ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhancing the Key Pre-Distribution on Wireless Sensor Networks by Reducing Storage Overhead

Manoj R[1]
[1,]Assistant Professor, GITAM University, Hyderabad Campus/IT Dept, Hyderabad, India
manojr11@gmail.com,manojr11@gitam.edu,

Tripti C[2]
[2] Assistant Professor,Rajagiri School of Engineering & Technology/CSE Dept, Cochin, Kerala, India
tripti84_05@rediffmail.com

Y.Md.Riyazuddin[3]
[3]Assistant Professor, GITAM University, Hyderabad Campus/IT Dept, Hyderabad, India
riyazymd@gmail.com.

G.Victor Daniel[4]
[4]Assistant Professor, GITAM University, Hyderabad Campus/IT Dept, Hyderabad, India
victordaniel.gera@gitam.edu

Abstract: Wireless Sensor Networks (WSNs) are characterized by resource constraints and large scalability. Many applications of WSNs require secure communication, a crucial component especially in hostile environments. However, the low computational capability and small storage budget within sensors render many popular public-key-based cryptographic systems impractical. Symmetric key cryptography, on the other hand, is attractive due to its efficiency. Nevertheless, establishing a shared key for communicating parties is a challenging problem.. Key management is challenging since sensors can land anywhere after deployment. Earlier approaches on key management mostly focus on key pre-distribution where a small number of keys are placed in sensors before deployment. Several symmetric-key pre-distribution protocols have been investigated recently to establish secure links between sensor nodes, but most of them are not scalable due to their linearly increased communication and key storage overheads. To address these limitations, in this paper, different key distribution mechanisms for wireless sensor networks with fixed key storage overhead, full network connectivity, and low communication overhead are proposed.

Keywords-Pre-distribution, Deployment, Symmetric key, Storage Overhead

I. INTRODUCTION

A wireless sensor network (WSN) consists of potentially hundreds of sensor nodes and is deployed in an ad hoc manner for collecting data from a region of interest over a period of time. Typically, a wireless sensor network is composed of a large number of sensors nodes; each sensor node is small, inexpensive wireless device with limited battery power, memory storage, data processing capacity and short radio transmission range. Depending on the equipped sensing units, wireless sensor nodes can measure various physical characteristics, such as sound, temperature, pressure, etc.

A number of wireless sensor nodes can be organized into clusters to track a particular object or monitor the surrounding environment in an interested area for encryption in WSNs, keys must be shared between communicating nodes. There is an excessive number of works done on key management in WSNs. The proposed techniques can be grouped into two: symmetric key management schemes, and asymmetric key management schemes. Asymmetric key management schemes are studied in is based on RSA cryptosystem. Elliptic curve cryptography (ECC) is computationally feasible on sensor are asymmetric schemes for sensor networks. Currently, the memory overhead of the public-key cryptography techniques is a barrier to secure most of the WSN applications. As a result, most WSNs use symmetric key schemes since these schemes require less computation time and space than their asymmetric counters do. Symmetric keys are required to be distributed for symmetric key cryptography and key pre distribution has emerged as a promising solution. Random key pre distribution schemes have been proposed for large- scale WSNs.

Two straightforward strategies exist to pre-load symmetric keys into sensors. The first one is called master-key approach, in which all the sensors are pre-loaded a unique symmetric key in its memory [6]. After the deployment, every two nodes in the network use the same symmetric key to encrypt/decrypt the exchanged data between them. This approach is extremely efficient since there is no communication overhead for key establishment and only one key is required to be stored in sensors, but it cannot provide sufficient security for wireless sensor networks.

In master-key approach [6], even one single node's capture could compromise the entire network, which is unacceptable for large-scale wireless sensor networks. Another method is pairwise-key based approach. In this approach, a set of symmetric keys are preloaded into each sensor node to make sure any two nodes have a unique key between them. This approach can provide sufficient security since any node's capture cannot compromise the secure communication between non-captured nodes, but it is not scalable due to its extremely large key storage overhead. For a network composed of n nodes, this approach requires each node stores at least (n-1) keys to ensure any two sensors can establish a secure link. The limited memory size of wireless sensors makes these approaches infeasible for real deployments. Above two straightforward approaches show that key pre- distribution schemes have a tradeoff between the security and the key storage overhead. To achieve sufficient security, a certain number of keys should be pre-loaded in each node; but the limited memory size of tiny sensors, on the other hand, decides that sensors cannot store

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

too many keys as they want. Key distribution problem has been a hot research topic recently and attempt to achieve both security and efficiency for large-scale wireless sensor networks.

To compensate for the unpredictability of the network topology prior to deployment, KPS requires a large amount of keying information to be preloaded in order to achieve desirable key-sharing probability between neighboring sensors. As a side effect, part of the keying information may never be utilized during the entire network lifetime. Such an inefficient use of the limited memory in sensors.

Most of the existing key distribution schemes consider wireless sensor networks have a highly distributed, flat architecture, which is easy to implement but not applicable for large-scale sensor networks, specifically for data-driven monitoring applications. Research shows that the hierarchical network architecture has better throughput and scalability than the flat structure for a large-scale wireless sensor network, since the redundant sensing data can be aggregated in the relay nodes and the destination node can be reached in fewer hops.

In this paper, we propose different Schemes to reduce storage overhead in key pre-distribution mechanism for large- scale wireless sensor networks to improve both security and performance. Compared with existing key pre-distribution schemes, Schemes not only achieves better network security, but also has improved the network performance in terms of network connectivity, communication overhead and key storage overhead.

The rest of this paper is organized as follows. Section 2 presents the overview of various Schemes to reduce storage overhead in key pre-distributions in WSN .Section 3 describes schemes in detail. Section 4 gives the overhead analysis and the conclusion in Section 5.

II. OVERVIEW OF THE SCHEMES TO REDUCE STORAGE OVERHEAD IN KEY PRE-DISTRIBUTION IN WSN

In this section, we elaborate on the Schemes to reduce storage overhead. iPAK, an in situ key bootstrapping scheme for large-scale sensor networks. This scheme contains three phases: the preloading of the key space information to each service node, the keying pair acquisition between worker sensors and service sensors, and the computation of a shared key between two neighboring worker sensors [1]. A secure channel is utilized for a worker sensor to obtain keying information from a service sensor in the vicinity. The “insitu” property of iPAK significantly improves its scalability and greatly reduces the storage overhead of worker sensors. Furthermore, the probability of key-sharing in iPAK is much higher compared to those in under the same storage constraint. Moreover, the introduction of the computationally asymmetric channel shifts the heavy computation overhead of Rabin’s decryption [7] to service sensors, conserving the resources of worker sensors. iPAK is more favorable when high-power service nodes are available in a heterogeneous sensor network.

An improved key distribution mechanism (IKDM) for large-scale wireless sensor networks. Approach has three phases, key pre-distribution phase, inter-cluster pairwise establishment phase and inter-cluster pairwise key establishment phase [2]. Hierarchical network architecture is more suitable for large-scale wireless senor network with its better scalability and network throughput. Compared with the existing key pre-distribution schemes, IKDM scheme can achieve better network resilience against node capture attack [2].

The communication overhead of our scheme is much lower than the LEKM protocol [4] and random key pre-distribution schemes [5]. In our scheme, each sensor node only needs to store two keys in its memory regardless of the network size and density, which extremely reduces the key storage overhead for tiny sensors and makes our scheme suitable for large-scale wireless sensor networks.

A key distribution model [3] using a mobile robot for shared key broadcast in wireless sensor networks. Sensors share a master key with the mobile robot pre-deployment. Mobile robot travels through the region and distributes the keys encrypted with the master key Moreover, the authentication of the mobile element by the sensor nodes is critical for the system.

Geometry based key distribution schemes using a mobile element. In the scheme mobile robot handles all the overload of key distribution requiring minimal resources at the sensors for key management [3]. A novel identity-based random key pre-distribution scheme called the identity based key pre-distribution using a pseudo random function (IBPRF) [8], which has better trade-off between communication overhead, network connectivity and resilience against node capture compared to the other existing key pre-distribution schemes. IBPRF always guarantees that no matter how many sensor nodes are captured, the secret communication between non-compromised sensor nodes are still secure.

IBPRF scheme and its improved approach is establishing pairwise secret keys between neighboring nodes with scantling communication and computational overheads. The improved IBPRF approach further supports a large-scale sensor network for the network connectivity [8]. Through the analysis we show that the improved IBPRF scheme provides better security and lower overheads than other existing schemes.

IBPRF, which is applied for a distributed wireless sensor network has negligible computation and communication overheads for establishing pairwise secret keys between neighbor sensor nodes during the direct key establishment phase. IBPRF [8] provides perfect security against node capture and reasonable network connectivity during the direct key establishment phase. In addition, IBPRF supports addition of new sensor nodes after initial deployment efficiently compared to the existing random key pre-distribution schemes. Our second scheme which is an improved version of IBPR supports a large-scale sensor network in a hierarchical architecture.

III. DETAILED OUTLINE ON DOWNSIZING STORAGE OVERHEAD

In this section, we elaborate on the different Schemes to reduce storage overhead in Key pre-distribution.

a. iPAK:

iPAK,[1] an in situ key bootstrapping scheme for large-scale sensor networks. This scheme contains three phases: the preloading of the keyspace information to each service node, the keying pair acquisition between worker sensors

and service sensors, and the computation of a shared key between two neighboring worker sensors. A secure channel is utilized for a worker sensor to obtain keying information from a service.

A. Key Space Preloading Phase:

During the pre deployment phase [1], each service node preloads with a key space (D, G), as defined in Blom's scheme [9], an integer n, and two large primes p and q such that n = pxq Keying shares from the key space are to be disseminated to the worker sensors in the vicinity after deployment through a computationally asymmetric channel protected by p and q based on Rabin's public Cryptosystem [7]

B. Keying Pair Acquisition Phase:

A public-key-assisted key exchange protocol to establish a secret key K between a worker sensor and a service sensor. Since worker sensors [1] are supposed to operate for years, whereas service nodes can die after their duty is complete, cryptographic algorithms that shift a large amount of the computation overhead to the service node are preferred.

C. Secure-Session Establishment:

Each service sensor broadcasts n, announcing its existence to worker sensors within one T0-hop away (called forwarding bound) [1].Note that the hop count T0is a design parameter that greatly affects the performance of the scheme in terms of key sharing probability and storage overhead. After receiving an announcement from a service node I, a worker sensor picks Ks and computes. Ks are the shared key between the worker sensor and the service sensor.

a. Improved key distribution mechanism (IKDM):

Focus on large-scale wireless sensor networks with the same three-tier hierarchical architecture in [2]. Illustrated by Fig. 1 our network model has three different kinds of wireless devices; sink node/base station (BS), cluster head node (CH) and sensor node (S). Cluster head node (CH): Cluster heads have considerably more resources than sensors. Equipped with high power batteries, large memory storages, powerful antenna and data processing capacities, cluster heads can execute relatively complicated numerical operations and has much longer radio transmission range than sensor nodes.

Base station (BS): Sink node is the most powerful node in a wireless sensor network, it has virtually unlimited computational and communication power, unlimited memory storage capacity, and very large radio transmission range which can reach all the nodes in a network.

Sensor node (S): Sensor nodes are inexpensive, limited-capability, generic wireless devices in this paper. Each sensor has limited battery power, memory size, data processing capability and short radio transmission range

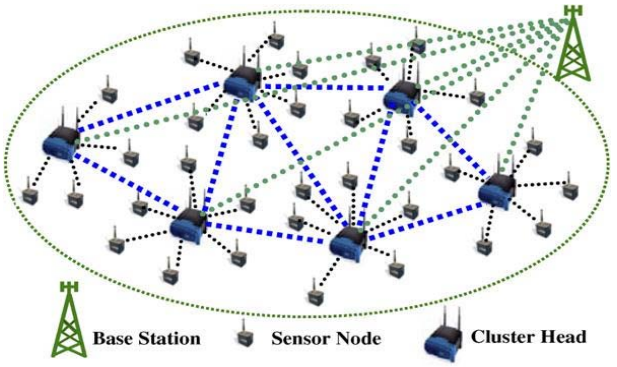

Figure. 1. A three-tier hierarchical wireless sensor network Architecture

This approach has three phases, key predistribution phase, inter- cluster pairwise establishment phase and inter-cluster pairwise key establishment phase. [2]

b. Key distribution model using a mobile robot:

A key distribution model [3] using a mobile robot for shared key broadcast in wireless sensor networks. Sensors share a master key with the mobile robot predeployment. Mobile robot travels through the region and distributes the keys encrypted with the master key. Key management with minimal overhead on the sensors.Most of the overhead of key management is handled by the mobile element. Adaptation of μTESLA [10] in order to support authentication for the mobile element efficiently. Geometry based distribution of keys to sensors. The mobile element's broadcast range does not cover all of the sensors; instead it covers only a small portion of all sensors. Therefore, the sensors which are far away from the mobile element suffer from computational overhead more than the nodes close to the mobile element do.

D. Authentication Mechanism:

An authentication mechanism is required for the communication between the mobile element and the sensors during key broadcasts. Without authentication, any node can pretend to be the mobile element. Our authentication mechanism is based on μTESLA [11] which makes use of symmetric key techniques.

a. identity-based random key pre-distribution scheme:

The bootstrapping protocol for the random key predistribution schemes [8] incurs much more communication overhead for establishing direct pairwise keys between sensor nodes in a sensor network. Thus, more communication overheads make the resource-constrained sensor networks to spend more energy consumption.

Our main goal is to design an energy-efficient protocol which will substantially reduce communication and computational overheads for establishing direct pairwise keys between neighbor sensors during direct key establishment phase of the bootstrapping. In order to achieve this goal, A new scheme called the identity based key pre distribution using a pseudo random function (IBPRF) [8] in a distributed static wireless sensor network (DWSN). Assume that sensor nodes are static after deployment in a target field.

IBPRF has the following interesting properties: There is negligible amount of communication over-head during direct key establishment phase for establishing direct

pairwise keys between sensors [8]. There is negligible amount of communication overhead during the addition of new sensor nodes. IBPRF is perfectly resilient against node capture. This means that no matter how many sensor nodes in the network are captured, the non-compromised sensor nodes communicate with each other with 100% secrecy.

E. Distributed wireless sensor networks:

A distributed wireless sensor network (DWSN) is shown in Figure 2.There is no fixed infrastructure and network topology is not known prior to deployment of the sensor nodes in the target field. Sensor nodes are usually deployed all over the target area randomly. After deployment sensor nodes form an infrastructure-less multi-hop wireless communication between them and data is routed back to the base station. Data flow in DWSN is similar to data flow in HWSN with a difference that network-wise (broadcast) flow takes place by every sensor node in the network.

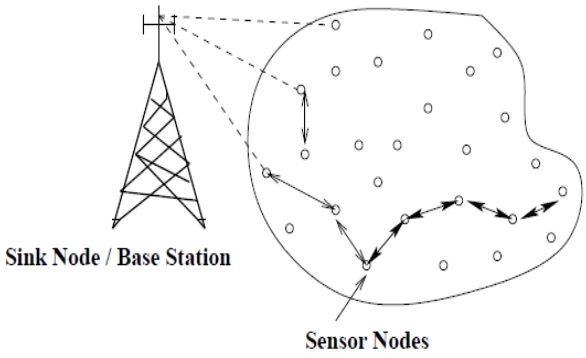

Figure 2: A distributed wireless sensor network (DWSN) architecture

The different phases in the scheme are Key Pre-distribution Phase, Direct Key Establishment Phase and Path Key Establishment Phase. IBPRF scheme [8] which achieves better network performances in the network so that (1) the storage overhead in each sensor node is small and fixed no matter how the sensors are deployed and (2) no extra communication overhead is introduced during the addition of new sensor nodes

IV. OVERHEAD ANALYSIS

A. Communication overhead & Storage overhead:

The communication overhead of a worker sensor [1] arises from two sources: the secret-key exchange and the shared key discovery. Note that the communication overheads of the service sensors are not considered because they are sacrifices. Localized key bootstrapping algorithm for shared-key establishment and the “inset” property of iPAK significantly improves its scalability and greatly reduces the storage overhead of worker sensors. iPAK [1] can achieve a very high key-sharing probability with low storage overhead. iPAK introduces a reasonable amount of storage overhead in worker sensors, but achieves a high key-sharing probability between neighbors.

In IKDM [2] each sensor only stores two keys in its memory and its handshaking message is much shorter than previous schemes, which reduces the communication overhead significantly in the network initialization phase. IKDM scheme is based on the polynomial share calculation; there is no additional key re-assignment and re-distribution operations needed when new sensors are joined into an existing network. By just pre-loading two keys into the new sensors with the same procedure in the key pre-distribution phase, fresh nodes can be easily deployed into an existing network to join a particular cluster. Sink node does not need to re-exchange key information with cluster heads, which extremely reduces the communication overhead in the network. Each sensor node only needs to store two keys in its memory regardless of the network size and density, which extremely reduces the key storage overhead for tiny sensors and makes our scheme suitable for large-scale wireless sensor networks.

Mobile robot [3] handles all the overload of key distribution requiring minimal resources at the sensors for key management. Key distribution that guarantee two neighboring nodes share a key and we provide heuristics based solution when sensor node locations are known.
IBPRF scheme which achieves better network performances in the network so that (1) the storage overhead in each sensor node is small and fixed no matter how the sensors are deployed and (2) no extra communication overhead is introduced during the addition of new sensor nodes.IBPRF has the following interesting properties: There is negligible amount of communication overhead during direct key establishment phase for establishing direct pairwise keys between sensors. There is negligible amount of communication overhead during the addition of new sensor nodes.

V. CONCLUSION

In this paper, we have proposed four approaches to reduce storage overhead in key Pre-distribution in WSN. iPAK can achieve a high key-sharing probability between neighbouring sensors and a strong resilience against node-capture attacks at the cost of low storage overhead. Improved key distribution mechanism for large-scale wireless sensor networks guarantees that two communicating parties can establish a unique pairwise key between them. Fixed key storage overhead, full network connectivity, and low communication overhead can also be achieved by the scheme. Mobile based key distribution can provide a comprehensive key management framework since it can also aid in detection of compromised nodes and do key revocation. IBPRF scheme and its improved approach is establishing pairwise secret keys between neighbouring nodes with scantling communication and computational overheads. IBPRF scheme provides better security and lower overheads

VI. REFERENCES

[1]. L. Ma, X. Cheng, and F. Liu, “iPAK: An In Situ Pairwise Key Bootstrapping Scheme for Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 18, No. 6 pp 1-10, June 2007

[2]. Yi Cheng, Dharma P. Agrawal,” An improved key distribution mechanism for large-scale hierarchical wireless sensor networks”, Ad Hoc Networks, Vol. 5, 35–48, 2007.

[3]. Baris Tas and Ali Saman Tosun,” Mobile Assisted Key Distribution in Wireless Sensor Networks”, IEEE ICC 2011 proceedings.

[4]. W. B. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, “An application-specific protocol architecture for wireless

micro sensor networks", IEEE Transactions on Wireless Communications, vol.1, no. 4, pp. 660–670, 2002.

[5]. Chan, H., Perrig, A., and Song, D. 2003.,"Random key predistribution schemes for sensor Networks,", IEEE Symposium on Research in Security and Privacy.

[6]. Eschenauer, L. and Gligor, V. D."A key-management scheme for distributed sensor networks," 9th ACM conference on Computer and Communications Security, 2002.

[7]. Menezes, Alfred; van Oorschot, Paul C.; and Vanstone, Scott A. Handbook of Applied Cryptography. CRC Press, October 1996

[8]. Ashok Kumar Das,"Improving Identity-based Random Key Establishment Scheme for Large-scale Hierarchical Wireless Sensor Networks", International Journal of Network Security, Vol.13, No.3, pp.181–201, Nov. 2011

[9]. 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

[10]. Donggang Liu,Peng Ning," Multi-Level μTESLA: A Broadcast Authentication System for Distributed Sensor Networks,", Proceedings of the 10th ISOC Annual Network and Distributed Systems Security Symposium