International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Multi-tier Framework for Optimizing Pairwise Key Predistribution in Sensory Applications

Vaneeta M, S. Swapna Kumar

Abstract**:** ***Security has been always a prominent concern in Wireless Sensor Network (WSN) irrespective of the evolution of various scientific approaches that mainly mechanizes key management approaches to secure the communication system among the resource constraints sensors. Out of various key management approaches, pairwise key is one effective approach to ensure cost effective key management scheme; however, review of existing approaches shows that they still are characterized by various issues connected to optimized performance. Adopting analytical research methodology, the proposed system implements an optimized multi-tier framework for resisting key-based threats and it targets to introduce a lightweight pair wise predistribution of keys by joint integration of enhanced public key encryption and digital signature. The study outcome shows that proposed system offer a better security performance in contrast to existing pair wise predistribution of keys.***

Keywords**:** ***Pairwise keys, predistribution, Key agreement, Security, Attacks.***

I. INTRODUCTION

The adoption of the Wireless Sensor Network (WSN) has been prominently increasing owing to its cost effective remote monitoring capabilities [1],[2]. The sensors follow various clustering schemes in order to carry out data aggregation process [3],[4]. In such communication scheme, usually the members nodes forward the physically sensed data to their assigned cluster head which is then forwarded to either sink (using single hop) or to different cluster head (using multihop). Although, WSN is completely backed up by a stable topology as well as infrastructure, but there are always good possibilities of faults among the operations being carried out by the resource constrained sensor. There are various possibilities of intrusion in WSN both in the form of internal or external attack. There are various studies that have been discussed for addressing key agreement issue with respect to self-enforcing approach, trusted-server approach, and key predistribution approach [5],[6]. Out of all these, key predistribution scheme is found to be more used in existing system that distributes the information of secret keys is carried out before the sensors are actually deployed in the simulation.

The decision of the keys can be well defined in advanced if the neighborhood information exists, which is quite impractical as majority of the deployment strategy of the sensors are actually randomized and not on predefined basis. At present, there are various predistribution schemes in WSN that doesn't use such dependency of apriori information of the deployment of sensors. The better form of the solution will be to allow the complete set of the sensors to use a secret key that can be considered as master key. In order to achieve a better form of key-agreement, it is now feasible for different sensors to utilize this master secret key and thereby get the pairwise secret key [7]. However, such approaches are found to reduce the resiliency of the WSN performance that is not anticipated. It will mean that upon event of a compromisation of even a single sensor than the complete network will be rendered vulnerable.

Existing mechanism from the literatures recommends reposting such master key over certain form of hardware that is free from any form of physical damage or any security risk [8],[9]. It will mean that hardware-based approach is claimed to offer protection towards such master key; however it is not completely feasible as it will maximize the consumption of resources as well as cost associated with each sensor. At the same time, there is no evidence till date that hardware based security approaches are always safe as there is the possibility to break-in. There are certain other forms of the predistribution scheme of the secret keys in WSN that allows the sensors to carry a specific number of secret keys in the form of pairwise and this information is accessible only for that specific sensor node while the another specific sensor node in the form of source and destination respectively. It is claimed that such security policies are potentially strong as it is not feasible for the adversary node to influence the security strength of other sensors. Unfortunately, such approaches are not considered as practical approaches as they cannot be supported by sensors with restricted memory.

Another significant problem is that it is not feasible for adding new sensors as there is no new secret key to be allocated by the existing deployed sensors. Therefore, the proposed system discusses about a novel approach of pairwise key distribution scheme where applicability of the different test environment is valid. The idea is to ensure multi-tier framework by including a superior authentication scheme using enhanced public key encryption and digital signature. The prime agenda of the work is also to resist various forms of malicious attacks of dynamic order.

Revised Manuscript Received on December 30, 2019.

***** Correspondence Author

Vaneeta M*, Department of Computer Science & Engineering, K.S Institute of Technology, Affiliated to VTU, Belagavi, India.

S. Swapna Kumar, Department of Electronics and Communication Engineering, Vidya Academy of Science and Technology, APJ Abdul Kalam University, Thrissur, India.

Retrieval Number: B6242129219/2019©BEIESP
DOI: 10.35940/ijitee.B6242.129219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The organization of the paper is as follows: Section "A" discusses about the existing literatures where different techniques are discussed for detection schemes used in power transmission lines followed by discussion of research problems in Section "B" and proposed solution in "C". Section II discusses about algorithm implementation followed by discussion of result analysis in Section III. Finally, the conclusive remarks are provided in Section IV.

A. Background

At present, there are various studies that have been carried out towards securing WSN that is briefed in our review work [10]. There are various works that has been carried out towards key predistribution in WSN. Most recently, the work of Albakhri and Harn [11] have used probabilistic scheme using group key based predistribution of the keys using multivariate polynomial scheme. Consideration of the mobility factor using Gandino et al. [12] where the q-s composite technique has been adopted for an effective design of key distribution policy in WSN. The work of Yagan and Makowski [13] has investigated the impact of the encryption keys for assessing the key strength over key predistribution. Harn and Hsu [14] have used polynomial-based approach for constructing a group keys using multi-variant function with claim over controlling computational complexity. Yavuz et al. [15] have used combination of the probability concept with scaling conditions for constructing arbitrary graph considering specific number of connectivity. Yagan and Makowski [16] have constructed a model on the basis of conventional scheme of the predistribution of the keys where the isolation technique has been used for securing the network. The works of Rasheed and Mahapatra [17] have presented key generation approach on the basis of the polynomial function over mobile sinks. Apart from this, there are various schemes towards securing key management in WSN. The recent work of Afianti et al. [18] has used elliptical curve encryption along with digital signature in order to offer better security in WSN.

The work of Du et al. [19] has used public key that is independent of any certificate along with usage of aggregate signature scheme. Deepa S. R. et al. [20] has shown that Cluster optimization in Wireless sensor networks using particle swarm optimization reduces the energy consumption as energy is very important in information security. Adoption of re-signature over proxy is considered in the work of Zhang et al. [21] on the basis of public-key encryption. Yang et al. [22] have also made use of the signature scheme that is independent of any certificate specifically meant for internet-of-things security aspects. Nearly similar environment is also considered in the work of Zhu et al. [23] where the authors have presented a short signature scheme that reduces computational overhead. Xie et al. [24] have enhanced the signature policy that doesn't uses certificates specifically used in medical sector for protecting privacy factor. Study considering generation of the signature from the gateway node is carried out by Chang et al. [25] using GPU acceleration. Shim [26] has presented an authentication scheme where ID based encryption mechanism has been used along with the signature scheme. Adoption of the signcryption has been seen in work of Ting et al. [27] where identity-based encryption and public key infrastructure has been used. Wei et al. [28] have used similar identity-based security scheme where signature policy has been constructive for secure sharing among the users. Adoption of elliptical curve encryption over hardware design of the sensor was investigated by Liu et al. [29] while the problems associated with the privacy factor is addressed in the work of Lo [30] using similar approach over vehicular sensor network. The next section discusses about the issues connected with existing approaches.

B. Research Problem

The significant research problems are as follows:

- Existing approaches are more focused on pairwise key distribution with less emphasis on the key storage optimization and faster response time.
- Adoption of public key encryption is not subjected to second level of security assessment that results in faster events of compromisation in case of internal attacks.
- Computational complexity associated with the implementation of the pairwise key predistribution mechanism is assessed less.
- Hybridized scheme of pairwise key predistribution still suffers from complexity problems in presence of dynamic attack that is required to be solved.

C. Proposed Solution

The proposed study is an extension of the prior work carried out in [6] where the emphasis was basically into pairwise key generation method. The current work is emphasizes on the evolving up with a multi-tier framework with an aid of pairwise key distribution. The mechanism used in the proposed system is as shown in Fig.1.It shows that the complete methodology is classified into two stages of implementation. The first phase of the implementation emphasizes over the strengthening the authentication system while the second phase emphasizes over the validation of the data being received by the sensor

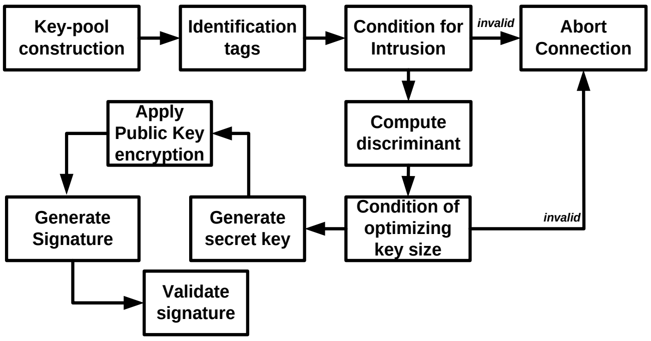

Fig.1 Adopted Methodology of Proposed System

The study uses the first phase of implementation prior to data aggregation where the communication is carried out between member node and cluster head node. The second part of the implementation is carried out during the post data aggregation stage where the communication is carried out between two cluster heads. The proposed system constructs a keypools where the identification of the tags are used for constructing a security token for safeguarding this key pools.

Upon setting up a condition of intrusion, when the positive event is matched then the connection is aborted which otherwise will be followed by applying a quadratic expression where the identification tags are used for constructing the tokens. These discriminants generate a root of quadratic expression that finally results in the secret key that is used for data aggregation.

For better optimization, the proposed system performs optimization of the key size further to control the size of the key without compromising the security strength of the secret key. Finally, an enhanced public key encryption is used followed by a mechanism that further generate signature for protecting the message being propagated. Finally, the received signature is subjected for validation where connected dependency leads to failure of authentication by the malicious node thereby resisting them. Finally, only the legitimate sensors are capable of performing authentication of the generated digital signature in cost effective manner leading to good balance between security and communication in WSN.

II. SYSTEM IMPLEMENTATION

The main agenda of the proposed system will be to frame up a multi-tier modelling where pairwise key distribution plays a significant role with a purpose of safeguarding the secure communication system in WSN. This section discusses about the assumptions considered, implementation strategy, and execution flow of the proposed system.

A. Assumption Considered

The *primary assumption* of the proposed system is that the deployments of the predistribution secret keys are carried out in random order. The study considers that there is a mutual secret key between two adjacent sensors for a secured communication. The *secondary assumption* of the proposed study is that there is certain form of algorithm being autonomously executed by the sensor in order to check and eliminate the revoke keys. The study also considers that no attackers that intrude the network in the beginning of simulation while the intrusion is only possible when the attacker resides within the transmission zone of the sensors. The *third assumption* of the proposed system is that base station is considered to have abundant resources as well as highly tolerant from any degree of fault. Hence they are highly secured from any form of attacks. The *fourth assumption* of the proposed system is that there is no privilege of the sensing data by the intermediate sensor and therefore the data stream will be free from any form of new embedded data while performing data aggregation.

B. Strategy of Implementation

The proposed study is designed using an explicit concept to offer security both prior and post of data aggregation using pairwise key distribution method. The study investigates about the implication of mobile sinks as well as novel multi-tier architecture for resisting replication attack in WSN. The prime aim of the proposed system is to design a secure framework using the concept of triple key distribution where the three nodes share the common keys for the purpose of secure data aggregation. The proposed security scheme performs secure data aggregation and ensures maintaining security by two phases. The first phase of implementation is before data aggregation: A multi-tier pair wise key distribution is proposed that ensure secure and reliable data transmission procedure among the entities of WSN. An attacker module is designed that can be static or mobile and can either be active (physically compromise the nodes) or passive (eavesdrop on messages) considering both inside and outside attacks. The system uses 128 bit key size chosen from key-pool. Therefore, a pair wise key distribution ensures secure communication between two nodes while multiple key pairwise distributions ensures secure communication between sensor nodes, cluster-node, and base station. Therefore, an optimal secure environment will be accomplished even before or at the point of initiating the data aggregation process. The second phase of implementation is after the data aggregation. This phase is basically further more enhancement of the previous phase where the user ID and the user public key will be used interchangeably without making any distinctions. Although the bio-inspired algorithms used in the previous modules of the work are capable enough to perform effective routing, efficient selection of aggregator node, but it lacks the counter policy to mitigate the threats of intrusion within the network. Hence, the capability of the bio-inspired computing to perform effective data aggregation is further more secured using cost-effective security measures.

The prime intention of this phase is to ensure sender node ambiguity and unforgeability. Therefore, for this purpose, the system uses Elliptical Curve Cryptography using SHA-1/MD5 based hash function to perform encryption on the message to be transmitted among the nodes. Finally, Elgamal Signature Scheme is considered where it is further more enhanced to perform the Sender anonymity, signature generation, followed by signature verification. The proposed concept also uses a concept of clustering, hierarchal data gathering in order to overcome the direct transmission energy loss and increase the network life time. Therefore data from individual nodes gets aggregated at cluster head and then goes to the sink node or base station. To avoid the effect of node capture attack a novel approach of three nodes share common keys is employed called triple key distribution for secure forwarding, in clustered sensor networks. Basically, the idea is to carry out multi-tier key distribution mechanism in WSN considering a better form of key agreement scheme for higher security standards in communication. The first part of the study considers generation of secret key very unique in multiple progressive steps which strengthen the authentication process prior to data aggregation. It will mean that this form of communication usually takes place between member node and cluster head. The second part of the study is to further optimize the authentication performance to boost up the key predistribution process in WSN where an enhanced digital signature scheme has been utilized for the purpose of validating the message being forwarded by the sensor.

This part of the implementation is carried out between the cluster head as the last phase of the data aggregation where the secured packet is finally forwarded to the sink node.

C. Execution Flow

The complete process of the execution of the proposed system is carried out by two processes where first process of key predistribution is carried out prior to data aggregation while the second process of key predistribution is carried out in after data aggregation.

a. Algorithm for Securing Distributed Keys Prior to Aggregation

This algorithm is responsible for formulating a unique secret key that will be used for primary authentication of the member node with its allocated cluster head. For this purpose, the sensor node is allocated a unique secure identification tags which are dynamic in order. The significant steps of the proposed algorithm are as follows:

Algorithm for Securing Distributed Keys Prior to Aggregation

```
Input: n (number of sensors)
Output: τ / σ(Secret keys)
Start
1. For i=1: n
2.     If $m_{A3}$=$m_{B3}$
3.         Flag ‘Abort communication’
4.     End
5.    If α>1
6.     compute $\beta_1$ & $\beta_2$.
7.     If β<γ
8.        compute $\tau_{AB}$ and $\sigma_{AB}$
9.     Else
10.       Flag ‘Abort communication’
11.    End If
End
```

The discussion of the steps of the algorithm is as follows: The algorithm considers all the sensor nodes *n* (Line-1) and then checks if an explicit variable *m* (which is also the part of secure identification tags) for both node A and node B is same or different (Line-2). In case if both the parameters are found to possess the same value then it is likely that node B is either attacker or compromised node as it is not supposed to possess the value of *m* and hence all the communication leading to node *B* is aborted (Line-3). The next part of the algorithm implementation is about computing the polynomial variable α (Line-5) which depends upon other two parameters m_1 and m_2; hence $m = \{m_1, m_2, m_3\}$ is considered as set of secured identification tags of sensors *A* and *B*. The study then computes the discriminant β_1 and β_2 obtained using m_1 and m_2, and α variable (Line-6). The interesting point here is that the obtained value of the discriminant β_1 and β_2 is used for comparing with the threshold secret key γ that can be allocated by the user (Line-7). This step of operation offers a significant control of computational complexity by controlling the balance between the generated key size and security strength. Upon finding the positive condition, the proposed system computes two keys τ_{AB} and σ_{AB}.

The first key τ_{AB} is computed by concatenating cumulative keys considering m1 factor for both node A and node B. The second key σ_{AB} is computed by applying cryptographic hash function on prior key τ_{AB} concatenated with identity information of node A and node B. Hence, this computation leads to a generation of final secret key σ_{AB} which will be used by the cluster head in order to carry out further secure transmission of the fused data to another cluster head (via multihop technique). If the condition stated in Line-7 is found not to be valid than it will mean that there is no common key between two communicating nodes. Absence of common key will state that one of the node has violated the proposed security protocol and is under captivity of adversary and hence any communication with uncommon node is truncated. It is to be noted that the algorithm fixes the value of *m* (=m_1, m_2, m_3) throughout the data aggregation process, although it can be changed by the user at any point of application. It also depends upon the communication demands of the sensor nodes.

Another interesting point to be noted in the algorithmic operation is that there are fair possibilities that the adversary could gain information about the identification tags of the sensor node A as well as sensor node B. Fortunately, the design is constructed in such a way that an adversary node will have to compromise the common key which is near to impossible as for that the adversary will be required to compute the shared key. Therefore, there are strict forms of dependencies of various variables which is just impossible for the attacker to have an access on. Another interesting part of the implementation is that it has a potential supportability towards mobile networks too as it just uses the pairwise keys for carrying out authentication between two nodes. However, this authentication mechanism can be further strengthened if the process of secret key generation is further more safeguarded against privacy problem. This mechanism is further followed by next algorithm where signature is used.

b. Algorithm for Securing Distributed Keys Post to Aggregation

The first algorithm discussed in Section 2.3.1 is responsible for generating a secret key purely on the basis of pairwise predistribution in WSN. However, the generated secret key is also required to be safeguarded against any possibilities of adversaries. Therefore, this part of the algorithm is responsible for applying enhanced elliptic curve encryption for further ensuring the best version of the secret key followed by applying enhanced digital signature for potential trap-door function. The significant steps of the proposed algorithm are as follows;

Algorithm for Securing Distributed Keys Post to Aggregation

```
Input: σ
Output: Valid/Invalid Signature
Start
choose rand(k)      k= σ
R=f(k, h, Q)
compute s→f(k, h)
generate U(msg)
validate if ($msg_1$)=1, 2, ….n
H→hash(msg, implicit_param)
compute private and public key
For ∑(implicit_param, public key)=private key ///rephrase this steo
    consider valid signature
Else
```

```
11.  Flag ‘Abort communication’
12. End
End
```

The discussions of the above algorithmic steps are as follows: In this case, the study considers that transmitting node (clusterhead) intends to forward the message *msg* with higher degree of privacy within the proximity of its network. The system considers that there are specific numbers of the authenticated transmitting node and therefore, the first step will be to perform the authentication process. The study considers the private key k, which is obtained from σ from the prior algorithm and the selection process is carried out randomly (Line-1). The system then computes a implicit parameter that is scalar product of β_A and |N|. This operation is followed by applying enhanced elliptical curve encryption using function *f*(x) whose dependable parameters are i) pairwise keys *k*, hashed value of the message *msg* and implicit parameter, and public keys *Q* (Line-2). The algorithm then performs computation of the signature s which is again depending upon a function with input arguments of pairwise key *k*, implicit parameter and hashed value *h* (Line-3). According to the proposed system, the algorithm defines the secret message msg using an explicit function U(x) which usually consists of message msg, set of all generated signatures S, implicit parameters, public key (Line-4). The encoded message is then forwarded by one cluster head to another cluster head owing to the adoption of the multipath propagation in WSN. The next part of the implementation is associated with the validation of the message. The first part of the validation process includes assessing the encoded message from the source cluster head to possess a replicate file of public key (Line-5). Upon successfully finding the copy of the public key, the receiving node then performs series of checks.

In the preliminary checks i) if the public key Q is more than 0, ii) the numerical score of the public key should lie within the same elliptical curve, and iii) there should be only specific number of public key. Upon finding all the validated cases of the public key, the next step of the algorithm will be to check the contents of the encoded message i.e. implicit parameter and public key are of integer type. In case, they are found not be of integer type than it is believed that certain malicious codes are internally being executed which could tamper the key and resulting in real numbers and hence in such case the signatures are rejected. This operation is followed by applying cryptographic hashing function over message *msg* and implicit parameter (Line-6). Private and public key are computed in subsequent step (Line-7). The final step of this algorithm is to assess if the value of the implicit parameter of the summation of the scalar product of implicit parameter and public key is found equivalent to private key. Otherwise, the algorithm declares the signature to be damaged and hence they finally reject the signature if found tampered. Only in validated condition, the algorithm allows successful continuation of data delivery or else it disrupts all the communication from the other node whose signature is revoked. This information is finally updated to other nodes so that the infected node cannot intrude other regular nodes during the process of data aggregation. Hence, the proposed system offers significant coverage of safety after the data aggregation process too.

III. RESULT ANALYSIS

The scripting of logic of the proposed study is carried out in MATLAB environment using 200-500 sensor nodes deployed in 1100x1200m^2 simulation areas. The study outcome is compared with existing schemes of predistribution of keys in WSN, where the outcomes are compared with probabilistic scheme, deterministic scheme, and hybrid scheme. All the outcomes of existing approaches are averaged in order to simplify the comparative analysis.

The outcome shown in Fig. 2 and Fig. 3 shows that proposed system offers reduced execution time in comparison to the existing strategies of key predistribution in WSN. It can be seen that execution time for authentication algorithm is quite reduced in comparison to the existing system. However, the time for the second algorithm is analysed with further two more factors i.e. Signature generation time and signature validation time. The signature generation time for proposed system is found to be 0.3869 seconds while that of existing system is 0.7442 seconds. Similarly, the signature validation time for the proposed system is 0.2651 seconds while that of existing system is found to be 0.5421 seconds. Hence, cumulatively, proposed system offers better performance in comparison to existing system of predistribution of keys in WSN. Another reason for faster processing time is reduced dependencies of storing the pre-distributed keys as the secret keys once relayed is directly used by the node and doesn’t required to be stored. Apart from this the signatures also undergo the same process and hence, there is less memory consumption for the proposed system in contrast to existing system.

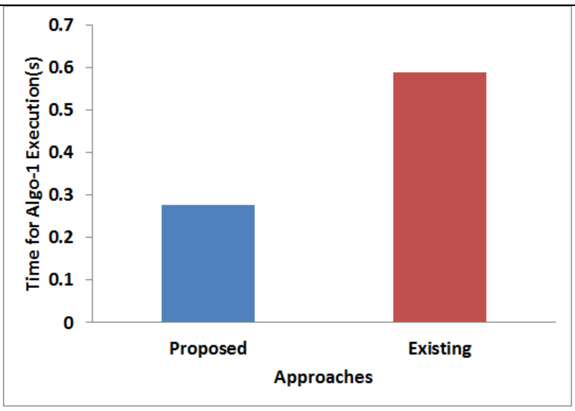

Fig. 2 Comparative Analysis of Execution Time of 1st Algorithm

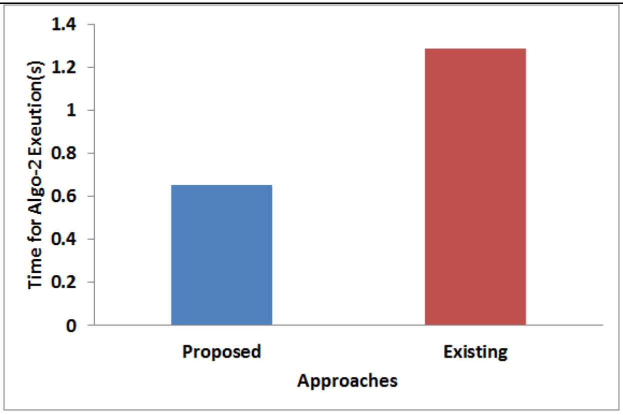

Fig. 3 Comparative Analysis of Execution Time of 2nd Algorithm

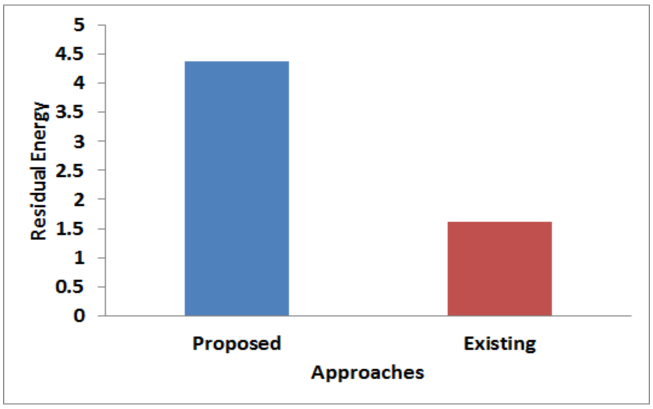

Fig. 4 Comparative Analysis of Residual Energy

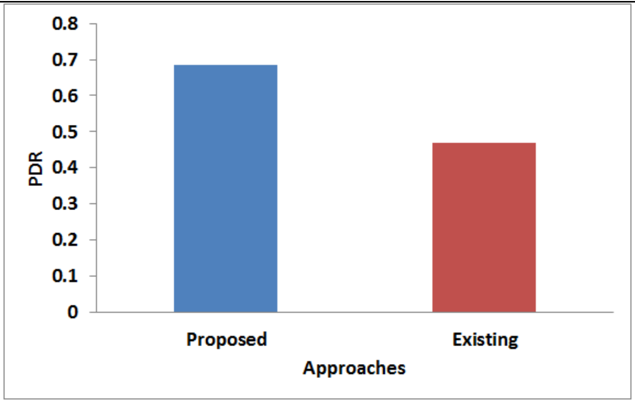

Fig. 5 Comparative Analysis of Packet Delivery Ratio

Fig. 4 and Fig. 5 highlight the comparative analysis of residual energy as well as packet delivery ratio. Owing to the usage of public key encryption, it is inevitable that there will be two forms of keys as well as it will be recursive in its operation. Therefore, there are fairer chances of drainage of energy among the sensors while performing data aggregation and security operation all together. The analysis shows that consumption of energy is quite reduced for proposed system as shown in Fig.4. The prime reason behind this is proposed system doesn't have any form of recursive operation and it is only progressive. Apart from this, the usage of elliptical curve cryptography is amended in such a way that it doesn't generate all the prime numbers (as private keys), but it generates one best number out of it. This causes 80% reduction of iterations for generation prime fields in elliptical curve cryptography and hence, no much memory or iterations are demanded in proposed system. Hence, residual energy is high for proposed system. On the other hand, packet delivery ratio of the proposed system is found to be in good performance as shown in Fig.5.

The prime reason behind this is proposed system uses multipath propagation where the authentication is carried out in very faster mode. This results in faster processing of secured routes with lesser dependency on key management schemes unlike existing system. Apart from this, the mechanism of validation also requires only few parameters which are based on encoded message and hashing thereby it leads to faster dissipation of the data packets where the authentication effort is reduced. Hence, a good score of packet delivery ratio can be witnessed in proposed system. Hence, the proposed system offers significantly better security and with its respective good balance with the communication performance too.

IV. CONCLUSION

Offering potential security standards for the resource constraint nodes in WSN is one of the most challenging tasks. However, there are many key management approaches being evolved in existing time where it is found that pairwise key predistribution offers better key management strategies in WSN. Therefore, this approach discusses about the novel simplified integrated framework that carry out optimization of the pairwise key predistribution approach using joint implementation of enhanced public key cryptography and digital signature. The study outcome shows that proposed system offers better outcomes in contrast to existing system.

ACKNOWLEDGEMENT

The successful completion of research paper would be incomplete without the mention of the people who made it possible and whose constant guidance was very much helpful. We express our sincere gratitude to our Management and Principal of K S Institute of Technology, Bengaluru and Vidya Academy of Science and Technology, Thrissur for providing all the facilities and resources required for accomplishing research work. We thank Dr. Rekha B.Venkatapur, Professor and Head, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for her encouragement.

REFERENCES

1. Jiang, Joe-Air, Chien-Hao Wang, Chi-Hui Chen, Min-Sheng Liao, Yu-Li Su, Wei-Sheng Chen, Chien-Peng Huang, En-Cheng Yang, and Cheng-Long Chuang. "A WSN-based automatic monitoring system for the foraging behavior of honey bees and environmental factors of beehives." Computers and Electronics in Agriculture 123 (2016): 304-318.
2. Song, Aijuan, and Guangyuan Si. "Remote monitoring system based on Zigbee wireless sensor network." In 2017 29th Chinese Control And Decision Conference (CCDC), pp. 2618-2621. IEEE, 2017.
3. Xu, Xi, Rashid Ansari, Ashfaq Khokhar, and Athanasios V. Vasilakos. "Hierarchical data aggregation using compressive sensing (HDACS) in WSNs." ACM Transactions on Sensor Networks (TOSN) 11, no. 3 (2015): 45.
4. Boubiche, Djallel Eddine, Sabrina Boubiche, Homero Toral-Cruz, Al-Sakib Khan Pathan, Azzedine Bilami, and Samir Athmani. "SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs." Telecommunication Systems 62, no. 2 (2016): 277-288.
5. Ali, Rifaqat, Arup Kumar Pal, Saru Kumari, Marimuthu Karuppiah, and Mauro Conti. "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring." Future Generation Computer Systems 84 (2018): 200-215.
6. Srinivas, Jangirala. "Design and Analysis of User Authentication and Key Agreement Schemes for Wireless Sensor Networks." PhD diss., IIT, Kharagpur, 2017.
7. Sodhi, Gurpreet Kour, Gurjot Singh Gaba, Lavish Kansal, Mohamed El Bakkali, and Faisel Em Tubbal. "Implementation of message authentication code using DNA-LCG key and a novel hash algorithm." International Journal of Electrical and Computer Engineering 9, no. 1 (2019): 352.
8. Choi, Younsung. "Cryptanalysis on Privacy-Aware Two-Factor Authentication Protocol for Wireless Sensor Networks." Indonesian Journal of Electrical Engineering and Computer Science 8, no. 2 (2017): 296-301.
9. Bhatia, Sugandh, and Jyoteesh Malhotra. "CSPCR: Cloud Security, Privacy and Compliance Readiness-A Trustworthy Framework." International Journal of Electrical and Computer Engineering 8, no. 5 (2018): 3756.
10. Vaneeta, M., and S. Swapna Kumar. "NPKG: Novel Pairwise Key Generation for Resisting Key-based Threats in Wireless Sensor Network." IJ Network Security 21, no. 1 (2019): 122-129.
11. Albakri, Ashwag, and Lein Harn. "Non-Interactive Group Key Predistribution Scheme (GKPS) for End-to-End Routing in Wireless Sensor Networks." IEEE Access 7 (2019): 31615-31623.
12. Gandino, Filippo, Renato Ferrero, and Maurizio Rebaudengo. "A key distribution scheme for mobile wireless sensor networks: $ q $-$ s $-composite." IEEE Transactions on Information Forensics and Security 12, no. 1 (2016): 34-47.
13. Yagan, Osman, and Armand M. Makowski. "Wireless sensor networks under the random pairwise key scheme: Can resiliency be achieved with small key rings?." IEEE/ACM Transactions on Networking (TON) 24, no. 6 (2016): 3383-3396.
14. Harn, Lein, and Ching-Fang Hsu. " scheme for establishing group keys in wireless sensor networks." IEEE Sensors Journal 15, no. 9 (2015): 5103-5108.
15. Yavuz, Faruk, Jun Zhao, Osman Yağan, and Virgil Gligor. "Toward $ k $-connectivity of the random graph induced by a pairwise key scheme with unreliable links." IEEE Transactions on Information Theory 61, no. 11 (2015): 6251-6271.
16. Yagan, Osman, and Armand M. Makowski. "Modeling the pairwise key scheme in the presence of unreliable links." IEEE Transactions on Information Theory 59, no. 3 (2012): 1740-1760.
17. Rasheed, Amar, and Rabi Mahapatra. "Key schemes for establishing pairwise keys with a mobile sink in sensor networks." IEEE Transactions on Parallel and Distributed Systems 22, no. 1 (2010): 176-184.
18. Afianti, Farah, Wirawan Wirawan, and Titiek Suryani. "Lightweight and DoS Resistant Multiuser Authentication in Wireless Sensor Networks for Smart Grid Environments." IEEE Access (2019).
19. Du, Hongzhen, Qiaoyan Wen, and Shanshan Zhang. "An Efficient Certificateless Aggregate Signature Scheme Without Pairings for Healthcare Wireless Sensor Network." IEEE Access 7 (2019): 42683-42693.
20. Deepa .S.R, Rekha .D, “Cluster optimization in Wireless sensor networks using particle swarm optimization” in Social Transformation – a Digital way, CCIS-Springer, Volume 836, pp 240-253
21. Zhang, Jianhong, Wenle Bai, and Yuehai Wang. "Non-Interactive ID-Based Proxy Re-Signature Scheme for IoT Based on Mobile Edge Computing." IEEE Access 7 (2019): 37865-37875.
22. Yang, Wenjie, Shangpeng Wang, Xinyi Huang, and Yi Mu. "On the Security of an Efficient and Robust Certificateless Signature Scheme for IIoT Environments." IEEE Access 7 (2019): 91074-91079.
23. Zhu, Hongliang, Ying Yuan, Yuling Chen, Yaxing Zha, Wanying Xi, Bin Jia, and Yang Xin. "A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature." IEEE Access 7 (2019): 90036-90044.
24. Xie, Yong, Xiang Li, Songsong Zhang, and Yanggui Li. "$ iCLAS $: An Improved Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Networks." IEEE Access 7 (2019): 15170-15182.
25. Chang, Chin-Chen, Wai-Kong Lee, Yanjun Liu, Bok-Min Goi, and Raphael C-W. Phan. "Signature gateway: Offloading signature generation to IoT gateway accelerated by GPU." IEEE Internet of Things Journal (2018).
26. Shim, Kyung-Ah. "BASIS: a practical multi-user broadcast authentication scheme in wireless sensor networks." IEEE Transactions on Information Forensics and Security 12, no. 7 (2017): 1545-1554.
27. Ting, Pei-Yih, Jia-Lun Tsai, and Tzong-Sun Wu. "Signcryption method suitable for low-power IoT devices in a wireless sensor network." IEEE Systems Journal 12, no. 3 (2017): 2385-2394.
28. Wei, Zhuo, Yang Yanjiang, Yongdong Wu, Jian Weng, and Robert H. Deng. "HIBS-ksharing: Hierarchical identity-based signature key sharing for automotive." IEEE Access 5 (2017): 16314-16323.
29. Liu, Zhe, Hwajeong Seo, Johann Großschädl, and Howon Kim. "Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes." IEEE Transactions on Information Forensics and Security 11, no. 7 (2015): 1385-1397.
30. Lo, Nai-Wei, and Jia-Lun Tsai. "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings." IEEE Transactions on Intelligent Transportation Systems 17, no. 5 (2015): 1319-1328.

AUTHORS PROFILE

Vaneeta M is Associate Professor in Department of Computer Science and Engineering, K. S Institute of Technology, Bengaluru, Affiliated to VTU, Belagavi, Karnataka, India. She received B.E degree in in Computer Science and Engineering from Dr. BAMU University, Maharashtra and M.E degree in Computer Science and Engineering, Anna University. She is currently pursuing her Ph.D. degree in Computer Science and Engineering, Visvesvaraya Technological University, Belagavi. She is a member of the institution of engineers IEI (India).She has also a life membership of several professional bodies, including Indian Society for Technical Education (ISTE) and CSI. 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 and 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 a books on ``A Guide to Wireless Sensor Networks'' and ``MATLAB easy way of learning''. Dr. S. Swapna Kumar is a Fellow Member and Chartered Engineer of the Institution of Engineers (INDIA). His area of interest includes Networking, Security system, Fuzzy Logic, Data Communication, Electronics, Communication Systems, Embedded Systems, MATLAB modeling and simulation.