International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:2, 2015

Establishing Pairwise Keys Using Key Predistribution Schemes for Sensor Networks

Y. Harold Robinson, M. Rajaram

***Abstract*—**Designing cost-efficient, secure network protocols for Wireless Sensor Networks (WSNs) is a challenging problem because sensors are resource-limited wireless devices. Security services such as authentication and improved pairwise key establishment are critical to high efficient networks with sensor nodes. For sensor nodes to correspond securely with each other efficiently, usage of cryptographic techniques is necessary. In this paper, two key predistribution schemes that enable a mobile sink to establish a secure data-communication link, on the fly, with any sensor nodes. The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's essential power. The proposed schemes are based on the pairwise key with the mobile sink, our analytical results clearly show that our schemes perform better in terms of network resilience to node capture than existing schemes if used in wireless sensor networks with mobile sinks.

***Keywords*—** Wireless Sensor Networks, predistribution scheme, cryptographic techniques.

I. Introduction

SENSOR Networks often have one or more centralized controllers called sinks. Usually many orders of magnitude more powerful than a sensor node, a sink can be mobile or localized in a fixed location. It typically serves as a gateway to other networks or data centres via a high-bandwidth communication link. Sinks can be used as a nexus to disseminate control information into the sensor network or extract data from sensor nodes.

Sensor nodes are typically limited in computation and information storage capability; highly power-constrained, and communicate over a short-range wireless interface. Thus, their sensed data must be aggregated. As a result, communication types should be either one-to-many to disseminate control commands from the mobile sink to each sensor node, or many-to-one to collect sensed data from each sensor to the mobile sink.

Security is a critical issue when sensor networks are deployed in a hostile environment where they are exposed to a variety of malicious attacks. For example, an adversary can easily capture sensors, impersonate a mobile sink, or provide misleading information. Traditional cryptographic algorithms in ad hoc networks will not be adapted to WSN in the near-term future, since battery-operated sensor nodes have low power, and both limited computation power and memory. For example, using a public-key cryptographic in a sensor network is expensive due to computation cost. Symmetric key algorithms have become the tools of choice to provide a secure, low-cost communication between sensor nodes. Many research proposals have addressed the way of setting up a (pairwise) key among the communication sensor nodes, referred to as key establishment that is required for symmetric cryptographic schemes.

Dynamic keying schemes go through the phase of rekeying either periodically or on demand as needed by the network to refresh the security of the system. In this paper, we exploit the use of either the probabilistic generation key predistribution scheme or the Q-composite scheme in conjunction with the polynomial pool-based key predistribution scheme to establish a secure link between a mobile sink and a sensor node and to improve network resilience to node captures.

First, we propose a scheme that combines the polynomial pool-based key predistribution with the probabilistic generation key predistribution scheme to establish a pairwise key between the mobile sink and any sensor node.

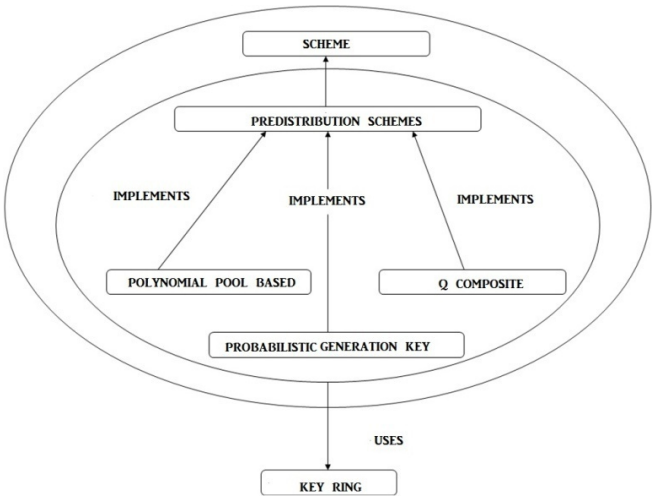

Fig. 1 Modular Structure

II. Related Work

The first key predistribution scheme [1] for sensor networks, which we will call the random key distribution scheme. In this scheme, a large pool of random keys is generated at the server prior to the network deployment. For each sensor node, the server randomly selects a subset of keys, called the key ring. Two sensor nodes that share at least one common key in their key rings are able to establish a protected

Harold Robinson Y. is Research Scholar with the Information and Communication Engineering, Anna University, Chennai, India (e-mail: yhrobinphd@gmail.com).

Prof.Dr. M. Rajaram is the Vice-chancellor of Anna university, Chennai, India (e-mail: rajaramgct@rediffmail.co.in).

connection. Nodes that cannot establish a secure link directly might engage in a key path discovery scheme [3].

Another scheme [2], the capture of a node may lead to compromising a link between two non-captured nodes since these two nodes may have used the same key to secure their communication. To decrease the little bit of compromise links between uncompromised nodes, a modification to the random key scheme, called the Q-composite scheme, is used. The authors of this scheme proposed that for two nodes to establish a secure communication link, they are required to share at least Q common keys in their key rings [4].

The common secret key is the hash of the Q common keys. [5] Proposed a probabilistic generation key predistribution scheme based on the random key distribution for heterogeneous sensor networks. Instead of generating a large pool of random keys, a key pool $|S_k|$ is represented by a small number of generation keys. It is assumed the network consists of a small number of dominant nodes, called High-end sensors, and a very large number of low-end sensors. The high-end sensors have more storage space, calculation, and storage potential. A total of CH key chains form the complete key pool $|S_k|$. The setup server assigns each L-sensor r random generation keys. From these random generation keys, r x N random keys can be calculated effectively, where $N = |S_k|/CH$. Each high-end sensor is preloaded with M randomly selected generation keys of corresponding key chains, where M » r. Threshold cryptography is another type of general network cryptographic algorithm [6]. This scheme was first proposed in and further investigated in. In this scheme, every sensor node is preloaded with coefficients of a symmetric bivariate polynomial evaluated at one of its variables using its identification value. The symmetry property of a polynomial allows every node to establish a pairwise key with every neighbor node or any node in the network evaluated at their ID values. For an adversary to compromise a communication link between two uncompromised nodes, it must capture at least a certain number of sensors to reconstruct the bivariate polynomial from its shares stored in the nodes and then break the system [7]. For a polynomial of degree t, the scheme provides unconditional secrecy if no more than t sensors collude. Liu et al. developed a general framework for pairwise key establishment based on the polynomial-based key predistribution protocol and the probabilistic key distribution. Their scheme shows that when the fraction of captured nodes is less than 60 percent, it provides a significantly higher probability for uncompromised sensors to establish secure communication links than that demonstrated in previous methods [8].

III. Overview of the Polynomial Pool-Based Key Predistribution Scheme

In this section, we briefly review the polynomial pool-based key predistribution scheme and the sensor network architecture. The key setup server randomly generates bivariate t-degree polynomials with coefficients. The polynomials have the property of f(x,y) = f(y,x).

$$f(x,y) = \sum_0^t a_{ij} x^i y^j \text{ where } a_{ij} = a_{ji} \quad (1)$$

To identify the different polynomials, the setup server may assign each polynomial a unique identification, referred to here as ID. For every sensor node u, the setup server chooses a subset of n polynomials from the polynomial pool and assigns shares of these n polynomials to node u. For each polynomial share of $f_{ID}(x, y)$, preloaded in sensor node u, the setup server performs $f_{ID}(u, y)$. For any u and v, node u computes the key $f_{ID}(u, v)$ at each of its randomly assigned shared polynomials by evaluating $f_{ID}(u, y)$ at point v. Node v can compute its key $f_{ID}(v, u)$ by evaluating $f_{ID}(v, y)$ at point u. If the two nodes can successfully establish a common key, there is no need to start path key establishment. Otherwise, sensors start path key establishment, trying to establish a pairwise key with the help of other intermediate nodes. In our sensor network architecture, we assume a typical sensor network that has hundreds to several thousand low cost, power-constrained, limited computation power and nodes with limited storage. Sensor nodes conserve communication energy by aggregating the data in their internal buffer.

In our sensor network architecture, we assume a typical sensor network that has hundreds to several thousand low cost, power-constrained, limited computation power and nodes with limited storage. Sensor nodes conserve communication energy by aggregating the data in their internal buffer. The network has a high-end mobile sink. Each sensor node is capable to store up to 210 keys; however, an MS is capable of storing up to 1,200 keys. The key establishment patterns for a secure link between a node and the MS falls into two categories: direct and indirect MS-sensor path key establishment. In the direct key establishment, the mobile sink and the sensor share at least a common bivariate polynomial and at least one common generation key. In MS-sensor path key establishment, the MS and a sensor node u try to establish a pairwise key with the help of an intermediate node i. Node i must share a pairwise key with both the MS and sensor node u. Node i randomly generates a new shared key that will be sent directly to MS and indirectly to node u over the secure path i-MS-u.

IV. Generation Key Predistribution Scheme Combined with the Polynomial Pool-Based Scheme

The basic idea of our scheme is the combination of polynomial pool-based Key Predistribution and the probabilistic generation key predistribution scheme.

Initially, the setup server separately generates two pools: a pool of $|S_p|$ random bivariate polynomials, each with a unique id, namely, ID_p and of degree t, and a pool of $|S_k|$ random generation keys each with a unique identification, ID_{gk}. Prior to network deployment, for every sensor node u, the setup server randomly picks a subset of s polynomials out of $|S_p|$ and assigns polynomial shares of these s polynomials to the sensor node. Applying the hash-based algorithm with modified algorithm, the n^{th} key using a generation key g_i, and a publicly known seed S is computed as:

$$K = Hash^{n}(S, g_i) \quad (2)$$

For the MS, the setup server picks randomly a subset of m (m >> k) generation keys out of $|S_k|$, and a subset of s polynomials out of $|S_p|$. Having a large number of generation keys in the mobile sink guarantee that MS can discover a single common generation key with a sensor with high probability. The MS can establish a pairwise data communication key with any sensor node on the fly. If the MS and a sensor node share at least one generation key and a common bivariate polynomial, the two can establish a secure data communication link directly.

A. Mobile Sink-Sensor Direct Key Establishment

In the case of establishing a secure MS-sensor link dynamically between the MS and any node u within its communication range, the MS and a sensor u need to discover that both have the polynomial containing the MS_{id} (ID_{ms}). Sensor node u within the MS range that heard the hello message can compute its keys by evaluating each of its assigned polynomial shares $f_{ID}(u, y)$ at point ID_{ms}. If the MS responds with the correct answer to at least one client puzzle, it is thus identified as having the same polynomial shares of a common polynomial.

Second, after discovering a shared polynomial between MS and the sensor node u, the MS broadcasts messages which contain a randomly generated number n where $[0 \leq n \leq C]$. After the shared polynomial and the shared generation key discoveries, a new MS-sensor data-communication link key K_d is generated as the hash of the key evaluated from the shared polynomial and the key computed from the shared generation key. MS-sensor key setup is not performed between the MS and any node if at least the two do not share a common generation key or do not have the polynomial shares of a common polynomial.

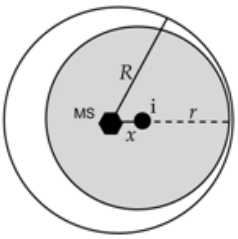

Fig. 2 Sink with MS

B. Mobile Sink-Sensor Path Key Discovery

This phase occurs between any sensor node, such as node Y and the MS. If the MS fails to establish an MS-sensor secure link directly with node Y, then it must start the MS-sensor path key discovery phase. In this phase, the MS needs to discover at least one of node's Y neighbour's that can act as an intermediate node which shares a common polynomial with the MS and a common polynomial with the destination node Y. We consider that MS can find a common generation key with the node Y with high probability (0.99). The MS broadcasts a request message, which includes two lists of polynomial IDs (one for the MS and the other for the destination node Y). If an intermediate node v receives this request message, it tries to identify the polynomials in common with the MS and the polynomials in common with the destination node Y. If node v is able to identify at least one common polynomial with the MS and one common polynomial with node Y, then node v can establish a common key with both of MS and the destination node Y to establish a pairwise key with both MS and the destination node Y. Node v replies with a message that contains two encrypted copies of a randomly generated key K_c: one encrypted by the pairwise key with the MS; the other by the pairwise key with the destination node.

C. Security Analysis

The probability p that both the MS and a sensor node u share the same bivariate polynomial is the probability can be approximated by

$$p = 1 - \frac{2s\,x\,s}{(s+2s)} \quad (3)$$

The probability q, that both MS and a sensor node u have a common generation key in their generation key rings is the probability that both MS and node u can establish a MS-sensor random key-based secure link, which can be computed as

$$q = 1 - \frac{|Sk-k|}{|Sk|} \quad (4)$$

Similar to the scheme in [8], to improve the security of the polynomial pool-based scheme and to thwart an attacker who has some knowledge of the polynomial distribution over the sensor nodes derived by compromising t + 1 nodes, we assume each polynomial be used at most t + 1 times (We count the MS as one of the t + 1 nodes). As a result, an attacker cannot recover a polynomial unless all related nodes are captured, including the mobile sink.

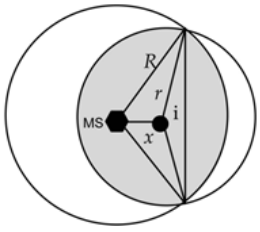

Fig.3 Sink with MS with probability key predistribution

V. Q-Composite Generation Key Scheme Combined With the Polynomial Pool-Based Scheme

The operation of this scheme is similar to that of the previously proposed scheme, differing only in that several number of generation keys overlap, instead of just one, are used to establish secure communications. This scheme is based on the Q-composite scheme and polynomial pool-based scheme to establish pairwise keys. As it was described in the previous section, a sensor node and MS can establish a

pairwise key if the two share a single common generation key and a common polynomial in their key and polynomial rings. However, in this scheme, we increase the amount of generation key overlap with the inclusion of a commonly shared polynomial between MS and a sensor node required for key setup. Q common generation keys (Q > 1) and a commonly shared polynomial are needed, instead of just one generation key and one common polynomial. By increasing the number of common generation keys, we increase the resilience of the network against node capture.

The proposed scheme is different from the Q-composite scheme. In the Q-composite scheme, to preserve a given probability of connection between two sensor nodes that share Q common keys to establish a secure link, it is necessary to reduce the size of the key pool. However, in our scheme the probability of connectivity is being preserved (q = 0:99), since the MS is initially preloaded with large number of generation keys (m >> k) and it is guaranteed to find at least Q common generation keys with a sensor node.

VI. Performance Evaluation

In the last set of simulation experiments, we want to compare the theoretical initial key ring size with the actual key ring size in a larger network when the deployment region is a unit square. Purposely, the network size is 2,500, the average density is 35, the key pool is 1,05,000, and the considered necessary connectivity is 99.9%. The theoretical initial key ring size for modified EG scheme under this parameter set up is 289. The simulation result suggests that the initial key ring size should be at least 398 for a connectivity of 99.91%. In the 2500-node case, the difference between the theoretical and simulation results is 39.5%, which is much lower than the 57.4% error for the 1000-node case. When the network size increases, the accuracy of the (asymptotic) random graph theory result improves, but the estimation error is still noticeable even when n = 10, 200 nodes.

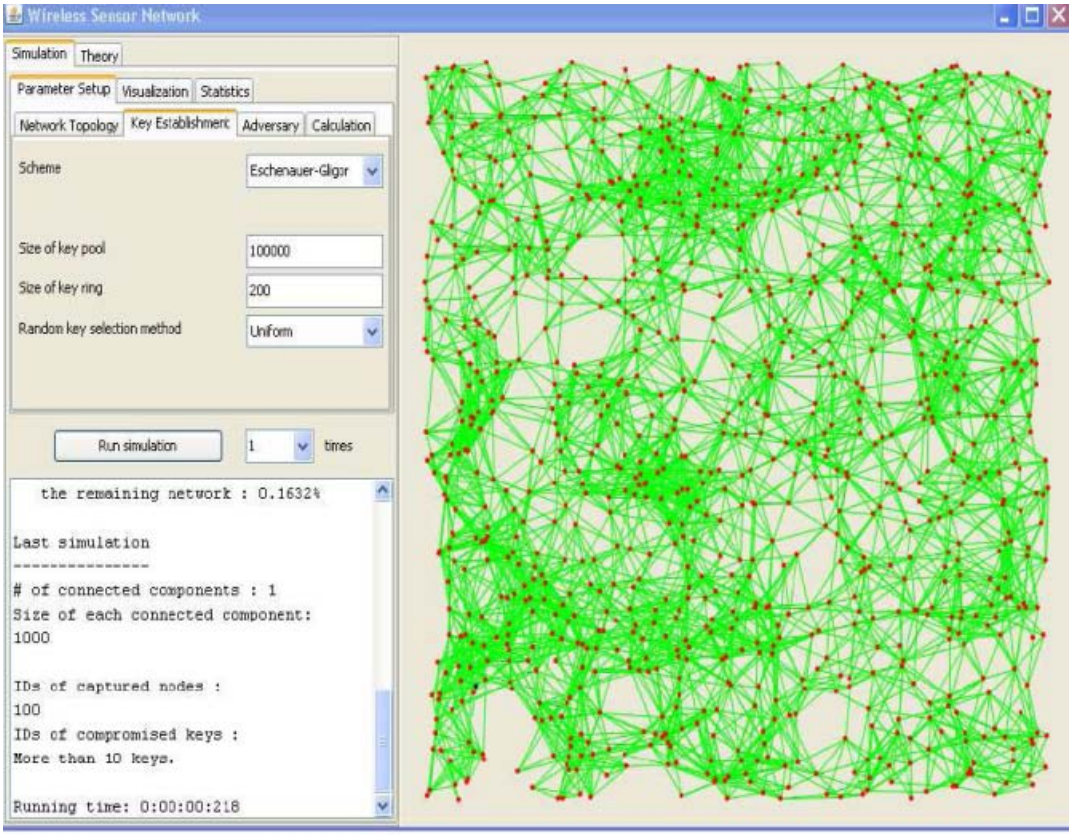

Fig. 4 Sensor nodes with 1000 nodes

VII. Conclusion

In this paper, we developed two key predistribution schemes for sensor network with mobile sink. The two proposed schemes are based on the polynomial pool-based scheme, the probabilistic generation key predistribution scheme, and the Q-composite scheme. We show that both schemes have the threshold property; i.e., they remain perfectly secure up to the capture of a certain fraction of sensor nodes. Security analyses indicate that the proposed schemes provide a higher probability for non-compromised sensors to establish a secure communication with the mobile sink than previous schemes. The schemes also provide both security and MS connectivity as the optimization criteria.

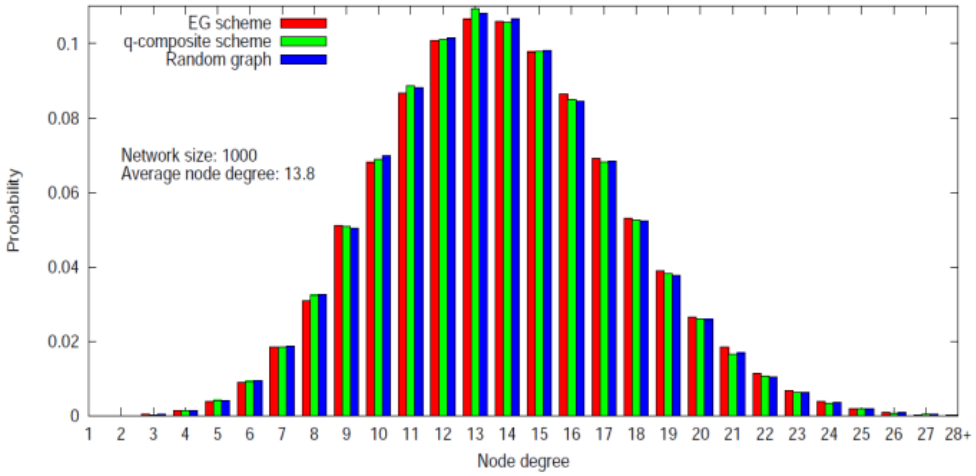

Fig. 5 Longer network with deployment

REFERENCES

[1] G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, pp. 51-58, 2010.
[2] T. Gao, D. Greenspan, M. Welesh, R.R. Juang, and A. Alm, "Vital Signs Monitoring and Patient Tracking Over a Wireless Network," Proc. 27th Ann. Int'l Conf. IEEE Eng. in Medicine and Biology Soc. (EMBS), Sept. 2009.
[3] L. Gu, D. Jia, P. Vicaire, T. Yan, L. Luo, A. Tirumala, Q. Cao, T. He, J.A. Stankovic, T. Abdelzaher, and B.H. Krogh, "Lightweight Detection and Classification for Wireless Sensor Networks in Realistic Environments," Proc. Third ACM Conf. Embedded Networked Sensor Systems, Nov. 2009.
[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2009.
[5] J. Kahn, R. Katz, and K. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," Proc. ACM MobiCom '2008.
[6] T. Small and Z. Haas, "The Shared Wireless Infostation Model—A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is a Way)," Proc. ACM MobiHoc, 2009.
[7] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D.Rubenstein, "Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with Zebranet," Proc. 10th Ann. Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2007.
[8] Amuthan Mathy.P , Gowri Sankar.U "Filtering Injected False Data in Wireless Sensor Networks by Using L, F, S Nodes and Key Distribution" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014.

Y. Harold Robinson is currently working as an Assistant Professor, Dept of CSE in SCAD College of Engineering and Technology, Tirunelveli. He finished ME degree in Anna University, Chennai. He is Pursuing his Ph.D. from Anna University Chennai. His research interests are Wireless Networks Mobile Computing, Wireless Sensor Networks. He has published several Research papers in International Journals. He has presented many papers at National and International conferences in Network Security, Mobile Computing and Cloud Computing.

Prof. Dr.M.Rajaram M.E., Ph.D. is the Vice-Chancellor of Anna University, Chennai. As a research guide, Dr.M.Rajaram produced 30 Ph.D.'s and four M.S. scholars in various fields. At present, ten research scholars are pursuing their Ph.D. under his direct supervision. He has contributed to the areas of Computer Networks, High Voltage Engineering, Measurement and Instrumentation, Adaptive Controller, Electro-Magnetic Theory, and Intelligent Computing with his 157 publications in renowned research journals, 111 research publications in International Conferences, 73 research publications in National Conferences, more than 100 technical reports and six technical books some of which he has co-authored.