International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2019, pp. 2682~2690
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp2682-2690

N-tier modelling of robust key management for secure data aggregation in wireless sensor network

Jyoti Metan[1], K. N. Narashinha Murthy[2]
[1]Department of Computer Science & Enggineering, ACS College of Engineering, India
[2]Faculty of Engineering, Christ University, India

Article Info

Article history:

Received Jun 20, 2018
Revised Jan 12, 2019
Accepted Mar 4, 2019

Keywords:

Attack
Adversary
Cryptography
Public key encryption
Wireless sensor network

ABSTRACT

Security problems in Wireless Sensor Network (WSN) have been researched from more than a decade. There are various security approaches being evolving towards resisting various forms of attack using different methodologies. After reviewing the existing security approaches, it can be concluded that such security approaches are highly attack-specific and doesnt address various associated issues in WSN. It is essential for security approach to be computationally lightweight. Therefore, this paper presents a novel analytical modelling that is based on n-tier approach with a target to generate an optimized secret key that could ensure higher degree of security during the process of data aggregation in WSN. The study outcome shows that proposed system is computationally lightweight with good performance on reduced delay and reduced energy consumption. It also exhibits enhanced response time and good data delivery performance to balance the need of security and data forwarding performance in WSN.

Corresponding Author:

Jyoti Metan,
Department of Computer Science & Enggineering,
ACS College of Engineering,
Bangalore, India.
Email: jyotimetan@gmail.com

1. INTRODUCTION

A Wireless Sensor Network (WSN) has completely redefined itself as it enters the arena of futuristic technology called as Internet-of-Things (IoT) [1]. It is believed that IoT is all about integrating sensor nodes with cloud in order to exponentially expand the network size as well as capability [2]. At present, there are various research work already carried out towards WSN domain [3, 4] as well as on IoT domain [5, 6]. However, it is required to think much number of times about the successful possibility of implication of this.

The first reason of security challenges will be difference in the form of network or heterogeneity aspect of it. Both cloud and WSN are totally different technologies and have different form of protocols to control data communications. Middleware is used in gateway nodes in order to handle the heterogeneity aspect in cloud itself as well as in WSN itself. However, these forms of middleware are very much advanced in work operation in contrast to middleware devices used in gateway system of IoT as they have comparatively very much reduced capability for assisting in data translational services [7].

This problem will result in non-implications of security problems that are already proven to be successful in handling threats in cloud as well as in WSN individually, However, there is no universal or common security protocol that could control security threats when WSN is connected in cloud. Hence, usage of such system will cause failure in identification of threats itself. Hence, irrespective of lot of work in intrusion prevention system in WSN, they are not directly applicable in IoT [8]. This is the prime reason that foretells why at present IoT uses simplified node connectivity and not actually the connectivity described by

WSN. It will directly mean IoT deploys sensors but not directly typical WSN at present in any commercial application. It is still in nascent stage of research.

The second reason of security challenges is that there are serious of robust encryption algorithms over cloud or internet [9]; however, very least proportion of any of such security algorithms can be actually implemented over sensor node. It is because a sensor node has very less computational capability as well as less availability of necessary resources to carry out high end processing. Hence, complex cryptographic algorithm that runs successfully over other networks will not work out in sensor nodes.

The third reason of security challenges in WSN is that it has a supportability of wide ranges of applications of different types. These applications have different forms of data forwarding requirements that usually depends on routing behaviour. Irrespective of availability of secure routing protocols in WSN [10], there are very a smaller number of schemes that has been proven to be resilient against upcoming or all major threats in it.

The third reason behind this security problem is also about modeling approach used till date. There is less utilization of hybridizing models and more emphasis is given to evolve up with a solution that could just minimize the security threat. It has to be understood that security problems are also closely related to many other problems in WSN. It will mean that an inappropriate modeling will definitely lead to various hidden problems among the sensor node. In such case, robust security can be achieved at the cost of inferior data delivery performance. Therefore, proposed system offers a solution towards such security problem in WSN so that they can be securely integrated to IoT applications in future.

The manuscript presents a discussion of an analytical model that uses n-tier approach to resists the maximum forms of lethal threats in WSN. Section 1.1 discusses about the existing literatures where different techniques are discussed for security schemes used in WSN followed by discussion of research problems in Section 1.2 and proposed solution in 1.3. Section 2 discusses about algorithm implementation where a detection algorithm as well as an optimized version of its is presented followed by discussion of result analysis wih respect to comparative analysis with frequenty used encryption algorithms as well as most cited research work in Section 3. Finally, the conclusive remarks are provided in Section 4.

This section discusses about the existing security approaches in WSN as a part of extension of our prior review work [11]. The work carried out by Nurellari et al. [12] has presented a mechanism to identify the attacker using probability theory. Most recently a unique security approach was presented by Yang et al. [13] where duty cycle is considered as one of the main indicators of security. Rana et al. [14] have discussed about attack resistivity in vehicle system using WSN. The author has developed a hardware-based control system that uses feedback for obtaining system stabilization in WSN. Guan and Ge [15] have presented a study that could offer security against jamming attack in multichannels. The authors have used Markov chain in order to design the solution.

Wei et al. [16] have presented a technique where the localization of the WSN is protected against Byzantine attack using probability theory modeling on received signal strength. Zou et al [17] have presented a discussion about the eavesdropping attack in order to understand the attack behaviour. Deng et al. [18] have applied stochastic-based geometrical approach as a solution towards security problems in physical layers. The authors have considered three-tier approach that has resulted in optimization of secrecy rate. Li et al. [19] have presented solution towards resisting wormhole attack where the solution is modeled on the basis of connectivity among the neighboring nodes. The work also addresses the localization problems that occur in malicious environment.

Kim and An [20] have presented a thematic model for resisting denial of service attack. Similar direction of work is also being carried out by Gope et al. [21]. Different forms of complex attacks in WSN have been discussed by Wu et al. [22] where an analytical-based modeling has been designed with respect to discrete rule set with the sink node to offer security. The technique also introduced a novel virtualization technology to further offer better resistivity in WSN. Solution towards resisting node capture attack has been carried out by Zhao et al. [23] using key Predistribution scheme. Channel state information is also reported to contribute security feature as seen in the work of Gong et al. [24]. The study carried out by Ren et al. [25] have addressed problems associated with selective forwarding attack using reputation-based approach in order to identify thestate of compromization in WSN.

The work of Al-Hamadi and Chen [26] has implemented a secure multipath routing mechanism for prevention purpose against lethal threats in WSN. Chu et al. [27] have presented a hardware-based approach n order to develop a lightweight encryption protocol for assisting in authentication. Hsueh et al. [28] have presented a cross layer-based approach to address the problems associated with energy depleting attacks in WSN. Solution towards jamming attack and sinkhole attack has been discussed by Pintea et al. [29] and Han et al. [30] respectively. Soosahabi et al. [31] have presented a detection mechanism for offering better form of physical layer security in WSN. The study also uses probability theory in order to perform modeling that was carried out using analytical approach.

Jyoti Metan and Narashinha Murthy [32] have introduced a structure for security in data aggregation in the WSN for improving the key managing. Manjunath B.E and Rao [33] have demonsgtaretd a technique of security in the framework of WSN which is presented two kinds of sensor node deployed with various abilities. Fissaoui et al. [34] have illustrated and published to enhance power consumption in every field of the WSNs, such as, a) localization, b) a) routing, c) coverage, d) security, etc. The next section highlights the significant limitation explored from above mentioned security-based approach in WSN.

The significant research problems are as follows:

- Existing security-based approaches are highly specific to attack and there is no solution considering hybridizing the attack or considering uncertainty part of it.
- More work is carried out towards detection technique as compared to prevention technique towards different threats models.
- Irrespective of lot of work on key management technique, there are very less number of techniques that could offer robust security to the generated key.
- Less work towards optimizing the encryption process has been reported in existing system that fails to resists the computational overhead in existing security system.

Therefore, the problem statement of the proposed study can be stated as "*Developing a cost effective modeling towards incorporating higher degree of resiliency against maximum forms of threats in WSN is a computational challenging task*". The next section presents the solution to this problem.

The prime goal of the proposed system is to develop an n-tier modeling of key management for securing communication in WSN. The proposed system is built considering n-tier model, which is a standard architecture for industry-based software models. The complete idea is based on the fact that a clusterhead will have an increasing dependency of a secret key especialy during the data aggregation process and in absence of secure key, the clusterhead may poison the complete network very slowly leading to collateral attack scenario. Hence, an analytical approach is considered to develop an approach that can generate a secret key to be used in data aggregation. The core emphasis of the proposed implementation plan is also to ensure highest deal of privacy and integrity in any forms of communication of WSN considering all the major scenario of threats.

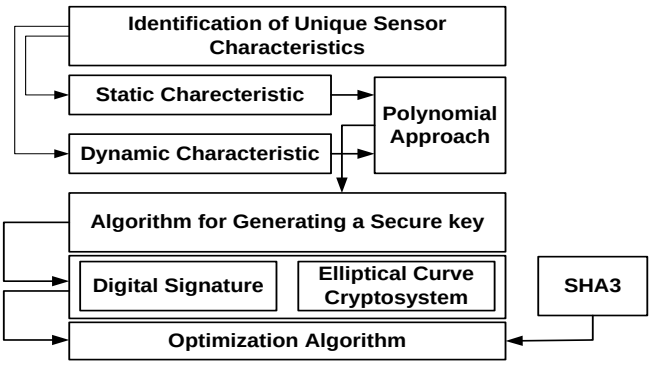

Figure 1. Flow of adopted policy towards key management

Unlike conventional security algorithms, the proposed system chooses to represent the sensor node not merely with an id but with different form of id that bears both static charecteristics (e.g. name, IP address, MAC address, Factory default keys etc) and dynamic charecteristic (time stamp). A mathematical expression using polynomial approach has been constructed that uses both the features in order to generate a secret at the end. The first algorithm for generation of secret key is designed on the basis of the concept that factory-default keys should not be used for authentication and should generate new secret key. It is because factory default keys can be easily compromised during usage of public key encryption. This algorithm further encrypts this key using novel SHA3 in order to compute the exact value of shared key. The possession of shared key can be only with legitimate nodes. Even if they are captured, the time stamp factor would assists in identifying whether the received key has been generated by the regular node or the malicious node. The further improvement is carried out by incorporating optimization towards the process of generating the secret key. For this purpose, the system redesigns the digital signature and improves Elliptical Curve Encryption for yielding faster secret key with non-overlapping charecteristics among the generated keys. The next section further illustrates the algorithm design principle.

2. ALGORITHM IMPLEMENTATION

In order to design an algorithm for performing an n-tier modeling of key generation system, it is required to identify some of the unique elements to be used in key design. Emphasing on the forward and backward secrecy, the proposed algorithm considers that a sensor node be identified using three different elements where two elements i_1 and i_2 represent static feature of node while third element i_3 represents dynamic feature of node. The proposed n-tier modeling of key management technique in WSN is carried out using two essential algorithms viz. Algorithm for generating a secure key and Optimized Algorithm for Secure Key Generation.

The first algorithm is responsible for ensuring the fact that there should be presence of certain unique key when two sensor nodes from different clusters perform communication among each other. The term level means routing stages of data aggregation i.e. 1st level corresponds to securing routes between member nodes and clusterhead, 2nd level corresponds to that of clusterhead to another clusterhead, while third level corresponds to securing link between clusterhead to sink. As the clusterhead bears enough physical information of its member node along with other information e.g. battery life, buffer etc, hence chances of member node being rogue is not considered. Hence, the study is more dominant for 2nd and 3rd level of data aggregation. For this purpose, the system initially considers assuming intruder module that has recently intruded the network either using inside or outside attacking strategy. The discussion of the algorithm is as follow:

Algorithm-1: Algorithm for Generating a Secure key
Input: τ (Sensor key), θ (sensor tag)
Output: K (Secure key)
Start
1. init τ, θ,
2. **For** i=1:n_{node}
3. **If** ($i_{3A} \neq i_{3B}$)
4. **If** ($p \neq 0$)
5. **If** (γ_1 && $\gamma_2 < \tau$)
6. K=$\psi((D_{ij} || \theta || \theta)$, 'SHA3')
7. **End**
8. **End**
9. **End**
10. **End**
End

The primary assumption of this algorithm is to realize the pitfalls of usage of symmetric keys during the broadcasting mechanism on the wireless channels of sensor network. Therefore, possibility of attacking the factory-built keys are quite highalways. Therefore, this algorithm doesn't depent on using factory-built keys for securing communication rather its re-compute dynamicall the secret key to offer more level of security. The algorithm initializes the sensor key as well as sensor tags (Line-1), where each tag bears the novel charecteristics of sensor i.e. i_1, i_2, and i_3. The algorithm compares the dynamic feature of the sensor A i.e. i_{3A} with that of sensor B i.e. i_{3B} (Line-3). This operation is carried out only for communicating nodes (n_{node}) and only genuine node is expected to have different dynamic features otherwise one of the communicating nodes is considered to be compromised if the dynamic feature from two communicating sensors is found to be same. The algorithm then applies a polynomial function over the two-static feature of the sensor node i.e. $f(x) \rightarrow (i_1, i_2)$.

In case of non-negative value of polynomial function (Line-4), the mathematical expression is considered to be valid and the algorithm further checks for the scenario shown in Line-5, where γ_1 and γ_2 are considered to be two sub-polynomial expressions derived from $f(x) \rightarrow (i_1, i_2)$. The secure key is generated by applying an encryption algorithm of SHA3 over the double concatenated data of (γ_1 and γ_2) and [θ θ]. This leads to generation of a secure key that could be used for securing the data aggregation. The proposed system applies SHA3, which is a novel cryptpgraphic algorithm. An interesting fact to find in usage of this algorithm is that there is only one step of encryption, which states that the algorithm does not have recursive encryption operation nor does it could bring more amount of network overhead. Owing to intellectual usage of both static and dynamic charecteristic of a sensor node, this algorithm has a higher supportability of both forward and backward secrecy that is highly essential to securing communication in WSN. Another important point to observe is that SHA3 is comparatively a new encryption technique which doesn't has a full specification of implementation till date as it is quite novel. Hence, it is required to further optimize the security strength of the key generation algorithm that is carried out in next stage of implementation.

This algorithm uses improved version of digital signature in order to further optimize the security strength of Elliptical Curve Cryptography emphasizing on the privacy and integrity issues. One of the unique facts about usage of such public key encryption mechanism is its capability to generate much number of robust secret keys. However, the proposed system develops a simple objective function to select only one secret key out of all the possibilities of generation of secret key altering the prime numbers. This can be controlled by restricting the order value of Elliptical Curve Cryptography. Hence, the order with its corresponding limit is emphasized in this algorithm. The initiation of the algorithm calls for forwarding the message by the transmitting node to the receiving sensors. In order to control the necessary network and computational overhead, the algorithm performs random selection of the key with the limit of 1 and (U-1). Therefore, the complete hybridization process of n-tier modeling is carried out considering Digital Signature and Elliptical Curve Cryptography. The steps involved are as follows:

Algorithm-2: Optimized Algorithm for Secure Key Generation
Input: n (number of communicating nodes)
Output: K_{op} (optimized secure key)
Start
1. **For** i=1:n
2. **If** α=0
3. Select r_1
4. **Else**
5. Compute V_1 and V_2
6. **If** $V_2 \rightarrow 0$
7. Compute α
8. **Else**
9. $k_{op} \rightarrow (\alpha, V_2)$
End

The algorithm implements Elliptical Curve Encryption in order to perform optimization which performs optimization towards further increasing the security strength. The algorithm chooses all the communicating nodes and checks if α is equivalent to zero (Line-2). The computation of α is carried out by scalar multiplication of location information of node with highest limit of order. In case α=0 than the algorithm randomly selects an integer type r_1 (Line-3); otherwise, the algorithm performs computation of two variables V_1 and V_2 (Line-5). The computation of V_1 is carried out by applying an encryption function over contro message and computed α value while the computation of V_2 is carried out by adding a random variable with the product of r_1 and upper limit of order. The algorithm further computes α if V_2 is found to be equivalent to zero (Line-6) otherwise the extraction of the optimized key k_{op} is carried out over α and V_2 (Line-9) to complete the step of optimization. A closer look into the above algorithmic steps will show that it hybrids the elliptical curve cryptography with typical signature in order to generate a light weight and dynamic security token that is required to maintiain higher degree of privacy as well as confidentiality. At the same time, the algorithm also contributes to minimization of the computational overhead as well.

After the execution of the optimization process is over, the next step is to perform validation operation that is usually carried out over the receiver side that assumes the possession of public key of the source node. The algorithm aborts any form of communication if its finds absence of any non-zero public key otherwise it assesses the numerical content within the key. The numerical content of this key is expected to be within the range of order defined in previous algorithm. Interesting, if there is presence of any non-integer form of key than it is considered to be generated by malicious node and any connection with such node is instantly dropped. Apart from this information related to such node as well as neighboring nodes of such victim/compromized node is instantly updated to all the other sensor nodes for additional security. Another interesting fact is that the algorithm doesn't repeat the same steps used in encryption or in key generation process, which makes the proposed system more resistive towards backward secrecy. In such case, the algorithm considers the location-based information in order to perform validation apart from usage of V_1. The reason behind selection of location-based information is not to retain priorly-used dynamic feature i.e. time-stamp but to replace it with location. This design principle significantly reduces network overhead as well as computational overhead too to a large extent. The algorithm doesn't allow the routing to be confirm and aborts the connection once the first stage of validation itself fails. Hence, in a smart manner, the algorithm offers security to its neighboring nodes also. Moreover, owing to utilization of non-recursive approach, the algorithm offers significant advantage in terms of communication efficiency with reduced computational burden apart from its security capability.

3. RESULTS AND ANALYSIS

The implementation of the proposed study has been carried out considering IEEE 802.15 MAC protocols where the sensors are initialized to 0.5 joules of energy. Considering 1100x1200m^2 simulation area, the results have been captured for 600-1000 sensor nodes over 1000 simulation rounds with beacon size of 250 bytes and packet size of 1000 bytes. For better analysis, the proposed system performs comparative anlaysis with the existing system with respect to each algorithm implementation.

The first algorithm towards generating secure key is compared with the work carried out by Tang [35] and Roy [36] owing to similiarity in the research goal towards resisting potential attacks in WSNe.g. flooding attack, sinkhole attack, Sybil attack, etc. The outcome shows that proposed system offers significantly less delay as compared to existing system as shown in Figure 2 and more energy retention as shown in Figure 3. The prime reason behind this is that the exitsing approaches of Tang [35] and Roy [36] have increasingly used higher number of recursive steps in order to offer resistance againsts maximum number of defined threats. This causes the algorithm to focus more on security and less on its adverse effect towards communication process. However, the proposed algorihm is completely free of any such features. In due course of time, proposed algorithm offers better results. This fact is further verified with respect to response time as shown in Figure 4. When compared with the standard and frequently used encryption algorithms e.g. MD5, SHA-1, SHA-2, and blowfish, the proposed study is found to offer faster response time. This evidently proves that proposed algorithm for generating a key is less computationally complex and therefore is highly scalable in nature of implementation.

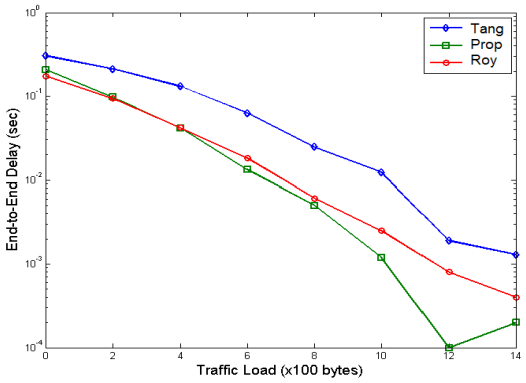

Figure 2. Delay performance

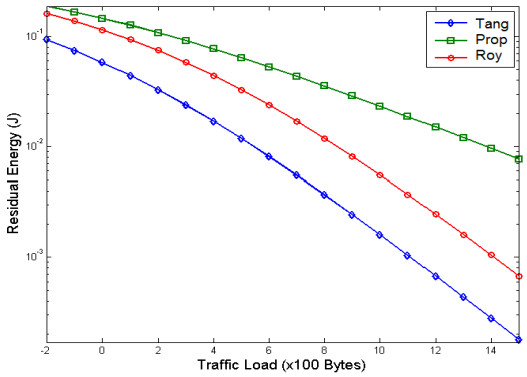

Figure 3. Residual energy performance

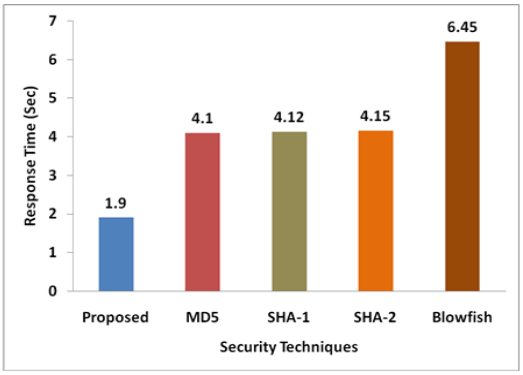

Figure 4. Response time analysis with standard encryption techniques

The result shown in Figure 5 until Figure 8 represents the outcome of optimized algorithm implementation, which is the second algorithm in this paper. It should be known that AES is one of the most secured encryption algorithms adopted world wide owing to its lightweight operations in any device. A closer look into Fig.5 will show that proposed system offers better delay control even compared to AES. Although, SHA-2 is found to offer slightly reduced delay than AES, but they are never recommended tobe used owing to its dependencies over higher value of key sizes. Apart from this, proposed syste also exhibits better energy conservation as compared to existing AES or SHA-2. It should be known thatproposed system doesn't completely implement SHA3 as complete specification of SHA3 is yet not available. However, a slight

initiative towards SHA3 development shows much better energy conservation for proposed system, which is truly a contribution towards energy efficient security system over WSN. The proposed n-tier modeling can thereby be claimed to offer reduced delay over increasize packet size and higher control of energy depletion over increase of inclusion of number of sensors.

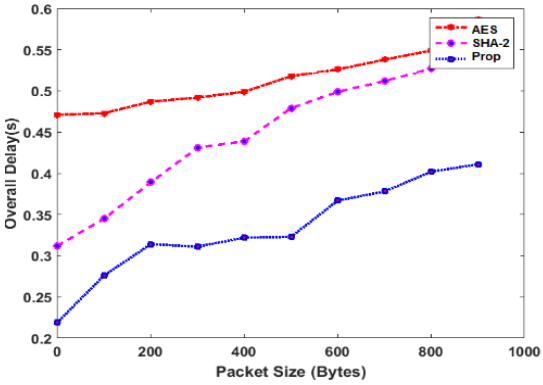

Figure 5. Delay analysis with standard encryption

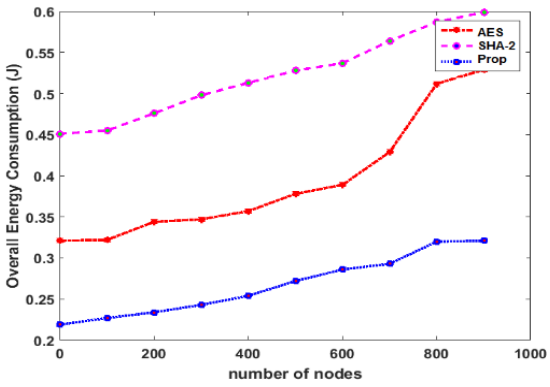

Figure 6. Energy consumption analysis with standard encryption

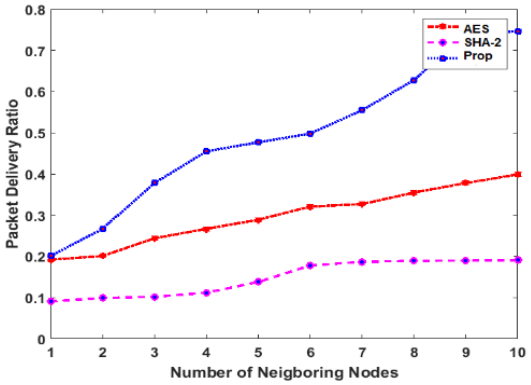

Figure 7. Packet delivery ratio analysis with standard encryption

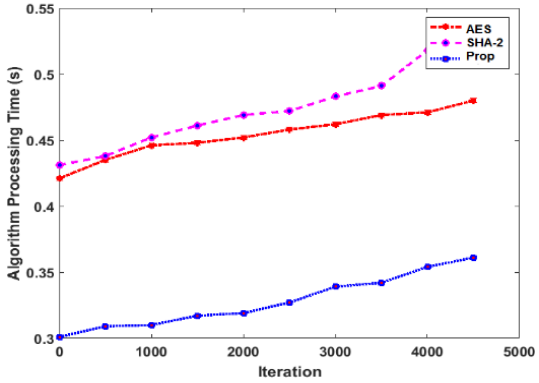

Figure 8. Optimization algorithm processing time analysis

From the data-delivery viewpoint, proposed system is found to offer increased packet delivery ratio with increasing of number of neighboring nodes as shown in Figure 7. Owing to non-inclusion of any kinds of iterative steps, the proposed study offers good deal of packet delivery ratio. In contrast to the existing system. Total time for an optimized algorithm execution is also assessed with respect to iterations to find that proposed system offers highly reduced algorithm processing time. A closer look into Figure 4 and Figure 8 will show that optimization positively contributes to reduce the algorithm processing time of proposed system, where priorly it was 1.9 seconds and later after optimization, it results in less than 0.35 seconds. It also highlights that performance of Elliptical Curve Cryptography is highly improved and it is now capable of offering secure key management as fast as possible and is better than any frequently used encryption technique or approaches practiced in present times.

4. CONCLUSION

The paper has presented an analytical model with the base idea that – when a clusterhead uses a compromised key or weaker version of any secret key, it not only victimizes itself but also make the complete network vulnerable. During data aggregation, a clusterhead must focus on forwarding an aggregated data and less on performing authentication, which will mean that an algorithm should have faster response time to keep a pace with the rate of data aggregation. Therefore, the proposed algorithm offers following contribution viz. i)

the complete modeling is carried out using n-tier architecture that has not been attempted previously in WSN. The advantage of this modeling is its closer acceptance towards indusrial modeling thereby showing applicability of proposed concept, ii) the complete work is made for resisting maximum number of lethal threat and its never meant for addressing only one form of threats, unlike existing system, iii) the proposed system retains a good balance between security and data delivery performance using non-recursive optimization steps.

REFERENCES

[1] R. Gravina, et al., "Integration, Interconnection, and Interoperability of IoT Systems," Springer, 2017.
[2] F. Al-Turjman, "Cognitive Sensors and IoT: Architecture, Deployment, and Data Delivery," CRC Press, 2017.
[3] Z. Zhang, et al., "A Survey on Fault Diagnosis in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 11349-11364, 2018.
[4] S. Boubiche, et al., "Big Data Challenges and Data Aggregation Strategies in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 20558-20571, 2018.
[5] H. Hejazi, et al., "Survey of platforms for massive IoT," *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*, Eger, pp. 1-8, 2018.
[6] I. I. Lysogor, et al., "Survey of data exchange formats for heterogeneous LPWAN-satellite IoT networks," *2018 Moscow Workshop on Electronic and Networking Technologies (MWENT)*, Moscow, pp. 1-5, 2018.
[7] E. Kim and C. Keum, "Trustworthy gateway system providing IoT trust domain of smart home," *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, Milan, pp. 551-553, 2017.
[8] S. H. Choi, et al., "Wireless intrusion prevention system using dynamic random forest against wireless MAC spoofing attack," *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, pp. 131-137, 2017.
[9] Z. Qin, et al., "A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing," *IEEE Transactions on Services Computing*, 2016.
[10] B. Bhushan and G. Sahoo, "A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks," *2017 International Conference on Signal Processing and Communication (ICSPC)*, Coimbatore, pp. 294-299, 2017.
[11] J. Metan and K. N. Narasimha Murthy, "Group Key Management Technique based on Logic- Key Tree in the Field of Wireless Sensor Network," *International Journal of Computer Applications*, vol/issue: 117(12), 2015.
[12] E. Nurellari, et al., "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol/issue: 4(2), pp. 325-337, 2018.
[13] X. Yang, et al., "CSI-based low-duty-cycle wireless multimedia sensor network for security monitoring," *Electronics Letters*, vol/issue: 54(5), pp. 323-324, 2018.
[14] M. M. Rana, "Attack Resilient Wireless Sensor Networks for Smart Electric Vehicles," *IEEE Sensors Letters*, vol/issue: 1(2), pp. 1-4, 2017.
[15] Y. Guan and X. Ge, "Distributed Secure Estimation Over Wireless Sensor Networks Against Random Multichannel Jamming Attacks," *IEEE Access*, vol. 5, pp. 10858-10870, 2017.
[16] C. Y. Wei, et al., "Local Threshold Design for Target Localization Using Error Correcting Codes in Wireless Sensor Networks in the Presence of Byzantine Attacks," *IEEE Transactions on Information Forensics and Security*, vol/issue: 12(7), pp. 1571-1584, 2017.
[17] Y. Zou and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," *IEEE Transactions on Industrial Informatics*, vol/issue: 12(2), pp. 780-787, 2016.
[18] Y. Deng, et al., "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach," *IEEE Transactions on Information Forensics and Security*, vol/issue: 11(6), pp. 1128-1138, 2016.
[19] J. Li, et al., "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wireless Sensor Systems*, vol/issue: 8(2), pp. 68-75, 2018.
[20] D. Kim and S. An, "PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks," *IEEE Sensors Journal*, vol/issue: 16(8), pp. 2217-2218, 2016.
[21] P. Gope, et al., "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," *IEEE Sensors Journal*, vol/issue: 17(2), pp. 498-503, 2017.
[22] J. Wu, et al., "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities," *IEEE Access*, vol. 4, pp. 416-424, 2016.
[23] J. Zhao, "On Resilience and Connectivity of Secure Wireless Sensor Networks under Node Capture Attacks," *IEEE Transactions on Information Forensics and Security*, vol/issue: 12(3), pp. 557-571, 2017.
[24] X. Gong, et al., "Cooperative security communications design with imperfect channel state information in wireless sensor networks," *IET Wireless Sensor Systems*, vol/issue: 6(2), pp. 35-41, 2016.
[25] J. Ren, et al., "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol/issue: 15(5), pp. 3718-3731, 2016.
[26] H. Al-Hamadi and I. R. Chen, "Adaptive Network Defense Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks," *IEEE Transactions on Network and Service Management*, vol/issue: 12(3), pp. 451-466, 2015.
[27] S. I. Chu, et al., "Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for Wireless Sensor Networks," *IEEE Systems Journal*, vol/issue: 11(4), pp. 2718-2725, 2017.

[28] C. T. Hsueh, et al., "A Secure Scheme against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks," *IEEE Sensors Journal*, vol/issue: 15(6), pp. 3590-3602, 2015.
[29] C. M. Pintea, et al., "Denial jamming attacks on wireless sensor network using sensitive agents," *Logic Journal of the IGPL*, vol/issue: 24(1), pp. 92-103, 2016.
[30] G. Han, et al., "Intrusion Detection Algorithm Based on Neighbor Information against Sinkhole Attack in Wireless Sensor Networks," *The Computer Journal*, vol/issue: 58(6), pp. 1280-1292, 2015.
[31] R. Soosahabi and M. N. Pour, "Scalable PHY-Layer Security for Distributed Detection in Wireless Sensor Networks," *2012 IEEE Vehicular Technology Conference (VTC Fall)*, Quebec City, QC, pp. 1-5, 2012.
[32] J. Metan and K. N. N. Murthy, "FSDA: Framework for Secure Data Aggregation in Wireless Sensor Network for Enhancing Key Management," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 8(6), pp. 4684-4692, 2018.
[33] B. E. Manjunath and P. V. Rao, "Balancing Trade off between Data Security and Energy Model for Wireless Sensor Network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 8(2), pp. 1048-1055, 2018.
[34] E. Fissaoui, et al., "Scalability aware energy consumption and dissipation models for wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 7(1), pp.424-431, 2017.
[35] D. Tang, et al., "Cost-aware secure routing (CASER) protocol design for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, pp. 960-973, 2013.
[36] S. Roy and A. K. Das, "Secure hierarchical routing protocol (SHRP) for wireless sensor network," in J. L. Mauri, et al., (eds.), *SSCC 2014. CCIS*, vol. 467, pp. 20-29, 2014.

BIOGRAPHIES OF AUTHORS

Jyoti Metan has received B.E. from Pune University, Pune, India in 2002 and M. Tech from VTU, Bangalore, India in 2009. She joined Department of Computer Science & Engineering, ACS College of Engineering Bangalore as Assistant Professor since 2012. Her research interest includes Cryptography, Wireless Sensor Networks and Security. She is a Life Member of the Indian Society for Technical Education (ISTE).

K. N. Narashinha Murthy received his PhD from Anaa University, Chennai, India in 2013. His research area includes Image processing, Wireless Sensor Network, Security and Key Managmenet. At present he is working as a Professor in the department of faculty of engineering, Christ University, Banaglore, India. He is having more than 17 years of teaching experience.