



6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8
December 2017, Kurukshetra, India

An attack model based highly secure key management scheme for wireless sensor networks

Priyanka Ahlawat*, Mayank Dave

*Department of Computer Engineering
National Institute of Technology, Kurukshetra Haryana*

Abstract

Wireless sensor network (WSN) security is a critical issue due to its inherent characteristic and unattended operation which makes it vulnerable to many attacks. Key management plays a fundamental role for providing security services to such networks. In this paper, we aim to reduce the node capture impact by incorporating an efficient adversarial model for cellular model of WSN. The adversarial model exploits several vulnerabilities present in the network such as high node density, placement of the sink node, neighbour influence factor to compute the compromise probability of each cell. It then defines the hash chain length for each cell with different rekey interval to increase the network resistance against node capture attack. The proposed scheme is compared with other existing schemes in terms of the probability of key compromise and the number of links rekeyed. The results confirm its effectiveness in increasing the WSN security.

© 2018 The Authors. Published by Elsevier B.V.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications.

Keywords: Wireless sensor network; Rekeying; Key management scheme; Attack model; Node capture attack

* Corresponding author. Tel.: 01744233479 fax: +0-000-000-0000 .
E-mail address: priyankaahlawat@nitkkr.ac.in, mannpammy@gmail.com

1. Introduction

Wireless Sensor Networks (WSN) are composed of small, resource constrained sensors placed in hostile environments, thus are very susceptible towards node capture attacks. In such attacks, adversary captures the node and steal the secret keying information from it. Thus, to provide secure communication even in presence of adversary is a challenge in WSN security[1]. Key management scheme (KMS) plays a very fundamental role in providing security to networks. It is defined as a set of mechanism that support any ongoing communication between valid nodes. These sensors find enormous applications in the areas of battlefields, wild life monitoring, fire detection, medical applications like patient monitoring and tracking, smart environments, traffic surveillance, flood detection etc.[2] In this paper, a highly secure key management scheme based on efficient adversarial model is proposed. Attacker is assumed to be intelligent and tend to capture minimum number of nodes to destroy the complete network traffic. In the proposed scheme, compromise probability of each cell is computed and then, a hash chain is created based on it [3]. We aim to assign the hash chain length of a cell based on the security requirement of that network.

This paper is organized as follows: In Sect. 2, we briefly discuss the related existing key predistribution schemes in WSNs. Sect. 3 discusses proposed scheme. The performance analysis of the proposed scheme with other schemes is presented in Sect. 4. Finally, we conclude the paper in Sect. 5.

2. Background Study

A number of KMSs are proposed in the literature for WSN. It plays a very important role in providing confidentiality, integrity of ongoing communication between the nodes. The earliest scheme was proposed by Eschenaur and Gligor for homogenous networks [4]. In this scheme, key distribution server (KDS) assigns equal number of keys to every node in the network. Neighboring nodes can only communicate when they have at least one common key in their key ring. It was further enhanced by Chan et al where instead of sharing one key, nodes share at least q keys to establish a secure connection [5]. Du et al. [6] presented a deployment based KMS where the adjoining nodes share more keys than other non adjacent nodes. Requirement of prior deployment knowledge limits its use in many practical applications. Hash based mechanisms are used in [7-11] to enhance the security of the network. Authors in [7] applied hashing based on node identifiers value. It is shown that it has improved performance in terms of resilience against node capture, computation overhead and communication overhead. A scheme with two hash functions is presented in [8] in which a 2 dimensional hash chain is produced to increase its security. A large number of adversarial models are presented in [12-21]. These are broadly classified as system theoretic analysis, epidemic theory, probability analysis method, vulnerability evaluation method and graph theory. These models assume that adversary is intelligent and has bounded potential. Attack model using sink as a factor are given in [20-21]. A rekeying approach is discussed in [22]. A hybrid KMS is presented in [23] to increase the security of KMS. A matrix based attack modeling is presented in [24-25] to increase the destructiveness of attacker.

So far, most of key management schemes are designed independent of underlying attack model. Thus, these schemes may fail in some real time applications. Even the hash based mechanism are applied without considering any attacking behavior of the adversary. The attacking pattern can be effectively used to design various counteracts in WSNs. The proposed matrix based attack model enhances the defender capability to defend against attacks before their occurrence in the system. In conclusion, there is a need to design the key management schemes according to actual security requirements. We also observe that different attack models, hash mechanisms can be effectively combined to design attack resistant KMS for WSNs.

3. An attack model based highly secure key management scheme for WSN

The attacker aims to destroy the confidentiality and integrity of the network by capturing of the nodes. In the proposed scheme, before pre-distributing the keys in the nodes, a matrix based attack model is constructed and compromise probability of every cell is then computed. The whole pool of keys is divided in to m sub key pools where m is the total number of cells. A 2-D hash chain is then created based on the compromise probability of each cell[8]. Each node of same cell is assumed to have same compromise probability. In shared key discovery, the nodes

broadcast their key identifiers along with the value of hash function. In proposed scheme, we focus on two issues that how we can increase the resistance of the system without decreasing the node connectivity.

3.1 System models

Sensor nodes are often placed in hostile environments making them vulnerable to several attacks. This section details the various models used to support the proposed scheme.

(i) Network model

The nodes are assumed to be homogenous in nature. The sink is responsible for collecting the data through various intermediate sensor nodes from the source nodes. The sensor nodes are deployed randomly in the network and the whole area is portioned in to square grid area .

(ii) Adversary model

The adversary is assumed to be intelligent and has limited number of resources. Before capturing the nodes, it exploits the various vulnerabilities of the networks. It knows the topology of the network, routing information and key identifiers[17-19]. It aims to capture the sink node so as to disrupt the whole traffic. If it is not able to capture the sink node, it will capture the nearby nodes of the sink. It tries to disrupt the whole traffic of the network with minimum number of captured nodes. It is also assumed that the adversary tends to attack more on the nodes closer to the data sink than nodes that are far away[24-25].

(iii) Random key management scheme

In this scheme, the keys are assigned to each sensor node by a KDS from a large pool of keys. The number of keys to be stored in the nodes is denoted by its key ring size. Two neighboring nodes can establish a secure communication only if they share at least one common key in their respective key rings. It consists of three phases namely key predistribution phase, shared key discovery phase and path key establishment phase. The rekeying is often performed when there is compromise of sensor nodes. This is either time based or on detection of compromised nodes by some intrusion detection system[4,5].

3.4 Computation of compromise probability of each cell

In this section, we discuss the computation of the compromise probability of each cell. For this, we create a matrix based attack model. The various assumptions taken for this model are as under [12-24]

- The communication between the nodes of the adjacent cells is more frequent than the nodes in non adjacent cells. The adjacent is defined only for first neighbouring cell only.
- Cell containing the sink well as source is more likely to be attacked by the adversary than other cells. Thus, placement of sink is a critical issue for estimating the compromise of the cells of the network.
- The compromise probability of the cells is also effected by its neighbouring cells due to the spatial temporal characteristic. This characteristic states that after attacking a cell, an attacker tend to move to its neighbouring cells. It is expressed in terms of neighbour influence factor. The cell containing sink node has highest neighbour influence factor than other cells.

After discussing the various assumptions taken for the proposed scheme, we present the various criteria taken to create the matrix based attack model. These are as under:

- (i) Placement of the sink / source the cell.
The cells containing the sink/ source are more likely to be attacked by the adversary. Thus, these cells have higher value of compromise probability than other cells[24].
- (ii) Neighbour influence factor
The cells when attacked by the adversary contributes influence to other neighbouring cells. The horizontal/ vertical neighbouring cells are more likely to be attcaked after attacked the cell than its diagonal neighbours[23,24].

The construction of the attack model starts by identifying these vulnerabilities by the network designer. The cells containing the sink node is assigned one and other cells as zero. For constructing the PS, we construct an *placement of source/sink* and it is denoted by PS which equals to $[ps_i]_{1 \times N}$. It is computed as follows:

$$ps_i = \begin{cases} 1 & \text{if cell } c_i \text{ contains the sink / source} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where, N is total number of cells of the network

After that, we create another matrix depicting *neighbour influence factor* and it is denoted by NF which equals to $[nf_{ij}]_{1 \times N}$. It is computed as follows:

$$nf_{i,j} = \begin{cases} 1 & \text{if } c_i \text{ has horizontally/vertically adjacent } c_j \text{ with sink/source} \\ 0.5 & \text{if } c_i \text{ has diagonally adjacent } c_j \text{ with sink/source} \\ 0.25 & \text{if } c_i \text{ has horizontally/vertically adjacent } c_j \text{ with no sink/source} \\ 0.125 & \text{if } c_i \text{ has diagonally adjacent } c_j \text{ with no sink/source} \\ 0 & \text{if } c_i \text{ is not to adjacent } c_j \end{cases} \quad (2)$$

To compute the compromise probability on the neighbour influence, we create another matrix using Eq. (2) as given below:

$$cnf_i = \sum_{j=1}^N nf_{i,j} \quad (3)$$

The compromise probability of each cell is computed using Eqs (1-3) as follows:

$$cp_i = cnf_i + ps_i \quad (4)$$

3.4 Key predistribution phase of proposed scheme

This phase dedicated to the key pool generation of each cell. In this phase, the keys are assigned to every node of the cell. We extend this key pool by hash chain [8]. The length of this hash chain is determined by the value of the compromise probability (CP). Two one way hash functions are used to generate this hash chain say h and h' . Fig. 2 shows the illustration of hash chain. The root of this chain is k_1 which is domain key pool. It is further extended by applying h and h' on k_1 $i-1$ times and $j-1$ times respectively. The size of chain length for a cell depends on the compromise probability of that cell. After generating the hashed key pool, we assign the these sub key pools to every cell of the network. Each cell is assigned m key chains where at least one key should be assigned to the cell. For example, sub key pool $k_1^{0,0}$ generates $k_1^{0,1}$ using h and $k_1^{1,0}$ using h' . The key information is assigned to each node of the cells which comprised of the keys along with their identifiers, chain identifiers and cell identifiers.

3.4 Link key establishment in proposed scheme

The link key establishment proceeds as follows: Suppose node X and Y wants to establish pair-wise key. Assume that each owns a key from the same key chain and X has $h^{i_x}(h'^{j_x}(k_1))$ $Y = h^{i_y}(h'^{j_y}(k_1))$. There are four cases:

1. $i_x \leq i_y$ and $j_x \leq j_y$ then node X will proceed to hash chain to get the pairwise key $h^{i_y}(h'^{j_y}(k_1))$.
2. $i_x \geq i_y$ and $j_x \geq j_y$ then node Y will proceed to hash chain to get the pairwise key $h^{i_x}(h'^{j_x}(k_1))$.
3. $i_x \geq i_y$ and $j_x \leq j_y$ then pairwise key is $h^{i_x}(h'^{j_y}(k_1))$.
4. $i_x \leq i_y$ and $j_x \geq j_y$ then pairwise key is $h^{i_y}(h'^{j_x}(k_1))$.

In conclusion, two nodes can establish the key as a pair-wise key $h^{\max(i_x, i_y)}(h'^{\max(j_x, j_y)}(k_1))$. If the nodes of neighboring cells wants to establish pairwise key, then cell identifiers has also to be taken account in addition of above procedure[7].

3.4 Rekeying in proposed scheme

In the proposed scheme, rekeying is done either when some compromised node is detected by the intrusion detection system or based on time. In time based rekeying, it is invoked timely based on compromise probability associated with a cell. We compute this probability offline based on above discussed factors and then according to the estimated threat, time of rekeying is performed. In basic rekeying scheme, there is problem of 1 affects n where one compromise of one cell affects all other nodes in a network. It should provide backward and forward secrecy. Scalability, efficiency and performance are critical issue in rekeying[22-23]. The rekey interval is defined by a function D which maps it one of the time slice based on compromise probability (cp_i) of the cell. It is given by Eq. (5)

$$rt_i = D(cp_i) = \begin{cases} t_1 & \text{if } cp_i < w_1 \\ t_2 & \text{if } w_1 \leq cp_i < w_2 \\ \dots & \dots \\ t_{n+1} & \text{if } w_n \leq cp_i \end{cases} \quad (5)$$

4. Comparative analysis of the proposed scheme

In this section, we compare the proposed scheme with other schemes based on two metrics namely probability of key compromise and the number of links rekeyed. To conceal the pre-distributed keys, the KDS applies hash based mechanisms to the stored keys. It is based on the value of compromise probability of that cell. Due to one way property of hash function, adversary is not able to recover the original keys from derivative keys. Thus, it improves the security of the network. Hash based predistribution induces some extra overhead in terms of storage of hash function and negligible amount of computation overhead. The storage overhead of the scheme depends on the amount of the memory required to store keying information in the nodes. If the size of hash function is small, then storage overhead incurred in our scheme is negligible [4]. The proposed scheme has the same key connectivity as basic RKP because the key ring size remains unaffected [4, 7,8].

(i) Probability of key compromise

During a node capture attack, adversary steals the keying information stored in nodes to mount further attacks in the network. In RKP, the capturing of a node not only reveal its own keys but also the keys of some uncompromised links[4,5]. These are nodes that use these keys as their link keys. The probability of key compromise is the probability of getting the link keys of uncompromised nodes when x nodes are captured by the adversary [8]. The probability of key compromise in basic scheme P is given as $(1 - (1 - m/k)^x)$. A link is secured by $h^{\max(i_x, i_y)} k_0$. Suppose that adversary captures by $h^{i_c i_e} k_0$. Let α be the probability that it is less than the current link key. and thus, able to obtain that key by key chaining. For any discovered key, it is initially hashed l times ($0 \leq l \leq L-1$) with a probability $1/L$. When a key is hashed, forward values can be computed where as it is impossible to compute backward values. We find that the total ' l ' choices i.e. 0 to $l-1$. It makes the total outcomes as l^3 . Hence, we have

$$1 - \alpha = \frac{\sum_{i=1}^{l-1} i^2}{l^3} \quad (6)$$

Now, the probability of key compromise in proposed scheme (m as key ring size and K as key pool size) using Eq. 6 is given as

$$P = \left(1 - \left(1 - \alpha^2 \frac{m}{|K|}\right)^x\right) \quad (7)$$

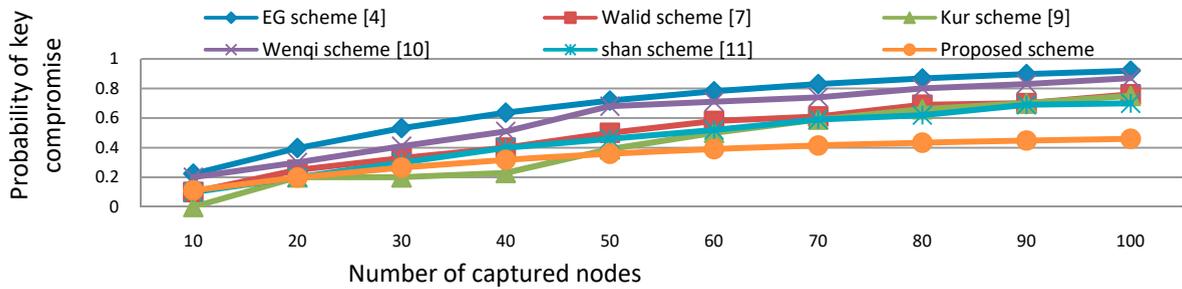


Fig. 1 Comparison of probability of key compromise for different schemes

Fig. 1 depicts the probability of key compromise for different schemes. We find that it is least in proposed scheme and maximum in EG scheme. It is due to hash chaining in the predistribution phase of the proposed scheme. Due to one way property of hash functions, capturing of derived versions does not reveal the original keys. Hence, results in least value of probability. To plot this graph, we have taken $P=800$, $k=20$, $S=100$, $q=3$, $\alpha=0.71$ ($l=10$).

(ii) Rekey overhead

The network nodes are compromised in a random order and the number of network links that are rekeyed is counted [4]

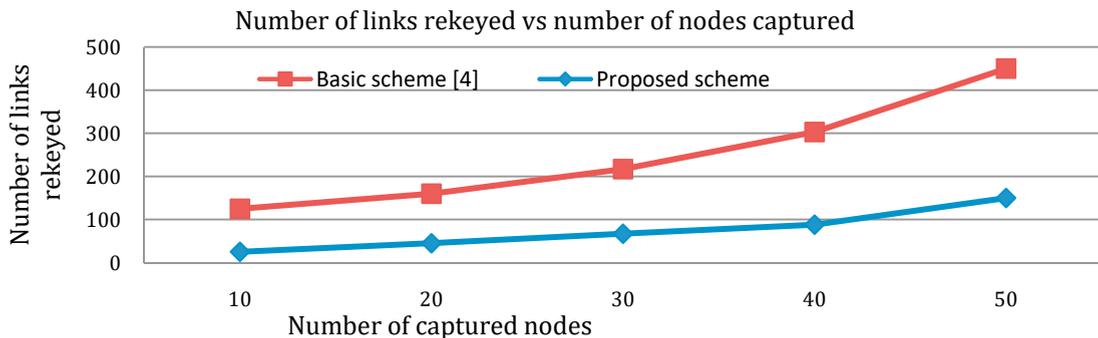


Fig. 2 Comparison of probability of key compromise for different schemes

The x-axis denotes the number of compromised nodes while the y-axis denotes the number of links that are rekeyed. As can be seen from Fig. 2, the number of links rekeyed is less in proposed scheme than basic scheme. It is due to the hash chain approach which reduces the number of nodes effected during a rekeying process. It further results in less number of links rekeyed. The one way hash property that original keys cannot be derived from derivative keys makes the adversary to get less fraction of the key pool. Hence, security is increased in proposed scheme.

5. Conclusion and Future scope

We find that considering the attacking behavior during the design of key management scheme can greatly reduce the node capture impact in WSN. This paper presents a highly secure key management scheme based on an efficient attack model for cellular model of networks. The attack model is designed based on the placement of sink in a cell and neighbor influence factor. This makes it efficient to smartly deal with node capture attacks in such networks. The hash chain key predistribution phase of the proposed scheme is computed using the estimated compromise probability of each cell. In this way, the key pool of cells that are more prone to attacks are placed at the end of hash chain. This results in least value of probability of key compromise. Further, the rekeying overhead is also reduced in

proposed scheme as number of effected nodes is least. It ultimately leads to least number of links rekeyed. The results shows that the proposed scheme is highly secure to node capture attacks. In future, we will design an adaptive way to compute the neighbor influence factor for different types of cell.

References

- 1 He, X., Neidermeier, M., Meer, H. (2013). Dynamic key management in wireless sensor network: a survey. *Journal of Network and Computer Applications*, vol 36, pp. 612-622.
- 2 Aikyildiz, I.F., Su, W., Sankarasubramanian and Cayir, E. (2002). Wireless sensor networks: a survey. *Computer Networks*, vol. 38, no.4, pp.393-422.
- 3 Zhang, J., Varadharajan. (2010). Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications*, vol 33, pp. 63-75.
- 4 Eschenauer, L., Gligor, V. (2002). A key-management scheme for distributed sensor networks. *Proceedings of 9th ACM Conference on Computer and Communications Security*, pp. 41–47.
- 5 Chan, H., Perrig, A., Song, D. (2003). Random key predistribution schemes for sensor networks. *Proceedings of 2003 IEEE Symposium on Security and Privacy*, California, USA, pp. 197–213.
- 6 Du, W., Deng, J., Han, Y. S., Chen, S., Varshney, P. K. (2004, March). A key management scheme for wireless sensor networks using deployment knowledge. In *INFOCOM 2004. Twenty-third Annual Joint conference of the IEEE computer and communications societies* (Vol. 1). IEEE.
- 7 Bechkit, W., Challal, Y., Bouadallah, A. (2013). A new class of hash chain based key predistribution scheme for WSN. *Computer Communications*, vol. 36, pp. 243-255.
- 8 Ehdai, M., Alexiou, N., Ahmadian, M., Aref, M. R., Papadimitratos, P. (2016). 2D Hash Chain robust Random Key Distribution scheme. *Information Processing Letters*, 116(5), 367-372.
- 9 Kür, J., Matyáš, V., Švenda, P. (2012, September). Two improvements of random key predistribution for wireless sensor networks. In *International Conference on Security and Privacy in Communication Systems* (pp. 61-75). Springer Berlin Heidelberg.
- 10 Wenqi Yu. A pairwise key management scheme based on hash function for wireless sensor networks, IEEE Second inter. Workshop on education technology and computer science, 2010.
- 11 T. Shan, C. Liu. Enhancing the key pre-distribution scheme on wireless sensor networks, IEEE Asia-Pacific Conf. Services Computing, IEEE Computer Society, 2008.
- 12 Mishra, A., Turuk, A. (2011). Adversary information gathering model for node capture attack in wireless sensor networks. *International Conference on Devices and Communications, ICDCom2011*, pp. 1–5.
- 13 Bonaci, T., Bushnell, L., Poovendran, R. (2010). Node capture attacks in wireless sensor networks: a system theoretic approach. *Proceedings of 49th IEEE conference on Decision and Control, CDC 2010*, IEEE, pp. 6765–6772.
- 14 De, P., Liu, Y., Das, S. (2009). Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory. *ACM Transactions on Sensor Networks*, vol. 5, no 3, pp. 1-33.
- 15 Tague, P. (2009). Identifying, modeling, and mitigating attacks in wireless ad-hoc and sensor networks. Ph.D. thesis. University of Washington, Washington, USA, 2009.
- 16 Tague, P., Slater, D., Rogers, J., Poovendran, R. (2009). Evaluating the vulnerability of network traffic using joint security and routing analysis. *IEEE Transactions on Dependable and Secure Computing*, vol.6, pp. 111–123.
- 17 Wu, G., Chen, X., Obaidet, M.S., Lin, C. (2012). A high efficient node capture attack algorithm in wireless sensor network based on route minimum key set. *Security and Communication Networks*, vol.6, pp. 230-238.
- 18 Lin, C., Wu, G., (2013). Enhancing the attacking efficiency of the node capture attack in WSN: a matrix approach. *Journal of Supercomputing*, vol. 66, no. 2, pp. 989-1007.
- 19 Lin, C., Wu, G., Qiu, T. and Deng, J. (2015). A low cost node capture algorithm for wireless sensor networks. *International Journal of Communication Systems*, DOI: 10.1002/dac.3097.
- 20 Chen, X., Makki, K., Yen, K., Pissinou, N. (2007). Attack distribution modeling and its applications in sensor network security. *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, pp. 1-11.
- 21 Yu, C-M., Li, C-C., Lu, C-S., Kuo, S-Y. (2011). An application driven attack probability based deterministic pair-wise key predistribution scheme for non uniformly deployed sensor networks. *International Journal of Sensor Networks*, vol. 9, No. 2, pp. 89-106.
- 22 Biswas, S., Haque, M. M., Rashwand, S., Mistic, J. (2009, June). Fast, seamless rekeying in wireless sensor networks. In *Distributed Computing Systems Workshops, 2009. ICDCS Workshops' 09. 29th IEEE International Conference on* (pp. 166-171). IEEE.
- 23 Ahlawat, P., & Dave, M. (2016, December). An improved hybrid key management scheme for wireless sensor networks. In *Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on* (pp. 253-258). IEEE.
- 24 Lin, C., Qiu, T., Obaidat, M. S., Yu, C. W., Yao, L., & Wu, G. (2016). MREA: a minimum resource expenditure node capture attack in wireless sensor networks. *Security and Communication Networks*.
- 25 Ahlawat, P., Dave, M. (2017). A Hybrid Approach for Path Vulnerability Matrix on Random Key Predistribution for Wireless Sensor Networks. *Wireless Personal Communications*, 94(4), 3327-3353.