Journal of Engineering Science and Technology Review 14 (1) (2021) 95 - 99

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Enhanced Privacy Preservation in the Routing layer with Variable-length packet data for Attack Free IoT Sector

G. Kalyani[1,2*] and Shilpa Chaudhari[3]

[1]*School of Computing and Information Technology, REVA University, Bangalore.*
[2]*Department of CSE, Sreenidhi Institute of Science and Technology, Hyderabad, India.*
[3]*Department of CSE, MS Ramaiah Institute of Technology, Bangalore,India.*

Received 29 September 2020; Accepted 14 January 2021

Abstract

In IoT, a significant challenge is to attain a reasonable network life span when meeting the requirements of quality of service (QoS). Depending on a layered model, numerous energy-efficient approaches were introduced. The privacy preservation of the MAC layer is proven in our previous contribution. The existing routing techniques obtain the route selection based on various constraints but lack data privacy. In this paper, we have proposed data privacy preservation scheme for the packet using ElGamal cryptosystem after route selection. This paper intends to demonstrate the routing layer for secured data privacy preservation-based services in IoT. The security analysis of the proposed framework is evaluated in terms of key sensitivity by varying the data length and resistance to cryptanalysis attacks in this work.

Keywords: Routing layer; QoS; Internet of Thing; Optimization; Security.

1. Introduction

IoT was established in 1999 for envisioning the theory of linking physical objects, such as smart-phones and sensors, thus aiding wireless connection with the internet. This facilitates a huge range of appliances in an "Internet-like framework" [1-2]. The terminals that are linked to the Internet can communicate with these objects. On the other hand, to maintain more number of budding appliances, the wireless MAC [3-4] and the routing protocols should be interoperable, scalable and they should contain a solid consistency base to sustain upcoming innovations.

In IoT applications, the effectual routing of information is a much significant aspect [5-7]. The decision over diverse routes is very much dependent on "link performance indicators, which are influenced by the MAC parameters". Besides, the traffic load distribution in the network is determined by routing [8-9] that considerably affects the aforesaid indicators. The privacy mechanism is necessary to maintain trust and also to reduce the risks of information sharing and communication with malevolent nodes [10-11].

MAC protocol is exploited for scheduling the transmissions amongst the neighbors and its objectives are superior channel exploitation, lower latency, real-time support, and best-effort services[19-20]. The transmissions are coordinated by the MAC layer for minimizing and avoiding collisions [12-14]. Nevertheless, the MAC protocol should be modeled such that the limited bandwidth should be exploited proficiently [15-18]. The overhead should be maintained minimum and also, the routing protocols have to handle limits such as lower bandwidth, random node movements, higher error, and higher power utilization[21-22]. The main contribution of the proposed work is given below:

1. A new data privacy preservation mechanism for the routing layer is introduced.
2. The performance of the routing layer framework with proper security analysis is carried out.

2. Literature review

In 2019, David *et al.* [24] have developed a routing approach for preserving the IoT in opposition to attacks like SecTrust-RPL. Moreover, the trust-based model exploited the SecTrust-RPL for detecting the attacks while optimizing the efficiency of the network. The betterment was proved in terms of efficiency and robustness.

In 2018, Sarwesh P., *et al.* [25] have introduced a cross-layer model in which the Expected Transmission Range Threshold (ETRT) is evaluated using routing information. ETRT information extends the network lifetime with improved reliability and QoS by assigning optimum transmission power. In the results, it is observed that the ETRT model performs twice as superior to the standard one. In 2020, Deebak and Fadi [26] have suggested a novel secure routing protocol using TF symmetric key model for identifying and avoiding the issues in the overall sensor network. The introduced technique was modelled based on the ATE model. The proposed scheme has revealed betterment over several mobile challenges; and therefore, multipath delivery was confirmed.

In 2019, Bu *et al.* [27] have established a secure and robust technique for facilitating the transmission of private data in IoT networks. As per the implemented scheme, TSS has isolated the data into shares that were then resaved by a set of devices. Furthermore, the suggested scheme has assured

*E-mail address: ghanta.kalyani@gmail.com

ISSN: 1791-2377 © 2021 School of Science, IHU. All rights reserved.
doi:10.25103/jestr.141.10

the integrity and privacy of the information even though more attackers could hijack the devices.

In 2019, Mahadev *et al.* [28] proposed an ACO-AODV routing protocol to resolve route selection and to optimize the information acquired from various layers such as the MAC layer, physical layer, Application layer, and Transport layer. The network performance is increased in terms of QoS by utilizing the proposed model.

In 2011, Xin *et al.* [29] have developed an algorithm to calculate approximately the distance of two nodes without positioning service. EGD method is utilized to assess the quality of links among neighbors and then eliminate the weak links. It reduces the frequency of path failures and route discoveries. The protocol has extensively reduced the routing overhead and improved the routing performance in high-mobility networks.

In 2010, Ben *et al.* [30] to efficiently balance the energy utilization and to recover from node failures Energy-efficient and QoS based multi-path routing protocol (EQSR) for WSNs has been developed. A light-weight XOR-based Forward Error Correction technique is used to increase the reliability of data delivery. It uses the buffer size, residual energy, and Signal-to-Noise Ratio (SNR) to predict the neighbor hop through the path construction phase.

In 2015, Lobiyal *et al.* [31] have proposed an algorithm based on 'Particle Swarm Optimization' (PSO) to find an optimal path combination in 'Ad-hoc on-demand multipath distance vector routing' (AOMDV). It achieved a low Average delay, fall in Network Routing Load and trivial drop in Packet Drop Rate.

3. A Framework for Secured Data Privacy in Routing Layer

In the network layer, the interactions between the routing algorithm and other layers should be considered to make it appropriate for the IoT. Usually, the conventional layered protocol model was exploited for designing the protocols for WSN, where the Routing and MAC protocols operate independently. Accordingly, the previous contributions have concerned with the security or privacy preservation of the MAC layer. The usage of optimization techniques in routing protocols can lessen the difficulty of routing to the maximum extent. Most of the routing techniques developed in the precedent ignored performance.

In this paper, an improvised scheme for data privacy preservation in the routing layer in the IoT environment is introduced Fig. 1 depicts the proposed system architecture. Initially, the route selection is done using existing techniques like estimated distance (EstD)-based routing protocol (EDRP), energy-efficient and QoS aware multipath routing protocol (EQSR), ad-hoc on-demand multipath distance vector routing (AOMDV), ant colony optimized ad-hoc on-demand distance vector (ACO-AODV) routing protocol and SecTrust-RPL which are based on various constraints like distance, packet drop rate, energy, bandwidth, link quality, hop count and security for data communication. Here, the routing layer uses the Elgamal cryptosystem for key generation and a CM-LA model for optimal key selection. It includes the private key in the packet and encryption is performed using the public key and the packet is forwarded to the MAC layer. The MAC layer generates the frames and performs the encoding and decoding process to keep the transmitted packets as small as possible. At the receiver end, the reverse process is carried out.

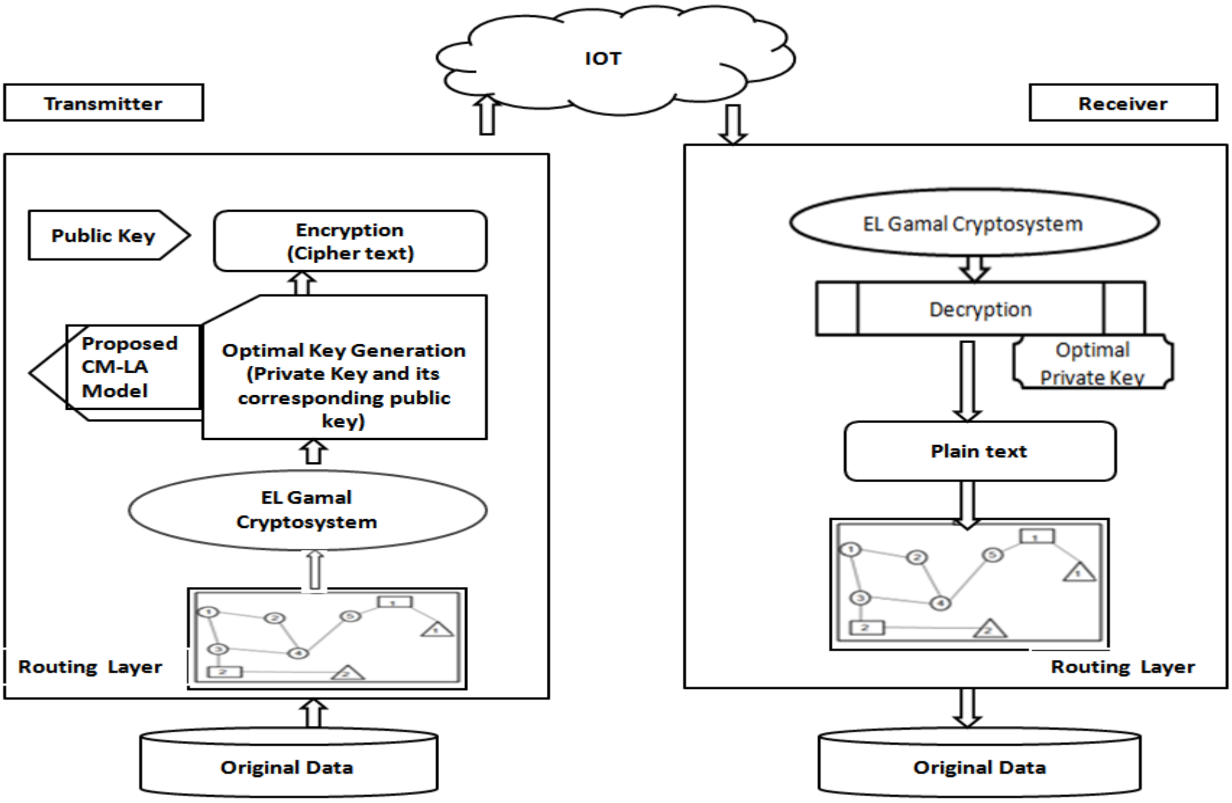

Fig. 1. Framework of the proposed model

3.1 Privacy Preservation of Data in the Routing layer

The user transfers and receives data in the IoT channel in a protected mode via security facilitated routing protocol. In this context, the packet payload is facilitated with security (confidential key Xi). Besides, the encrypted text is generated via the public key Yi of "ElGamal cryptosystem" in the routing layer is provided for the message $\{M_1, M_2\}$ to packet payload together that holds the cipher text $\{c_1, c_2\}$. Encoding is done at the transmitter side in the MAC layer and offers encrypted cipher data. Decoding is done by MAC at the receiver and it offers cipher-text $CT = \{c_1, c_2\}$ that is passed over from the receiver. At last, the decryption is performed by utilizing xi to achieve the original data $\{M_1, M_2\}$.

Proposed CM-LA Algorithm

Here, to achieve the precise cipher-text, the confidential key in the "ElGamal cryptosystem" is subjected to optimization [34].

LA [32] includes 6 essential stages namely "pride generation, fertility evaluation, proposed mating, territorial defense, territorial takeover, and termination".

Pride Generation: Let C^M denote territorial lion, lioness as C^F, and nomadic lion as C^N and its related vector elements be c_i^M, c_i^F, and c_i^N with max and min limits of j>1, in which i=1,2…I, I, denotes the lion pride length. Here,,j and k refers to the integers to evaluate the length of lion pride.

Fertility Evaluation: Here, C^M turns out to be laggard and its equivalent lagardness rate B is enlarged by 1 when $F(C^M)$ surpassing F^{REF} the reference fitness. Besides, while B surpasses B^{max} (max limit), then territorial defense starts. The sterility rate E assures fertility C^F and E rises to 1 after crossover. Based on this, the updating process of female, $C^{F,}$ C^{F+} will occur.

Mating: Mutation and crossover are two major processes carried out during mating. During mating, C^M and C^F creates up to 4 cubs. The proposed logic is as follows: as per the adopted scheme, the mutation process of LA takes place as per CS [33] Levy update i.e. based on Eq. (1) and thus, the mutated cubs are produced. Eq. (1), C_i^{loc+1} signifies the location of the nest C_i^{loc} and α indicates "positive step size scaling factor", s indicate the step size and Levy distribution is specified by L(s,κ).

$$C_i^{loc+1}= C_i^{loc} +\alpha L(s,\kappa) \qquad (1)$$

LA Operators: The local optima issues are neglected by deploying territorial defense and several solutions are attained with equal fitnesses. Particularly, the coalition procedure is generalized using the "winner-take-all technique" to find out $C^{e\text{-}nomad}$. In a territorial takeover, C^M and C^F are updated, if $C^{m\text{-}cubs}$ and $C^{f\text{-}cubs}$ surpasses the max maturity age M_{max}.

Termination: Eventually, LA evaluation is completed when any one of the conditions is satisfied. (i) When the maximum number of generations is reached or (ii) when the absolute variation between $F(C^M)$ and $F(C^{Optional})$ is less than or equal to the error threshold.

4. Results and Discussion

4.1 Simulation Setup

The presented scheme was executed in **MATLAB 2019a** [36] and the simulation was done under data privacy preservation for secure routing. The data privacy preservation using the proposed CM-LA [34] and the outcomes were achieved under key sensitivity and attacks.

Table 1. KPA and CPA Analysis by varying the data lengths

Data lengths	KPA	CPA
10	-0.09047	0.027613
20	0.007133	0.073591
30	-0.08953	0.050942
40	-0.03986	-0.16107
50	-0.04459	0.095761

4.2 Key Sensitivity Analysis

Fig. 2 shows the key sensitivity analysis of the recommended scheme by varying the data lengths in bytes from 10, 20, 30, 40 and 50 and also by varying the percentage level of a key from 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90%, and 100%. To find the robustness of the optimal key, key sensitivity analysis is performed. The correlation between the original cipher and the deciphered data with deviation should be -low to achieve improved performance. Consequently, for attaining enhanced performance; the key sensitivity should be low. Suppose if anyone of the bits in the secret key is altered, it should not decrypt the text. That is why the percentage level of the key is varied. The key sensitivity should be low, if not even for small variations in the secret key the text will be decrypted. On analyzing Fig. 2, the key sensitivity of the presented CM-LA model at data length 40 has attained an optimal value when compared over the key sensitivities attained at data lengths 10, 20, 30, 40 and 50. Thus, the effectiveness of the presented scheme is confirmed from the simulated outcomes.

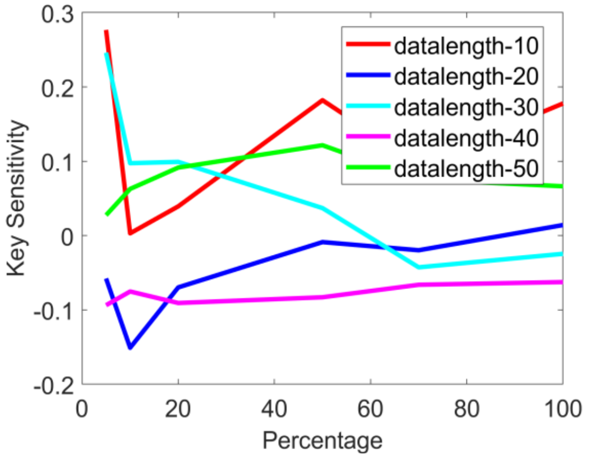

Fig. 2. Analysis on Key Sensitivity by altering the data lengths

Table 2. KCA Analysis by varying the data lengths

% Deviation	Data lengths 10	Data lengths 20	Data lengths 30	Data lengths 40	Data lengths 50
5	0.00726	-0.10861	-0.26368	-0.16762	-0.21422
10	-0.09272	-0.21176	-0.19399	-0.17397	-0.0901
15	0.043941	-0.27356	-0.02442	-0.18254	-0.06517

20	-0.05396	-0.22553	0.058925	-0.19284	-0.05459
25	-0.10516	-0.18341	0.10854	-0.19364	-0.01594

4.3 Analysis of Attacks

According to Kerckhoff's rule [35], the security of any cryptosystem depends on the key only, assuming that the challenger knows the encryption and decryption algorithms. The most familiar attacks are 1) The KPA (known plain text) is an attack model for cryptanalysis where in the attacker has access to both the plain and its encrypted edition of the text. They can be used to access keys. 2) CPA (chosen plain text attack) is an attack model where the attacker pretends to get the cipher-texts for the corresponding plaintexts. The attack intends is to choose the data that minimizes the security of the encryption scheme. 3) KCA is a model for cryptanalysis where the attacker comprises only encrypted texts. 4) The CCA is a model for cryptanalysis to attain the decryptions of chosen ciphertexts. From this information, the challenger can recover the hidden secret key used for decryption. Perceptibly, if a cryptosystem can resist the chosen cipher text and plain text attack which is the most prevailing attack, it can defend against other attacks. The analysis on attacks such as KPA, CPA, KCA and CCA attacks are summarized in this section. Tab.1 shows the analysis on KPA and CPA attacks, whereas Tab.2 and Tab.3 show the analysis on CCA and KCA attacks with text deviations like "5%, 10%, 15%, 20%, and 25%". To attain improved performance, the correlation should be minimal and resist against all types of attacks. Here, the entire analysis was done by varying the data lengths from 10, 20, 30, 40 and 50. The correlations must be minimal to accomplish the improved outcomes, which have been proved from the accomplished outcomes for KPA, CPA, KCA and CCA attacks. Fig. 3 shows the KCA Analysis by varying percentage level of text deviation as "5%, 10%, 15%, 20%, and 25%" with data length as 40 and compared with existing methods such as GA [23], LA [32] and CS [33].

Table 3. CCA Analysis by varying the data lengths

% Deviation	Data lengths 10	Data lengths 20	Data lengths 30	Data lengths 40	Data lengths 50
5	-0.54959	0.062225	-0.14522	0.25769	-0.03055
10	-0.58825	-0.01064	-0.14039	0.25159	-0.02932
15	-0.33173	0.051587	-0.01255	0.20973	0.033042
20	-0.43055	-0.02165	0.061206	0.17874	0.020841
25	-0.35598	-0.08714	0.058111	0.16153	0.029893

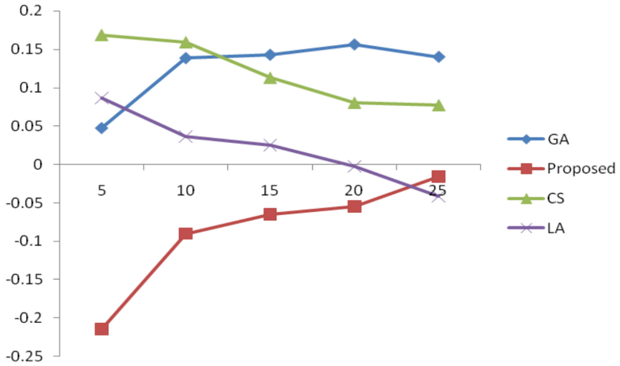

Fig. 3. KCA Analysis by varying percentage level of text deviation

5. Conclusion

This work has provided a demonstration of the efficiency of secure data privacy preservation in the routing layer. For this, an experimental analysis of the secured routing layer framework was portrayed with proper analysis of security. It is observed that the key sensitivity of the proposed model at data length 40 has attained an optimal value with an increase in the data length. The adopted model has also resisted attacks by varying the data length. Thus, the superiority of the presented model has been validated effectively.

References

1. Subramanian Balaji, Eanoch Golden Julie, Yesudhas Harold Robinson, Raghvendra Kumar, Le Hoang Son, "Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model", Computer Standards & Interfaces, vol.66, October 2019, Article 103358.
2. A. Raoof, A. Matrawy and C. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1582-1606, Second quarter 2019.
3. Tong Xu; Deyun Gao; Ping Dong; Hongke Zhang; Chuan Heng Foh; Han-Chieh Chao, " Defending Against New-Flow Attack in SDN-Based Internet of Things", IEEE Journals & Magazines, Vol.05, pp.3431 - 3443, 2017.
4. Nadav Schweitzer; Ariel Stulman; Roy David Margalit; Asaf Shabtai, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks", IEEE Journals & Magazines, Vo.16, no.08, pp. 2174 - 2183, 2017.
5. Richard K. Lomotey, Joseph Pry, Sumanth Sriramoju, "Wearable IoT data stream traceability in a distributed health information system", Pervasive and Mobile Computing, 15 July 2017.
6. Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Hannu Tenhunen, "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways", Procedia Computer Science, Vol. 52, pp. 452-459, 2015.
7. S. Sciancalepore, G. Piro, E. Vogli, G. Boggia, G. Cavone, " LICITUS: A lightweight and standard compatible framework for securing layer-2 communications in the IoT", Computer Networks, Vol. 108, pp. 66-77, 24 October 2016.
8. Bo Zhou, Quan Zhang, Qi Shi, Qiang Yang, Yinyan Yu, "Measuring web service security in the era of Internet of Things",Computers & Electrical Engineering, 28 June 2017.
9. Vasileios A. Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, B.B. Gupta, "An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework", Future Generation Computer Systems, 9 May 2017.
10. Tong Xu; Deyun Gao; Ping Dong; Hongke Zhang; Chuan Heng Foh; Han-Chieh Chao, " Defending Against New-Flow Attack in SDN-Based Internet of Things", IEEE Journals & Magazines, Vol.05, pp.3431 - 3443, 2017.
11. Nadav Schweitzer; Ariel Stulman; Roy David Margalit; Asaf Shabtai, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks", IEEE Journals & Magazines, Vo.16, no.08, pp. 2174 - 2183, 2017
12. K. Sudeendra Kumar, G. Hanumanta Rao, Sauvagya Sahoo, K.K. Mahapatra, "Secure split test techniques to prevent IC piracy for IoT devices", Integration, the VLSI Journal, Vol. 58, pp 390-400, June 2017.
13. Mahmood Salehi, Azzedine Boukerche, Amir Darehshoorzadeh, "Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks",Ad Hoc Networks, Vol. 50, pp. 88-101,1 November 2016.
14. Krishna Jyothi, Shilpa Chaudhari ," Optimized Neural Network Model for Attack Detection in LTE Network: Impact of Improved

Whale Optimization Algorithm", Computers and Electrical Engineering, Elsevier,2020 , In Communication.

15. G.Kalyani, Shilpa Chaudhari, “Security Aware Routing: Rule based Attack Detection on Optimal Shortest Route Selection”, In Communication.
16. G.Kalyani, Shilpa Chaudhari, “Survey of Security Approaches in Internet of Things Solution Architectures for Communication Layer”, Journal of Advance Research in Dynamical & Control Systems, In press.
17. Krishna Jyothi, Shilpa Chaudhari ,"Cluster-based Authentication for Machine Type Communication in LTE Network using Elliptic Curve Cryptography", International Journal of Cloud Computing , In press.
18. Kalyani, G., Shilpa Chaudhari. "An efficient approach for enhancing security in internet of things using the optimum authentication key", International Journal of Computers and Applications, Vol.42no.3, pp: 306-314,2020.
19. K. Krishna Jyothi, Shilpa Chaudhari, “A secure cluster-based authentication and key management protocol for machine-type communication in the LTE network”, International Journal of Computers and Applications, pp:1-11 ,DOI: 10.1080/1206212X.2019.1693000.
20. Kalyani G., Chaudhari S. (2020), “Survey on 6LoWPAN Security Protocols in IoT Communication”, In: Kumar A., Paprzycki M., Gunjan V. (eds) ICDSMLA 2019. Lecture Notes in Electrical Engineering, vol 601. Springer, Singapore.
21. H. Sedjelmaci, S. M. Senouci and M. Feham, “An efficient intrusion detection framework in cluster-based wireless sensor networks”, Security and Communication Networks, vol. 6, no. 10, pp. 1211–1224, 2013.
22. A. Abduvaliyev, S. Lee and Y. K. Lee, “Energy efficient hybrid intrusion detection system for wireless sensor networks”, In International Conference On Electronics and Information Engineering, vol. 2, pp. 25–29, 2010.
23. John McCall, "Genetic algorithms for modelling and optimisation", Journal of Computational and Applied Mathematics, vol. 184, no. 1, pp 205-222, 2005.
24. David Airehrour, Jairo A.Gutierrez and Sayan KumarRay, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things", Future Generation Computer Systems, vol. 93, pp. 860-876, April 2019.
25. Sarwesh P, N. Shekar V. Shet, and K. Chandrasekaran, "ETRT – Cross layer model for optimizing transmission range of nodes in low power wireless networks – An Internet of Things Perspective", Physical Communication, Volume 29, Pages 307-318, August 2018.
26. Deebak B.D., Fadi Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks", Ad Hoc Networks, vol.97, February 2020, Article 102022.
27. Lake Bu, Mihailo Isakov, Michel A. Kinsy,”A secure and robust scheme for sharing confidential information in IoT systems”, Ad Hoc Networks, vol. 92, September 2019, Article 101762.
28. Mahadev A. Gawas, Sweta S. Govekar” A novel selective cross layer based routing scheme using ACO method for vehicular networks,” Journal of Network and Computer Applications, vo1.43, pp.34–46, 2019.
29. Xin Ming Zhang, En Bo Wang, Jing Jing Xia, and Dan Keun Sung,” An Estimated Distance-Based Routing Protocol for Mobile Ad hoc Networks,” IEEE Transactions On Vehicular Technology, Vol. 60, No. 7, September 2011.
30. Jalel Ben-Othman, Bashir Yahya,” Energy efficient and QoS based routing protocol for wireless sensor networks,” Journal of Parallel and Distributed Computing, Vol. 70, pp.849-857, 2010.
31. D K Lobiyala, C P Kattia,A K Giria,”Parameter Value Optimization of Ad-hoc On Demand Multipath Distance Vector Routing using Particle Swarm Optimization”, Procedia Computer Science, Vol. 46, pp. 151–158, 2015.
32. Rajakumar Boothalingam, "Optimization using lion algorithm: a biological inspiration from lion’s social behavior", Evolutionary Intelligence, vol.11, no. 1-2, pp.31–52, 2018.
33. Ramin Rajabioun, "Cuckoo Search Optimization Algorithm", Applied Soft Computing, vol.11, pp. 5508–5518, 2011.
34. G.Kalyani, Shilpa Chaudhari, “Data Privacy Preservation in MAC Aware Internet of Things with Optimized Key Generation”, journal of King Saud University-Computers and Information Science, 2019,In Press.
35. Jiahui Wu, Xiaofeng Liao, Bo Yang, “ Color image encryption based on chaotic systems and elliptic curve ElGamal scheme”, Signal Processing, vol.141, pp.109-124,2017.
36. https://matlabacademy.mathworks.com/.