A NOVEL AND EFFICIENT DYNAMIC KEY MANAGEMENT TECHNIQUE IN WIRELESS SENSOR NETWORK

Priyanka Goyal*

Mukesh Sharma**

ABSTRACT

Key management in wireless sensor network is a challenging task because public key cryptosystem are unsuitable for using in resource constrained sensor nodes, and the nodes could be physically compromised by a rival. Due to resource constraints, it is infeasible to apply traditional key management techniques in WSN. Numerous dynamic key management schemes have been proposed so far, for maintaining secure channels among communicating nodes but they all are not efficient in terms of resource constraints parameters. This paper proposes a dynamic key management scheme by combining the advantages of simple cryptography and random key pre-distribution scheme. In this, when distance between two nodes increases the remaining energy of nodes are also increases. This scheme enables to establish a secure links between any two communicated nodes. Beside this, it also removes node addition attack and increases the security strength within the cluster by introducing the cluster key. Finally, the security analysis show that proposed scheme is more efficient and meets the security needs of sensor network.

* M.Tech Student, *Department of Computer Science and Engineering, The Technological Institute of Textile and Science, Bhiwani, Haryana*

** Assistant Professor, *Department of Computer Science and Engineering, The Technological Institute of Textile and Science, Bhiwani, Haryana*

1. INTRODUCTION:

Wireless sensor network might be deployed in a hostile environment, the sensor may be captured and the data packets sent among sensor nodes may be intercepted or modified. To achieve security in wireless sensor networks, it is important to be able to encrypt and authentication messages among sensor nodes. Pair wise key establishment play a fundamental role in research on security issue in wireless sensor networks, which is the basis of other security services like authentication. Due to resource constraints, achieving such key establishment in wireless sensor network is nontrivial.

Many key pre distribution schemes have been proposed to address these problems .Eschenauer and Gligor in [1], have proposed a basic random key scheme, in which sensor nodes are assigned a random subset of keys from a large key pool before deployment of network. After deployment, two nodes find at least one common key in their key rings that is used as a pair wise key for communication. But such key for communication are vulnerable to a colluding minority of attacker-controlled nodes. Chan et al. [2] proposed a q-composite random key pre distribution scheme which require at least q (q>1) shared key to establish a secure communication instead of just one common key as in [1].By increasing the value of q this scheme achieves better network resiliency against node capture. Du et al. [3] proposed a key scheme based on computation of a symmetric matrix which provides a key space for all sensors that posse a public and a private share of the key space. In this scheme first time the Blom's key predistribution [5] is used for shared key establishment in sensor network. Liu et al. [4] proposed a pair wise key scheme based on Blundo's polynomial-based key pre distribution scheme[6].These two key schemes are very similar in nature except the key space are defined differently. These two key schemes have threshold in residence against node capture. The communication between non compromised sensor nodes is less than a critical value. But when a critical value is exceeded, the rival would attack all pair wise key.

To improve scalability a deployment knowledge base key management method is proposed [7].In this scheme, multiple deployment point are identified in sensor network and for each deployment point, a key space is pre computed This scheme has strong requirement on deployment, but achieves better scalability as compared to all those previously defined scheme. A location aware deployment model for shared key establishment is presented in [8].In the LEAP protocol multiple keying mechanism are there. Four different keys are used depending on to which type of node it is communicating with. Sensors are preloaded with an initial keys are established [9]. The node addition attack after the single initial global key, adversary can easily launch Hello flood attack and replay attack. To address the above issue this paper proposes a dynamic key management scheme in which keys are generated dynamically after deployment of sensor nodes that remove the node addition attack after the single initial key is compromised in LEAP. And also introduce the cluster head broadcast key and to remove the HELLO flood attack, Sybil attack and replay attack during the pair wise key establishment phase in LEAP.

2. KEY MANAGEMENT SCHEMES IN WIRELESS SENSOR NETWORK:

The success of a key management scheme is determined in part by its ability to efficiently survive attacks on highly vulnerable and resource challenged sensor networks. Key management schemes in sensor network can be classified broadly into static or dynamic based on whether update of administrative keys is enabled post network deployment.

- **Static Key management schemes**: This scheme assumes that once the administrative keys are pre deployed in the nodes, they will not be changed. Administrative keys are generated prior to deployment, assigned to nodes either randomly or based on some deployment information, and then distributed to nodes. For communication, this scheme use overlapping of administrative keys to determine the eligibility of neighboring nodes to generate a direct pair wise key. Communication keys are assigned to links rather than nodes. In order to establish and distribute a communication key between two non neighboring nodes and a group of nodes, that key is propagated one link at a time using previously established direct communication keys [10].

- **Dynamic Key management schemes**: Dynamic key management schemes may change administrative keys periodically, on demand or on detection of node capture. The major advantage of dynamic keying is enhanced network survivability, since any captured keys are replaced in a timely manner in a process known as rekeying. Provide better support for network expansion; upon adding new nodes, the probability of network capture increase is prevented. The major challenge in dynamic keying is to design a secure yet efficient rekeying mechanism[10].

3. BACKGROUND:

In this section we briefly review the key management protocol LEAP, which is the basis of our new proposed scheme. LEAP is a key management protocol intended for sensor networks based on symmetric key algorithms that utilizes multiple keying mechanisms. LEAP uses four different type of key depending upon to which type of node it is communicating with. It also detail how each of the key is established [9]. Four different keys are as follows:

Individual keys are symmetric keys which it shares with base station and each of nodes. This key is preloaded into node before deployment and is used for transmission of any special information between base station and node such as exclusive instruction to a node. To save the base station memory, each of these individual keys is generated using a master key and the node unique id. Pair wise shared key are symmetric keys shared between a node and all immediate neighbors. A pair wise shared key with a single hop neighbor requires four phases: key distribution, neighbor discovery, pair wise key establishment, key erasure. Cluster keys are shared between a node and all of its neighbors. These cluster key can be used for locally broadcast message such as routing protocol might use and are also used for updating group key. In this generation of random key, encryption this key with pair wise key and then transmission of this encrypted key take place. Group keys are shared with all nodes of network and base station. These keys allow encrypted and authenticated message to broadcast through whole network.

4. PROPOSED SCHEME:

There is a severity flaw in most existing key pre distribution schemes, which an adversary can get key info of uncompromised nodes from the

compromised nodes. In these key predistribution scheme, the communication pair wise key between sensor nodes either uses the preloaded keys directly [1, 2], or can be derived from the preloaded secret shares [3, 4, 5, 6]. Then once some sensor nodes are captured, the rival may crack other sensor nodes or even the entire network through the compromised keys or secret shares. To alleviate this issue, in the proposed scheme there is no storage of keys like traditional key management scheme. In the proposed scheme keys are generated dynamically after deployment of sensor nodes.

A. **Network Assumption**: There are following network assumption for the proposed scheme:

- Environment is dynamic for wireless sensor network.
- All sensor nodes are homogeneous in nature means each node is similar in their computational and communication capabilities.
- Base station keeps the co-ordinate of each node.
- Every node has space for storing the large number of keys.

B. **Design Goals**: Our proposed scheme is designed to remove node addition attack after the single initial key is compromised in LEAP. Also during the pair wise key establishment HELLO flood attack, Sybil attack and replay attack is removed.

C. **Types of keys**:

- **Individual key**: Individual keys are those keys that are shared between base station and a node.
- **Pair wise key**: Pair wise keys are those keys that are shared between a node and all of its immediate neighbors.
- **CH-broadcast key**: CH uses this key to broadcast any message within cluster.

D. **Establishing Individual Key**: Every node needs to keep an individual key that is shared with the base station. Each node uses one of the initial keys randomly to generate its individual or master key i.e. for node u keys are generated randomly ,there is no preloading of key, after deployment keys are generated dynamically that is used by node as initial key. In this for master key generation $K_{\underline{u}} = f_k$ where f is pseudorandom function. In the proposed scheme, the base station saves the memory by not keeping a list of individual keys but only an id list , which BS need to communicate with any node, it derives the individual keys on the fly. So, if initial key compromises, attacker can-not detect which node uses which initial key to generate its master key. As the memory overhead is negligible because keys are generated after deployment. It also avoids the major node addition attack and prevents any node to compromise easily.

E. Establishing Pair wise Key:

- **Secret Pre-Distribution**: BS determine the coordinate for each node U before their deployment as U: $ID_u = (x, y)$. The keys are randomly generated for each node, so that key is used for generating the master key for that particular node.

$$T = \text{Random (generate pair key)}, K_u = f_T(u).$$

- **Neighbor Discovery:** For each initial key, proposed scheme fixed the code. Node u broadcast the nonce and id_u

$$U^{*}: \text{nonce}, ID_u \longrightarrow$$

The nonce is the code of initial key, or encrypted initial key. Neighbor v who receives the broadcast message checks the neighbor list to find out whether u is adjacent to it, if so then replies with the ACK message.

$$\text{ACK: nonce+1, IDv, MAC } (K_v, ID_v \text{ 11 } ID_{u)}.$$

- **Pair wise key Establishment**: Node u computes pair wise key $K_{uv} = f_{kv}(u)$ where K_{uv} is pair wise key between node u and node v. By checking the id of node in neighbor list, we prevent the node cloning attack.

F. **Cluster Head (CH) – Broadcast Key**: A cluster head and cluster nodes must share cluster keys for communication. If CH wants to broadcast any message then it broadcast its id, nodes belonging within the cluster checks their cluster list for authenticity of cluster head (CH). Nodes also check their energy level, if energy level is less than threshold value, they discards themselves from the cluster.

5. SECURITY ANALYSIS: The security aspects of dynamic key management scheme to deal with classes of attacks such as replay attack, HELLO flood attack , node addition attack and node cloning attack.

- **HELLO Flood Attack:** Every node needs to broadcast a HELLO message to inform its neighbor about its presence and trying to create a pair wise key with each other. Neighbors receiving such a message will assume that it is within radio range, calculate the necessary message and send back to the new joining node, such steps can be memory and energy consuming. A laptop-class adversary can simply send HELLO message to a large radio range to waste the CPU cycle, and fill up the queue of the node within the range. Furthermore, rival can convince these nodes that it is their next hop neighbor, and misdirect the routing in the network.

  This proposed scheme reduces the affected area by checking the id in the HELLO message is coming from the adjacent neighbor, if not, the HELLO message will drop.

- Node Addition Attack: As there are two initial keys, and the location of the nodes is already pre determined by the base station, therefore before establishing any key, authorization of the node is checked, if the node is not valid, it will detect the node is fraud, therefore, scheme also checks for node addition attack.

- Sybil Attack: Most key management scheme assumes that nodes obtain one unique identity. In Sybil attack, rival presents multiple identities and claim to be in multiple locations. Such an attack is effective in topology maintaining, and

geographical routing since legal node can easily misdirect or confused by these fake identities and locations, this attack is bas on the concept of identity fraud.

The proposed scheme is effective in preventing the unauthorized user to join the network. When unauthorized nodes receive the HELLO message from the new joining node, it can-not compute individual key since individual can only be calculate by correct id and correct initial key. So rival cannot deceive the legal joining nodes without knowing the correct id and master key.

- Replay Attack: Due to unattended nature of sensor network, it is easy for adversary to capture any message that is broadcasted in the network. While the term replay attack usually uses in replaying the routing information to create loops and attract the traffic, here we discuss the reply on the keying message exchanged in the scheme. In our scheme, every message exchanged during the key establishment phase except the HELLO message is different. Adversary catches the ACK message can-not replay it to other node's HELLO message since every node has a unique id. Adversary catches the HELLO message can-not authenticate itself to others because the nonce in the message will be different for each neighbor.

6. PERFORMANCE EVALUATION:

The proposed scheme have simulated for energy consumption with increasing number of neighbors, energy consumption of nodes with variation of distance between two nodes and time taken in individual key establishment with the number of nodes in the network.

A. **Simulation Parameters:** The following are the simulation parameters considered for the implementation of our proposed new dynamic key management scheme.

- The distance between the BS and the network is taken as 125m.
- Size of message is 80 bytes.
- Free space attenuation coefficient (Efs) is 10 pJ/bit/m^2 .

- Multipath attenuation coefficient (EMP) is 0.0013 pJ/bit/$m^{4.}$
- Electronic power (E elec) is 50 nJ/bit.
- Size of committing value 8 bytes.
- Size of MAC 8 bytes.
- Number of SNs within cluster is 11
- Average distance between SNs within cluster is assumed to be 7.5m.
- Cluster area is $10m^2$.

B. **Results and Discussion**: For realistic, our simulation uses the first order radio model [11, 12] as the communication model. Equation (1) and (2) represent the energy dissipation when a SN sends or receives an l-bit message.

$$E_{trans} = \begin{cases} l * \left(E_{elec} + E_{fs} * d^2\right), if\ d \leq \\ l * \left(E_{elec} + E_{mp} * d^4\right), if\ d > \sqrt{\frac{E_{fs}}{E_{mp}}} \end{cases} \quad (1)$$

$$E_{recieve} = l * E_{elec} \quad (2)$$

Figure 6.1 shows that the energy increases linearly with increasing number of neighbors in cluster. Figure 6.2 shows that energy consumption when the distance between two nodes is varying with the number of neighbors assumed to be 1. It is observed that energy decreases as the distance between two nodes increases and finally, Figure 6.3 shows the variation of time taken in establishment of individual keys of node when the number of nodes in the network is varying.

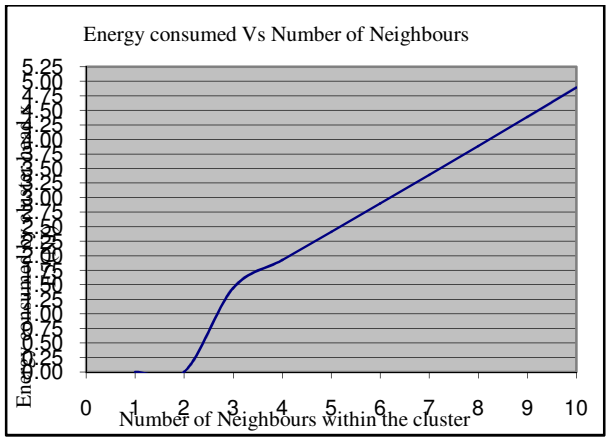

Figure 6.1 Energy consumed by Cluster Head Vs Number of neighbours

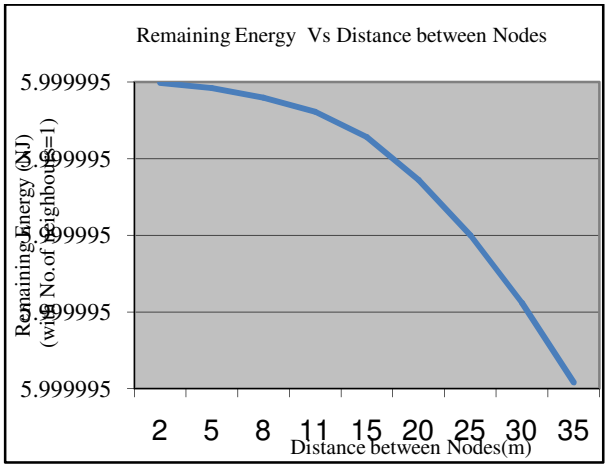

Figure6.2 Remaining Energy of nodes Vs Distance between two nodes

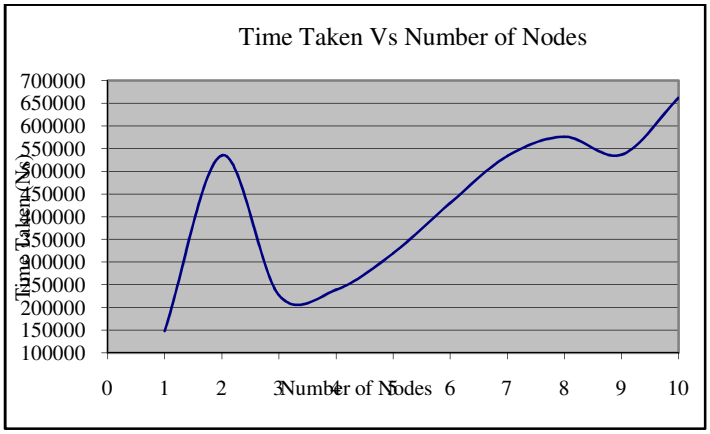

Figure 5.11 Time taken in individual key establishment Vs Number of nodes in network

7. Conclusion and Future Scope: Based on LEAP scheme, we have proposed a new scheme for dynamic wireless sensor network which enable establishing secure links between any two SNs located within their communication range. The novelty of this new scheme is that, no need for storing the keys in a key pool because the keys are generated randomly after deployment of nodes. Master key is generated by applying pseudo random function on one of initial key that is generated for that particular node. At different time, different initial keys are generated so adversary can-not get any key information during establishment. It removes the node addition attack, node cloning attack, HELLO flood attack and also increases the security within cluster by introducing cluster key.

The proposed scheme can be extended for heterogeneous network. Instead of each node having same capability, all nodes have different capability for computing and communication. And also in proposed scheme all communication is handled through BS, so we can extend the scheme by making the system distributed in nature.

7. REFERENCES:

[1] L. Eschenauer and V.D. Gligor, "A key-management scheme for distributed sensor networks". in: Proc. of the 9the ACM Conference on Computer and Communications, Washington DC, USA, pp.41-47,Nov. 2002

[2] H. Chan, A. Per rig and D. Song, "Random key predistribution schemes for sensor networks", in: Proc. 20003 IEEE Symposium on Security and Privacy, pp.197-313, May 2003

[3]. W.Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A pair wise key predistribution schemes for sensor networks". ACM Transactions on Information and System Security, Vol.8. No2, May (2005)228-258

[4]. D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks". ACM Transactions on Information and System Security, vol.8, pp.41-77, Feb. 2005

[5]. R. Blom, "An optimal class of symmetric key generation systems. Advance in Cryptography". London, UK: Springer-Verlag, pp.335338, 1985

[6]. C. Blundo, A. D. Santis, A. Herzberg. S. Jutten, U. Vaccaro, and M.Yung. "Perfectly secure key distribution for dynamic conference", Information and Computation, vol.1, pp.1-23, Jan. 1995

[7]. W.Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution schemes for sensor networks using deployment knowledge". IEEE INFOCOM, pp597, 2004.

[8]. D.Liu and P.Ning, "Location-Based pairwise key establishment for static sensor networks", Proc. 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp.72-82, 2003.

[9]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanism for large scaled distributed sensor networks," in Proc.CCS'03: 10th ACM conference on Computer and communications security. New York: ACM Press, 2003, pp.62-72.

[10]. R.Divya, T. Thirumurugan,"A Novel Dynamic Key Management Scheme Based On Hamming Distance For Wireless Sensor Networks", Proc. International Conference on Computer, Communication and Electrical Technology-ICCCET 2011, 18th &19th March, 2011, pp. 181-185.

[11]V.Mhatreand and C.Rosenberg,"Design guidelines for wireless sensor networks: Communication, clustering and aggregation, "Ad-hoc Networks,2(1):45-63,January 2004.

[12]. W. Li, "Energy Efficient Clustering Algorithm in Wireless Sensor Networks Based on Geometric Programming", in Proceedings of 2009 Second International Symposium on Electronic Commerce and Security,Nanchang,China,May 22-24,2009,2: 525-527