nodes. Second, compared to existing key pre-distribution schemes, our scheme is substantially more resilient against node capture. Our analysis and simulation results have shown, for example, that to compromise 10% of the secure links in the network secured using our scheme, an adversary has to compromise 5 times as many nodes as he/she has to compromise in a network secured by Chan-Perrig-Song scheme or Eschenauer Gligor scheme. Furthermore, i have also shown that network resilience can be further improved if i use multi-hop neighbors I have conducted a thorough overhead analysis to show the efficiency of our scheme. The communication overhead analysis has shown that when p actual $\geq$ 0 .33 , a node can almost (with very high probability) reach its neighbor within at most 3 hops. For the computation overhead, although our scheme involves modular multiplications, i have shown that the energy cost is about the same as encrypting a message of length 3200 bits using AES

.

REFERENCES

[1] Wireless Integrated Network Sensors, University of California, Available: http://www.janet.ucla.edu/WINS

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine , 40(8):102–114, August 2002

[3] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In Proceedings of the Second Usenix Workshop on Electronic Commerce , pages 1–11, November 1996.

[4] 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

[5] 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

[6] D. W. Carman, P. S. Kruus, and B. J. Matt. Constraints and approaches for distributed sensor network security. NAI Labs Technical Report #00-010, available at http://download.nai.com/products/media/nai/zip/nailabs report-00-010-final.zip

[7] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy , pages 197–213, Berkeley, California, May 11-14 2003.

[8] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory , 22:644–654, November 1976