An Energy Aware Key Pre-Distribution Scheme for Wireless Sensor Networks

Jeenyta Desai
M.E Student
Department of Computer Science & Engineering
HTC, Vehla, Ahmedabad

Abstract— Taking the considerations of WSNs application, there is a need of a highly scalable key pre distribution scheme for WSNs. Along with this there needs to be considerations of the limitation of the resources used in WSNs and the key management challenges also. Network scalability, resiliency are the main concerns when designing a key management scheme. Network scalability means, the network should support very large numbers of nodes so that the large network can be deployed. Good secure connectivity and the large network scalability can be implemented using the Unital design theory. Unital is the complete new approach for the WSNs for key management. The basic Unital mappings for the key pre distribution can be used. Along with network scalability there should be good key sharing probability also. Conduction of approximate analysis and simulation and comparison to the existing system can be shown. Also the limitation of storage overhead, Network scalability, Resiliency, network connections are to be considered. Proposed methodology show that the network scalability is enhanced while providing high secure connectivity and other performances also at the same network size. The proposed work reduces the storage overheads also.

Key words: WSNs, Network Resiliency, Network Scalability, Secure Connectivity

I. INTRODUCTION

WSNs having there weakness is in the low power and tiny sensor nodes, it becomes a difficult task to handle network scalability along with low storage capacity. Also with increasing application of the WSNs in area, Environmental, Air, Pollution, Waste monitoring, Forest fire detections, water quality, civilian to military applications. Hiked applications of WSNs lead to cravings of utilization of WSNs walking with the harsh constraints. Main characteristics are its power consumption constraints for nodes using batteries, mobility of nodes, communication failures to scalability of networks and resiliency factors. And the above constraints are to be maintained in order to get a feasible and satisfaction filling efficient WSNs. Upon this security is the basic requirement of the application so key pre distribution is one of the biggest issues. Because of the lack of infrastructure and no trusted third party the attribute of pair wise secret keys to the neighboring nodes are used. Also the pre key distribution has most solutions to the secret key distribution among the neighborly nodes. In key pre distributions the design of key rings is strongly related to network size, but the main problem is that this solution also suffers from low scalability, Connectivity, storage overheads and network resiliency in the large scale network.

Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, WSNs have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Attackers may device different types of security threats to make the WSN system unstable. Here in this section we present a layer based classification of WSN security threats and also based on the capability of the attacker and defenses proposed in the literature [4].

Hence a need of a designed which ensures the security, large scalability, low key storage overhead and good network resiliency. For this we use the concepts of novice Unital design theory for efficient key pre distribution. Mapping increases the number of keys, which increases the security and scalability but decreases the key sharing probability.

II. RELATED WORKS: KEY PRE-DISTRIBUTION IN KEY MANAGEMENT

Key management for key pre-distribution in WSNs is much surveyed and several solutions have been proposed. Symmetric methods are either classified into two categories: Probabilistic or Deterministic methods. There is a direct secure link with secure connection coverage between the two nodes and in probabilistic method there are shared keys between the neighboring nodes; which means secure connectivity is not guaranteed.

A. Eschenauer and Gligor’s Scheme:

Eschenauer and Gligor [7] proposed the probabilistic key pre-distribution scheme. This scheme is referred as basic scheme because of its simplicity and the use of basic global keying method. Three phases- Key pre distribution, Shared key discovery and path establishment are the phases which follow to be set up. In key pre distribution phase each sensor node randomly assigned some variable different keys from a huge key pool.

![Fig. 1: Key Pool](image)

Fig. 1: Key Pool

Wireless Sensor Networks (WSNs) are ad-hoc mobile networks that include sensor nodes with limited...
computation and communication capabilities. WSNs are dynamic in the sense that they allow addition and deletion of sensor nodes after deployment to grow the network or replace failing and unreliable nodes. WSNs may be deployed in hostile areas where communication is monitored and nodes are subject to capture and surreptitiously use by an adversary. Hence WSNs require cryptographic protection of communications, sensor capture detection, key revocation and sensor disabling. In this paper, we present a key-management scheme designed to satisfy both operational and security requirements of WSNs.

The keys are stored in each sensor networks and these stored keys are known as Key ring of the node. Each key in the key ring has a unique ID which corresponds to a specific key. Once when the nodes are deployed the other two phases are set up. Shared key discovery phase is a phase in which the same keys are discovered between the nodes and a secure connection is established between them. Neighboring nodes have same keys because of which the link can be established within the given range. Figure 2 shows sample the sample graph after shared key discovery. In this network node pairs X and Y, and X and Z can set up secure links through their common keys.

In a large scale sensor network, distribution of signature key is a problem. This signature key is possible to be pre-distributed but once if the signature key is compromised the adversary can duplicate the revocation messages from the base station this creates the jamming effect.

B. Zhang et al. Scheme[5]:
Zhang et. Al. proposed a key revocation scheme [9]. This scheme is also a centralized key revocation scheme.

![Fig. 3: Centralized Revocation Key](image)

Whenever the area is large, the large area is divided into the small areas. These divided areas are known as the subareas. Each sub Area is known as the revocation area. For establishing the connection the revocation message is send. The revocation area is divided into sub-areas if the revocation area is large. A revocation message is sent to a certain node within each area to the neighboring nodes. [10].
It is the drawback if the message is dropped if it is outside the revocation area.

C. Chan Et Al. Scheme: [11]:
Chan proposed a distributed key revocation scheme for sensor networks. Voting system is used in this scheme. The vote is taken and the vote is checked among the nodes in the network. These votes are exchanged among the nodes and decryption is done. At least x number of sensor nodes cast their votes against the target node. This scheme is based on the lemma that each node knows its neighboring nodes before deployment. And the construction of the network according to the real world use is the main need and so it is difficult to satisfy this requirement. The distributed key revocation scheme is faster compared with the centralized key revocation scheme because it requires local broadcast. However, the distributed key revocation scheme is more complex than the centralized key revocation scheme. Detail information about the distributed key revocation scheme is included in [11-12].

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. We present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, we trade off the unlikeliest of a large-scale network attack in order to significantly strengthen random key pre-distribution’s strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, we show how to strengthen the security between any two nodes by leveraging the security...
of other links. Finally, we present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

To achieve security in wireless sensor networks, it is important to be able to encrypt messages sent among sensor nodes. Keys for encryption purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement in wireless sensor networks is nontrivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable 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. Recently, a random key pre-distribution scheme and its improvements have been proposed. A common assumption made by these random key pre-distribution schemes is that no deployment knowledge is available. Noticing that in many practical scenarios, certain deployment knowledge may be available a priori, we propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. We show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can be substantially improved with the use of our proposed scheme. The scheme and its detailed performance evaluation are presented in this paper.

Wireless sensor networks are usually deployed to operate for a long period of time. Because nodes are battery-operated, they eventually run out of power and new nodes need to be periodically deployed to assure network connectivity. This type of networks is referred to as Multi-phase WSN. Current key pre-distribution schemes, such as [2] and [10], are not adapted to multi-stage WSN. With these schemes, the security of the WSN degrades with time, since the proportion of corrupted links gradually increases. In this paper, we propose a new pre-distribution scheme adapted to multi-phase WSN. In the proposed scheme, the pre-distributed keys have limited lifetimes and are refreshed periodically. As a result, a network that is temporarily attacked (i.e. the attacker is active only during a limited amount of time) automatically self-heals, i.e. recovers its initial state when the attack stops. In contrast, with existing schemes, an attacker that corrupts a certain amount of nodes compromises a given fraction of the total number of secure channels. This ratio remains constant until the end of the network, even if the attacker stops its action. Furthermore, with our scheme, a network that is constantly attacked (i.e. the attacker regularly corrupts nodes of the network, without stopping) is much less impacted than a network that uses existing key pre-distribution protocols. With these schemes, the number of compromised links constantly increases until all the links are compromised. With our proposal, the proportion of compromised links is limited and constant.

D. Liu and Ning [6]:
proposed a key management scheme in which nodes are pre-loaded with bivariate polynomials instead of 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 two neighboring nodes share a common polynomial, the session key is derived by computing the polynomial value at the neighbor identifier. This approach allows to compute distinct secret keys which enhances the resilience against node capture. However, it requires more memory to store the polynomials.

E. Novel Deterministic Key Pre-distribution Scheme [8]:

Encryption and the authentication can be provided to the system using the symmetric key cryptography and the asymmetric key cryptography. In WSNs for the security purpose, the key management problem is the crucial one and the fundamental also. To achieve security message among sensor nodes must be secure. Before doing so the keys for performing encryption must be agreed upon the communication node. However, due to the resource constraints on the sensor nodes, many key agreement mechanisms such as Diffie-Hellman and other public based schemes, are not feasible in sensor networks. Compared to previous proposed schemes, the proposed method could significantly improve the performance and energy efficiency of the sensor nodes, making it suitable for the sensor nodes that are limited in power, computational capacities and memory. The proposed schemes more resiliently against the node capture.

1) Start
2) First System randomly choose a positive integer \(t\)
3) System randomly selects a pool of secret keys \(k_{ij}<t\), such that \(k_{ij}=k_{ji}\) for \(i=\{1,2,3,...\}\) and \(j=\{1,2,3,...\}\)
4) Then the system generates the secret information \(S_i\), such that \(S_i=k_i,1+ki,2t+k_i,3t...ki,m^t\&m-1\)
5) Finally \(i\) and \(t\) are assigned to each node \(N_i\), \(N_j\), therefore any node \(N_i\) and \(N_j\) can compute \(k_{ij}=k_{ji}\) using their secret information \(S_i\) and \(S_j\) respectively. Also \(i\) and \(j\) is the common key between both the nodes \(N_i\), and \(N_j\)
6) Therefore any pair of nodes \(N_i\) and \(N_j\) could compute \(k_{ij}=k_{ji}\) using their secret information \(S_i\) and \(S_j\) respectively. Also \(i\) and \(j\) is the common key between both the nodes \(N_i\), and \(N_j\)
7) End.

Therefore we are trying to find a method which although being tough in encryption strategy reduces the storage space and computational aspects and increases the scalability along. And for this here I am trying to use the mapping technique with the help of set theory concepts. Also along with the set theory we will try to map that both the node who want to have secure communication, commute two ways so that if one link fails then the other link can establish secure communication, thereby increasing the resiliency and fault tolerant and scalability. For this the concepts of the Unital Theory and employed in the wireless sensor nodes in order to highly support Scaldability issues, which are actually basic. In those mappings the thing is clear that it is providing scalability but degrading other performance measures like resiliency and good key sharing probability over the scarce resource of Storage.

F. Unital Set Theory:
Set of \(m^3+1\) point arranged in the subset of size \((m+1)\)
\(U=\{ m^3+1,...........\}\) subset of \(\{m^1,........\}\)
So that every pair of distinct points of set are contained in exactly one subset.
\(m=\{1,2,3,........\}\)
then \( U = \{2, 9, 65, \ldots \} \) subset of \( \{2, 3, 4, \ldots \} \)

Unital is a \( 2-(m^2 + 1, m+1, 1) \) block design.

Where \( m^2 + 1 \) is the key pool, \( m+1 \) is key ring size for \( n \) nodes

By using this theory the key sharing probability comes out to be

\[
P_c = \frac{(m+1)^2}{(m^3+m+1)}
\]

However this naïve solution degrades the key sharing probability to \( O(1/K) \) [12] [13].

The main proposal here is based on some observations:

1) That Unital Set Theory is providing the best scalability (one of the most important criteria) compared to all the naïve approaches used till date.

2) That the use of Unital Theory is degrading the performance measures like key sharing probability.

3) When trying to correct the above factor of key sharing probability, then the Resiliency with Storage overheads are disturbed, which is also not acceptable at low storage capacity sensor nodes.

4) Hence ahead in this survey, we need some kind of a Scheme or a Function which will implement the same scalability with the resiliency, storage and key sharing probability.

III. PROPOSED NEW HIGHLY SCALABLE KEY PRE-DISTRIBUTION IN KEY MANAGEMENT

START

(Before Deployment of Nodes)

1) Step1: Deployment of Nodes in \( n/w \) \( \{N1, N2, N3, \ldots \} \)

2) Step2: Create Disjoint Unital Blocks \( Ub \) (with distinct keys) according to \( n/w \) size.

3) Step3: Create Global Key pool : \( S \)

4) Step4: Generate \( n \) no. of Key Rings \( K = \{KR1, KR2, \ldots \} \) of size \( (m+1) \) each for every node-Communication Key Rings have distinct keys

5) Step5: Mappings of Unital Blocks to the Key Rings.

(After Deployment of Nodes)

6) Step6: (For Communicating Nodes N1 and N2) If(Secure Connection)

\[
\begin{align*}
\text{- exchange identifiers } & N1_{(id)} \text{ and } N2_{(id)} \text{ between } N1 \\
\text{- nodes share Zero Key Block and } ku \text{ key of } N2. \\
\text{- } ku \text{ key will be shared from other node.}
\end{align*}
\]

Else(No Secure Connection)

\[
\begin{align*}
\text{Connection failed} \\
\text{Go to Step 6.}
\end{align*}
\]

END

After the implementation of Unital Block Theory – this has its own specified key ring and Unital Blocks which are shared. The key ring has certain keys which need to be matched and exchanged. Whereas in case when we are using the Dummy fixed block or Zero block, then only a kind of a signal is send that, it is the sender who wants to communicate. In turn that dummy symbol or symbol is filled with the receiver key and fetched to the sender and communication through the router is established. While when we are computing the energy consumption of Basic Unital Block Theory and our Dummy symbol Unital Theory that time, certain calculations of energy should be assumed. Those assumptions are stated as follows:

1) Energy for the transmission of bits

2) Energy to receive the bits

3) Key Ring

4) Number of Neighbors in between

5) Size of the key with near ceiling value

The energy efficiency of symmetric key cryptographic algorithms applied in wireless sensor networks (WSNs) and in our study we consider both stream ciphers and block ciphers. We work on the computational energy cost of the ciphers under considerations by energy required to perform encryption. After evaluating a number of symmetric key ciphers, we compare the energy performance of stream ciphers and block ciphers [3].
An Energy Aware Key Pre-Distribution Scheme for Wireless Sensor Networks (IJSRD/Vol. 3/Issue 04/2015/342)

Fig. 5: Total Energy Calculations Basis

Total Energy (TE) will be computed by the summation of the transmission by the source taking along the calculation of size of the key ring as well as the size of the key and the neighbors in between (i.e. multihopping/resiliency factor) and energy used in receiving the key along with the receivers key ring size and its key size.

Total Energy (TE) = Ts * k * ks + N * Rd * k * ks

Where,
Ts, transmission by source
K, key ring
Ks, key size
N, number of neighbors
Rd, receiving by destination

Now when the above energy calculations are applied on the Basic Unital Block Theory and the Dummy symbol Unital Theory at that time we assume the factor of Ts and Rd remain static in both the cases, Only the key ring and size of the key may vary because key ring and the size of the key ring in Unital will be larger than the Dummy symbol Unital theory making the considerable difference in the energy of both points.

REFERENCES


[3] Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks Xueying Zhang, Howard M. Heys,and Cheng Li Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John’s, NL, A1B 3X5, Canada


[5] International Journal of Application or Innovation in Engineering & Management (IJAEM)Web Site: www.ijaem.org Email: editor@ijaem.org, editorijaem@gmail.com Volume 2, Issue 2, February 2013 ISSN 2319 – 4847


[12] IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013 BECHKIT et al.: A HIGHLY SCALABLE KEY PRE-DISTRIBUTION SCHEME FOR WIRELESS SENSOR NETWORKS