Wireless Personal Communications (2019) 108:939–955
https://doi.org/10.1007/s11277-019-06442-7

Novel Approach of Key Predistribution for Grid Based Sensor Networks

Kaushal A. Shah[1] · **Devesh C. Jinwala**[1]

Published online: 3 May 2019

Abstract
Grid based sensor networks are significant for applications such as monitoring goods in a warehouse, studying traffic level of city streets, monitoring energy consumptions through smart meters deployed in a colony of houses. We propose a novel Key Predistribution Scheme (KPS) for networks where objects being monitored form a square grid. The confidentiality and integrity of the data being communicated in grid based sensor networks are critical since, compromise to the same could reveal the personal traits of the consumer and any alteration of data could yield erroneous results. On the other hand, since the deployment of such a network is on the nodes that are typically resource constrained, devising the security protocols for such networks is challenging. Our focus in this work is on designing a KPS that requires less storage in terms of number of keys and providing same level of resilience as other existing KPSs. The proposed KPS requires only 3 keys per node for providing the same level of resilience as a pairwise KPS (considered to provide maximum resilience) that requires $O(N-1)$ keys (N is the total number of nodes). To the best of our knowledge, this is the first attempt at considering linearity for designing a lightweight KPS and proposing a scheme that requires $O(1)$ keys per node, and yet offering maximum resilience in grid based sensor networks.

Keywords Grid based sensor networks · Key predistribution schemes · Key management · Resilience

1 Introduction

Symmetric Key Cryptography (SKC) is useful for providing security properties in those devices that are typically resource constrained. However, one of the issues with the SKC is the key management. Typically, in a large network, the number of keys required to be stored in the entire network is also high and may not match with the available storage in the deployed network nodes. Let us consider a scenario where thousands of sensor nodes (smart meters) are used to monitor some environmental parameters in specific surrounding. Specifically, let us consider the grid based sensor networks where the objects being

✉ Kaushal A. Shah
shah.kaushal.a@gmail.com

[1] SVNIT, Surat, India

monitored form a square grid. A few of the examples of such networks are the networks deployed:

1. to monitor goods in a warehouse,
2. to monitor and regulate traffic on city streets,
3. to monitor the electricity consumption of houses through smart meters with the houses being laid in a row by row fashion.

In all such applications and the likes, the integrity and the confidentiality of the data communicated to the base station is vital in order to preserve the application semantics. Hence, it is necessary to devise and deploy an effective security protocol that ensures these security properties. However, with the nodes used in deployment being resource constrained—in terms of the available storage, computational power, bandwidth and the energy, the design of the security protocol must ensure minimal resource overhead [1]. In addition, any security protocol deployed needs an effective key management scheme that must not impose large demands on the memory required to store the keys, while offering effective resilience at the same time. As for example, when using simple pairwise key distribution, the network resilience is very high—with the compromise of one node leading to only that part of the network being affected; however such a scheme requires the total number of keys to be stored in the network to be of the order of $O(N^2)$, where N is the total number of nodes in the network.

The goal of our work here, is to design a Key Pre-distribution Scheme (KPS) that requires comparatively lesser number of keys and provide the same level of resilience as pairwise KPS scheme. The literature in this field of KPS considered no knowledge of deployment of nodes [2–10]. However, the knowledge of the placement of nodes yields an efficient KPS as keys can be shared between those nodes that are not in the communication range. This is so, because the neighbour discovery phase is not needed and this helps in reducing the overhead in key setup phase.

The scheme that takes the advantage of deployment knowledge is discussed in [11, 12]. The KPS for grid based sensor networks is discussed in [13]. Their scheme is based on the concept of costas array [14]. The resilience of the scheme is dependent on the size of costas array. As compared, the scheme that we propose here is independent of any parameter. To illustrate, let us consider a scenario in which there is a colony of houses. All these houses are laid out in a row by row fashion as shown in Fig. 1. All the 50 houses are equipped with the devices to communicate the respective electricity consumption readings. The houses are installed with smart meters that periodically take the readings and communicate the same to the aggregator nodes (in the considered example, AG_1 is aggregator node for that region). The aggregation is used to obviously conserve the communication costs—instead of sending in N different readings, an aggregated value sent saves the bandwidth. There can be many aggregator nodes whose job is to take up the readings from the assigned region of the entire colony. Aggregator nodes finally transfer the reading to the Base Station (BS) or the control center where further processing of the received data takes place. The same scenario can be considered for other applications forming a square grid (monitoring goods in warehouse, monitoring the traffic or pollution level on city streets, etc.).

Our proposed KPS takes the advantage of linearity in the deployment of the grid based sensor networks. A linear sensor networks is defined as the network where each node has either one or two neighbours, with exception of the terminal nodes. The terminal nodes are those with just a single neighbour. The construction proposed in [15] requires 4 keys per

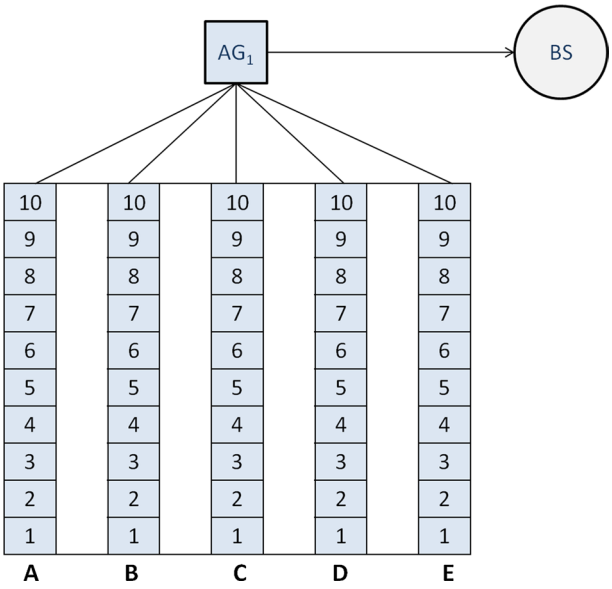

Fig. 1 Considered scenario of colony

node, whereas our proposed KPS requires 3 keys per node to provide same level of resilience. They applied their scheme only to linear sensor networks whereas we extend that idea to grid based networks. There are several applications forming a square grid network but we consider the deployment of smart grid, as it has many advantages (discussed in Sect. 2), and is widely deployed [16–18]. Such grids have generated lot of interest in the research community from the point of view of securing the same [19–21]. To the best of our knowledge, ours is the first attempt at exploiting the linearity in designing a KPS for grid based sensor networks with the storage requirement of only 3 keys per node while ensuring the same level of resilience as the other existing schemes.

The rest of the paper is organized as follows : we give a brief overview of the smart grid in Sect. 2. In Sect. 3, we discuss a brief background about the ultralight weight KPS and costas array based KPS. These schemes takes linear and grid based deployment of nodes under consideration respectively. In Sect. 4, we discuss the proposed KPS and give the mathematical proof to prove its resilience. The comparison with the existing schemes is done in Sect. 5, whereas we conclude the paper in Sect. 6.

2 Smart Grid Architecture and Significance

The entire thought of the smart grid is to have enough Information Technology (IT) knowledge to control the framework better and make it more self-sufficient and self-healing; as discussed in [22, 23]. Smart grid provides more advantages than traditional power grid as discussed in [16, 24]. The authors of [23], discuss how to tidy the conventional power framework. However, the security aspect is not considered in their work. The energy effective framework for electricity dispersion is proposed in [25]. Smart grid is also used to exploit new innovations, for example, Plug-in Hybrid Electrical Vehicles (PHEVs) [26], different types of dispersed generations, solar energy [27], smart metering [28], lighting administration frameworks, distribution robotization, and some more.

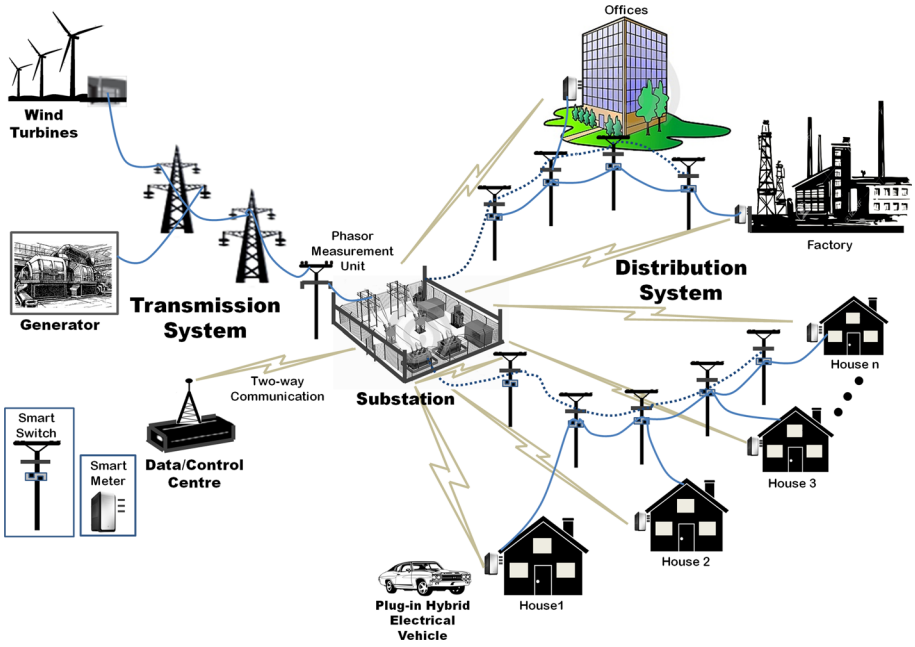

Fig. 2 Typical architecture of smart grid

The typical architecture of a smart grid is as shown in Fig. 2. As we can see from the figure, smart grid carries four main components:

i. Generation
   This component is responsible for generating the required power in a smart manner. The renewable energy generators like wind turbines can be used for the production as discussed in [27, 29].
ii. Transmission
   This component is responsible for energy-efficient transmission network that will carry the power from the bulk generation facilities to the power distribution systems as discussed in [30].
iii. Distribution
   This component is responsible for distributing power from substation to end users. The impact on distribution systems through smart grid is discussed in [31].
iv. Consumers
   The classification of this component is as follows:

- Industrial customers
- Commercial customers
- Residential customers

The consumers play a major role in smart grid through saving the energy in off-peak hours, demanding the energy in emergency and valley-filling as discussed in [32].

All these four components are related to operations, markets and service providers. The other components are HAN (Home Area Network), electrical vehicles, smart appliances,

home monitoring, etc. The communication between the smart meter hanging outside houses, offices, factory etc. (forms a HAN) and the substation is two way. The communication between data centre and substation is also two way. This allows the generation of the power to be in control and consumers to remain in constant touch with their electricity usage.

Although smart grid uses IT knowledge for the mentioned functionalities, it has some differences from IT infrastructure. Therefore, solutions applicable to IT infrastructure cannot fit directly to smart grid as discussed in [21]. The difference between smart grid and IT infrastructure is as shown in Table 1. As we can see from the table, the availability plays a major role in smart grid because if the service fails to remain available, then the entire region will face the blackout which is not accepted. Therefore, availability plays a major role in smart grid whereas it is not the first priority for IT. Privacy must be guaranteed for smart grid whereas it is optional for IT. In terms of architecture, technology and Quality of Service (QoS), smart grid and IT differs as described in the Table 1.

The data being communicated in smart grid has to be kept secret as compromise of the same can yield adverse results. There are works related with authentication and key management as discussed in [36–40]. However, the literature does not consider the constrains of smart meters like limited storage, memory, bandwidth etc., which motivates the idea of lightweight KPS. The lightweight key distribution scheme based on group ID and elliptic curve based cryptography based mechanisms are described in [41, 42] respectively. However, they do not consider the specific topology that smart grid forms. Therefore, we come up with a novel solution for lightweight KPS for the grid based sensor networks (e.g. smart grid).

3 Related Work

In this section, we discuss a brief background related with ultralight weight KPS and costas array. Moreover, we describe the KPS inspired from costas array and show how it fits to the grid based sensor networks. The ultralight weight scheme takes linear deployment of sensor nodes under consideration. Costas array based KPS takes grid based deployment of nodes under consideration. The proposed KPS is applicable to both.

3.1 Ultralight Weight KPS: Linear Sensor Networks

We first look at the construction proposed in [15] (Construction 1). The construction requires, each node to store 4 keys for getting the same level of resilience as pairwise KPS. The parameter k of the construction decides how many nodes needed to be captured by the adversary before making the network fallible (when no node from the left half of captured nodes can communicate securely with right half of the captured nodes, the network is said to be fallible). The network is said to be k-fallible if capturing $k-1$ nodes does not divide the network in two halves.

Construction 1 *Assign keys to the nodes of a linear network such that each node shares unique pairwise keys with each of the nodes at distance k and 1.*

Example 1 If Construction 1 is applied to a linear network with nine nodes and $k = 3$, then the nodes share keys as illustrated in Fig. 3. Consider each circle in the figure as nodes

Table 1 Difference between IT and smart grid

Categories	IT	Smart grid
Security aim	Confidentiality is at the highest priority	Availability is at the highest priority [33]
Privacy	Not always required	It is must [34]
Architecture	Dynamic and central sever requires more protection	Square grid or tree based and requires same level of security for deployed devices
Technology	IP based communication, works on public networks and different operating systems	Specific communication protocols, works on private networks and proprietary operating systems
QoS	Rebooting is allowed, delays are tolerated	Rebooting is not accepted, delays are highly restricted [35]

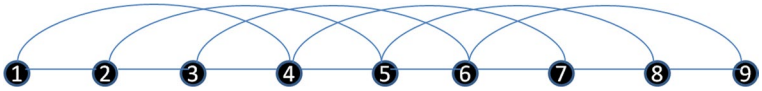

Fig. 3 Construction in which all the nodes requires 4 keys to achieve k-fallibility

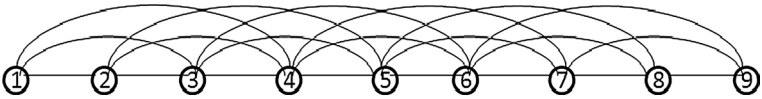

Fig. 4 Local pairwise KPS when $r = 3$

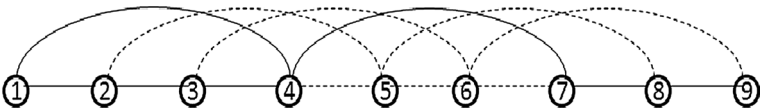

Fig. 5 After capturing 2 nodes from Fig. 4

(meters) and lines coming out of it as keys they share with other nodes. i.e. 1, 2, 3, … . represents nodes and line from 1 to 4 means nodes 1 and 4 are sharing symmetric key.

The Example 1 shows that intermediate (node number 4, 5, 6) nodes require 4 keys to have a 3-fallible network whereas local pairwise setting would require 6 keys per intermediate node as can be seen from Fig. 4. If the adversary captures lesser than 3 nodes, then there remains a secure path from left half of captured nodes to right half as can be seen from Fig. 5 (the dashed lines represent captured path, after capturing node 5 and 6 there is still a secure path from node 4–7). Therefore, in order to make the network fallible adversary has to capture one more node i.e. capture k nodes (3 for the considered example). In order to achieve k-fallibility, the local pairwise setting requires $2 * k$ number of keys whereas Construction 1 requires 4 keys per node. Our proposed KPS requires only 3 keys per node to achieve k-fallibility.

3.2 Key Pre-distribution Through Costas Array: Grid Based Networks

The KPSs for the grid based networks are discussed in [13, 43, 44]. The KPS proposed in [13] is based on Costas Array and the solution proposed in [43, 44] is based on symmetric bi-variate polynomials. We study the solution for key pre-distribution inspired from the costas array and then device a solution for the considered scenario of the colony. The (4×4) costas array is as shown in Fig. 6. The definition of costas array of order n follows:

i. Its an $n \times n$ matrix.
ii. Each entry in the matrix is either blank or a dot.
iii. Each column and row contains exactly one dot.
iv. Any two vectors (lines passing through dots with a direction) are different (difference is either a length or a direction).

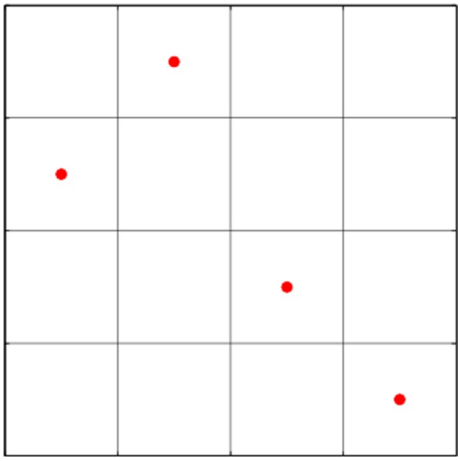

Fig. 6 Costas array of order 4

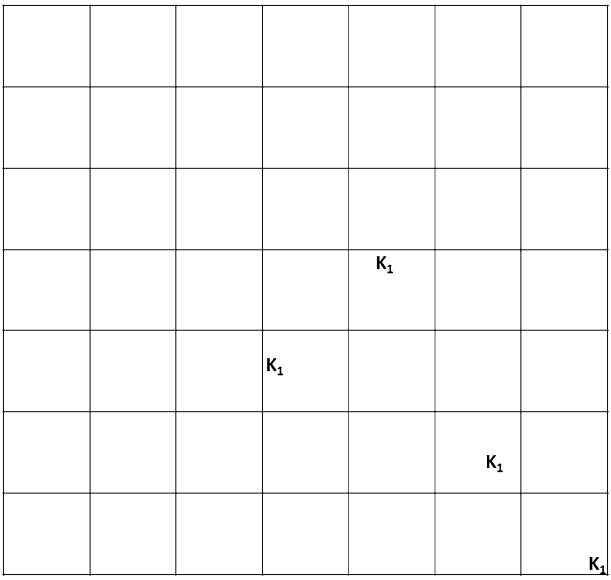

Fig. 7 Initialization of KPS through costas array of order 4

The property that makes costas array special is, the separation between any pair of dots in the matrix is not rehashed for another pair of dots. The use of costas array for key pre-distribution in grid based sensor network is given in [13]. One can start imposing costas array on a square grid of sensor nodes from any corner. Here, we consider each square shown in Figs. 7 and 8 as a sensor node (smart meter). The costas array of order 4 is used for the distribution of keys. The initialization of the KPS through costas array is as shown in Fig. 7. If we continue to apply costas array on the network of nodes, then the key predistribution is as shown in Fig. 8. We can clearly observe:

i. Each node stores exact 4 keys.
ii. Each key has been stored with 4 nodes.

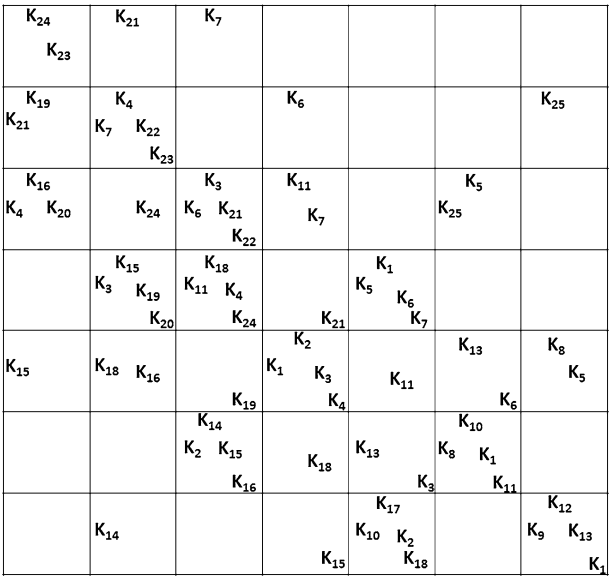

Fig. 8 KPS through costas array of order 4

The number of keys stored by nodes for the KPS shown in Fig. 8 is dependent on the size of costas array.

In the next section, we take the advantage of having a linearity in smart meters' deployment and form a KPS based on that. The number of keys stored per node is 3 without depending on any parameter. The resilience of the network is same as the other existing KPSs in the literature.

4 Proposed Key Predistribution Scheme

If we look at just a single row from the considered scenario of the colony shown in Fig. 1, we can clearly see that it forms a linear sensor network. The proposed solution for key pre-distribution provides lesser storage of keys than pairwise KPS, ultralight weight KPS, and the KPS based on costas array. Moreover, the proposed KPS is applicable to both linear as well as grid based networks. The idea is inspired from the KPS we proposed in [45]. Moreover, the proposed KPS is k-resilient. i.e. the network is $k+1$ -fallible (adversary has to capture k nodes in order to partition the network). The proposed method of key predistribution is as defined in Algorithm 1. The example of proposed KPS on network with 9 nodes and $k = 2$ is as shown in Fig. 9. As we can see from the figure, each smart meter requires at the most 3 keys whereas the ultralight weight KPS requires 4, and the KPS inspired from costas array requires the size of costas array as the number of keys. As we can see from Fig. 10, the single row of houses is considered along with aggregator node and BS and the proposed construction is applied with 11 nodes. The same when applied to the considered scenario of colony of houses forms a network as shown in Fig. 11. We assume that the BS cannot be captured. The aggregator node and the BS are considered to be resource rich as compared to the other nodes (meters) and can store more number of keys. The resilience of the proposed scheme is k (maximum number of consecutive nodes (meters) allowed to be captured) and we prove

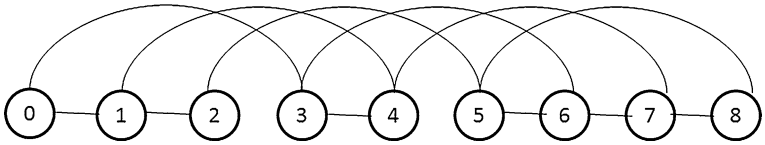

Fig. 9 Example of proposed KPS on 9 smart meters with $k = 2$

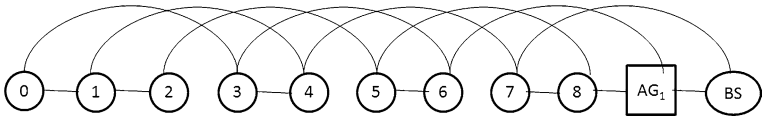

Fig. 10 Example of proposed KPS by considering a single row of grid with $k = 2$

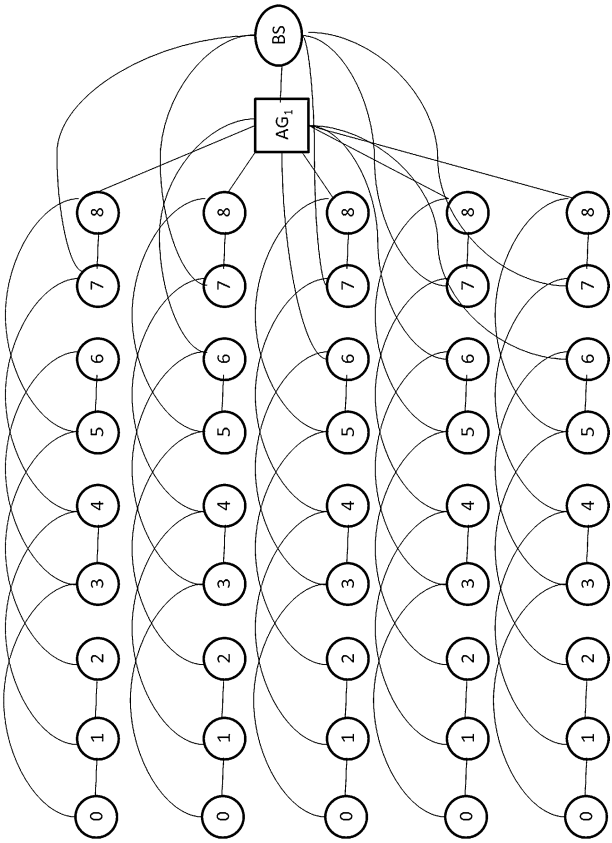

Fig. 11 Example of proposed KPS on the considered scenario of grid with $k = 2$

the same in Theorem 1. We assume no smart meters are compromised initially. Attacks on network of nodes or meters are possible after they are deployed. Attacker can be insider or outsider. The proposed scheme avoids both the kind of adversaries by providing resilience against consecutive node (meter) captures.

Algorithm 1 Pseudo-code of the Proposed Scheme

```
1: function KEY_ASSIGN(x,y)
2:     Assign pairwise keys between nodes with label x and y.
3: procedure PROPOSEDKPS(N,k)
4:     for each row of the grid do
5:         Assign labels to sensor nodes from 0 to N − 1
6:         for <i=0 to N-k-2> do
7:             call KEY_ASSIGN(i,i+k+1)
8:         for <i=0 to k-1> do
9:             call KEY_ASSIGN(i,i+1)
10:        for <i=k to N-k-1> do
11:            if (i mod 2)==1 then
12:                call KEY_ASSIGN(i,i+1)
13:            else
14:                EXIT
15:        for <i=N-k to N-2> do
16:            call KEY_ASSIGN(i,i+1)
```

Theorem 1 *The KPS of the proposed construction is k-resilient.*

Proof We prove the theorem with the help of proving the following propositions.

Setup:

The smart meters of the network are labeled from 0 to $(N-1)$, where N is the total number of meters in the network. The maximum number of consecutive meters that an adversary can capture is k.

Proposition 1 *There is a meter with label $l \in (0,k)$, so that no meter with the value $l(mod(k+1))$ is captured.*

Proof After applying the mod operation to the labels of smart meters of the network with respect to modulus $(k+1)$, $n/(k+1)$ congruent sets are produced with the same values ranging from $0, 1, \ldots, k$. The size of each set is $(k+1)$. An adversary captures k meters and they can be captured from any of the different $n/(k+1)$ sets. As the size of every set is $k+1$, after capturing k meters there is always a single meter left that is not captured. Because of the congruence all the congruent meters to that uncaptured meter are not captured as well.

Therefore, Proposition 1 holds.

Setup: There are 2 meters with labels x_1 and x_2 at distance at least $(k+2)$ from captured meter and the label of x_1 is greater than the label of x_2.

Proposition 2 *There is always a secure path from meter x_1 to x_2.*

Proof The secure path from meter x_1 to x_2 is found using following steps:

1. From meter x_1 within the same set, go towards meter x_2 with hops of length $(k+1)$ till a meter with label equivalent to $l(mod(k+1))$ is reached. If meter x_1 itself is equivalent to $l(mod(k+1))$, then no need to take any hop. These hops are secure as no captured meter lies within distance $(k+2)$ of x_1.

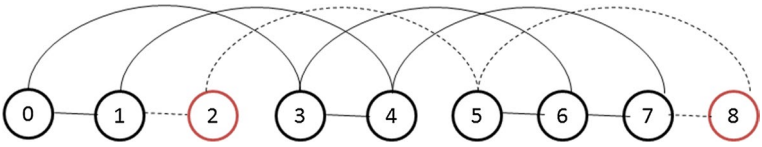

Fig. 12 Example of proposed KPS with 2 captured nodes

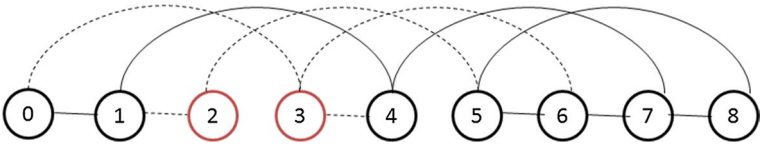

Fig. 13 Example of proposed KPS with 2 consecutive captured nodes

2. Continue applying step 1 till we reach a meter that is at distance less than $(k+1)$ from x_2.
3. Complete the path by taking hops of length 1 or $(k+1)$ until meter x_2 is reached. These hops are secure as there are no captured meters lying within the distance $(k+2)$ of x_2. Hence, we can say that no matter which k meters adversary captures, there always remains a secure connected path for the remaining meters.

Therefore, Proposition 2 holds.
Therefore, the resilience of the proposed construction is k. Hence, the Theorem 1 holds. □

Let us look at an example to understand the theorem. If we capture meters 2 and 8 from the example shown in Fig. 9, then the network looks like the Fig. 12. As we can see, there is no partition as left half of the captured nodes can communicate with right half through a secure path. E.g. 0–3, 1–4, 0–1–4–7–6–5, etc. Now, in order to take the advantage of the consecutive node capture, if adversary captures meter 3, then the network looks like the Fig. 13. As we can see, there is no partition. i.e. secure paths are still there (0–1–4, 0–1–4–7–6–5, etc.). Therefore, the proposed KPS is k-resilient. i.e. even after capturing k (2 in the considered example), the network is not partitioned in two halves.

We apply the following standard algorithm for checking the connectivity (between nodes) in an underlying graph of the proposed construction as shown in Algorithm 2.

Algorithm 2 : Algorithm for checking the connectivity of given Graph G (formed through the proposed construction)

1: **procedure** IsConnected
2: Choose an arbitrary node $'a'$ from the graph G as the starting point.
3: Determine the set S of all the nodes which can be reached from a.
4: If S is equal to the set of nodes of G, the graph is connected; otherwise it is disconnected.

The implementation of the proposed construction for verifying the connectivity between nodes is done using python language. The pseudo-code of the same is as shown below in Algorithm 3.

Algorithm 3 Pseudo-code for implementing proposed construction in python

```
procedure IsConnected(self, verticesVisited = set(), startingVertex=None):
    gdict = self.__graph_dict
    vertices = gdict.keys()
    if notstartingVertex then startingVertex = vertices[0]
    verticesVisited.add(startingVertex)
    if len(verticesVisited)! = len(vertices) then
        for vertex in gdict[startingVertex]
        if vertexnotinverticesVisited then
            if self.isconnected(verticesVisited, vertex) then return True
        elsereturn True
     return False
```

The proposed construction is implemented with different values of *N* such as 10, 20, 50, 100, 1000, 2000, 5000 and 100,000. For all the values of *N*, implementation of proposed construction shows that it remains connected. The total number of keys required for the proposed construction is calculated using the total number of edges in the underlying graph of proposed construction. The comparison of the same with other existing schemes is shown in the next section.

5 Comparison of Different KPSs

The local pairwise KPS requires more number of symmetric keys as compared to the one proposed in [15]. The proposed construction requires even lesser storage in terms of symmetric keys required and can get the same fallibility value as compared to the approach considered in [15] and in local pairwise KPS. The costas array based [13] or group ID based [41] approaches for key pre-distribution in smart grid require number of keys that is dependent on size of costas array or the way groups are formed. The scheme proposed in [43] talks about a hierarchical grid based KPS. This scheme uses symmetric bi-variate polynomials for generating keys of symmetric nature. The number of keys required to be stored per node is again dependent on *N* for the scheme proposed in [43]. Our proposed construction by considering linearity in smart meters' deployment requires just 3 keys to be stored in each smart meter. Comparison in terms of number of symmetric keys required is as shown in Table 2. For all the approaches, we considered '*N*' as total number of nodes (smart meters) in the network. The proposed KPS requires only 3 keys per smart meter in order to provide the same level of resilience as compared to other schemes. As shown in Table 2, the total number of keys required for the proposed scheme is lesser as compared to the other existing schemes.

The performance analysis on the number of symmetric keys required is shown in Table 3. This table shows the exact number of keys required for the network of *N* meters. The proposed scheme is scalable as the keys are pre distributed in the manner that handles the increment and decrement in total number of meters. As we can see from the Table 3

Table 2 Comparison of key pre-distribution schemes

KPS	Maximum No. of symmetric key required per node (meter)	Total number of symmetric keys (upper bound) required in the network with $N = 1000$
Local pair-wise scheme	$(N - 1)$	999,000
Ultra lightweight scheme [15]	4	4000
Costas array based scheme [13]	(*Size of costas array*)	1000 * (*size of costas array*)
Hierarchical grid based KPS [43, 44]	$Log_2 N$	9965
Our proposed construction	3	3000

Table 3 Total number of symmetric keys required for different ciphers

Total number of nodes ($N)	Total number of symmetric keys required				
	Pair wise KPS	Ultra light-weight KPS	Costas array (size = 4) based KPS	Hierarchical gird based KPS	Proposed KPS
10	48	40	33	32	28
20	108	80	86	72	58
50	288	200	282	192	148
100	588	400	664	392	298
200	1188	800	1529	792	598
500	2988	2000	4482	1992	1498
1000	5988	4000	9965	3992	2998
2000	11,988	8000	21,931	7992	5998
10,000	59,988	40,000	132,877	39,992	29,998

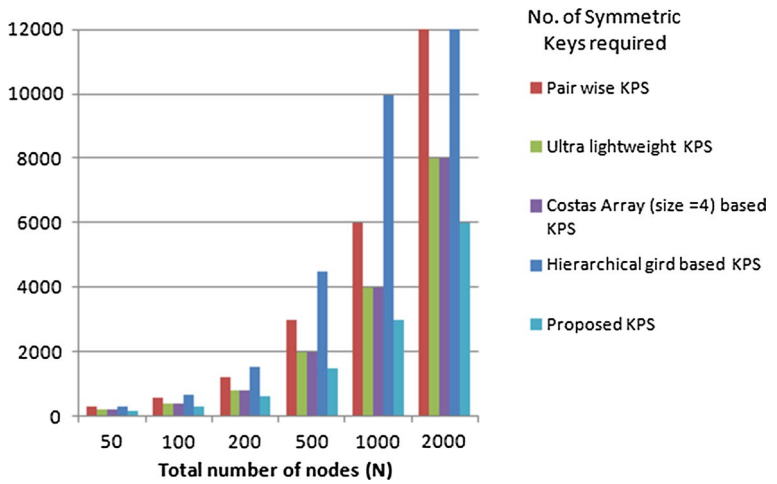

Fig. 14 Performance analysis

and the chart shown in Fig. 14, the proposed KPS requires the least number of keys as compared to the other existing schemes for providing same level of resilience.

6 Conclusions

Sharing just a single key in an entire network of nodes (smart meters) solves the purpose of security of data with very less storage requirement. However, adversary needs to capture just a single key to disrupt the entire service and compromise the security of the network. Sharing pair-wise keys with every meters gives a maximum resilience as adversary has to capture $O(N-1)$ keys, where N is the total number of smart meters in the network. However, the storage requirement is $O(N^N)$ for pair-wise key distribution. We proposed a KPS that requires constant storage i.e. only 3 keys per meter. The mathematical analysis and the associated proof shows that the proposed scheme provides the same level of resilience as pair-wise KPS with very less key storage requirement (3 keys per meter).

References

1. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, *52*(12), 2292–2330.
2. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *2003 symposium on security and privacy, 2003. Proceedings* (pp. 197–213). Washington: IEEE.
3. Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, *8*(2), 228–258.
4. Camtepe, S. A., & Yener, B. (2004). Combinatorial design of key distribution mechanisms for wireless sensor networks. In *European symposium on research in computer security* (pp. 293–308). Berlin: Springer.
5. Çamtepe, S. A., Yener, B., & Yung, M. (2006). Expander graph based key distribution mechanisms in wireless sensor networks. In *2006 IEEE international conference on communications* (Vol. 5, pp. 2262–2267). Washington: IEEE.
6. Chakrabarti, D., Maitra, S., & Roy, B. (2005). A hybrid design of key pre-distribution scheme for wireless sensor networks. In *International conference on information systems security* (pp. 228–238). Berlin: Springer.
7. Delgosha, F., & Fekri, F. (2005). Key pre-distribution in wireless sensor networks using multivariate polynomials. In *SECON* (pp. 118–129).
8. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on computer and communications security* (pp. 41–47). New York: ACM.
9. Hwang, J., & Kim, Y. (2004). Revisiting random key pre-distribution schemes for wireless sensor networks. In *Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks* (pp. 43–52). New York: ACM.
10. Lee, J., & Stinson, D. R. (2005). *A combinatorial approach to key predistribution for distributed sensor networks*. Waterloo: Faculty of Mathematics, University of Waterloo.
11. Du, W., Deng, J., Han, Y. S., & Varshney, P. K. (2006). A key predistribution scheme for sensor networks using deployment knowledge. *IEEE Transactions on Dependable and Secure Computing*, *3*(1), 62–77.
12. Shah, K., & Jinwala, D. C. (2016). A secure expansive aggregation in wireless sensor networks for linear infrastructure. In *Region 10 symposium (TENSYMP), 2016 IEEE* (pp. 207–212). Washington: IEEE.
13. Blackburn, S. R., Etzion, T., Martin, K. M., & Paterson, M. B. (2008). Efficient key predistribution for grid-based wireless sensor networks. In *International conference on information theoretic security* (pp. 54–69). Berlin: Springer.

14. Golomb, S. W., & Taylor, H. (1984). Constructions and properties of costas arrays. *Proceedings of the IEEE*, *72*(9), 1143–1163.
15. Martin, K. M., & Paterson, M. B. (2009). Ultra-lightweight key predistribution in wireless sensor networks for monitoring linear infrastructure. In *IFIP international workshop on information security theory and practices* (pp. 143–152). Berlin: Springer.
16. Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart gridthe new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, *14*(4), 944–980.
17. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., et al. (2011). Smart grid technologies: communication technologies and standards. *IEEE Transactions on Industrial Informatics*, *7*(4), 529–539.
18. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., et al. (2013). A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, *9*(1), 28–42.
19. McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security and Privacy*, *7*(3), 75–77.
20. Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, *1*(1), 99–107.
21. Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials*, *14*(4), 981–997.
22. Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18–28.
23. Amin, S. M., & Wollenberg, B. F. (2005). Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine*, *3*(5), 34–41.
24. Ipakchi, A., & Albuyeh, F. (2009). Grid of the future. *IEEE Power and Energy Magazine*, *7*(2), 52–62.
25. Masoum, M., Moses, P., & Deilami, S. (2010). Energy-efficient distribution in smart grid. In *Innovative smart grid technologies (ISGT)* (pp. 1–7).
26. Fan, Z. (2012). A distributed demand response algorithm and its application to phev charging in smart grids. *IEEE Transactions on Smart Grid*, *3*(3), 1280–1290.
27. Potter, C. W., Archambault, A., & Westrick, K. (2009). Building a smarter smart grid through better renewable energy information. In *Power systems conference and exposition, 2009. PSCE'09. IEEE/PES* (pp. 1–5). Washington: IEEE.
28. Rosenfeld, A. H., Bulleit, D. A., & Peddie, R. A. (1986). Smart meters and spot pricing: Experiments and potential. *IEEE Technology and Society Magazine*, *5*(1), 23–28.
29. Cecati, C., Citro, C., & Siano, P. (2011). Combined operations of renewable energy systems and responsive demand in a smart grid. *IEEE Transactions on Sustainable Energy*, *2*(4), 468–476.
30. Li, F., Qiao, W., Sun, H., Wan, H., Wang, J., Xia, Y., et al. (2010). Smart transmission grid: Vision and framework. *IEEE Transactions on Smart Grid*, *1*(2), 168–177.
31. Brown, R. E. (2008). Impact of smart grid on distribution system design. In *Power and energy society general meeting-conversion and delivery of electrical energy in the 21st century, 2008 IEEE* (pp. 1–4). Washington: IEEE.
32. Wang, Z., & Wang, S. (2013). Grid power peak shaving and valley filling using vehicle-to-grid systems. *IEEE Transactions on Power delivery*, *28*(3), 1822–1829.
33. NIST, U. (2010). Guidelines for smart grid cyber security (Vol. 1–3). *NIST IR-7628*
34. Locke, G., & Gallagher, P. D. (2010). *Nist framework and roadmap for smart grid interoperability standards, release 1.0* (p. 33). Gaithersburg: National Institute of Standards and Technology.
35. Wei, D., Lu, Y., Jafari, M., Skare, P., & Rohde, K. (2010). An integrated security system of protecting smart grid against cyber attacks. In *Innovative smart grid technologies (ISGT)* (pp. 1–7). Washington: IEEE.
36. Yan, Y., Qian, Y., & Sharif, H. (2011). A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid. In *2011 IEEE wireless communications and networking conference* (pp. 909–914). Washington: IEEE.
37. Vaidya, B., Makrakis, D., & Mouftah, H. T. (2011). Device authentication mechanism for smart energy home area networks. In *2011 IEEE international conference on consumer electronics (ICCE)*.
38. Xia, J., & Wang, Y. (2012). Secure key distribution for the smart grid. *IEEE Transactions on Smart Grid*, *3*(3), 1437–1443.
39. Liu, N., Chen, J., Zhu, L., Zhang, J., & He, Y. (2013). A key management scheme for secure communications of advanced metering infrastructure in smart grid. *IEEE Transactions on Industrial Electronics*, *60*(10), 4746–4756.
40. Nicanfar, H., Jokar, P., Beznosov, K., & Leung, V. C. (2014). Efficient authentication and key management mechanisms for smart grid communications. *IEEE Systems Journal*, *8*(2), 629–640.

41. Kamto, J., Qian, L., Fuller, J., & Attia, J. (2011). Light-weight key distribution and management for advanced metering infrastructure. In *2011 IEEE GLOBECOM Workshops (GC Wkshps)* (pp. 1216–1220). Washington: IEEE.
42. He, D., Wang, H., Khan, M. K., & Wang, L. (2016). Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. *IET Communications*, *10*(14), 1795–1802.
43. Mohaisen, A., & Nyang, D.-H. (2006). Hierarchical grid-based pairwise key predistribution scheme for wireless sensor networks. In *European workshop on wireless sensor networks* (pp. 83–98). Berlin: Springer.
44. Mohaisen, A., Maeng, Y., & Nyang, D. (2007). On grid-based key pre-distribution: Toward a better connectivity in wireless sensor network. In *Pacific-Asia conference on knowledge discovery and data mining* (pp. 527–537). Berlin: Springer.
45. Shah, K. A., & Jinwala, D. C. (2017). Novel approach for pre-distributing keys in WSNS for linear infrastructure. *Wireless Personal Communications*, *95*(4), 3905–3921.

Kaushal A. Shah is a Ph.D. research scholar in Computer Engineering at the Department of Computer Engineering, S. V. National Institute of Technology, Surat, India. He has received his M.E. degree in Computer Science and Engineering from Government Engineering College, Modasa, India. His research interests broadly include Information Security, Wireless Sensor Networks and Protocol designing.

Devesh C. Jinwala has been working as a Professor in Computer Engineering at the Department of Computer Engineering, S. V. National Institute of Technology, Surat, India since 1991. His principal research areas of interest are broadly Security, Cryptography, Algorithms and Software Engineering. Specifically his work focuses on Security and Privacy Issues in Resource-constrained environments (Wireless Sensor Networks) and Data Mining, Attribute-based Encryption techniques, Requirements Specification, and Ontologies in Software Engineering. He has been/is the Principal Investigator of several sponsored research projects funded by ISRO, GUJCOST, Govt of Gujarat and DiETY-MCIT-Govt of India.