Turkish Journal of Electrical Engineering and Computer Sciences

Volume 24 | Number 3 Article 23

1-1-2016

A novel key distribution scheme against storage-bounded adversaries using attack probabilities

MOHAMMAD FARHADI BAJESTANI

ALI PAYANDEH

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2016) 24: 1014 – 1021

doi:10.3906/elk-1310-73

A novel key distribution scheme against storage-bounded adversaries using attack probabilities

Ali PAYANDEH[1], **Mohammad FARHADI BAJESTANI**[2,*]
[1]Department of Information and Communication Technology, Malek Ashtar University of Technology, Tehran, Iran
[2]Department of Information Technology, University of Tehran, Tehran, Iran

Received: 08.10.2013 • **Accepted/Published Online:** 29.01.2014 • **Final Version:** 23.03.2016

Abstract: Key establishment proves to be a challenging problem in wireless sensor networks. A key establishment scheme needs to incorporate properties like scalability and energy efficiency. We propose a scheme that, besides enjoying a desirable scalability, consumes resources according to attack probability within each region. In this scheme, the distribution area is divided into regions of varying attack probability. It is assumed that the adversary is storage bounded and that not all communications can be stored by the adversary. This scheme is highly resistant to node compromises and there is an extremely low probability of discovering the key by the adversary in the case of eavesdropping. The results of probabilistic analysis and simulation analysis suggest that the scheme provides desirable efficiency and that the level of energy consumed by the scheme remains constant, regardless of changes in the size of the network.

Key words: Storage-bounded model, key distribution, wireless sensor networks, attack probability

1. Introduction

Wireless sensor networks (WSNs) are weak equipment that, without a definite infrastructure, together forms a network. Such equipment is commonly distributed in irregular patterns bereft of protection and hence directly exposed to attacks [1].

One of the major security issues in WSNs concerns key establishment, since other security services like authentication and confidentiality rely on a secure key for communication. The links between sensor nodes and aggregation nodes are assumed to be secure. Here, to ensure confidentiality of the traffic between sensor nodes and aggregation nodes, an appropriate key distribution mechanism should be employed [2]. In designing an appropriate key distribution scheme in these networks, energy consumption, computing power, and memory storage need to be taken into consideration.

In the present study, the storage-bounded model [3] is used. It is typically assumed that the adversary is able to eavesdrop on all radio communications. We, however, suggest that this may not hold true in all cases. Due to the limited coverage area of a sensor, its poor radio quality, or the adversary's engagement with another sensor, the adversary cannot pick up all the messages exchanged by sensors. It is conceptually assumed that the adversary is storage bounded; thus not all communications can be stored by the adversary [4].

Drawing on the storage-bounded model, a method is proposed in this study that is grounded on the adversary's inability to eavesdrop communications. In order for energy consumption in a region to be proportionate to attack probability in that region, the method was designed in a group-based fashion, so that based on attack

*Correspondence: mohamad_farhadi@ut.ac.ir

probability in each region, sensors regulate algorithm parameters. In this method, a priori sensor deployment knowledge and pre-distribution are not required and key-sharing probability between two neighboring sensors is close to 1.

The remainder of this paper is organized as follows: the used metrics and notations are presented in Section 2, Section 3 reviews contributions in the field, the proposed method is introduced in Section 4, security properties of the method are discussed in Section 5, Section 6 provides a simulation to evaluate efficiency using the NS simulator, and finally the study is concluded in Section 7.

2. Evaluation metrics and notations

To evaluate the efficiency of the proposed method, as compared to other methods, four metrics were considered:

- *Security* – To evaluate the security of the method two issues were examined: key-sharing probability between two sensors and probability of eavesdropping on a shared key.
- *Storage overhead* – In sensor networks, as sensors are inexpensive and small devices, their storage space is limited. Thus the algorithms designed for such networks should function efficiently when using memory.
- *Communication overhead* – The number of broadcasted bits and the traffic imposed on the network should also be computed by algorithms with information exchange, since they exert direct effect on other functions within the network.
- *Energy* – As sensors, which are battery powered, are energy constrained, energy consumption is a major concern in WSNs. Exchanging information and performing computations drain the battery. The algorithm should be designed in a way that consumes minimum energy possible.
- *Scalability* – A change in the size of the network should not reduce the efficiency of the algorithm. The algorithm must, instead, perform well for any number of sensors.

We summarize in the Table the main symbols that we use in the remainder of this paper.

Table. Summary of notations.

N	The number of sensors in the network
η	The number of bit strings stored in sensor
σ	The ratio of shared neighboring nodes to total neighboring nodes
P	The probability of store string by each sensor
β	Repetition frequency of algorithm
γ	The probability of receiving string by each sensor
Δ	Adversary's probability of eavesdropping on bit string
S	The set of bit strings stored in each sensor

3. Literature

A variety of key distribution schemes have been thus far proposed in the sensor networks literature, a couple of which were reviewed in [4,5]. One of the preliminary methods was introduced by Blom [6], where a third party node imbeds pre-distribution symmetric matrices in sensors. As a result, both sensors could reach the secret shared key, using these matrices. Blundo et al. [7] proposed an alternative method that shares its basis with Blom's; however, in this method matrix calculations are substituted by bivariate polynomial calculations.

Yet these methods are not exclusive to WSNs. Designed primarily for WSNs, the random key pre-disposition (RKP) technique was first proposed by Eschenauer and Gligor [8]. In this method, each sensor node has a key ring consisting of randomly chosen keys from a pool of keys, which in the key pre-distribution phase, are loaded into each sensor node. Once two sensors wish to communicate, they can discover the shared key through searching common keys in their key rings.

The bulk of proposed methods like [9–12] have been products of an alteration in or a merger between the above-mentioned methods, thus mounting resistance to various attacks such as node compromise. The attack probability-based key distribution scheme [13–15] is a variant of group-based schemes that, by introducing a change in Eschenauer and Gligor's [8], applies more protections with greater efficiency [4]. In this scheme, the distribution site is divided into regions of varying attack probability. With the consideration of attack probabilities, the number of keys stored on each sensor node will be increased or decreased.

Tsai et al. [16] proposed two key establishment schemes in which it is assumed that the adversary is storage bounded and that not all communications can be stored by the adversary. In these schemes, key pre-disposition is not required. In the first scheme, there are some nodes denoted as beacons that broadcast random bits that are then randomly received and stored by each sensor. Two neighboring sensor nodes use common bit strings to establish their shared key. In this case, as the adversary is storage constrained, it cannot store all the strings and infer the shared key. The second scheme is similar to the first one with the difference that each sensor can play the role of a beacon node in the network. Our proposed scheme is comparable to the latter, though more efficient and secure.

4. The proposed scheme

We assume that sensors are randomly distributed in the network with no pre-distribution. It is further assumed that the adversary is present in the entire network with varying ability to eavesdrop in each region and so incapable of picking up all message exchanges.

In the proposed scheme, each sensor broadcasts random bit strings for its neighbors. As shown in Figure 1, any two sensors that are within communication range share at least a common node. Using bit strings received from their neighbors, the two sensors establish their shared key.

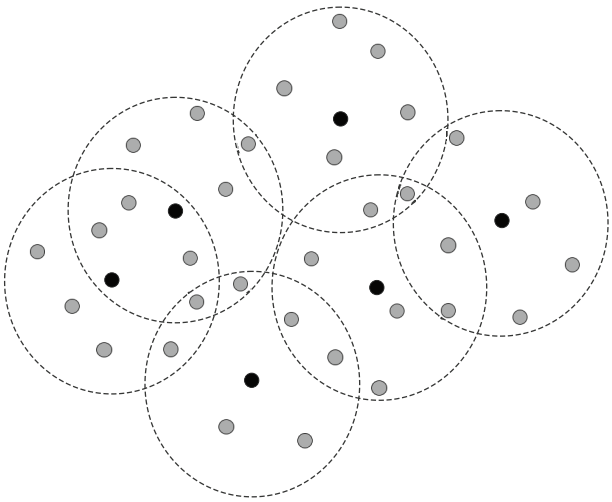

Figure 1. Deployment of sensor nodes in a field. Sensor nodes broadcasting random bits.

4.1. Method

As illustrated in Figure 2, the distribution area is divided into several regions and each sensor is deployed based on the desired security and efficiency within a particular region. Such deployment is made according to the change in potentiality of storing bit strings by each sensor in each region. Sensors that are in communication range establish the shared key (Figure 3).

0.23	0.34	0.8	0.7
0.5	0.3	0.64	0.1
0.25	0.95	0.21	0.43
0.34	0.41	0.77	0.54

Figure 2. An example of attack probability on a region.

1. Each V_i, $n > i > 0$, broadcasts bit strings within the network.
2. Each V_i, $n > i > 0$, stores received string with probability P_i.
3. Once the number of strings stored in V_i reaches η, V_i informs its neighbors.
4. Both V_i an V_j do the following.
   a. Switch sets S_i and S_j.
   b. Let $S_{ij} = S_i \,!\, S_j = \{s_1, s_2, \ldots, s_l\}$. compute $k_{i,j,\beta} = H(r_{s1}\, r_{s2} \ldots r_{sl})$, store $k_{i,j,\beta}$.
   c. Compute $K_{i,j} = (k_{i,j,1}|k_{i,j,2}| \ldots |k_{i,j,\beta})$, if $|K_{i,j}| < k$, go to 1.
   d. Erase the stored parameters from its memory.

Figure 3. Steps of establishing shared keys between sensor nodes.

The whole concept is that each sensor starts sending α random bit strings into space. Receiving bit strings from their neighbors, the sensors store them with probability p. After storing η bit strings, each sensor signals the neighbors that it has exhausted its memory storage. Once it recognizes that all neighbors have exhausted their memory storage, the sensor stops broadcasting random bit strings. If two sensors want to establish the shared key, they need to exchange their node IDs. Two sensors establish the shared key K_{ij} through combining and taking the hash of common bit strings S_{ij}.

If the number of common bit strings is small i.e. $S_{ij} < l$, the two sensors save the value in this phase, inform neighbors, and repeat the above algorithm. The two sensors repeat the process until achieving a shared key.

5. Security analysis

The security properties of the proposed scheme were evaluated on three grounds: the probability of two sensor nodes sharing a key, the probability that the adversary discovers the key in the case of eavesdropping on message exchanges within the network, and examining security advantages of the scheme over Tsai's.

5.1. Probability of establishing shared keys

There are η bit strings stored in each sensor. It is also possible that the algorithm is repeated β times until the common bit strings outnumber the minimum number possible. The existence of bit strings in the two sensors can be verified using a Bernoulli distribution (whether the string is common or not). Thus there is $\beta.\eta$ independent Bernoulli. The Chernoff bound was used to examine the probability of existing shared keys. Let X_1,...,X_n be independent random variables. They need not have the same distribution. Assume that $0 \leq X_i \leq 1$ always, for each i. Let $X = X_1 + \ldots + X_n$. Write $\mu = E[X] = E[X_1] + \cdots + E[X_n]$. Then for any $\varepsilon \geq 0$,

$$Pr[X \leq (1-\varepsilon)\mu] \leq \exp(\frac{\varepsilon^2}{2}\mu) \tag{1}$$

In the network, there is a possibility that, due to some reasons like interference, noise, or busy sensor, the broadcasted message is not received by the sensor. Therefore, this possibility needs to be considered in calculations.

In sensors i and j different parameters are considered, including the ratio of common nodes to total nodes of neighboring sensors, probability of storing a string by the two sensors P_i and P_j, and probability of receiving a string by each sensor. As a result, the probability of a common string in each examination is as follows:

$$\theta = P_i.P_j.\gamma.\sigma e^{-k/4} \tag{2}$$

Suppose that each bit string is X_i and consider $E(X_i) = \theta$, $0 < i < \beta.\eta$; then we would have $E(\sum_{i=1}^{\beta.\eta} Xi) = \theta.\beta.\eta$. If the value of 2k is considered the average number of common keys (mathematic expectation), then algorithm loop count is $\beta = \frac{2k}{\eta\theta}$. Through the use of the Chernoff bound technique, the probability that the number of common bit strings between sensors v_i and v_j is smaller than k is as follows:

$$Pr(S_i \cap S_j < k) = e^{-k/4} \tag{3}$$

If the two sensors have properties of $k = 128$, $\eta = 200$, $P_i = P_j = 0.8$, $\gamma = 0.98$, and $\sigma = 8/10$, then the probability of an existing common string is $\theta = 0.49$, algorithm loop count $\beta = 3$, and the probability that the number of common bit strings between sensors is larger than $k = 128$ would be equal to $1\text{-}e^{-k/4} \approx 1$.

5.2. Probability for the adversary to discover the key

To calculate the probability of discovering the key, it is supposed that all bit strings broadcasted by common neighbors of the sensors v_i and v_j (that result in establishing a shared key between the two sensors) are sent from a single source. We suppose that the adversary can receive $\tau = \delta\alpha$ out of α random bit strings. Then, using the Chernoff bound technique, the probability of discovering the key by the adversary can be calculated. The following lemma presents this calculation. Here, set B refers to common bit strings between sensors v_i and v_j, and its length is $l = 2k$:

Lemma ([16]): Let A be a fixed subset of $\{1, 2, \ldots, \alpha\}$ with $|A| = \tau$ and B, $|B| = l << \tau$, a multisubset randomly chosen from $\{1, 2, \ldots, \alpha\}$ with replacement. It holds that

$$Pr[|A \cap B| \geq (\delta + \varepsilon)l] \leq e^{-l\varepsilon^2/(3\delta)} \tag{4}$$

If $k = 128$, $\delta = 3.5$, and $\varepsilon = 1.4$, then we will have

$$Pr[|A \cap B| \geq (17/20)l] < e^{-8.8}$$

Under such conditions, the adversary will not have (1-δ-ε)1 $\approx$ 38 common bit strings between two neighbor sensors and the probability that it knows more bit strings will be $e^{-8.8}$.

Unlike the method proposed by Tsai [16], in which the value of δ is constant, in our proposed scheme this value is associated with the probability of key storing in sensors (P_i). The higher the probability of key storing in a region, the heavier the traffic in that region, thus the more limited the ability of the adversary to eavesdrop. As a result, given the segmentation of the sensing region, it is possible to reduce the value of P in each region that is more likely to be attacked by the adversary.

In the Tsai method [16], the adversary could pick up the entire bit strings through compromising the beacons (nodes that broadcast bit strings) or forging their identity. In our proposed method, however, this is done by all sensors, preventing the adversary from sending fake bit strings. Further, although in the Tsai method the adversary could sit on the beacon and eavesdrops on all messages sent by the beacon, this is not the case in our method.

6. Simulation and efficiency

The proposed method was simulated using the NS2 simulator, the results of which were used to evaluate the method. The following is an analysis of the results in terms of different parameters, including storage overhead, communication overhead, energy consumption, and scalability.

1) Storage overhead: The space needed by the method in each algorithm run is η and after running the algorithm the values in the algorithm are cleared. Based on the simulation results, storage overhead in the method will be O(1).

2) Communication overhead: Communication overhead in this method will not change as the number of sensors within the system changes. It will also undergo a minor change as the network density changes (increase or decrease in the number of neighboring sensors). Communication overhead in this method is directly related to the probability of key storing in each region. As the key sharing probability is decreased, the sensors need to distribute more bit strings. Figure 4 illustrates the changes in the degree of information exchange according to the key storing probability. As shown in the figure, each sensor stores up to 200 bit strings. Here the graph shows the number of packets sent by a senor with varying probabilities. According to applied segmentation, through increasing the storing probability in regions that are less likely to be attacked, a lighter traffic can be imposed. The number of packets sent in each region can be achieved by computing $(\frac{\eta}{p}).\gamma n'$. As the number of broadcasts increases, the probability of receiving broadcasted information (γ) is slightly decreased. This is primarily due to the fact that sensors broadcast a large number of packets in a nonconnection-oriented manner in a short time, which causes interference.

3) Energy consumption: Evidently, the transmitter is one of the most energy-consuming apparatuses in sensors. Energy consumption in this method is thus dependent on the number of broadcasts within the network [17]. Consequently, it can be inferred that energy consumption is also directly related to the key storing probability (p). Figure 5 shows the level of energy consumption in a sensor according to different attack probabilities. As shown, as attack probability increases, energy consumption goes up. Unlike Tsai's method in which energy consumption is the same in the entire network, in our method, considering the segmentation of the sensing region, in case where high security is not required, the number of broadcasts

can be reduced by increasing the value of p (storing probability), thereby reducing power consumption. Yet a further possibility is that based on the attack probability and power level of their batteries, the sensors could appropriately tune the algorithm to prolong the network lifetime.

4) Scalability: Given the issues discussed above, it can be observed that in the method none of the mentioned parameters (storage overhead, communication overhead, and energy) is related to the number of sensors and that the values of the parameters are constant regardless of the number of sensors. It is thus safe to say that the method is not limited in terms of scalability. Moreover, the simulation yielded uniform results and an increase or decrease in the number of sensors did not bring about any change in the efficiency of the algorithm.

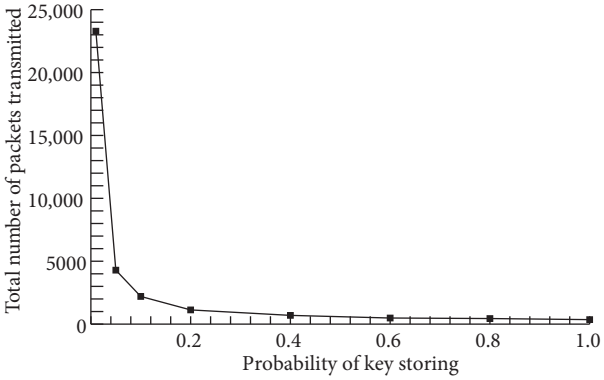

Figure 4. Total number of packets transmitted in each loop according to the key storing probability.

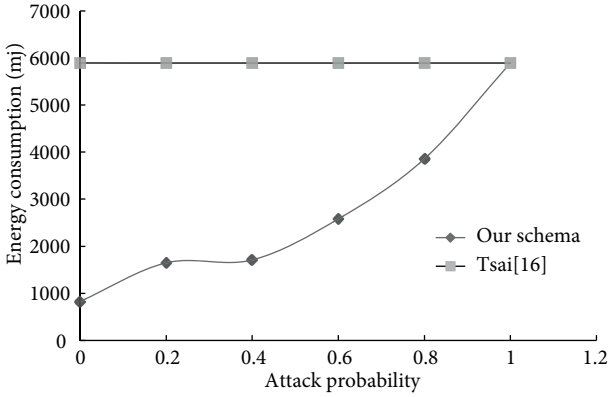

Figure 5. Energy consumption according to the attack probability.

7. Conclusion

This paper proposes a novel location-based key distribution scheme. Based on the storage-bounded model and segmentation of distributing regions, the scheme offers desirable efficiency with a high degree of security. It was shown that the scheme is resistant to node compromises and that there is an extremely low probability of discovering the key in the case of eavesdropping. Drawing on these properties, this will be an efficient key distribution scheme in WSNs.

References

[1] Yavuz A, Alagoz F, Anarim E. A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption. Turk J Elec Eng & Comp Sci 2010; 18: 1-21.

[2] Bahsi H, Levi A. k-anonymity based framework for privacy preserving data collection in wireless sensor networks. Turk J Elec Eng & Comp Sci 2010; 18: 241-271.

[3] Cachin C, Maurer U. Unconditional security against memory-bounded adversaries. Security and communication networks In: Advances in Cryptology-CRYPTO'97; 17–21 Aug 1997; Heidelberg, Germany: Springer. pp. 292-306.

[4] Chen C, Chao H. A survey of key distribution in wireless sensor networks. Security and Communication Networks 2011; 7: 2495-2508.

[5] Zhang J, Varadharajan J. Wireless sensor network key management survey and taxonomy. J Netw Comput Appl 2010; 33: 63-75.

[6] Blom R. An optimal class of symmetric key generation systems. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT); Jan 1985; Heidelberg, Germany: Springer. pp. 335-338.

[7] Blundo C, Santis AD, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-secure key distribution for dynamic conferences. In: Proceedings of the 29th International Cryptology Conference (CRYPTO); Jan 1993; Heidelberg, Germany: Springer. pp. 471-486.

[8] Eschenauer L, Gligor V. A key-management scheme for distributed sensor networks. In: Proceedings of the Annual ACM Computer and Communications Security (CCS); Nov 2002; New York, NY, USA: ACM. pp. 41-47.

[9] Deng J, Han YS. Babel: using a common bridge node to deliver multiple keys in wireless sensor networks. In: Proceedings of IEEE Global Telecommunications Conference (GLOBECOM); 26–30 Nov 2007; Washington, DC, USA: IEEE. pp. 161-165.

[10] Zhang W, Tran M, Zhu S, Cao G. A random perturbation-based scheme for pairwise key establishment in sensor networks. In: Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc); 9–14 Sep 2007; Montreal, QC, Canada: ACM. pp. 90-99.

[11] Yu C, Lu C, Kuo S. Noninteractive key establishment scheme for sensor networks. IEEE T Inf Foren Sec 2010; 5: 556-569.

[12] Fan X, Gong G. LPKM: a lightweight polynomial-based key management protocol for distributed wireless sensor network. LCIS Soc Infor Telecommun Eng 2013; 111: 180-190.

[13] Chan S, Poovendran R, Sun M. A key management scheme in distributed sensor networks using attack probabilities. In: IEEE Global Communications Conference, Exhibition & Industry Forum (Globecom); 28 Nov–2 Dec 2005; St. Louis, MO, USA: IEEE. pp. 5-12.

[14] Rezaeirad M, Orooji M, Mazloom S, Perkins D, Bayoumi M. A novel clustering paradigm for key pre-distribution: toward a better security in homogenous WSNs. In: Consumer Communications and Networking Conference (CCNC); 11–14 Jan 2013; Las Vegas, NV; USA: IEEE. pp. 308-316.

[15] Yu C, Li C, Lu C, Kuo S. An application-driven attack probability-based deterministic pairwise key pre-distribution scheme for non-uniformly deployed sensor networks. International Journal of Sensor Networks 2011; 9: 89-106.

[16] Tsai S, Tzeng W, Zhou K. Key establishment schemes against storage-bounded adversaries in wireless sensor networks. IEEE T Wirel Comm 2009; 8: 1218-1222.

[17] Lee H, Lee K, Shin Y. An Enhanced Key Distribution Scheme for the Energy Consumption and the Security in the Wireless Sensor Networks. In: 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT); 19–23 July 2010; Seoul, Korea: IEEE. pp. 157-160.