NPKG: Novel Pairwise Key Generation for Resisting Key-based Threats in Wireless Sensor Network

M. Vaneeta[1] and S. Swapna Kumar[2]

(Corresponding author: M. Vaneeta)

Department of Computer Science, Engineering, K. S. Institute of Technology[1]
14, Raghuvanahalli, Kanakapura Main Road, Bengaluru, India
Department of Electronics, Communication Engineering, Vidya Academy of Science [2]
Thalakkottukara, Thrissur, Kerla, India
(Email: vaneeta.res2014@gmail.address)

(Received July 5, 2017; revised and accepted Jan. 12, 2018)

Abstract

Securing the communication system in Wireless Sensor Network (WSN) is still an open-end problem in spite of series of dedicated research work for more than a decade. This paper presents a Novel Pairwise Key Generation (NPKG) technique intended for resisting replication attacks as well as other forms of attacks that are related to secret keys in WSN. The proposed system also harness the potential role of a base station and trusted authority which otherwise represents a mock module in existing studies. Designed using an analytical method, the proposed study particularly emphasize on achieving a balance between minimal resource utilization and ultimate security feature of both forward and backward secrecy for further strengthening privacy, confidentiality, and non-repudiation in WSN. The algorithm is exclusively designed to handle the possible security issues in a dynamic network of WSN for its upcoming applications. The study outcome shows better algorithm performance in contrast to the existing system.

Keywords: Key Generation; Pairwise Key Predistribution; Security; Wireless Sensor Network

1 Introduction

The study of Wireless Sensor Network (WSN) has been consistently a major point of focus among the research community of wireless network. The usage of WSN applications has undergone revolutionary changes at present than what it was five years back [17, 19]. At present, WSN is sought as one of the contributory technology in Internet-of-Things (IoT), which is more about machine-to-machine communication [10, 23]. The conventional research-based study of WSN was in the direction of solving energy problems, routing problem, traffic management problem, security problem etc [16, 26, 27] and there are more than thousands of research papers that have discussed the solution to such problems. The present paper is focused on discussing security problems in WSN, which is an unsolved problem till date. Although there has been series of potential research on strengthening the security features of WSN [31], still none of the security protocols are found to be resistive to potential key-based threats in WSN.

Basically, the source reason for all security problems in WSN is the miniature form of a sensor node from hardware structure viewpoint. Basically, such sensor nodes are so small that they cannot be embedded with lots of complex cryptographic algorithms that run on the wired network. This is because execution of such complex cryptographic algorithm calls for heavy usage of resources that a sensor node cannot afford. It is also known that a sensor node operates on a battery, while every routing operation (where a sensor node is forwarding data packet or just in a listening mode) is associated with significant drainage of energy. Hence, usage of complex cryptographic-based operation is kind of forbidden in WSN [20, 21].

Majority of the conventional applications of WSN considers that all the nodes are static. On the contrary, the sensory application in IoT is highly mobile and uses dynamic topology. Although IoT based applications claim to support better communication performance, there is no scheme to claim for ultimate secure communication when sensors are integrated with cloud applications that are already exposed to trillions of malicious programs. An existing security-based technique that often uses symmetric key-based cryptographic approach [24] are found most suitable to work on the low-resource node but suffers from extreme overheads and higher dependencies to-

wards memory use. At the same time, the rate of scalability degrades along with declination of secure communication properties. Hence, the existing techniques of using symmetric-based approaches are definitely not appropriate to offer full-fledged secure communication in WSN. Mohammed Hassouna *et al.* [13] introduced an integrated hierarchical certificateless scheme with a Level 3 trust authority merging the traditional PKI hierarchy and the certificateless technology in one scheme. The new scheme employs the X509 certificate format and is free of the scalability and certificate management problems of the PKI.

However, they are actually proven to provide symptomatic effectiveness towards only a few types of attacks and they are never resistive against key-based attacks in WSN. Therefore, we present a novel technique of pairwise key establishment especially focusing on resisting key-based attacks in WSN. We also find that there is a need for a multitier architecture design embedded within a node to withstand multiple forms of attacks. This is only possible when the randomness of the node is further controlled to support a good balance between security features and communication performance in WSN. The proposed system offers a novel solution where multiple layers of security are incorporated using very lightweight cryptography that ensures that neither the compromised node nor the attacker node will pass the authentication system incorporated by proposed pairwise key predistribution process.

Section 1.1 discusses the existing literature where different techniques are discussed for pairwise key predistribution in WSN followed by a discussion of research problems in Section 1.2 and proposed solution in 1.3. Section 2 discusses algorithm implementation followed by a discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

1.1 Background

This section discusses the existing work being carried out towards pairwise key distribution in WSN. The recent work carried out by Gandino *et al.* [8] has introduced a composite protocol using an arbitrary distribution of the keys also focusing on memory minimization. Yuan *et al.* [32] have presented a technique that optimizes the predistribution of keys considering the case study of heterogeneous WSN and super network theory. Yagan and Makowski [30] have investigated the impact of arbitrariness towards the key pair distribution. Usage of graph-based techniques can be found in work of Ding *et al.* [5] towards designing blocks using predefined knowledge of blocks. Halford *et al.* [11] emphasized on the usage of public keys towards strengthening the secure communication using group keys during multicast operation. A similar trend of using group keys was also carried out by Harn and Hsu [12] using multivariate polynomial approach. Zheng *et al.* [33] have constructed an algorithm using seeds and path key for enhancing the legitimate arbitrary secure key during the distribution method in WSN. The similar trend of work is also carried out by Zhou *et al.* [34]. Gandino *et al.* [9] have considered static WSN and presented a unique key management technique for further enhancing the randomness in the pre-distribution process.

Chen *et al.* [28] have considered multiple encryption keys to evolve up with the hierarchical management of secret keys in heterogeneous WSN.

Hu and Gharavi [14] have presented a multi-way handshaking mechanism using Merkle-hash tree for enhancing the key distribution scheme. Choi *et al.* [3] have addressed the randomness in key distribution scheme by incorporating eigenvalue incorporated on the keypools to understand any form of malicious tampering of the secret keys in WSN. Bag and Roy [1] have achieved consistency in the key establishment process for securing the group-based communication over grid interface of WSN. Bechkit *et al.* [2] have presented a unital distribution process of secret keys that minimizes the feasibility of common key to get compromised. Khan *et al.* [18] have presented a key distribution of symmetric form especially emphasizing on achieving memory minimization during predistribution process. Eslami *et al.* [7] proposed an identity-based group key exchange protocol which addresses these security concerns. We prove that our scheme achieves semantic security in the presence of the adversarial model. Yagan [29] have investigated the Eschenauer-Gligor key and discusses its effectiveness towards achieving better connectivity during key predistribution in WSN. Doraipandian *et al.* [6] proposed KMS using LLT matrix for both Node-to-Node communication and Group communication emphasizing Local-connectivity, efficient node revocation method, perfect resilience, three-level authentication, reduced the storage.

Therefore, it can be seen that there have been various schemes towards improving the security performance by further strengthening the pairwise key predistribution scheme. All the existing studies have focused on a different form of sub-problems under key predistribution scheme with a common goal of secure communication in WSN. Although there are security advantages claimed in all the above-mentioned schemes, there are also significant pitfalls in existing scheme. The next section outlines some of the significant limitation that the current paper chooses to discuss.

1.2 Research Problem

The significant research problems identified are as follows:

Computational complexity: It is seen that existing system does not emphasize on minimizing computational complexity while performing pairwise key predistribution process.

Dynamic Topology: Dynamic topology is less often considered in existing techniques and thus it does not support mobility factor during secure key management.

Attacks: Study towards node replication, as well as a solution towards key-based attacks, are less and moreover existing system does not offer a full round of security on its encryption steps.

Clustering: The impacts of clustering towards the secret key generation process during predistribution of keys are not studied well.

Therefore, the problem statement of the proposed study can be stated as *to design and develop a pairwise key distribution system that has supportability of dynamic topology, highly resistive towards lethal key-based threats, and does not adversely affect energy consumption during the security operation.*

1.3 Proposed Solution

The prime purpose of the proposed system is to introduce a novel framework of security towards key management in WSN by emphasizing on evolving up with pairwise key predistribution using analytical research methodology. The core goal of this technique is to offer

1) Significant resistance against replication attack and other key-based attacks;
2) Offers more immunity towards nodes getting compromised;
3) Enhanced secrecy, *etc.* the schematic diagram of the proposed methodology is as shown in Figure 1.

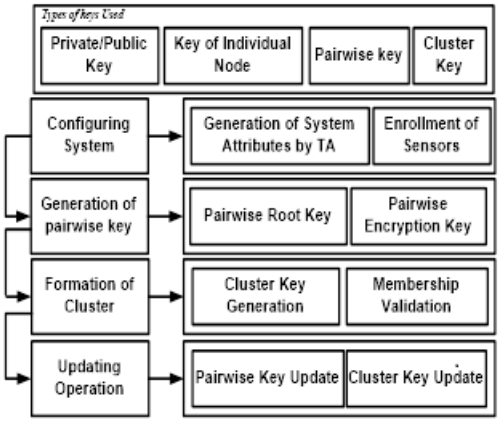

Figure 1: The proposed scheme

The adopted methodology uses 4 different types of keys to perform key management in WSN. There are 4 discrete modules firstly responsible for configuring the system followed by generation of a pairwise key, the formation of clusters, and updating operation. The proposed system also formulates the scenario of mobility where a node may possibly join a new cluster and leave an old cluster in order to assess the impact on both forward and backward secrecy. Basically, the proposed system focuses on generating pairwise keys followed by multiple steps of securing the generated pairwise as well as cluster keys in such a way that neither the adversary nor the compromised node would be able to perform decryption of these keys. The presented technique also focuses on utilizing trusted authority (TA) and base station for assisting in validating the updated key as well as secure management of revoked key list in order to ensure privacy and non-repudiation towards secure communication system in WSN. The next section highlights the algorithm implemented for this purpose.

2 Algorithm Implementation

The proposed system offers a novel mechanism for key management. It is responsible for securing the communication channels in WSN using multiple forms of key attributes. The proposed system uses

1) Key of the individual sensor (kind);
2) Key of public and private encryption (kpriv, kpub);
3) Key for pairwise distribution (kpair);
4) Key during clustering (kclust).

The Notations used in algorithm are as follows in Table 1.

Table 1: Notations

Notation	Meaning
N1, N2	# of Member and CH nodes
a	Simulation Area
ψ	Arbitrary Orientation
α	Security Attribute
$\sigma 1, \sigma 2, \sigma 3, \sigma 4, \beta$	System Parameters
bound	Boundary Area
$\tau 0, \tau 1, \tau 2, \tau 3$	Hash Functions
arb(1)	Generate one Arbitrary Number.
arb(N1)	Generate N Arbitrary Numbers.
$\gamma 1, \gamma 2$	Partial public/private keys at BS
$\lambda 1, \lambda 2, \delta, \mu 1, \mu 2, \mu 3$	Security Parameters.
SI	Security Index.
Thres	Threshold value

The proposed algorithm generates key of public and private encryption (kpriv, kpub) and key for pairwise distribution (kpair), of the system in Algorithm 1.

In the above algorithm (Line-2) initializes N1, N2, a, ψ, α, $\sigma 1$, $\sigma 2$, $\sigma 3$, $\sigma 4$. In (Line-3) random x and y coordinates are generated using random function arb (N1) and member nodes are deployed under boundary area bound. Similarly, Cluster heads are deployed in mesh grid topology. In (Line-4) ψ (arbitrary orientation angle) is calculated to apply random mobility to all nodes. The complete execution of the algorithm is carried out in following subsections.

Algorithm 1 Algorithm for novel pairwise key generation (NPKG)

1: Begin
2: init N1, N2, a,α,$\sigma1$,$\sigma2$,$\sigma3$,$\sigma4$
3: [x y] $\leftarrow$ bound+(a-2$\star$ bound)$\star$ arb(N1)
4: [x y] $\leftarrow$ N2 in meshgrid
5: $\psi \rightarrow 2\pi$.arb(N1)
6: **for** $i = 1 : N$ **do**
7: $[\tau 0] \rightarrow$ arb(1)$\star\sigma 1^2$, $[\tau 1] \rightarrow \sigma 1^3\star$arb(1)$\star\sigma 3$
8: $[\tau 2\ \tau 3] \rightarrow \sigma 1\star$arb(1)$\star[\sigma 1\star$arb(1)$]\star\ [\sigma 1\star$arb(1)$]\star\ \sigma 1$
9: β = [$\sigma 1$, $\sigma 2/\sigma 1$, $\sigma 3$, $\sigma 4$, $\sigma 5 = \theta\star\sigma 4$, $\tau 0$, $\tau 1$, $\tau 2$, $\tau 3$]
10: $\gamma 1 \rightarrow$ [1+arb(N)]. $\sigma 4$
11: $\gamma 2 \rightarrow$ [1+arb(N)]+ mod([1+arb(N1)$\star\ \tau 0$ (Sensor Node ID+ $\gamma 1$+([1+arb(N1)]. $\sigma 4$),prime-number)])
12: kpriv = [($\gamma 2$)', [1+arb(N1)]'] & kpub = [([1+arb(N1)].$\sigma 4$)', $\gamma 1$']
13: **for** $j = 1 : N1$ **do**
14: Compute $\lambda 1$, $\lambda 2$, δ
15: Compute $\mu 1$, $\mu 2$, $\mu 3$
16: **if** ($\mu 3\star\sigma 4$ == Thres) **then**
17: $\lambda 2 = \sigma 1$.c
18: **end if**
19: **end for**
20: **end for**
21: generate kpair $\leftarrow \lambda 2$
22: End

2.1 Configuring System for Key-Management

In the first step, it is assumed that the base station considers a prime number of α-bit as security attribute, tuple ($\sigma 1$, $\sigma 2/\ \sigma 1$, $\sigma 3$, $\sigma 4$) of natural numbers, and selects a root private key θ and computes the public key of the system as $\sigma 5$, which is a product ofθ and $\sigma 4$. $\tau 0$, $\tau 1$, $\tau 2$, $\tau 3$ are cryptographic hash functions defined in (Line-6 and Line-7). A typical empirical mechanism is used for computing the four different hash functions. Finally, in (Line-8) a system parameter β is defined as a set of ($\sigma 1$, $\sigma 2/\ \sigma 1$, $\sigma 3$, $\sigma 4$, $\sigma 5 = \theta.\sigma 4$, $\tau 0$, $\tau 1$, $\tau 2$, $\tau 3$).

The next step is the enrollment process of the legitimate sensors with the base station. For this purpose, the base station is assumed to recognize the legitimacy of a sensor node using a specific identifier for both N1 and N2. The algorithm allows all the sensors (N=N1+N2) to compute a private key ? as a random number between 1-1000 using arbitrary function and then compute the product of θ and $\sigma 4$ as a public key of that node. At the same time, the trusted authority is assumed to receive a request for generating and the computation of the partial private and public key for all nodes is carried out by $\gamma 1$ and $\gamma 2$ as shown in Line-9 and Line-10 respectively.

All the member nodes perform validation of their private keys by assessing the condition of $\gamma 2$. This step is followed by further generation of full secret keys by all nodes in (Line-11). The full private key is the transpose of $\gamma 2$ and nodes private key. The full public key is the transpose of nodes public key and $\gamma 1$. In case of attacker node, the identifier validation fails at initial step only and there will be no generation of any form of full private or public key. The proposed algorithm uses any form of cryptographic function to generate a key of the individual sensor. Immediately, after all the 4 types of keys are generated, a confidential list of all the public keys and node identifiers are maintained along with a separate matrix for revoked keys. Hence, the algorithm fails the attackers in the first step of key management itself without affecting the existing communication or security-based operation. It should be noted that trusted authority plays a crucial role in this process.

2.2 Generation of Pair Wise Keys

This part of the algorithm is responsible for computing and generating a pairwise key. The first step of this process is to select the source node and compute its secure index SI as the product of its identifier and $\sigma 4$. Secondly, calculate distance among all nodes and find out nodes within the range. It then performs the computation of other two security parameters $\lambda 1$ and $\lambda 1$ as follows:

$$\begin{aligned} \lambda 1 &= arb(1) \cdot \tau 0.\text{nodes in range}(d, R).\sigma 4 \cdot \sigma 5 + \text{mod} \\ &\quad (arb(1) \star \text{ nodes in range}(d, R), \text{prime-number}) \\ \lambda 2 &= \tau 1.arb(1).\lambda 1.arb(1).\sigma 4.\text{nodes in range}(d, R) \end{aligned}$$

The above-mentioned expression leads to the generation of $\lambda 1$ and $\lambda 2$ respectively (Line-13) for all the member nodes (Line-12). The next step of the generation of the pairwise key is to compute three more security parameters i.e.$\mu 1$, $\mu 2$, $\mu 3$ (Line-14). δ and arb(1) are the random numbers. Following empirical mechanism is opted for computing these parameters:

$$\begin{aligned} \mu 1 &= \tau 2 \cdot SI \cdot \delta \cdot \lambda 1 \cdot a \cdot arb(1) \cdot \text{nodes, within,} \\ &\quad \text{range } (d, R) \\ \mu 2 &= \tau 3 \cdot SI \cdot \delta \cdot \lambda 1 \cdot arb(1) \cdot \text{nodes within range } (d, R) \\ \mu 3 &= arb(1).arb(1) \cdot \mu 1 \cdot arb(1) \cdot \mu 2. \end{aligned}$$

Assume that source node sends a packet as combination of Secure Index and $\mu 3$. The receiver node decapsulates the packet by performing product of an arbitrary number and secure index SI and recomputes $\mu 1$. In (Line-15) the system performs the comparison of the product of $\mu 3$ and $\sigma 4$ with dynamic threshold value Thres. The computation of Thres is carried out as follows:

$$\begin{aligned} Thres &= arb(1) + \tau 0 \cdot a \cdot arb(1) \cdot arb(1) \cdot \sigma 5 \\ &\quad + \tau 1 \cdot arb(1) \cdot \tau 2 \cdot arb(1). \end{aligned}$$

The third layer of security is considered by assuming the state of a compromised node by re-computing $\lambda 2$ and then upgrading the key generation process. In this, the updated value of the $\lambda 2$ will be as $\sigma 1$.c, where c is as

follows.

$$c = arb(1) \cdot \sigma 5 \cdot \lambda 1 \cdot arb(1) \cdot arb(1) \cdot \sigma 5 \cdot arb(1) \cdot nodesinrange(d, R).$$

The above step offers extra security for compromised nodes (Line-16) as if the node is compromised then it will be able to find the value of c as that will further result in failure. Hence, the algorithm could offer enough resistance to both adversaries as well as compromised nodes. Therefore, Line-20 results in the generation of the pairwise during each round of authentication in WSN.

2.3 Cluster Key Generation

The final step is the generation of cluster key. The cluster key is generated using any form of cryptographic hash function on the root private key *i.e.* θ and cumulative hash value from concatenation.

2.4 Updating Operation

Uniqueness in the implementation of the above algorithm is that the cluster updating operation is only carried out by cluster head nodes, hence if any of the member nodes try to alter or change the cluster key than that member node will be indexed directly as the adversary. The cluster head even considers the node mobility factor and notifies the base station about any form of alteration. There are multiple reasons for a sensor to either join a new cluster or leave from an old cluster. The proposed system offers maximum time-based synchronicity so that all the cluster heads are always connected to each other, which is quite essential during validation steps. The key revocation list is constructed by the cluster head and maintained by a trusted authority, hence there is no scope that it could be compromised by any means. Once the revocation list is constructed than only the base station has the privilege to update the security attributes and not the cluster heads. In this way, the proposed system maintains a good balance between forward and backward secrecy while performing any authentication of the nodes during the communication process of data aggregation in WSN. The next section highlights the outcome obtained after implementing the above mentioned pairwise key generation algorithm and discusses its effectiveness.

3 Result Analysis

The study outcome of the proposed system is implemented in Matlab with a large number of 100-500 sensor nodes in presence of multiple cluster heads. The simulation is repeated for 50 times, and results report the average values. The Proposed system is evaluated in terms of memory usage, time, security evaluation and computational complexity. As the proposed study has introduced a novel cryptosystem for incorporating security, so we emphasize on assessing the energy performance of a sensor node. However, energy factor is being evaluated with respect to two different forms of the time instances as shown in Figure 2 and Figure 3. The study outcome is also compared with the most frequently adopted techniques of pairwise key distribution using polynomial-based approach [15], combinatorial-based approach [25], Grid-based approach [22], and Multivariate-based approach [4].

Impact of updating cluster key on Energy Consumption: The first performance parameter evaluated is the impact of updating cluster key on energy consumption.

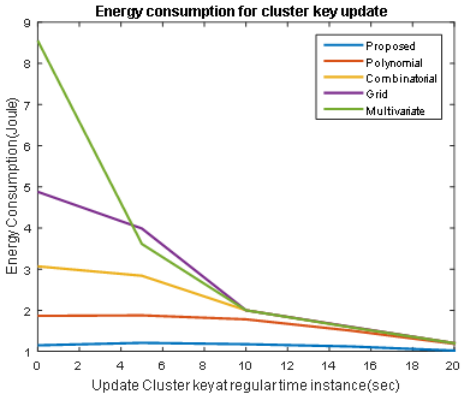

Figure 2: Impact of updating cluster key on energy consumption

The proposed system maintains this time instance in order to dynamically configure the cluster with the mobility of the nodes. This will mean that if the value of frequency of updating cluster key is equivalent to zero than updating process of cluster key is carried out only on demand(i.e. when node moves away or moves in the cluster) or else the cluster head waits till the specified time instance in order to update. The proposed system uses about 1.2 units of energy to update the key up to 10 sec and then gradually decreases. The outcome shows that proposed system offers significantly lower scale of energy consumption as compared to existing system. Polynomial-based approach is nearly similar form as that of proposed system as it works on finite field cryptosystem normally. However, it includes maximum processing towards computing the common key and consumes about 1.9 units of energy up to 10 sec and then decreases. Similarly, combinatorial-based key pair distribution may pose a potential mechanism toward privacy preservation but it includes increasing number of variables that has higher dependencies on heuristic-based data. This leads the algorithm to consume more amount of energy only during the key set up process. It consumes about 3.1 units of energy up to 5 sec and then decreases.

Existing techniques towards grid-based key predistribution calls for static positioning of the nodes. This

technique has two pitfalls *i.e.*

1) It does not address dynamism;
2) Similar effort for all member nodes leads to unnecessary power consumption. Moreover, redundant data could not be controlled as there is very poor communication among the cluster heads and hence there is much power drainage consuming 4.9 units of energy up to 5 sec and then steeply decreases to 2 units at 10 sec and the gradually decreases. Similarly, if the number of clustering key updating process is increased than multivariate schemes involves complete processing using static threshold factor that causes excessive drainage of approximately 8.5 units of energy in the first few rounds if mobility is considered. The proposed system overcomes all the above mentioned limitations of existing approaches by ensuring that algorithm process all the dynamic clustering and routing information without overburdening the memory of any sensor node. This is one of the prime factors that illustrates that proposed system is capable of supporting increasing number of updates without any potential adverse effect on the communication process.

Impact of Wait Time on Energy Consumption: The next performance parameter is wait time the time that allows the sensor to wait until root pairwise key is disposed of when it departs from the member nodes. Therefore, when the wait time is zero second revocation of the root pairwise key takes place as the node moves away from the existing cluster.

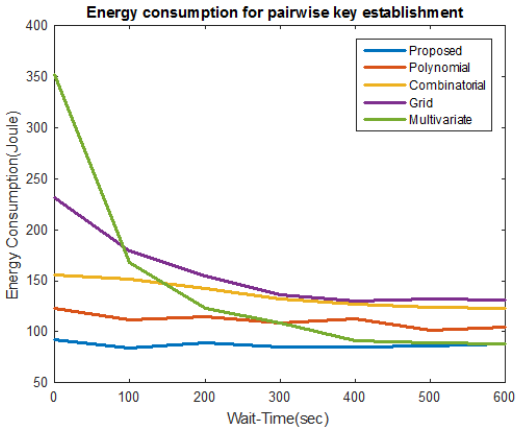

Figure 3: Impact of wait time on energy consumption

Figure 3 shows that with the increase of waiting time the energy consumption is also affected. A closer look shows that the proposed system and polynomial-based approaches show a similar trend of energy consumption, where both the system successfully maintains the similar scale of energy dissipation for wait time in the range of 0 to 600 second. Although the combinatorial-based approach is also evident with the similar trend, owing to increasing the number of processing in the initial level of key distribution, it suffers from increased energy consumption of about 153 units and then very gradually decreases up to 130 units. Both grid-based, as well as multivariate-based, are found to have a steep trend of energy but such trend is highly harmful to the nodes running the dynamic application in WSN. Grid approach consumes 230 units initially and steeps down to 150 after 300 seconds and then gradually decreases. Multivariate consumes 350 initially and steeply reduces to 170 after 100 seconds and then decreases further. From the energy viewpoint, it is essential that all the nodes should have a nearly equal rate of energy dissipation for any form of energy-efficient algorithm to work if the wait time is increased. Moreover, with an increase of wait time, the cryptographic process will further be delayed to get executed, which may be another cause of the further attack. We also find that increase in node mobility also increases the energy consumption in the existing system for both the performance factor of time.

Therefore, cumulatively, the study outcome finds that when the frequency of updating cluster key increases than proposed pairwise key distribution system witnesses minimized the rate of energy consumption. The proposed system takes approximately 1.48869 seconds to perform the entire process of computation because all the existing system consumes 7.47719 seconds in average.

Memory Usage: From memory viewpoint, the proposed system does not dispose extra memory. Memory is occupied by the hash functions, private, public and pairwise keys, ?. There is very less number of static variables and more number of dynamic variables. The proposed system optimizes its memory to a higher level under different circumstances of communication. These lets the algorithm work and respond faster in generating the pairwise key in contrast to the existing system.

Security Evaluation: A closer look at all the above mathematical expression will show that there are dependencies among multiple parameters. As this information will be never with any compromised or adversary, so even if adversary crosses the first process of system configuration, they will result in the failed computation of threshold, which will be a direct indication of the node being adversary.

Thus, the proposed algorithm offers comprehensive level of security in generating pairwise keys in WSN that can assist in performing validation of the member nodes as well as cluster heads during every round of data aggregation cycle. The algorithm also transmits significant amount of computed security results

to the base station to filter the list of genuine and illegitimate nodes existing in the network. However, the base station always does dual check on the messages that are aggregated from the other nodes (cluster head) by comparing the list that is maintained within itself with the one that is maintained by the trusted authority. As it is assumed that a trusted authority can never be compromised therefore there is no scope for any form of the error. Another interesting part of this algorithm implementation is that the updating pairwise key is a continuous process; however, the root of the private key is completely independent of any form of key updates.

Usage of Cryptographic Primitive: The usage of cryptographic primitive is very less and is only limited to applying any standard encryption for finally generating the cluster keys. Rest all are simple concatenation and conditional operation that makes the proposed algorithm quite lightweight to balance the security demands and enhanced network lifetime in order to meet the claimed security goals. Therefore, looking at the trend of outcome, the proposed system is better applicable in sensory application that demands consistent monitoring process, *e.g.* emergency application, tactical applications, combat field monitoring healthcare, *etc.*

4 Conclusion

Security is yet a challenging problem in WSN which renders prior security algorithm non-applicable for the upcoming application of IoT where sensory applications are used along with cloud computing. The present paper introduced a novel key management approach that is constructed keeping in mind the necessity of dynamic networks in upcoming application of WSN. The proposed algorithm is constructed for offering sustainable communication system with equal stress on highly resilient key generation process along with robust mechanism of the key updating process. The dynamic topology is constructed considering that a node may join or leave the cluster at any point in time so that both forward secrecy as well as backward secrecy is maintained. The study outcome of the proposed system is compared with existing approaches of key predistribution to find that proposed system offers better energy conservation.

References

[1] S. Bag and B. Roy, "A new key predistribution scheme for general and grid-group deployment of wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, pp. 145, 2013.

[2] W. Bechkit, Y. Challal, A. Bouabdallah and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, pp. 948–959, 2013.

[3] S. J. Choi, K. T. Kim and H. Y. Youn, "An energy-efficient key predistribution scheme for secure wireless sensor networks using eigenvector," *International Journal of Distributed Sensor Networks*, 2013. DOI 10.1155/2013/216754.

[4] F. Delgosha and F. Fekri, "A multivariate key-establishment scheme for wireless sensor networks," *IEEE Transactions on Wireless Communications*, pp. 1814–1824, 2009.

[5] J. Ding, A. Bouabdallah, and V. Tarokh, "Key predistributions from graph-based block designs," *IEEE Sensors Journal*, pp. 1842–1850, 2016.

[6] M. Doraipandian and P. Neelamegam, "An efficient key management scheme in multi-tier and multi-cluster wireless sensor networks," *International Journal of Network Security*, pp. 651–660, 2015.

[7] Z. Eslami, M. Noroozi, , and S. K. Rad, "Provably secure group key exchange protocol in the presence of dishonest insiders," *International Journal of Network Security*, pp. 33–42, 2016.

[8] F. Gandino, R. Ferrero, and M. Rebaudengo, "A key distribution scheme for mobile wireless sensor networks: q - s -composite," *IEEE Transactions on Information Forensics and Security*, pp. 34–47, 2017.

[9] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Transactions on Industrial Informatics*, pp. 1133–1143, 2014.

[10] H. Geng, *Internet of Things and Data Analytics Handbook*. Florida: John Wiley & Sons, 2017.

[11] T. R. Halford, T. A. Courtade, K. M. Chugg, Li, and G. Thatte, "Energy-efficient group key agreement for wireless networks," *IEEE Transactions on Wireless Communications*, pp. 5552–5564, 2015.

[12] L. Harn and C. F. Hsu, "Predistribution scheme for establishing group keys in wireless sensor networks," *IEEE Sensors Journal*, pp. 5103–5108, 2015.

[13] M. Hassouna, B. Barry, and E. Bashier, "A new level 3 trust hierarchal certificateless public key cryptography scheme in the random oracle model," *International Journal of Network Security*, pp. 551–558, 2017.

[14] B. Hu and H. Gharavi, "Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking," *IEEE Transactions on Smart Grid*, pp. 550–558, 2014.

[15] H. Ito, A. Miyaji, and K. Omote, "Rpok: A strongly resilient polynomial-based random key predistribution scheme for multiphase wireless sensor networks," in *IEEE Global Telecommunications Conference (GLOBECOM'10)*, pp. 1–5, 2010.

[16] S. R. Jondhale, R. S. Deshpande, S. M. Walke, and A. S. Jondhale, "Issues and challenges in rssi based target localization and tracking in wireless sensor networks," in *International Conference on Au-*

tomatic Control and Dynamic Optimization Techniques (ICACDOT'16), pp. 594–598, Sep. 2016.

[17] Kamila and N. Kumar, *Research on Wireless Sensor Network Trends and Technologies and Applications*, Florida: IGI Global, 2016.

[18] E. Khan, E. Gabidulin, B. Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks," *IET Wireless Sensor Systems*, pp. 108–114, 2012.

[19] S. Khan, Al-Sakib K. Pathan, and N. A. Alrajeh, *Wireless Sensor Networks: Current Status and Future Trends*, Florida: CRC Press, 2016.

[20] C. T. Li, M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks",*Information Sciences*, vol. 181, no. 23, pp. 5333–5347, Dec. 2011.

[21] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[22] N. X. Quy, V. Kumar, Y. Park, E. Choi, and D. Min, "A high connectivity pre-distribution key management scheme in grid-based wireless sensor networks," in *International Conference on Convergence and Hybrid Information Technology*, pp. 35–42, 2008.

[23] M. H. Rehmani and Al-Sakib K. Pathan, *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*, Florida: CRC Press, 2016.

[24] S. Roy, J. Karjee, and U.S. rawat, "Symmetric key encryption technique: A cellular automata based approach in wireless sensor networks," *Elsevier-Procedia Computer Science*, pp. 408–414, 2016.

[25] S. Ruj and B. Roy, "Key predistribution using combinatorial designs for grid-group deployment scheme in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN'09)*, 2009.

[26] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: Issues and challenges," in *Proceeding of the IEEE International Conference on Space Science and Communication (IconSpace'13)*, pp. 176–180, July 2013.

[27] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," *International Conference on Machine Intelligence and Research Advancement*, pp. 58–62, 2013.

[28] C. M. Chen, X. Zheng and T. Y. Wu, "A complete hierarchical key management scheme for heterogeneous wireless sensor networks," *The Scientific World Journal*, pp. 13, 2014.

[29] O. Yagan, "Performance of the eschenauergligor key distribution scheme under an on/off channel," *IEEE Transactions on Information Theory*, pp. 3821–3835, 2012.

[30] O. Yagan and A. M. Makowski, "Wireless sensor networks under the random pairwise key predistribution scheme: Can resiliency be achieved with small key rings?," *IEEE/ACM Transactions on Networking*, pp. 3383–3396, 2016.

[31] M. B. Yassen, S. Aljawaerneh, and R. Abdulraziq, "Secure low energy adaptive clustering hierarchal based on internet of things for wireless sensor network (WSN): Survey," in *International Conference on Engineering & MIS (ICEMIS'16)*, pp. 1–9, Agadir, 2016.

[32] Q. Yuan, C. Ma, X. Zhong, G. Du, and J. Yao, "Optimization of key predistribution protocol based on supernetworks theory in heterogeneous WSN," *Tsinghua Science and Technology*, pp. 333–343, 2016.

[33] S. Zheng, Y. Tian, L. Jin, and Y. Yang, "A portable random key predistribution scheme for distributed sensor network," *Journal of Sensors*, pp. 14, 2014.

[34] B. Zhou, J. Wang, S. Li, and W. Wang, "A new key predistribution scheme for multiphase sensor networks using a new deployment model," *Journal of Sensors*, pp. 10, 2014.

Biography

M. Vaneeta is Associate Professor in Department of Computer Science and Engineering, K. S Institute of Technology, Bengaluru, Karnataka, India. She received B.E degree in Department of Computer Science and Engineering from Dr. BAMU University, Maharashtra and M.E degree in Department of Computer Science and Engineering, Anna University. She is currently pursuing her Ph.D. degree in the Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi. Her research interests include wireless sensor networks, secure communication networks and Image processing.

S. Swapna Kumar is Professor and Head of Department of Electronics and Communication Engineering, in Vidya Academy of Science & Technology, Thrissur, Kerala, India. Presently, he is a Supervisor for the Ph.D. scholars under Visvesvaraya Technological University (VTU) and also an external examiner for Thesis evaluation/ Public Viva-voce of Ph.D. students. He has been in the teaching for profession courses under UG/PG level for nearly decade, and has worked for various national and international industries.He is a reviewer of several National and International journals. Besides, he has also authored books on "Guide to Wireless Sensor Networks and LAB easy way of learning". Dr. Swapna Kumar is a Fellow Member and Chartered Engineer IEI (INDIA). He has also a life membership of professional bodies, including ISTE and IEEE. His area of interest include Networking, Security system, Fuzzy Logic, Data Communication, Electronics, Communication Systems, Embedded Systems, MATLAB modelling and simulation.