

# Key Pre-Distribution Scheme for Wireless Sensor Networks

N. K. Vijay Kumar<sup>1</sup>, H. N. Suresh<sup>2</sup>

<sup>1</sup>Lecturer, Dept. of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, India

<sup>2</sup>Professor, Dept. of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, India

**Abstract:** In wireless sensor networks (WSN's), majority of its applications necessitate the confidentiality of information they transmit. This can be achieved through secure key management schemes. In this paper, a key pre-distribution scheme for randomized secured routing is proposed for WSN. Initially, the sink utilizes the one hop neighbor information of nodes to pre distribute keys. It randomly chooses  $(n/2)$  nodes and distributes with  $(k+m)$  keys and other nodes obtain  $(k)$  keys.

Nodes with more shared keys are considered as high resilient nodes. During data transmission, high resilient nodes are preferred to other normal nodes and the next hop is randomly selected from the secured minimum hop neighbors. When there is more than one secure minimum hop links, then a weight function is assigned and the best path is elected. The proposed scheme is simulated in NS-2 and it is shown that it provides high resilience and delivery ratio with reduced energy consumption.

**Keywords:** Wireless Sensor Network (WSN), Key Management, Security, Pre-distribution.

## 1. Introduction

### A. Wireless Sensor Networks

The prominent technology of wireless sensor network (WSN), which is operated to monitor physical environment has been evolved as a result of integrating wireless communications with embedded computing technologies. [1] As of now a wide acceptance is achieved by WSN's. More applications are using tiny wireless sensors to accomplish monitoring, sensing and communication tasks. Most of these applications are adopted in hostile environment, where the success is dependent on its security from malicious attackers.

### B. Key Management in WSN

Key management is an important feature of security in wireless sensor networks. The processes such as authentication and privacy are also relied on key management. [6] As like security, key management is also pondered as a cross layer issue. Because, the process of key management is initiated in the link layer and upper layers like network and application layers are also required to forward keys securely. Several security critical applications highly necessitate key management process along with high level of fault tolerance. However, handling both the requirements at the same hand is a daunting task in wireless sensor network as it possesses

stringent constraints such as bandwidth and network life time. [7].

### C. Issues of Key Management

Ensuring confidentiality of information is the main objective of a key management scheme. The defined keys are useful for authenticating legitimate nodes. However, while transmitting data between nodes, an adversary may attempt to crash secret key and can take out confidential information. When we use keys for authentication process, confidential information can be obtained by an adversary by pretending as a legitimate node. At the same time as attempting to crash a key, the attacker stab to understand the message fashions and predicts the secret key. So as to avoid the attackers from predicting keys, a key management scheme has to introduce a rekeying technique at periodic time intervals. Here, the time interval may relies on regularity of communication and key usage.

Apart from above-mentioned issues, adversaries can also make several challenges to a sensor network such as jamming the wireless signals of sensor network, attempting to cause noises and other means to disrupt communications. Further, attacks like jamming cannot be managed by key management techniques [6].

### D. Problem Identification

Wenjun Gu et. al. [8] have proposed a key pre distribution scheme. Their scheme has distributed more keys to some nodes so that the links between those nodes tend to have much higher resilience than the link resilience under uniform key pre-distribution. These high resilient links are preferred during routing to enhance the end to end secure communications.

But if those high resilient nodes are captured, all these keys can be disclosed. Moreover, this work uses GPSR as the routing protocol which uses geographical positions of the nodes. This leads to a high risk of malfunctioning the actual co-ordinates of the nodes. In order to solve the above problems, in this paper a key pre-distribution scheme for randomized secured routing in WSN is proposed.

## 2. Related works

Wenjun Gu et. al. [8] have designed an end to end secure communication protocol in randomly deployed WSNs. Their

protocol is rooted on a methodology known as differentiated key predistribution. Their main objective is to share various numbers of key to different sensors to improve the resilience of certain links and then accomplish routing. During data communication, packets in nodes are routed through the links with higher resilience.

Christian Lederer et al. [9] have proposed an energy-efficient implementation of Elliptic Curve Diffie-Hellman (ECDH) Key Exchange for Wireless Sensor Networks. Initially, they have introduced an improved version of hybrid method for multi-precision multiplication. This hybrid method necessitates a fewer single-precision additions. To lessen the execution time of ECDH key exchange at the expense of a slight increase in memory requirements, they have utilized fast algorithms for elliptic curve scalar multiplication (window method, comb method). Finally, they have considered schemes for securing their ECDH implementation against side-channel attacks.

Arif Selcuk Uluagac et. al. [10] have proposed an energy-efficient Virtual Energy-Based Encryption and Keying (VEBEK) scheme for WSNs. The authors have initiated their work with an objective of lessening the number of transmissions requiring for rekeying to avoid unused and old keys. Their VEBEK's secure communication framework has presented a technique to verify data in line. After the verification, their technique drops false packets from malicious nodes. By this process, their VEBEK's manages the lifetime of the sensor network. Further, their technique has updated the keys without exchanging control messages for key renewals.

Shu Yun Lim et al. [11] have proposed two group key management schemes. They have presented those schemes with the aim of conserving energy by keeping the cryptographic burden on sensors with higher computation power, the access points and on forwarding nodes. Both of the key management schemes enable a sensor network to set up cryptographic keys in an autonomous fashion. Their first technique requires a small amount of keys independent of the network size, and hence achieves high scalability. A group key establishment scheme is introduced as a second technique with initial shared keys for authenticating and establishing a set of secure group-wise local links.

A key re-distribution and authentication based technique for secured communication in clustered wireless sensor networks with node mobility is proposed in [12] by Saswati Mukherjee et al. To establish secure communication in network the authors have considered a hierarchical cluster based WSN. They have exploited Improved key distribution mechanism (IKDM) to employ key distribution. Whenever nodes move from one cluster head (CH) to another key re-distribution is evolved. Further, they have constructed an authentication model to recognize an intruder in a cluster.

Haijun Liang and Chao Wang [13] have presented a new energy efficient dynamic key management for wireless sensor networks. Initially they divide a cluster into many virtual grid and there is only one node is active in a grid to reduce energy

consumption. Then they have adopted a scheme to achieve dynamic key management, namely, pair-wise key based on common polynomial and random number.

Pengcheng Zhao et al. [14] have proposed a hybrid key management scheme. Their scheme is based on clustered wireless sensor networks. They have built a d-dimensional key tree between cluster head and base station using shared function to generate front-end session key. Cluster members generate their own key and adjacent key pair based on the information of their geographic location and pre-loaded master key.

### 3. Proposed solution

#### A. Overview

In this paper, a random key pre-distribution scheme for secured routing in wireless sensor network (WSN) is proposed. Initially after the nodes are distributed in the network, the sink divides the nodes into multiple classes and utilizes the one hop neighbor information of nodes to distribute keys. The sink randomly selects  $(n/2)$  nodes of a node's neighbors and allocates with  $(k+m)$  keys whereas other remaining nodes are acquire  $(k)$  keys.

As soon as pre distribution of keys is finished, each node constructs all possible direct and indirect key paths to their neighbors. With help of constructed paths the pair wise key is established between neighbors. For data transmission proposed scheme makes use of Non-Repetitive Random Propagation (NRRP) routing algorithm. When a node desires to transmit data to the sink, the next hop is randomly selected from the secured minimum hop neighbors. In the event such as when there is the presence of more than a secure minimum hop links, then weight function is assigned and the best path is elected.

#### B. Distinguished Key Pre-Distribution Scheme

The distinguished key pre distribution scheme supposes that nodes are secured and they cannot be compromised before pre distribution of keys. The proposed distinguished key pre distribution scheme consist of two phases namely initial key pre distribution and pair wise key generation.

##### 1) Initial Key Pre-distribution

Initially, the sink (S) partitions the nodes into H number of classes such that  $N_i$  ( $1 < i < H$ ) nodes. The technique describes the nodes according to their class names. For instance, nodes in  $i_{th}$  class are defined as class i nodes and so on. Then, the sink selects distinct keys  $K_i$  from the key pool of size  $K_{and}$  shares out to nodes in class i.

In order to distribute secret keys to nodes in a group, the sink makes use of NT information of a node. As it is described in section-3.2, each node constructs NT by collecting one-hop neighborhood information. Consider node  $N_i$  of  $i$ th class has n one-hop neighbors, and then the sink randomly selects  $(n/2)$  one-hop neighbors and shares  $(K_i+m)$  keys, where m is a changeable variable. Other nodes in the NT table will obtain  $K_i$  keys. The nodes are selected by the sink randomly and it does not depend on any parameters.

Since,  $(n/2)$  nodes are selected randomly to distribute  $K_{i+m}$  keys; it is difficult for an adversary to disclose all keys by compromising a single node. This process is repeated by the sink until nodes in entire groups are distributed with pre distributed secret keys. Nodes that possess  $K_{i+m}$  keys have high resilience against failures. Further, these nodes assure an extra reliability and security when compare with nodes with  $K_i$  keys. Therefore, while transmitting data between any pair of source and destination, nodes with  $K_{i+m}$  keys are preferred to other nodes.

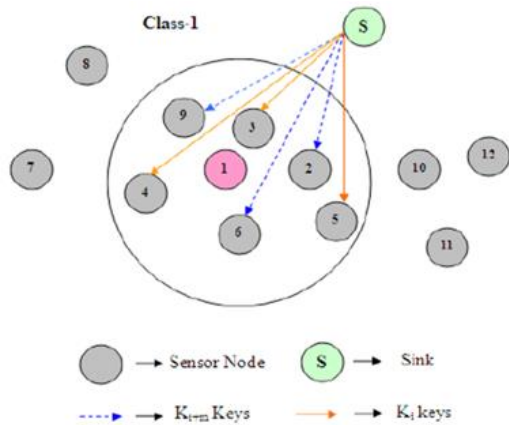


Fig. 1. Key distribution phase

Consider the sketch given in figure 1, the sink (S) invokes the key pre distribution phase as nodes are distributed in the network. Figure-2 includes the nodes that correspond to class-1. To distribute keys, initially the S exploits NT of node N1. The node N1 has six neighboring nodes namely N2, N3, N4, N5, N6 and N9. Among six neighbors ( $n=6$ ), the S randomly chooses  $(6/2)$  (i.e) three nodes namely N2, N6 and N9 and distributed with  $K_{i+m}$  keys. Other nodes namely N3, N4 and N5 obtain  $K_i$  keys. Algorithm-1 describes the process of initial key pre-distribution

*Algorithm-1:*

1. Let H be the set of classes  $i$ , where  $i=1, 2 \dots H$  and S be the Sink
  2. Consider N as a set of sensor nodes and n as the number of neighboring nodes
  3. Let  $NT_i$  be the neighbor table of node  $N_i$
  4. Consider  $K_i$  and  $K_{i+m}$  as keys taken from the key pool of size K
  5. Nodes are distributed and S is positioned in the network
  6. S classifies the nodes into H classes
  7. It selects the class  $i$  from H and chooses node  $N_i$  from N
  8. S acquires  $NT_i$  and calculates n
  9. It calculates  $(n/2)$
  10. Randomly selects  $(n/2)$  nodes and distributes  $K_{i+m}$  keys to them
  11. S distributes  $K_i$  keys to the remaining nodes in  $NT_i$
  12. Steps 5 to 11 are repeated until S reaches the
- 2) *Pair Wise Key Generation*  
 As soon as the sink completes the pre distribution of keys to

nodes, every sensor node forwards K info message to their one-hop neighbor. K-info message contains the key-ID's information. Subsequently, every node receives a set of K-info messages from its one-hop neighbors. The key ID information of neighboring nodes is keep tracked in Key ID of NT. By utilizing this information, every node generates direct and indirect key paths with its neighbors. Here, direct key path refers to one-hop key path and indirect key path denotes two-hop key path. The construction of direct and indirect key paths is as follows.

- (i) When node  $N_i$  distributes keys with node  $N_{i+1}$ , then node  $N_i$  generates a direct key path with  $N_{i+1}$ . The node  $N_i$  can construct as many as "Direct key paths" to their neighbors.
- (ii) When node  $N_i$  desires to generate indirect key path with node  $N_{i+2}$ , then it first forwards a request message to all its neighbors including the node id's of  $N_i$  and  $N_{i+2}$ . Once, the neighboring node (say  $N_{i+1}$ ) receives the request, it checks whether it has shared pre distributed keys with both node  $N_i$  and  $N_{i+2}$ . If so node  $N_{i+1}$  forward back a reply to node  $N_i$ . Thus,  $N_i$  generates Indirect key path as,



A node can construct many "Indirect key paths" regardless of "Direct key path" along any specific node.

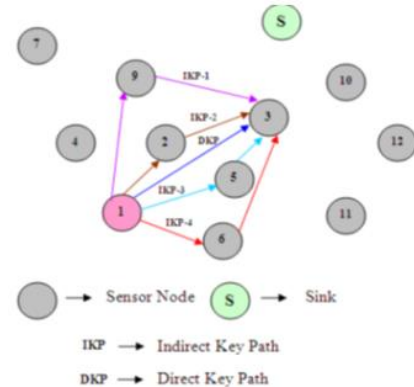


Fig. 2. Direct and indirect key paths construction

Take into account the picturization given in figure 2. In that, node N1 creates direct and indirect key paths to node N3. It constructs only one direct key path described as DKP and four indirect key paths namely IKP-1, IKP-2, IKP-3 and IKP-4.

After a node ( $N_i$ ) constructed all possible "Direct and Indirect key paths" to an another node ( $N_{i+1}$ ), node  $N_i$  will produce multiple random shares and forwards every key share on every key path such as Direct and Indirect key paths. With the use of combination of XOR, all key shares are encrypted and decrypted hop by hop along the path. Eventually, the combination of all the key shares that is forwarded between node  $N_i$  and  $N_{i+1}$  is termed as the pair wise key of those two nodes. This generated pair wise key is used for securing transmission during routing.

*C. Route Selection*

To route data from any node to the sink, in this paper we

enhance the Non-Repetitive Random Propagation (NRRP) routing algorithm [15].

1) *Weight Function Computation*

In order to calculate the weight function of a path, let us consider the distinguished key pre distribution scheme given in section 3. Assume  $K(i,j)$  as the number of keys shared between node  $N_i$  and  $N_j$ . This information can be obtained from the trusted offline authority (OA). Then the number of defense keys ( $D(i,j)$ ) between  $N_i$  and  $N_j$  can be given as

$$D(i, j) = K(i, j) + \sum_{g=1}^T \min(K(i, OA_g), K(OA_g, j))$$

In the above expression,  $T$  denotes the number of indirect key paths between  $N_i$  and  $N_j$ . The defense keys define strength of a link. Through this, we can describe how resilient the link is. To perform data communication, node  $N_i$  assigns weight to all its neighboring nodes. The weight function is as follows,

$$W_{N_j} = \frac{D(i, j)^\beta}{\sum_{k \in M(i)} D(i, k)^\beta}$$

Here, node  $N_i$  assigns weight only to the nodes to which it has established pair wise keys. Let  $M(i)$  be the set of secure neighboring nodes of node  $N_i$ , which are closer to the sink than itself.  $N_j W$  is the weight probability that node  $N_i$  selects  $N_j$  as the forwarder.  $\beta$  is referred as priority variable. The value of  $\beta$  can be assigned as per the requirement of communication as,

- If ( $\beta = 0$ )
- then Equal priority will be given to all nodes in  $M(i)$
- Else if ( $\beta = \text{positive value}$ )
- then Higher priority will be given to more resilient links
- Else if ( $\beta = \text{infinity}$ ) then
- Most resilient links are selected for routing End if

2) *Non-Repetitive Random Propagation (NRRP) Routing Algorithm*

When node  $N_i$  intends to transmit data to the sink, it utilizes the  $M(i)$  nodes for transmission.  $M(i)$  is the set of secure neighboring nodes of  $N_i$ , where it has established pair wise secret key with them. First, it randomly selects a node from  $M(i)$  and transmits a data packet. Similarly, data packets are transmitted. To enhance the efficiency of propagation and to assure loop-free routing, NRRP routing algorithm includes the node-in-route (NIR) field. Initially, this field is set to zero. Whenever a data packet is forwarded from a node to another node,

The corresponding node ID is appended in NIR field such that the source does not select the same node again and again. Thus, when determining next hop, the node  $N_i$  selects a minimum and secure next hop from  $M(i)$ .

In Energy case, when the source has more minimum hop secure paths, then weight function ( $N_j W$ ) is utilized. The node  $N_i$  assigns weight function to each path and chooses the best path.

*Merits of Proposed Scheme*

- In the distinguished key predistribution scheme, as

$(n/2)$  nodes are selected randomly to distribute  $K_i+m$  keys; it is difficult for an adversary to disclose all keys by compromising a single node.

- The enhanced Non-Repetitive Random Propagation (NRRP) routing algorithm increases efficiency in propagation and assures loop free routing paths.

D. *Performance Metrics*

The performance of RSR is compared with the Differentiated Key Management scheme of [8]. The performance is evaluated mainly, according to the following metrics.

*Energy:* It is the average energy consumed for the data transmission.

*Delay:* It is the average time taken by the packets to reach the destination.

*Fraction of Compromised communications:* It denotes how a node capture affects the rest of network resilience. It is calculated by estimating the fraction of communications compromised between non compromised nodes by captured nodes

*Average Packet Delivery Ratio:* It is the ratio of the number of packets received successfully and the total number of packets transmitted.

4. **Conclusion**

In this paper, a key pre-distribution scheme for randomized secured routing in WSN is proposed. Initially, using a distinguished key pre-distribution scheme, the sink utilizes the one hop neighbor information of nodes to pre distribute keys. It randomly chooses  $(n/2)$  nodes and distributes with  $(k+m)$  keys and other nodes obtains  $k$  keys. Nodes with more secure keys are considered as high resilient nodes.

For data transmission the proposed scheme makes use of Non-Repetitive Random Propagation (NRRP) routing algorithm. When a node desires to transmit data to the sink, the next hop is randomly selected from the secured minimum hop neighbors. Since,  $(n/2)$  nodes are selected randomly to distribute  $(k+m)$  keys; it is difficult for an adversary to disclose all keys by compromising a single node. Simulated results show that it provides high resilience and delivery ratio with reduced energy consumption.

References

- [1] Sasha Slijepcevic, Vlasios Tsiatsis, Scott Zimbeck, "On Communication Security in Wireless Ad-Hoc Sensor Networks", Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002.
- [2] W. Gu, X. Bai, S. Chellappan and D. Xuan, "Network Decoupling for Secure Communications in Wireless Sensor Networks," 2006 14th IEEE International Workshop on Quality of Service, New Haven, CT, 2006, pp. 189-198.
- [3] Saurabh Singh, Harsh Kumar Verma, "Security for Wireless Sensor Network", Vol. 3 No. 6 June 2011
- [4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, ICACT 2006.

- [5] Rajeshwar Sing, Singh D.K. and Lalan Kumar, "A review on security issues in wireless sensor network", *Journal of Information Systems and Communication*, Vol. 1, Issue 1, 2010, PP-01-07
- [6] Syed Muhammad Khaliq-ur-Rahman Raazi, Zeeshan Pervez and Sungyoung Lee, "Key Management Schemes of Wireless Sensor Networks: A Survey", 2009.
- [7] Johnson C. L. Ee and Victor C. M. Leung, U Niversity of british columbia, "Key Management Issues in Wireless Sensor Networks: Current Proposals and future developments", *IEEE Wireless Communications*, October 2007.
- [8] Wenjun Gu, Neelanjana Dutta, Sriram Chellappan, and Xiaole Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks", *IEEE Transactions on Network and Service Management*, Vol. 8, No. 3, September 2011.
- [9] Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großschädl, Alexander Szekeley, and Stefan Tillich, "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks", *WISTP 2009, LNCS 5746*, pp. 112–127, 2009. IFIP International Federation for Information Processing 2009.
- [10] Arif Selcuk Uluagac, Raheem A. Beyah, Yingshu Li, and John A. Copeland, "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, July 2010.
- [11] Shu Yun Lim and Meng-Hui Lim, "Energy Efficient and Scalable Group Key Management for Hierarchical Sensor Network", *Journal of Ubiquitous Systems & Pervasive Networks*, vol. 2, no. 1, 2011.
- [12] Saswati Mukherjee, Matangini Chattopadhyay, Samiran Chattopadhyay, Amrita, "A Key Re Distribution and Authentication Based Technique for Secured Communication in Clustered Wireless Sensor Networks with Node Mobility", *International Journal of Computer Networks & Communications (IJCNC)*, vol. 2, no.6, November 2010.
- [13] Haijun Liang and Chao Wang, "An Energy Efficient Dynamic Key Management Scheme Based on Polynomial and Cluster in Wireless Sensor Networks", *Journal of Convergence Information Technology*, vol. 6, no. 5. May 2011.
- [14] Pengcheng Zhao, Yong Xu and Min Nan, "A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks", *Wireless Sensor Network*, August 2012.
- [15] Tao Shu, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes", *IEEE Transactions on Mobile Computing*, pp. 941- 954, 2010.