International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 6, December 2018, pp. 4684~4692
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp4684-4692

FSDA: Framework for Secure Data Aggregation in Wireless Sensor Network for Enhancing Key Management

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 Mar 7, 2017
Revised Jul 14, 2018
Accepted Jul 28, 2018

Keyword:

Encryption
Key management
Security
Wireless Sensor Network

ABSTRACT

An effective key management plays a crucial role in imposing a resilient security technique in Wireless Sensor Network (WSN). After reviewing the existing approaches of key management, it is confirmed that existing approachs does not offer good coverage on all potential security breaches in WSN. With WSN being essential part of Internet-of-Things (IoT), the existing approaches of key management can definitely not address such security breaches. Therefore, this paper introduces a Framework for Secure Data Aggregation (FSDA) that hybridizes the public key encryption mechanism in order to obtain a novel key management system. The proposed system does not target any specific attacks but is widely applicable for both internal and external attacks in WSN owing to its design principle. The study outcome exhibits that proposed FSDA offers highly reduced computational burden, minimal delay, less energy consumption, and higher data transmission perforance in contrast to frequency used encryption schemes 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 network is always shrouded by different forms of networking challenges that not only affects communication process about also equally affects the security features [1]. From different forms of wireless networks, Wireless Sensor Network (WSN) is one of the most successful deployments in commercial market. A sensory node assists in performing data aggregation from the environment where it is completely exposed to swarm of attackers. Till last decade, there has been various studied associated with attacks [2] and security solutions [3], [4] but none of them are claimed to be 100% resilient against all the attacks. Majority of the existing approaches towards security in WSN are mainly cryptographic in nature whereas there also exists studies that are non-cryptographic in nature e.g. [5], [6]. The cryptographic approaches mainly deals with key management system followed by iterative encryptions using either symmetric or asymmetric keys while non-cryptographic approaches deals with observation of certain form of significant behaviour of nodes followed by formulation of rule set to offer inference to such behaviour in terms of malicious or regular pattern.

In last 5 years, there has been various forms of improvement in WSN where heterogeneity is further studied in order to make it well prepared to be used in reconfigurable networks like Internet-of-Things (IoT) [7]. IoT is complete a new concept to design a smart city and calls for mainly integrating WSN with pervasive environment like cloud computing [8]. However, the biggest security concern in this regards are i) the attacks studied in WSN are very different from that in cloud environment, which has most potential to induce collateral network damage, ii) the translation mechanism of control message (generated from query

system) is quite challenging to be realized if heterogeneous WSN is integrated with cloud (at present IoT is implemented either in low scale network or in homogenous network), iii) identification of attacks from either side is quite difficult and has good chance of bypassing any firewall system if the security protocols doesn't have wide consideration of its environmental parameters, and iv) cost effectiveness is not emphasized in IoT nodes as majority of the IoT nodes do have fair possibilities of resources when demanded (unlike conventional WSN). There are also various studies on IoT that discuses about security improvement but very less work has been actually carried out till date owing to the novelty of the technology [9], [10]. With new levels of features being incorporated within IoT there is one thing that is going to be always there and that is *data aggregation*. Unlike conventional WSN, IoT offers data aggregation from only registered nodes but with new proliferation of mobile nodes it is very likely that adoption of mobile nodes will be leveraged for performing dynamic data aggregation.

Hence, an effective key management scheme is highly demands in this. Normally, the biggest challenge in forming a novel key management technique is to select the process of generation of key, which has to be motivated from certain existing encryption scheme. Unfortunately, existing encryption schemes are too specific of attacks and hence their applicability is quite narrowed [11]-[13]. There is a need of such design principle that can be equally applicable for resisting intrusions in WSN. Hence, we introduce one such solution by harnessing the potential features of public key encryption system in order to generate a lightweight ciphering policy that can be claimed for secure key management scheme in WSN. We also show that it is feasible for contruct a robust encryption scheme that is less iterative and more progressive without much demands of resources for its execution. Section 1.1 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 1.2 and proposed solution in 1.3. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

1.1. Background

This section updates research approaches towards strengthing key management followed by our prior investigation [14]. The work carried out by Wang *et al*. has presented a clustering approach for improving security in WSN using a verification of message [15]. Porambage *et al.* have introduced an authentication scheme for improving key management on certificates [16]. Study on mobile networks with an emphasis of key management was carried out by Kang *et al.* [17]. The authors have used key sharing approach as well as rekeying approach that is claimed to maintained better forward-backward secrecy. Lee *et al.* have presented a typical encryption scheme meant for securing ubiquitous devices [18]. Chen *et al.* have presented their key management scheme using symmetric encryption approach applicable on heterogeneous network [19]. Pereira *et al.* have investigated the security strength of different encryption techniques on Internet-of-Things (IoT) [20].

Adoption of Elliptical Curve Cryptography has been seen in work of Ibrahim and Dalkilic for secure transmission of node tags ID using mutual authentication process [21]. Sarkar and Mukherjee have discussed their key Predistribution scheme which has been repeatedly used even in past with few evidences of benchmarking [22]. Qi *et al.* have implemented a compressive sensing along with block encryption of 8-bit integer on sensor data [23]. Wu *et al.* have presented a framework design that performs identification of attacks using virtualization and software defined networks [24]. Deng *et al.* have used a stochastic approach for securing physical layers in WSN using multiple sink approach [25]. Umar *et al*. have used a cross-layer based approach that allows the trust factor to be used along with fuzzy logic implementation in order to offer resource security in WSN [26].

Nearly similar approach on physical layer as well as trus-based approach of security has also been carried out by Zhu *et al*. [27] as well as Qin et al. [28]. Shin *et al.* have presented a route optimization-based approach using trust factor for fault tolerant implementation of communication security in IoT [29]. Guan and Ge have used a random modeling approach using probability scheme for resising jamming attack in WSN [30]. Dai *et al.* have presented a verification method on its encoding system for minimizing the cost involved in secure query process [31]. The mechanism uses hashing and symmetric encryption. Al-Turjman *et al.* have presented a key aggrement strategy hat offers secure communication using mobile sinks with an aid of elliptical curve cryptography [32]. A framework for investigating the security strength of harvester node is designed by Vo *et al.* [33].

The authors have also presented a scheduling approach for improving the security upon physical layer. Lu *et al.* have presented a discussion of various conventional encryption schemes used in WSN [34]. There is various scale of security approaches used in improving key management techniques in recent times with more dominancy of usng elliptical curve cryptosystem, Secured Hash Algorithm (SHA), Advanced Encryption Standard (AES), etc. However, all of these approaches are also featured by pitfalls that are

required to be addressed in order to obtain supreme security. The next section briefs about such pitfall followed by proposed solution for addressing such pitfalls.

1.2. Identification of Issues

The unaddressed issues explored after reviewing existing approaches are:

a. Usage of complex and highly iterative cryptographic approaches ensures higher degree of security but doesn't emphasize on its applicability on sensors with constraints of resources.
b. Elliptical Curve Cryptography offers lightweight encryption by controlling the minimum key size but on the other hand it also increases the ciphered message size that results in complexity.
c. Existing approaches of digital signatures doesn't discuss the cost of certificate revocation which is not only expensive affair but also offer insecurity of its private keys.
d. Usage of digital signatures has higher involvement of computational time that could introduce significant amount of network delay and hence not much supportive for emergency application.

Therefore, the statement of the problem is "*Constructing a unique encryption scheme using public key cryptography that could offer lightweight features with maximum coverage of security standards in wireless environment of sensory application*." The next section outlines proposed solution.

1.3. Proposed Solution

This paper presents an extended version of our previous investigation [35] towards a novel key deployment strategy. This paper further optimizes the security feature by hybridizing the potentials of elliptical curve cryptography and digital signature. Figure 1 highlights the adopted scheme of proposed system.

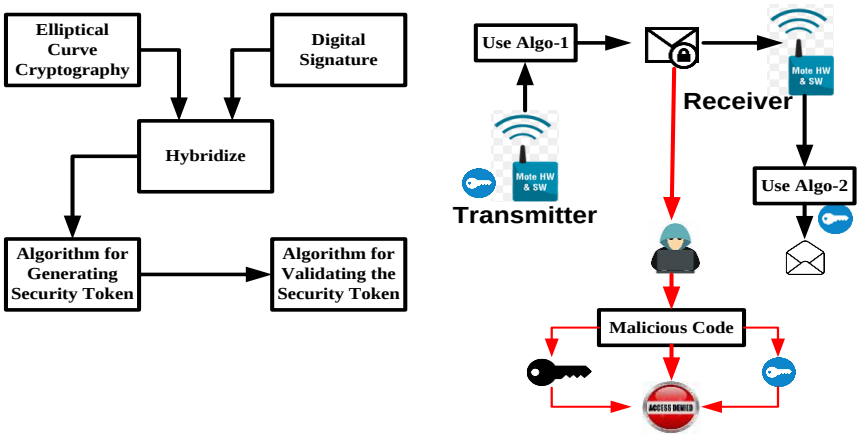

Figure 1. Adopted schema of proposed system

The above shown scheme is mainly intended for higher degree of privacy, confidentiality, as well as data integrity by hybridizing approach. The proposed system considers the potentials of generating higher degree of private keys by elliptical curve cryptography however they are higher in number that could introduce significant amount of computational complexity in low powered sensors. Hence, the proposed system considers the reference point derived from the order of elliptical curve in order to ensure that only the best value of private could be considered in each passes. The next contribution of proposed system is that it doesn't use conventional digital signature as it is expensive in terms of large scale deployment over the sensors.

Hence, the proposed system hybridizes both of them and generates two algorithms ie. 1st algorithm uses random approaches in order to generate a security token which will be used for ciphering the message by the transmitting node in order to forward it to the receiver. On the other hand, the receiver node will use public key cryptography as well as second algorithm in order to perform validation of the received security token. A successful identification of security token allows authorization on the received message. Any form of man-in-middle attacks will not be able to decrypt the content of the message eventually having possessin of same public key. Hence, the novel contribution of proposed system is that it offers better security coverage

from maximum threats in WSN using a lightweight and hybrid encryption technique. The next section discusses about the algorithm implementation.

2. ALGORITHM IMPLEMENTATION

The proposed algorithm presents a novel design of digital signature that is constructed by enhancing the structure of elliptical curve cryptography. The construction of this novel algorithm results in generation of a security token that will be further subjected to validation process. This section will discuss about the mechanism adopted in order to enhance the operations undertaken by elliptical curve cryptography with a prime intention of leveraging data integrity, privacy, as well as confidentiality. Following are the description of implemented algorithm.

2.1. Algorithm for Generating Security Token

In order to maintain a better form of confidentiality of the data as well as node's identity it is essential that proposed system should develop such a mechanism that could dynamically perform secure generation of digital signature. Hence, the prime responsibility of the proposed algorithm is to generate a highly dynamic and secure token that consistently alters in every communication process as well as is also lightweight in nature. The algorithm takes the input of O_u (upper limit of order), a (arbitrary value of integer type) that after processing results in generation of s_{tok} (security token). The steps of the algorithm are as follows:

Algorithm for Generating Security Token
Input: O_u (upper limit of order), a (arbitrary value of integer type)
Output: s_{tok} (security token)
Start
1. init O_u,
2. Choose a_1
3. Compute $\theta=p_1 \mid O_u \mid$
4. **If** $\theta=0$
5. Go to Step-2
6. **Else**
7. Compute $\sigma_1 \rightarrow \sigma(b, \theta)$
8. Estimate $\alpha=\beta+a_1|O_u|$
9. **If** $\alpha=0$
10. Go to Step-3
11. **Else**
12. Obtain $s_{tok} \rightarrow (\theta, \alpha)$
End

The algorithm starts by initiating upper limit of order O_u captured from the elliptical curve (Line-1). The execution of the algorithm begins by transmitting sensor node initiating a communication with receiving sensor node. In this process, the first step is to perform an arbitrary selection of a_1 whose value ranges between 1 and (O_u-1) (Line-2). This is the first novelty which reduces computational complexities associated with elliptical curve cryptgraphy by selecting one point within its order scope and not all the infinite number of points in its curve. The next step of implementation is to compute θ that will be required in generation of security token at the end (Line-3).The computation of θ is carried out by scalar product of positional information p_1 and upper limit of order in elliptical curve O_u (Line-3).

It should be known that (p1, q1) represents the positional information of a node whose empirical value is considered to be equivalent to arbitrary integer value a1 and function of reference point $f(p_f, q_f)$. The function of reference point is considered to lie within the elliptical curve and its order is considered is maximum score of O_u. This mechanism contributes to novel amalgamation of new digital signature as well as ellipitical curve cryptography. The next part of implementation is to compute an encryption attribute σ applied on beacon (or control message) *b* and computed variable θ (Line-7). It can be also noted that under any circumstances, the value of this variable θ is considered as non-zero number (Line-4 and Line-5). This process is followed by generation of preliminary security token α by adding up a new variable β and scalar product of arbitrary integer value a_1 with upper limit of order O_u in eliptical curve cryptography.

We perform the evaluation of new variable β as product of i) variable θ obtained from Line-3, ii) an arbitrary integer [1 (O_u-1)] that is always considered to be its private key, and iii) σ_1 obtained from Line-8. We also ensure that the empirical value of the preliminary security token α is always non-zero and finally the

algorithm leads to selection of final set of security token s_{tok} acquired from variable θ obtained from Line-3 and variable α obtained from Line-8. 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.

2.2. Algorithm for Validating the Security Token

The execution of this algorithm could only begin after successful generation of security token by the transmitting sensor node. This generation security token is then forwarded to receiving sensor node where the the latter performs validation. The input to this algorithm is s_{tok} (secure token) and k_{pub} (public key) that results in outcome of V+ / V- (Successful/failed validation). The important steps of the algorithm are as follows:

Algorithm for Validating the Security Token
Input: s_{tok} (secure token), k_{pub} (public key)
Output: V+ / V- (Successful / failed validation)
Start
1. **If** $k_{pub} \neq 0$
2. **If** $k_{pub} \subseteq EC$
3. successful 1st stage of validation
4. **End**
5. **End**
6. **If** $(\theta, \alpha) \in Z\text{-}1$ Z is integer
7. Compute $\sigma_1 \rightarrow \sigma(b, \theta)$
8. Compute $P \rightarrow \alpha f\text{-} \beta|O_u|$
9. **If** $\theta = p_1|O_u|$
10. $V^+ \rightarrow$ flag s_{tok} as valid
11. **else**
12. $V^- \rightarrow$ flag s_{tok} as invalid
13**. else If**
14. $V^- \rightarrow$ flag s_{tok} as invalid
15. **End**
End

Before trying to understand the implementation scheme of the above validation algorithm, it is essentialto understand one important assumption that a receiving sensor node must have a replica or access of public key k_{pub} of transmitting sensor node. Otherwise, this validation cannot be performed. The complete process of validation of the received security token by the receiving sensor node is carried out in two stages viz. primary stage and secondary stage. In the primary stage, the algorithm checks if there is presence of non-zero public key (Line-1). In case of non-availability of non-zero public key, the communication is aborted instantly stating that its external attack scenario. However, if it is valid than it checks if the numerical value of this public key k_{pub} actually resides within the ranges of elliptical curve (Line-2).

This completes the primary validation stage. The next step of the algorithm targets to perform secondary validation of obtained security token s_{tok}. For this purpose, it ensures that both the variables θ and α should be of integer type as well as their scope has to be mandatorily reside within lower limit of 1 and higher limit of $(O_u\text{-}1)$ (Line-6). In case of exploration of non-integer value type, the algorithm considers it equivalent to eavesdropping or message tamepering and thereby it flags the obtained security token as invalid (Line-14). Upon confirming that they (θ and α) areof integer type than the algorithm performs computation of encryption attribute σ_1 by applying any form of cryptographic function on the control message b and θ. It should be noted that the implemented function σ (Line-7) is similar to that used in previous algorithm of security token generation.

The next validation step of the algorithm calls for computing the a single communication vector of positional information i.e. P, where$P = (p_1, p_2)$. It should be noted that position information of transmitting and receiving nodes are $(p_1\ q_1)$ and $(p_2\ q_2)$ respectively. This computation of single communication vector of positional information P is empirically formed to be corresponding to $\alpha f\text{-} \beta|O_u|$ (Line-8). A closer look into this empirical formulation wil show that first component is a scalar product of preliminary security token α and function of reference point $f(p_f\ q_f)$ while the second component corresponds to β and upper limit of order i.e.O_u. The empirical value of β is considered same as product of variable θ and an arbitrary integer $[1\ (O_u\text{-}1)]$ that is always considered to be its private key. The final step of validation of security token is carried out by

checking of value of the variable θ is equivalent to $p_1|O_u|$ (Line-9). If the left hand side of expression exhibited in Line-9 is not found equivalent to right hand size than the algorithm confirms that obtained security token is highly invalid.

An interesting fact about this algorithm construction is that their false statement precisely corresponds to the attack scenario which could begenerated from any node. Hence, 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 capablity.

3. RESULT ANALYSIS

This section outlines the outcomes obtained after implementing the proposed FSDA using MATLAB. For this purpose, we perform simulation study with 1000 sensors bearing configurations of MEMSIC nodes. The simulation area is considered to be 1100x1300m^2 with 10 meters of transmission range. As the proposed study introduces a hybrid approach with elliptical curve cryptography as well as digital signature hence it is anticipated to offer lightweight encryption scheme for claiming an effective key management scheme. This lightweight feature can be only proven if the algorithm offers less computational burden and equivalently maintains optimal communication performance. Therefore, we choose to consider algorithm processing time, end-to-end delay, energy consumption, and packet delivery ratio as the performance parameter. The study also performs comparative analysis with the most frequently implemented encryption schemes of key management.

The outcomes clearly indicates that proposed system offers significantly better outcomes in comparison to existing AES or SHA. From the Table 1, it can be seen that proposed system offers approximately 64.67%, 63.12%, 4.94%, and 60.02% of improvement with respect to overall energy consumption, overall delay, packet delivery ratio, and algorithm processing time. Owing to non-recursive based operation, FSDA exhibits lower algorithm processing time Figure 2 and it offers enhanced security with faster response time with increasing iterations. This also offers complimentary benefits to delay factor, which is found to be extremely less Figure 3.

Table 1. Summary of Percentage of Improvement

Technique	Overall energy Consumption (%)	Overall Delay (%)	Packet Delivery Ratio (%)	Algorithm Processing Time (%)
AES	39.28	51.54	29.73	45.42
SHA-2	52.08	44.81	14.77	47.39
FSDA	26.69	33.23	49.44	32.79

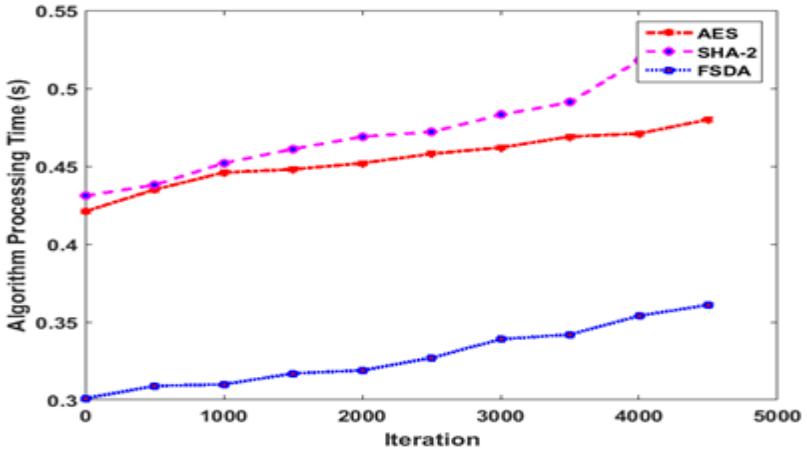

Figure 2. Comparative evaluation of algorithm processing time

The proposed system also make use of first order radio energy model that essentially computes energy dissipation in order to find that FSDA consumes less energy and hence offers network longevity

Figure 4. Finally, the number of encryption steps are not massive for which reason more number of resources are available for longer duration resulting in an effective resource allocation. This causes significant improvement in exploring better communication channel with utmost security Figure 5. The trend of increasing pattern of packet delivery ratio over increasing number of neighboring nodes not only show its better scalability performance but also exhibits that FSDA offers non-repudiation along with data integrity,privacy and confidentiality. Hence, applicability of FDSA is more for any sensory application that demands longer term of security surveillance over uncertain communication as it offers equal resistivity performance to maximum attacks.

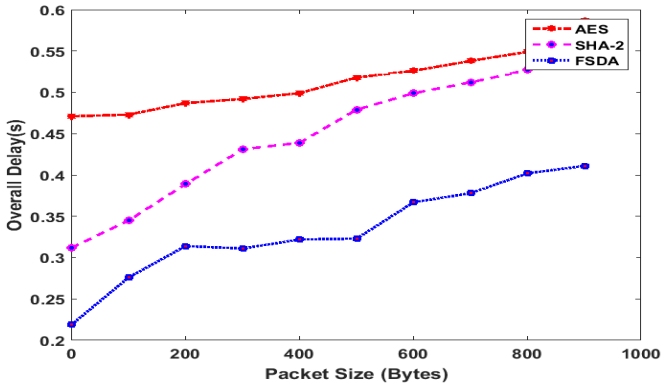

Figure 3. Comparative evaluation of delay

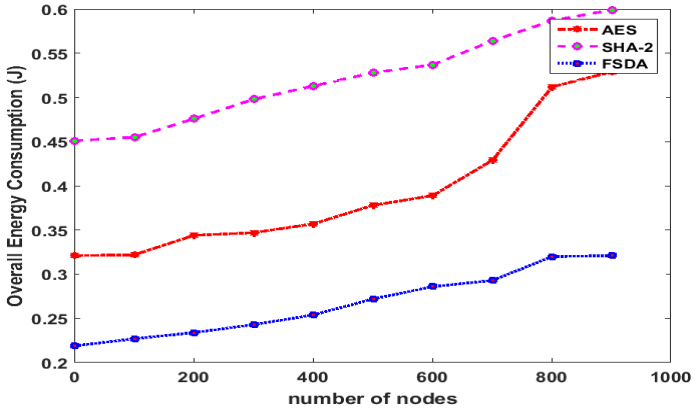

Figure 4. Comparative evaluation of energy consumption

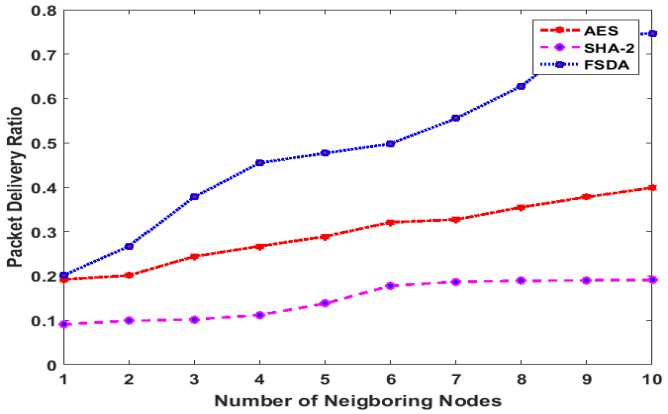

Figure 5. Comparative evaluation of packet delivery ratio

4. CONCLUSION

Security is one of the most challenging problems in WSN irrespective of massive amount of research work beng carried out till date. We observed that existing approaches of key management emphasizes on specific form of attacks which narrows down the applicability of key management when the attack scenario is changed. At the same time, we find that there are much potential of using elliptical curve cryptosystem in order to generate private keys but the process is too much recursive and leads to increased message size. At the same time, usage of digital signature is not too cost effective owing to its dependencies on certificates. Hence, we hybridize both elliptical curve cryptosystem as well as signature in order to construct a novel algorithm. The study outcome shows that proposed algorithm offers significant data integrity, confidentiality, and privacy in its process and is found to offer suitable balance between such security demands and communication performance.

REFERENCES

[1] W. Osterhage, Wireless Security, CRC Press, 2016

[2] T. Hamza, G. Kaddoum, A. Meddeb and G. Matar, "A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, pp. 1-5, 2016,.

[3] A. Modirkhazeni, N. Ithnin and O. Ibrahim, "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis," 2010 Second International Conference on Network Applications, Protocols and Services, Kedah, pp.228-233, 2010

[4] Shashikala and C. Kavitha., "A survey on secured routing protocols for wireless sensor network," Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, Coimbatore, pp. 1-8, 2012

[5] F. Khedim, N. Labraoui and M. Lehsaini, "Dishonest recommendation attacks in wireless sensor networks: A survey," 2015 12th International Symposium on Programming and Systems (ISPS), Algiers, pp. 1-10, 2015

[6] H. Yu, Z. Shen, C. Miao, C. Leung and D. Niyato, "A Survey of Trust and Reputation Management Systems in Wireless Communications," in Proceedings of the IEEE, vol. 98, no. 10, pp. 1755-1772, Oct. 2010.

[7] R. Dou and G. Nan, "Optimizing Sensor Network Coverage and Regional Connectivity in Industrial IoT Systems," in IEEE Systems Journal, vol. 11, no. 3, pp. 1351-1360, Sept. 2017.

[8] J. M. Williams et al., "Weaving the Wireless Web: Toward a Low-Power, Dense Wireless Sensor Network for the Industrial IoT," in IEEE Microwave Magazine, vol. 18, no. 7, pp. 40-63, Nov.-Dec. 2017.

[9] K. Yang, D. Blaauw and D. Sylvester, "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey," in IEEE Micro, vol. 37, no. 6, pp. 72-89, November/December 2017.

[10] L. Chen et al., "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey," in IEEE Access, vol. 5, pp. 8956-8977, 2017.

[11] Manjunath, B. E., 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) 8.2 (2018): 1048-1055.

[12] Singh, Pooja, and R. K. Chauhan. "A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN." International Journal of Electrical and Computer Engineering 7.4 (2017): 2232.

[13] Sukavasi, Hema Gopinath, Lokesh Kanagala, and Riaz Shaik. "Sufficient Authentication for Energy Consumption in Wireless Sensor Networks." International Journal of Electrical and Computer Engineering 6.2 (2016): 735.

[14] J. Metan, 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.117, No.12, May 2015

[15] G. Wang, D. Kim and G. Cho, "A secure cluster formation scheme in wireless sensor networks," International Journal of Distributed Sensor Networks, pp. 14, 2012

[16] P. Pawani, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," International Journal of Distributed Sensor Networks, vol. 10, no. 7, pp.357-430, 2014

[17] S. Kang, C. Ji, and M. Hong, "Secure collaborative key management for dynamic groups in mobile networks," Journal of Applied Mathematics, pp. 10, 2014

[18] J.D. Lee, H. J. Im, W.M. Kang, and J. H. Park, "Ubi-RKE: a rhythm key based encryption scheme for ubiquitous devices," Mathematical Problems in Engineering, pp. 8, 2014

[19] 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

[20] G. C. C. F. Pereira, Renan C. A. Alves, F. L. d. Silva, R.M. Azevedo, B.C. Albertini, and C.B. Margi, "Research Article Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems", Hindawi Security and Communication Networks, pp. 16, 2017

[21] A. Ibrahim and G. DalkJlJç, "Research Article an Advanced Encryption Standard Powered Mutual Authentication Protocol Based on Elliptic Curve Cryptography for RFID, Proven on WISP", Hindawi Journal of Sensors, pp. 10, 2017

[22] P. Sarkar and S. Mukherjee, "Secure connected scalable combinatorial KPS in WSN: Deterministic merging, localization," *38th Annual IEEE Conference on Local Computer Networks*, Sydney, NSW, 2013, pp. 622-629.

[23] J. Qi, X. Hu, Y. Ma and Y. Sun, "A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme," in *IEEE Access*, vol. 3, pp. 718-724, 2015.

[24] J. Wu, K. Ota, M. Dong and C. Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities," in *IEEE Access*, vol. 4, pp. 416-424, 2016.
[25] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan and R. K. Mallik, "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1128-1138, June 2016.
[26] I. A. Umar, Z. M. Hanapi, A. Sali and Z. A. Zulkarnain, "TruFiX: A Configurable Trust-Based Cross-Layer Protocol for Wireless Sensor Networks," in *IEEE Access*, vol. 5, pp. 2550-2562, 2017.
[27] J. Zhu, Y. Zou and B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks," in *IEEE Access*, vol. 5, pp. 5313-5320, 2017.
[28] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma and Q. Ding, "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network," in *IEEE Access*, vol. 5, pp. 9599-9609, 2017.
[29] D. Shin, V. Sharma, J. Kim, S. Kwon and I. You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks," in *IEEE Access*, vol. 5, pp. 11100-11117, 2017.
[30] Y. Guan and X. Ge, "Distributed Secure Estimation Over Wireless Sensor Networks Against Random Multichannel Jamming Attacks," in *IEEE Access*, vol. 5, pp. 10858-10870, 2017.
[31] H. Dai, M. Wang, X. Yi, G. Yang and J. Bao, "Secure MAX/MIN Queries in Two-Tiered Wireless Sensor Networks," in *IEEE Access*, vol. 5, pp. 14478-14489, 2017.
[32] F. Al-Turjman, Y. Kirsal Ever, E. Ever, H. X. Nguyen and D. B. David, "Seamless Key Agreement Framework for Mobile-Sink in IoT Based Cloud-Centric Secured Public Safety Sensor Networks," in *IEEE Access*, vol. 5, pp. 24617-24631, 2017.
[33] V. N. Vo, T. G. Nguyen, C. So-In and D. B. Ha, "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer," in *IEEE Access*, vol. 5, pp. 25196-25206, 2017.
[34] Yiqin Lu, Jing Zhai, Ronghuan Zhu, and Jiancheng Qin, "Research Article Study of Wireless Authentication Center with Mixed Encryption in WSN", Hindawi Publishing Corporation Journal of Sensors, pp. 7, 2016
[35] J. Metan and K. N. N. Murthy, "Robust and secure key management in WSN using arbitrary key-deployment," *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, pp. 246-250, 2015

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.