www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 11 November, 2013 Page No. 3197-3201

A Hamming Distance Based Dynamic Key Distribution Scheme for Wireless Sensor Networks

Ramu Kuchipudi[1], K.Vaishnavi Prapujitha[2], Y.G Shantha Reddy[3]

[1] MJCET, ITD,
Banjara Hills, Hyderabad, India
k_ramu2000@yahoo.co.in

[2] MJCET, ITD,
Banjara Hills, Hyderabad, India
vyshu37@gmail.com

[3] MJCET, ITD,
Banjara Hills, Hyderabad, India
yg.shantha84@gmail.com

Abstract: ***Key management schemes in sensor networks can be classified broadly into dynamic or static solutions based on whether rekeying (update) of administrative keys is enabled post network deployment.. The objective of key management is to dynamically establish and maintain secure channels among communicating nodes. Many schemes, referred to as static schemes, have adopted the principle of key predistribution with the underlying assumption of a relatively static short-lived network (node replenishments are rare, and keys outlive the network). An emerging class of schemes, dynamic key management schemes, assumes long-lived networks with more frequent addition of new nodes, thus requiring network rekeying for sustained security and survivability.***

This paper proposes a dynamic key management scheme by combining the advantages of simple cryptography and random key distribution schemes. When the hamming distance between the two nodes is found high, the unique key is changed instead of changing the set of keys and the communication takes place by using any one of the set of key x-oring with the new unique key. The security and performance of the proposed algorithm is compared with the existing dynamic key management scheme based on Exclusion Basis System and prove that the proposed scheme performs better when compared to existing Scheme by considering the number of nodes colluded with time. The result obtained by simulation also shows that the proposed scheme provides security solution and performs better than the existing scheme.

Keywords: WSN’s, dynamic key management, collusion, hamming distance, security

1. Introduction

Sensor networks comprise a large number of tiny sensor nodes that collect and (partially) process data from the surrounding environment. The data is then communicated, using wireless links, to aggregation and forwarding nodes (or gateways) that may further process the data and communicate it to the outside world through one or more base stations (or command nodes).

Base stations are the entry points to the network where user requests begin and network responses are received. Typically, gateways and base stations are higher-end nodes. It is to be noted, however, that various sensor, gateway, and base station functions can be performed by the same or different nodes. The sensitivity of collected data makes encrypttion keys essential to secure sensor networks.

2. Key Management Schemes in Sensor Networks

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 networks can be classified broadly into dynamic or static solutions based on whether rekeying (update) of administrative keys is enabled post network deployment.

2.1 Static Key Management Schemes

The static schemes assume that once administrative keys are predeployed 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 key management, most static schemes use the overlapping of administrative keys to determine the eligibility of neighboring nodes to generate a direct pair-wise communication 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/or a group of nodes, that key is propagated one link at a time using previously established direct communication keys.

2.2 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 key(s) is replaced in a timely manner in a process known as rekeying. Another advantage of dynamic keying is providing better support for network expansion; upon adding new nodes, unlike static keying, which uses a fixed pool of keys, the probability of network capture increase is prevented. The major challenge in dynamic keying is to design a secure yet efficient rekeying mechanism. A proposed solution to this problem is using exclusion-based systems (EBSs); a combinatorial formulation of the group key management problem

3. Sensor Network Model

Both the proposed and the existing security algorithm are based on a wireless sensor network consisting of a command node and numerous sensor nodes which are grouped into clusters. The clusters of sensors can be formed based on various criteria such as capabilities, location, communication range, etc. Each cluster is controlled by a cluster head, also known as gateway, which can broadcast messages to all sensors in the cluster. We assume that the sensor and gateway nodes are stationary and the physical location and communication range of all nodes in the network are known. Each gateway is assumed to be reachable to all sensors in its cluster, either directly or in multihop. Sensors perform two main functions: sensing and relaying. The sensing component is responsible for probing their environment to track a target/ event. The collected data are then relayed to the gateway. Nodes that are more than one hop away from the gateway send their data through relaying nodes. Sensors communicate only via short-haul radio communication.

The gateway fuses reports from different sensors, processes the data to extract relevant information and transmits it to the command node via long-haul transmission.

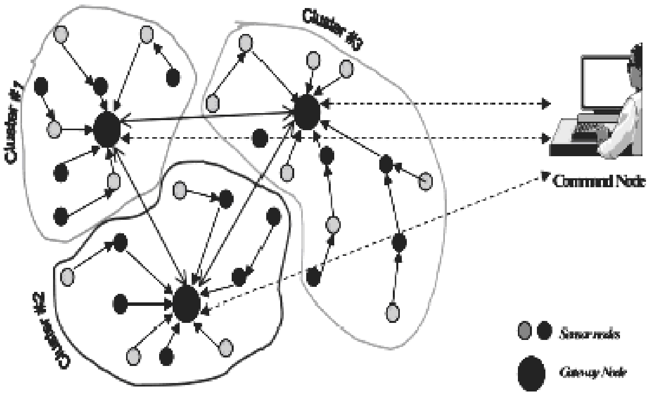

Fig. 1. Clustered Sensor Network

The network architecture is depicted in Fig. 1. Each tier of the network possesses different capabilities. The command node is resource-rich. However, the amount of traffic flowing between the command node and gateways causes the communication channel between the command node and gateways to be restrained. Most often, the command node is situated at a considerable distance from the deployment region,and might only be reachable through slow satellite links. Larger communication distances also incur increased security vulnerability and packet loss during long haul transmissions.

4. Collusion Problem

The security scheme proposed in [6] is based on the Exclusion Basis System (EBS) to address the collusion problem in EBS that performs location based key assignment to minimize the number of keys revealed by capturing collocated nodes. The network model is similar to the model developed in [6] with clusters and gateways. It uses the EBS framework to perform rekeying within each cluster. Keys are distributed to nodes by
the gateways. SHELL uses post-deployment location information in key assignment; collocated nodes share more keys than nodes that are not collocated

5. Existing Key Distribution Schemes

Due to swapping of keys the number of nodes getting colluded with the neighboring nodes is increased so capturing lesser nodes will reveal most of the keys and thus the whole network can be captured by the attacker. In order to reduce the number of colluding nodes a dynamic key assignment was chosen to employ the simple cryptography and random key distribution.

Both the simple cryptography and random key distribution has its own advantages and limitations. Thus the dynamic key management scheme with the advantages of both the schemes and by taking the hamming distance into consideration is proposed as a security solution.

5.1 Basic Probabilistic Approach

The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without sub-stantial computation and communication capabilities. It re-lies on probabilistic key sharing among the nodes of a ran-dom graph and uses simple protocols for shared-key dis-covery and path-key establishment, and for key revocation,re-keying, and incremental addition of nodes.

5.2 Q-Composite Random Key Pre-distribution scheme

This scheme [11] does not need to establish pair-wise key between every pair of nodes in a sensor network for a secure key management scheme for the wireless sensor networks. Communicating nodes should share at least Q number of keys. Thus in case of a key compromise, the nodes can communicate with the other keys. The value Q should be so selected such that the network maintains a certain desired level of connectivity. The size of the random key pool is reduced but this gives an advantage to the adversary. Only a few nodes need to be compromised to compromise the entire network.

5.3 Pairwise Key Predistribution Scheme

In 2003, Du *et al.* proposed a key management scheme [4] based on the pairwise keying model.This model extends Eschenauer and Blom's work [5] by using the same paradigm as Eschenauer and Gligor [3] but instead of individual keys, it uses the concept of Blom's key matrix, which is an array of keys. In Du's scheme,there are k key matrices in each node, and the key matrices are distributed randomly.

5.4 Localized Encryption and Authentication Protocol

Zhu, Setia, and Jajordia introduced the localized encryption and authentication protocol (LEAP)[6], which employs a hybrid approach. This is a jack-of-all-trades protocol offering network-wide,cluster/group, and pairwise keying capabilities. To accomplish this, LEAP uses four types of keys: individual, group, cluster, and pairwise shared keys. The individual key is unique for each sensor node to communicate with the sink node.The group key is a network-wide key for communication from the sink node to all sensor nodes.An authentication mechanism known as μTimed Efficient Streaming Loss-tolerant Authentication Protocol (μ*TESLA*) [7] is used for the broadcast authentication of the sink node, which ensures that packets sent with the group key are from the sink node only

5.5Location-Aware Combinatorial Key Management Scheme

The Scalable, Hierarchical, Efficient, Locationaware,and Light-weight (SHELL) protocol [8] is a complicated cluster-based key management scheme published recently. It is influenced by LEAP with its use of multiple types of keys but introduces a new distributed key management entity. Each cluster has its own distributed key management entity residing in a non-clusterhead node. Thus, the operational responsibility and key management responsibility are separated,leading to a better resiliency against node capture.

5.6 Energy and Communication Efficient Group Key Management Protocol

Panja *et al.* [13] recently introduced a hierarchical group keying scheme using the Tree-based Group Diffie-Hellman (TGDH) protocol. The main feature of this scheme is that each key is made up of many partial keys. By breaking up the keys into smaller components, it makes rekeying an efficient and simple task by revoking,changing, or adding one or more partial key(s).The TGDH keying scheme works on a hierarchical WSN that has one level of general sensor nodes and multiple levels of cluster heads; that is, there can be a *head of clusters* responsible for multiple cluster heads below it in a tree-like manner. The data collection process starts with a group of sensor nodes collecting data from a region of interest and sending it to the nearest cluster head.

5.7 Simple Cryptography

A simple cryptography of x-oring two keys is first tried as a dynamic key management. In this simple cryptographic scheme, each sensor node is assigned a set of keys and a unique key. Communication takes place through any one of the set of keys x-oring with the unique key. Once the encryption is over, the decryption takes place through the unique key that is known to the gateway node. The major drawback in this scheme is that the security level is low i.e. when any two key is known the other key may be revealed which results in revealing the keys of that node.

5.8 Random Key Distribution

Since the security level is low in x-oring of two keys, random distribution of keys is tried to enhance the security of the proposed method. In this random key distribution scheme, a set of keys is assigned to each sensor node. The communication takes place through any one of the set of keys. Once the hamming distance between any two nodes is found high the set of keys are randomly replaced and the new set of keys will be generated. Since all the keys are newly generated whenever the hamming distance is high the power consumption will be higher in this scheme and the security level is also enhanced since keys cannot be revealed by the reversing of x-or operation.

The term key may refer to a simple key (e.g., 128-bit string) or a more complex key construct (e.g., a symmetric bivariate key polynomial).A large number of keys need to be managed in order to encrypt and authenticate sensitive data exchanged. The objective of key management is to dynamically establish and maintain secure channels among communicating parties.

Typically, key management schemes use administrative keys (key encryption keys) for the secure and efficient
(re-)distribution and, at times, generation of the secure channel communication keys (data encryption keys) to the communicating parties. Communication keys may be pair-wise keys used to secure a communication channel between two nodes that are in direct or indirect communications, or they may be group keys shared by multiple nodes. Network keys (both administrative and communication keys) may need to be changed (re-keyed) to maintain secrecy and resilience to attacks, failures, or network topology changes.

5.9 Key Management Scheme for Distributed Sensor Networks

Numerous key Management schemes have been proposed for sensor networks. Most existing schemes build on the seminal random key predistribution scheme introduced by Eschenauer and Gligor [1].Subsequent extensions to that scheme include using deployment knowledge [2] and key polynomials [3] to enhance scalability and resilience to attacks. These set of schemes is referred as static key management schemes since they do not update the administrative keys post network deployment.

5.10 A Low-Energy Key Management Protocol for Wireless Sensor Networks

An example of dynamic keying schemes is proposed by Jolly et al. [4] in which a key management scheme based on identity based symmetric keying is given. This scheme requires very few keys (typically two) to be stored at each sensor node and shared with the base station as well as the cluster gateways. Rekeying involves reestablishment of clusters and redistribution of keys. Although the storage requirement is very affordable, the rekeying procedure is inefficient due to the large number of messages exchanged for key renewals.

5.11 Combinatorial Group Key Management Scheme for Large-Scale Wireless Sensor Network

Another emerging category of schemes employ a combinatorial formulation of the group key management problem to affect efficient rekeying [5, 6]. These are examples of dynamic key management schemes. While static schemes primarily assume that administrative keys will outlive the network and emphasize pair wise Communication keys. Dynamic schemes advocate rekeying to achieve resilience to attack in long-lived networks and primarily emphasize group communication keys. Since the dynamic scheme has the advantage of long lived network and rekeying when compared to the static schemes, the dynamic key management is chosen as a security scheme for the WSN's.

5.12 Polynomial based key pre-distribution scheme

Blundo et al. [16] distributes a polynomial share (a partially evaluated polynomial) to each sensor node using which every pair of nodes can generate a link key. Symmetric polynomial P(x, y) (P(x, y) = P(y, x)) of degree, d is used. The coefficients of the polynomial come from GF(q) for sufficiently large prime q. Each sensor node stores a polynomial with d+ 1 coefficients which come from GF(q). Sensor node Si receives its polynomial share of fi(y) = P(i, y). Si (resp. Sj) can obtain link key Ki,j = P(i, j) by evaluating its polynomial share fi(y) (resp. fj(y)) at point j (resp. i). Every pair of sensor nodes can establish a key.

6. Proposed Dynamic Key Assignment Scheme

The proposed dynamic key assignment takes the advantage of both the simple cryptography and random key distribution scheme to reduce the collusion of nodes. In this dynamic key management algorithm, each key combination can be represented in the form of bit strings of k 1's and m 0's, where k is the number of keys stored at each node and m is the number of rekey messages required. The Hamming distance between any two combinations is defined as the number of bits that the two key combinations differ in. Let d be the Hamming distance between a pair of key combinations.

$$
\begin{array}{ll}
2 \le d \le 2k & k < m \\
2 \le d \le 2m & m < k \\
2 \le d \le k + m & k = m
\end{array}
$$

When two nodes collude, they both will know at least d keys, since d is the number of keys that they differ in. addition, they will also know all the keys that are common to both nodes. The common keys are equal to k – d/2. Thus, the number of keys known to the two colluding nodes as k + d/2.This leads to the conclusion that the lower the Hamming distance (the value of d) fewer the total number of potentially revealed keys.

In this proposed dynamic key management, each sensor node is assigned a set of keys and a unique key as in the simple cryptography case. When the hamming distance between the two nodes is found high by the boundary condition, the unique key alone is changed instead of changing the set of keys and the communication takes place by using any one of the set of key x-oring with the new unique key. This method provides enhanced security with less power consumption when compared to the other two schemes.

7. Analysis of Proposed Solution

Both the dynamic key assignment and the SHELL are compared with static and mobile nodes. Again the number of nodes colluding with each other gets reduced in the dynamic key assignment. The number of nodes colluded when the nodes are static and mobile for both conventional and proposed scheme. It is observed that when both the schemes are compared for static and mobile nodes, the number of colluded nodes for the mobile nodes is lesser and approaches nearly zero preventing the collusion of nodes when compared to the static nodes because the hamming distance remains the same when the nodes are static and it differs when the nodes are given mobility. Thus by preventing the collusion of nodes the dynamic key assignment provides enhanced security when compared to other existing dynamic key management schemes.

It is found that the number of nodes getting colluded by the dynamic key assignment scheme is reduced to a greater extent. it is observed that as the number of nodes colluding with each other in the dynamic key assignment is reduced when compared to the other methods like simple cryptography, random key distribution and SHELL. The dynamic key assignment out performs the simple cryptography and random key distribution scheme as expected since it is a combination of both the schemes. The random key distribution performs better than the simple cryptography which in turn performs better when compared to SHELL.

8. Conclusion

The number of nodes getting colluded with each other in the dynamic key assignment scheme is greatly reduced when compared to the other dynamic key management schemes. The proposed dynamic key management performs far better than the SHELL and it is observed that by providing mobility to the nodes the collusion can be prevented. Thus the proposed dynamic key assignment prevents the collusion of nodes and provides enhanced security to the cluster based sensor network.

References

[1] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks," Proc. 9th ACM Conf. Comp. and Commun. Sec., Nov. 2002, pp. 41-47.

[2] W. Du et al., "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," Proc. IEEE INFOCOM '04, Mar. 2004.

[3] D. Liu and P. Ning, "Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks," ACM Trans.Sensor Networks, 2005, pp 204–39.

[4] G. Jolly et al., “A Low-Energy Key Management Protocol for Wireless Sensor Networks,” Proc. IEEE Symp. Comp. and Commun., June 2003, p. 335

[5] M. Eltoweissy et al., “Group Key Management Scheme for Large-Scale Wireless Sensor Network,” J. Ad Hoc Networks, Sept. 2005,pp. 796–802.

[6] M. Younis, K. Ghumman, and M. Eltoweissy, “Location aware Combinatorial Key Management Scheme for Clustered Sensor Networks,” to appear, IEEE Trans. Parallel and Distrib. Sys. 2006.

[7] D. W. Carman, P. S. Kruus, and B. J. Matt, “Constraints and Approaches for Distributed Sensor Security,” NAI Labs tech. rep. 00-010, 2000.

[8] N. Sastry and D. Wagner, “Security Considerations for IEEE 802.15.4 Networks,” Proc. 2004 ACM Wksp. Wireless Sec., 2004, pp. 32–42.

[9] W. Du et al., “A Pairwise Key Predistribution Scheme for Wireless Sensor Networks,” Proc. 10th ACM Conf.Comp. Commun. Sec., 2003, pp. 42–51.

[10] R. Blom, “An Optimal Class of Symmetric Key Generation Systems,” Proc. EUROCRYPT ’84 Wksp. Advances in Cryptology: Theory and App. of Cryptographic Techniques,1985, pp. 335–38.

[11] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,”Proc. 10th ACM Conf. Comp. and Commun.Sec., 2003, pp. 62–72.

[12] A. Perrig et al., “SPINS: Security Protocols for Sensor Networks,” Wireless Network, vol. 8, 2002, pp. 521–34.

[13] B. Panja, S. K. Madria, and B. Bhargava, “Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks,” SUTC ’06:Proc. IEEE Int’l. Conf. Sensor Networks, Ubiquitous, and Trustworthy Comp., 2006, pp. 384–93.

[14] S. A. Camtepe and B. Yener, “Key Distribution Mechanisms for Wireless Sensor Networks: A Survey,” Tech.rep. TR-05-07, Dept. of Comp. Sci., Rensselaer Polytechnic Inst., 2005.

[15] Chan, H., Perrig, A., and Song, D. 2003. Random Key Predistribution Schemes for Sensor Networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy (May 11 - 14, 2003). SP. IEEE Computer Society, Washington, DC, 197-213.

[16] Blundo, C., Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M. 1992. Perfectly-secure key distribution for dynamic conferences. In Crypto 92