УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2022 Том 22 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2022 Vol. 22 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2022-22-2-332-338

Lightweight ECC and token based authentication mechanism for WSN-IoT

Loganathan Sasirega[1]✉, Chandrabose Shanthi[2]

[1,2] Department of Computer Science, Vels Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu, 600117, India

[1] lsasirega1975@gmail.com✉, https://orcid.org/0000-0003-3771-8959
[2] shanc08071978@gmail.com, https://orcid.org/0000-0002-7976-2360

Abstract

The paper deals with Wireless Sensor Networks (WSN) registered in a specific Internet of Things (IoT's) network that have different kind of applications. They come into use once they are successfully registered within a specific IoT network. Elliptic Curve Cryptography (ECC) with Token based Security Scheme is proposed here for secured and authenticated communication. A lightweight authentication mechanism is proposed also in order to prevent the network from the unauthorized access. Network nodes are generated with token keys immediately after login, and the gateway generates token ID for each individual nodes. Then elliptical curve cryptography is applied to remove the malicious nodes completely if some adversaries missed out during token key verification process. If the user needs to access the data, he must go through the token key generation and verification phase, as well as through the data integrity and transmission phase.

Keywords

token key, elliptical curve cryptography, ECC, key generator, key verification, wireless sensor network, internet of things, IoT

For citation: Sasirega L., Shanthi C. Lightweight ECC and token based authentication mechanism for WSN-IoT. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 2, pp. 332–338. doi: 10.17586/2226-1494-2022-22-2-332-338

УДК 004.89

Облегченный механизм аутентификации на основе ECC и токенов для WSN-IoT

Логанатан Сасирега[1]✉, Чандрабос Шанти[2]

[1,2] Институт науки, технологий и перспективных исследований Велса, Ченнаи, 600117, Индия

[1] lsasirega1975@gmail.com✉, https://orcid.org/0000-0003-3771-8959
[2] shanc08071978@gmail.com, https://orcid.org/0000-0002-7976-2360

Аннотация

Рассмотрены беспроводные сенсорные сети, зарегистрированные в конкретной сети Интернета вещей (Internet of Things, IoT), которые имеют различные приложения. Они вступают в действие после успешной регистрации в конкретной сети IoT. В работе предложен метод, основанный на применении эллиптической криптографии (Elliptic Curve Cryptography, ECC) со схемой безопасности на основе токенов для защищенной и аутентифицированной связи. Представлен облегченный механизм аутентификации для предотвращения несанкционированного доступа к сети. Сетевые узлы генерируются с ключами токенов сразу после входа, а шлюз генерирует идентификатор токена для каждого отдельного узла. Затем применяется ECC на основе эллиптических кривых для полного удаления вредоносных узлов в случае пропуска злоумышленниками процесса проверки ключа токена. Если пользователю необходимо получить доступ к данным, он должен пройти этапы генерации и проверки ключа токена, а также проверку целостности и передачу данных.

Ключевые слова
токен-ключ, криптография на основе эллиптических кривых, ECC, генератор ключей, проверка ключей, беспроводная сенсорная сеть, интернет вещей, IoT

Ссылка для цитирования: Сасирега Л., Шанти Ч. Облегченный механизм аутентификации на основе ECC и токенов для WSN-IoT // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 2. С. 332–338 (на англ. яз.). doi: 10.17586/2226-1494-2022-22-2-332-338

Introduction

Wireless Sensor Network (WSN) is considered to be a significant network structure in the case of Industrial Internet of Things (IIoT), and this kind of technique can be widely applied in many industrial areas with the combination of cloud computing technology [1–3]. Here the information is collected in a secured and confidential manner by using mutual authentication process between users. The mutual authentication is carried out between sensor nodes, gateway and the users in order to protect the legal users from the malicious activity and to maintain the system privacy and security [4]. Generally, the WSN is formed by a collection of sensor nodes and base station or gateway node through wireless communication, nodes are located here at different areas to gather the environmental information from the specific area and transfer the data to the gateway through the wireless channel. In many applications like military and healthcare appliances in [5], the identification of user's identity will be a great challenge for providing security for Industrial IoT's. To provide security, the cryptographic technique carried out three operations that include converting original text to cipher text, identifying the keys used for conversion and processing the cipher text to plain text [6].

Lot of techniques and algorithms were processed for the initiation of public key cryptographic operations, and some of the public key cryptographic techniques are secured hash algorithm, diffie hellman, RSA, Elliptical Curve Cryptography (ECC), etc. For key generation process prime numbers are used in the public key cryptography technique [7]. To encrypt the text public key is used and to decrypt the secret code of the text or to remove the digital mark private key is used.

Related Works

Several research works has been carried out for security related applications and most of the algorithms cannot reach end-to-end security and durability. Some security related protocols are discussed here. Elliptic Curve basis asymmetric cryptosystem was implemented since it holds smaller key size [8] that highly reduces the computation cost. Elliptic curve is generally used to reduce the mathematical computations by generating the prime numbers. ECC holds their maximum key length size as 384 bits in order to provide the security keys.

Secured Discovery of Data and Dissemination based Hash (SDDDH) method was proposed using public key cryptography [9] that improves the network security features. To make the data more secured one-way hash function cryptographic process was applied, and in each round the gateway generates the signature packet for distribution of sensed information. Each sensor nodes receives the signature packet in order to complete the node verification process. For packet verification trickle algorithm is used here and to encrypt the data puzzle keys are used; however, encryption process consumes huge amount of energy.

Gateway generates an individual identity for each and every node that enters into the network in three factor anonymous authentication scheme [10]. The new nodes are registered with their respective ID's. Also, the random password is created between the users and the sensors, and tied up with the user's biometric signature. The data will be passed to the user if only the biometric password gets matched with the generated password. Various security and authentication mechanisms were proposed with respect to the independent security parameters [11]. To prove the security efficiency, two main tasks are carried out in [12], named as primary task and secondary task. Primary task dealt with the medical applications that include patient's health observation scheme which uses 'μ' TESLA for synchronization of nodes, and this task seems to be slightly difficult. Secondary task is accompanied with the process of performance of authentication which might causes little difficulties in communication overheads.

Token based Message Queue Telemetry Transport (TMQTT) was proposed in [13] for improving the authentication stability process by enabling token generation process. If allotted token time gets expired, then new token is generated. The valid token received is stored in its and used for the process of authentication. Token based Lightweight User Authentication (TLUA) scheme was proposed in [14] for IoT devices since password based user authentication method was not more efficient. This scheme was implemented based on the basis of token system authentication. The security strength is derived by computing the token level security and perfect forward secrecy rate.

ECC based Provable Secure Authentication Protocol (EPSAP) was proposed for privacy preserving of IIoT network [15]. Here only the valid users can access the data by using user authentication protocol. Random oracle model was applied for user authentication process that makes the authentication and verification more reliable. However, the computation cost increases as well as leads to computational delay. The group keying management scheme uses logical key tree [16]. Each root node should have the ability of computing keys from their respective leaf node. To detect the precedence node affiliation, the weight factor is used here. To decrease the excessive rekeying process, the logical Tree based Secure Mobility Management Scheme (TSMMS) was proposed in [17]. This scheme sets up a secure environment for data transmission by deploying group keys in the smart devices. Hence the group nodes can be used along with chaotic map that provides message integrity using one-way hash functions.

Proposed Method: ETSS

A lightweight two level security method called ECC and Token based Security Scheme (ETSS) are proposed for secured and authenticated communication. The nodes in the network should be prevented from the unauthorized access, and therefore the nodes are generated with token keys. Once the node is entered into the network, the gateway generates token ID for each individual nodes. Also, the generated token ID is registered and encrypted along with the data. The token keys that are generated are time-stamped since it reduces the replay and impersonation attacks. For each set of transmissions, new token keys are generated in random process. If the user needs to access the data, then the user should undergo the following phases like registration, token key generation and verification phase, acknowledgement verification phase, data integrity and transmission phase.

Token Key Generation and Verification Phase

The gateway node controls the wireless sensor network that maintains the IoT process from the root nodes to the end users. Once the node enters into the network, it should get registered with the gateway, and the token keys are generated in the random process for the respective nodes. The token key is said to be as the signature of the node and it is computed through the node ID. The hashing SHA-2 algorithm is applied to compute the token keys for authentication purpose. The gateway verifies the node's legitimacy after registration and the token keys are generated for the entering nodes. The number of nodes that are entered should be listed in the gateway node for proper token key derivations. The nodes that are entering the network will be the initiator and the gateway is the responder in the key generation and verification process.

Gateway sends the generated token key to the node, and the corresponding node computes the hashing signature for the generated token which is given in equation:

$$T_i \xrightarrow{gateway} Send(t_i K),$$
$$S_i = d_j Q_i + T_{ij},$$
$$A_{Th}(N_i) \xrightarrow{hashing} H(S_i \| T_{ij} \| N_i),$$

where T_i is the token for node i; K is the selected key for encryption; S_i is the source node i; D_i is the data for node i; Q_i is the qualified metrics for data d_i; T_{ij} is the token belongs to node i and j; A_{Th} is the authentication of node N_i; H is used for hashing the data.

The token keys are generated with the regular time-stamps to prevent the black-hole and impersonation attacks. Once the token authentication is done and the nodes are proved to be legitimate, the data communication between the nodes can take place with message integrity process.

The acknowledgement for the generated token key T_{ij}* with the signature t_j is then computed to verify the token key authentication given in equation:

$$T_{ij}^* \xrightarrow{gateway} Send(t_i^* K^*),$$
$$S_i^* = d_j^* Q_i + T_{ij}^*,$$
$$A_{Th}(N_i^*) \xrightarrow{hashing} H(S_i^* \| T_{ij}^* \| N_i^*),$$

where T_{ij}* is the generated token key for node i and j. Token with signature to be sent for node j from node i is t_j. Other variables such as K*, S_i*, d_j*, T_{ij}*, N_i*, H and N_i have the same meaning as in the above formula. Once the token authentication is done then the signature is computed for the routing nodes, the signature is computed along with the generated token key by applying hashing algorithm. The authenticated nodes are encoded as $\{(x_j\, y_j) \rightarrow (u_j\, v_j)\}$; here $u_j = h(x_j)$ and $v_j = h(y_j)$ are to neglect the malicious nodes joining from the routing process. By computing the authenticity of the nodes A_{Thij} the signature is generated for the routing nodes which are given in equation:

$$S_j = (x_j, y_j) \rightarrow (u_j, v_j);$$
$$hashing \Rightarrow u_j = h(x_j),\ v_j = h(y_j)$$
$$T_{ij}(k) = h(u_{ij} \oplus v_{ij})$$
$$A_{Th(ij)} = h(t_i \| T_{ij} \| K)$$

and the verification of the signature is given in equations

$$S_j^* = (x_j, y_j) \rightarrow (u_j, v_j);\ u_j = h(x_j),\ v_j = h(y_j)$$
$$T_{ij}(k) = h(u_{ij} \oplus v_{ij} \oplus u_i \oplus v_j)$$
$$verify \Rightarrow A_{Th(ij)} = h(t_i \| T_{ij} \| K)$$
$$create\ Ack_{ij} = h(t_i, Q_i)$$

and respectively:

$$Rcvd \Rightarrow Ack_{ij} = h(t_i, Q_i)$$
$$Verify\ Ack_{ij} \overset{N_i}{\longleftrightarrow} h(t_i, Q_i).$$

The verified nodes along with the authenticated token keys are considered to be the authorized nodes and the user can access the authenticated nodes for accessing the data by undergoing the message decryption process.

Message Integrity Phase

If the node identified to be legitimate during token authentication process, then it is required to confirm its legitimacy before the network initiates data transmission process. The illegitimate node is then labeled as malicious and broadcasted to all other nodes presented in the network. There are some possibilities like existing of malicious nodes during routing even after token key authentication process is done, and hence ECC mechanism is applied for further security process during transmission of data. This ECC method is applied using weirtstrass elliptic point function with the consideration of node coordinates.

The source node and its neighbor node co-ordinate points are considered to be C and D and it forms a straight line of point K which is typically shown in Fig. 1. Elliptical cryptosystem can be applied to deal with public-key cryptographic system which highly depends on the design consideration of mathematical model of elliptic curves with certain limits. Data transfer capacity can be highly maintained in ECC and it is considered to be good when compared with other public key cryptographic systems.

ECC intricacy is generally based on the point multiplication computation if computing factors for the given product get failed. The size of the elliptic curve determines the complexity of the security algorithm. ECC is defined over the elliptic curve by an equation.

$$y^2 = x^3 + cx + d.$$

Here the parameters such as x and y represent the directions of the point or factors of the point on elliptic

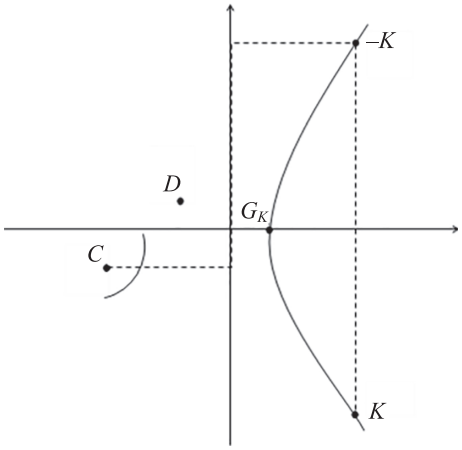

Fig. 1. Elliptic curves points represent neighbor node coordinates *C* & *D*

curve. The factors *c* and *d* are represented for the node coefficients which belongs to the elliptic curve point *K*. Thereby the discriminant analysis of this curve is generally taken as the function of $[-16(4a^3 + 27b^2) \neq 0]$. Node Security for ETSS method is shown in Fig. 2.

The coordinates of the node that forms the elliptic curve contain the infinity point, hence the public key is computed from the point of infinity and the random number is defined for the private key computation. Therefore the public key is computed for the nodes by considering the private key computation. The random number is chosen from the key generator point G_K in the curve for private key generation.

Algorithm for Message Integrity

1. Private keys are generated using elliptic curves point algorithm for each node N_i.

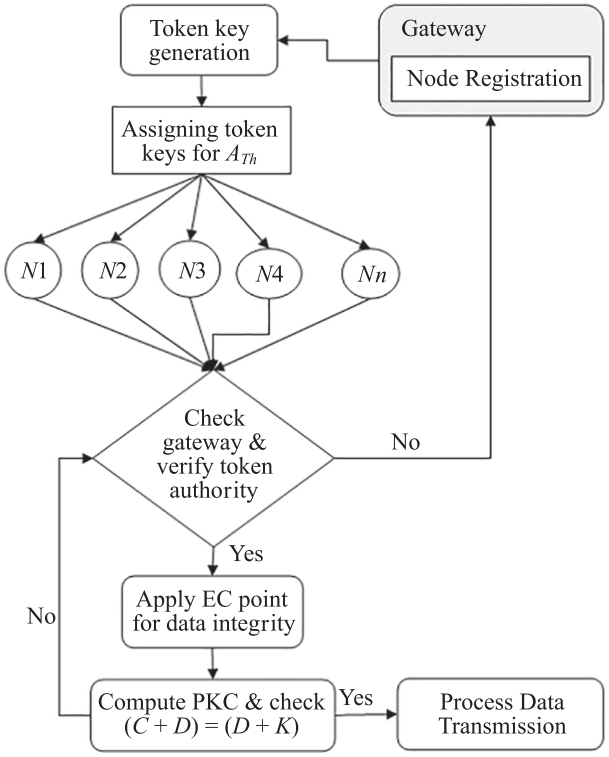

Fig. 2. Node Security for ETSS method

2. From the generated key values the preceding 8 byte succession is extracted.
3. Perform reverse series operation in extracted 8-byte series.
4. Reversed series succession is encrypted using private key to protect data integrity.

The generated public key and the private key are applied with the commutative property and the commutative function states in equation

$$K_{Public}(C + D) = K_{Private}(D + K).$$

The source nodes send the public key, and the destination node replies with private key, then the key verification is done by the gateway. If the key matches, then the nodes can be labeled as legitimate and the data transmission is done with the data integrity. If the generated key not matches $\{(C + D) \neq (D + K)\}$ then the nodes are proved to be illegitimate and the data transmission ends.

Results and Discussion

Network simulator of version 2.35 (NS-2.35) is used to simulate the proposed ETSS and existing protocols TMQTT and EASAP, respectively.

OTCL is the tool command language used in front end. The discrete events that occurred during data transmission between the sensor nodes and gateway are analysed in the network scenario. The metrics that are considered here to analyse the network performance of the proposed protocol are packet rate delivered, average delay, false node detection ratio, and key matching rate.

The other network parameters considered for simulation are given in the Table. Network animator window is used to view the simulation process and the trace files are used to record the process that the protocols are carried out.

Packet Rate Delivered

Packet rate delivered is defined as the ratio between the sum of packets sent and the sum of packets received successfully at the receiver end over the channel from the source that also includes number of intermediate hops. Packet Rate Delivered ($PR_{Delivered}$) is estimated through the number of packets received with respect to the sent packets and it is given in the equation:

$$PR_{Delivered} = \sum_{n=0}^{N} Total\ Pkts\ Sent/Total\ Pkts\ Rcvd.$$

Fig. 3 shows the rate of packets delivered for the scheme ETSS and the conventional methods TMQTT and EASAP.

Table. Simulation parameters

Parameter	Value
Type of Channel	Wireless
Density of nodes	100
Simulation Area, m^2	1100×1100
Transmission range, m	250
Data rate, Mbps	11
MAC	IEEE 802.11
Network Interface Type	WirelessPhy

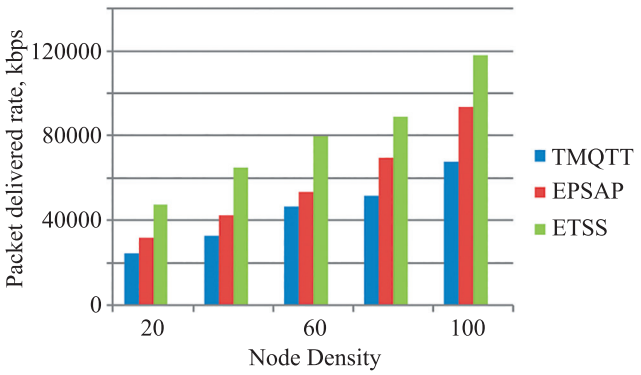

Fig. 3. Packet rate delivered

The scheme ETSS proposed here obtains better delivery rates of packets when compared with existing schemes TMQTT and EASAP. If node density gets increased, then simultaneously delivery of data packets also gets increased.

Average Delay

The data packets that take processing time for sending the sensed information from source to the destination is said to be average delay. This also includes the retransmission of unsuccessful packets and the packet queues with congestion delay. Equation below describes the transmission delay of packets during communication over the network. Here n represents the number of nodes.

$$Delay = \frac{\sum_{0}^{n} Pkt\ r\ e\ cvd\ time - Pkt\ send\ time}{n}.$$

The average delay for the proposed ETSS and existing methods TMQTT and EASAP are shown in the Fig. 4. Proposed ETSS protocol exhibits good performance in terms of the communication delay while comparing to the other TMQTT and EASAP schemes.

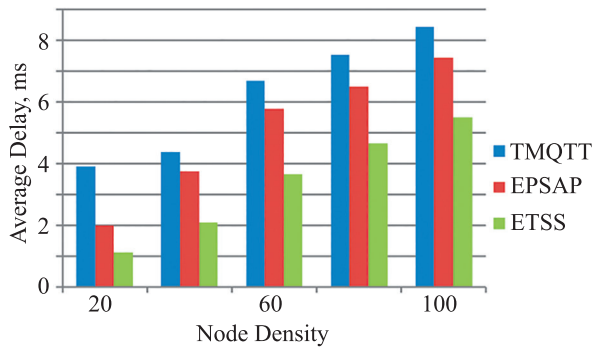

Fig. 4. Average delay

Ratio of False Node Detection

The computational ratio malignant nodes and normal nodes (that are detected through the process) is said to be False Node Detecting Ratio (FNDR). Based on the node behavior i.e. normal or malignant the FNDR can be determined. Normal nodes forward the packets without any packet losses or modifications. But malignant nodes forward the false information with some delays. Fig. 5

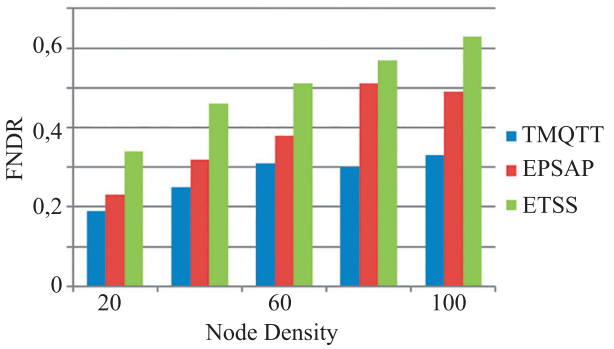

Fig. 5. FNDR

shows the FNDR of both the proposed and conventional method. It is shown that the proposed ETSS protocol has high FNDR rate compared to the conventional TMQTT and EASAP schemes, and this leads the network to achieve good throughput.

Key Matching Rate

Key Matching Rate (KMR) is defined to be the ratio of number of keys that is matched to the source and receiver end. Trusted nodes are chosen from the KMR values for secured and optimal data transmission. Fig. 6 shows the key matching ratio for both the proposed scheme ETSS and the existing TMQTT and EASAP methods with respect to node density.

The average KMR computed for proposed ETSS method is 0.891 and for conventional TMQTT and EASAP the average KMR obtained are 0.692 and 0.744, respectively. Hence the proposed scheme proves and possesses good key matching ratio between the nodes and the user's. The data can be sent without major loss during routing.

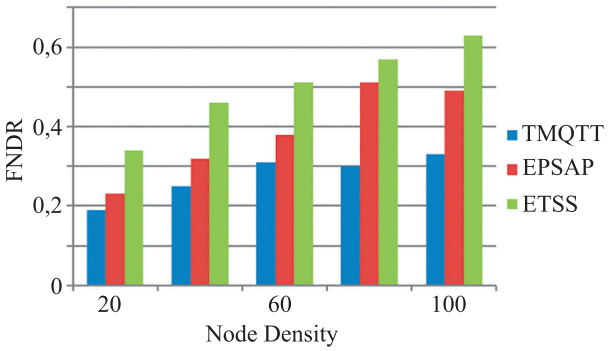

Fig. 6. Key matching ratio

Conclusion

A lightweight authentication protocol named ECC with Token based Security Scheme is proposed here to improve the security system. This scheme is mainly proposed to prevent the network from the unauthorized access. If the user needs to access the data, then the user should undergo the token key generation and verification phase, as well as data integrity and transmission phase. Therefore, two security checks are carried out in this process and the nodes

are generated with token keys. Initially, once the node is entered, the token keys are generated for each individual node by the gateway. Then Elliptical Curve Cryptography is applied to remove the malicious nodes completely if some adversaries missed out during token key verification process.

References

1. Zhang Q., Fu S., Jia N., Xu M. A verifiable and dynamic multi-keyword ranked search scheme over encrypted cloud data with accuracy improvement. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 2018, vol. 254, pp. 588–604. https://doi.org/10.1007/978-3-030-01701-9_32
2. Shen J., Shen J., Chen X., Huang X., Susilo W. An efficient public auditing protocol with novel dynamic structure for cloud data. *IEEE Transactions on Information Forensics and Security*, 2017, vol. 12, no. 10, pp. 2402–2415. https://doi.org/10.1109/TIFS.2017.2705620
3. Han G., Wang H., Miao X., Liu L., Jiang J., Peng Y. A dynamic multipath scheme for protecting source-location privacy using multiple sinks in WSNs intended for IIoT. *IEEE Transactions on Industrial Informatics*, 2020, vol. 16, no. 8, pp. 5527–5538. https://doi.org/10.1109/TII.2019.2953937
4. Far H.A.N., Bayat M., Das A.K., Fotouhi M., Pournaghi S.M., Doostari M.A. LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. *Wireless Networks*, 2021, vol. 27, no. 2, pp. 1389–1412. https://doi.org/10.1007/s11276-020-02523-9
5. Al-Turjman F., Alturjman S. Context-sensitive access in industrial internet of things (IIoT) healthcare applications. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14, no. 6, pp. 2736–2744. https://doi.org/10.1109/TII.2018.2808190
6. Stallings W. *Cryptography and Network Security: Principles and Practice*. 5th ed. Pearson Education, 2013.
7. Verma D., Jain R., Shrivastava A. Performance analysis of cryptographic algorithms RSA and ECC in wireless sensor networks. *IUP Journal of Telecommunications*, 2015, vol. 7, no. 3, pp. 15.
8. Ahmed M.H., Alam S.W., Qureshi N., Baig I. Security for WSN based on elliptic curve cryptography. *Proc. of the 1st International Conference on Computer Networks and Information Technology (ICCNIT)*, 2011, pp. 75–79. https://doi.org/10.1109/ICCNIT.2011.6020911
9. He D., Chan S., Tang S., Guizani M. Secure data discovery and dissemination based on hash tree for wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2013, vol. 12, no. 9, pp. 4638–4646. https://doi.org/10.1109/TWC.2013.090413.130072
10. Jawad K., Mansoor K., Baig A.F., Ghani A., Naseem A. An improved three-factor anonymous authentication protocol for WSN s based iot system using symmetric cryptography. *Proc. of the 2019 International Conference on Communication Technologies (ComTech)*, 2019, pp. 53–59. https://doi.org/10.1109/COMTECH.2019.8737799
11. Kandi M.A., Lakhlef H., Bouabdallah A., Challal Y. An efficient multi-group key management protocol for Internet of Things. *Proc. of the 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2018, pp. 438–443. https://doi.org/10.23919/SOFTCOM.2018.8555857
12. Zhou G.-D., Yi T.-H. Recent developments on wireless sensor networks technology for bridge health monitoring. *Mathematical Problems in Engineering*, 2013, vol. 2013, pp. 947867. https://doi.org/10.1155/2013/947867
13. Bhawiyuga A., Data M., Warda A. Architectural design of token based authentication of MQTT protocol in constrained IoT device. *Proc. of the 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1–4. https://doi.org/10.1109/TSSA.2017.8272933
14. Dammak M., Boudia O.R.M., Messous M.A., Senouci S.M., Gransart C. Token-based lightweight authentication to secure IoT networks. *Proc. of the 16th IEEE Annual Consumer Communications and Networking Conference (CCNC)*, 2019, pp. 8651825. https://doi.org/10.1109/CCNC.2019.8651825
15. Li X., Niu J., Bhuiyan M.Z.A., Wu F., Karuppiah M., Kumari S. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14, no. 8, pp. 3599–3609. https://doi.org/10.1109/TII.2017.2773666

Литература

1. Zhang Q., Fu S., Jia N., Xu M. A verifiable and dynamic multi-keyword ranked search scheme over encrypted cloud data with accuracy improvement // Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering. 2018. V. 254. P. 588–604. https://doi.org/10.1007/978-3-030-01701-9_32
2. Shen J., Shen J., Chen X., Huang X., Susilo W. An efficient public auditing protocol with novel dynamic structure for cloud data // IEEE Transactions on Information Forensics and Security. 2017. V. 12. N 10. P. 2402–2415. https://doi.org/10.1109/TIFS.2017.2705620
3. Han G., Wang H., Miao X., Liu L., Jiang J., Peng Y. A dynamic multipath scheme for protecting source-location privacy using multiple sinks in WSNs intended for IIoT // IEEE Transactions on Industrial Informatics. 2020. V. 16. N 8. P. 5527–5538. https://doi.org/10.1109/TII.2019.2953937
4. Far H.A.N., Bayat M., Das A.K., Fotouhi M., Pournaghi S.M., Doostari M.A. LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT // Wireless Networks. 2021. V. 27. N 2. P. 1389–1412. https://doi.org/10.1007/s11276-020-02523-9
5. Al-Turjman F., Alturjman S. Context-sensitive access in industrial internet of things (IIoT) healthcare applications // IEEE Transactions on Industrial Informatics. 2018. V. 14. N 6. P. 2736–2744. https://doi.org/10.1109/TII.2018.2808190
6. Stallings W. Cryptography and Network Security: Principles and Practice. 5th ed. Pearson Education, 2013.
7. Verma D., Jain R., Shrivastava A. Performance analysis of cryptographic algorithms RSA and ECC in wireless sensor networks // IUP Journal of Telecommunications. 2015. V. 7. N 3. P. 15.
8. Ahmed M.H., Alam S.W., Qureshi N., Baig I. Security for WSN based on elliptic curve cryptography // Proc. of the 1st International Conference on Computer Networks and Information Technology (ICCNIT). 2011. P. 75–79. https://doi.org/10.1109/ICCNIT.2011.6020911
9. He D., Chan S., Tang S., Guizani M. Secure data discovery and dissemination based on hash tree for wireless sensor networks // IEEE Transactions on Wireless Communications. 2013. V. 12. N 9. P. 4638–4646. https://doi.org/10.1109/TWC.2013.090413.130072
10. Jawad K., Mansoor K., Baig A.F., Ghani A., Naseem A. An improved three-factor anonymous authentication protocol for WSN s based iot system using symmetric cryptography // Proc. of the 2019 International Conference on Communication Technologies (ComTech). 2019. P. 53–59. https://doi.org/10.1109/COMTECH.2019.8737799
11. Kandi M.A., Lakhlef H., Bouabdallah A., Challal Y. An efficient multi-group key management protocol for Internet of Things // Proc. of the 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM). 2018. P. 438–443. https://doi.org/10.23919/SOFTCOM.2018.8555857
12. Zhou G.-D., Yi T.-H. Recent developments on wireless sensor networks technology for bridge health monitoring // Mathematical Problems in Engineering. 2013. V. 2013. P. 947867. https://doi.org/10.1155/2013/947867
13. Bhawiyuga A., Data M., Warda A. Architectural design of token based authentication of MQTT protocol in constrained IoT device // Proc. of the 11th International Conference on Telecommunication Systems Services and Applications (TSSA). 2017. P. 1–4. https://doi.org/10.1109/TSSA.2017.8272933
14. Dammak M., Boudia O.R.M., Messous M.A., Senouci S.M., Gransart C. Token-based lightweight authentication to secure IoT networks // Proc. of the 16th IEEE Annual Consumer Communications and Networking Conference (CCNC). 2019. P. 8651825. https://doi.org/10.1109/CCNC.2019.8651825
15. Li X., Niu J., Bhuiyan M.Z.A., Wu F., Karuppiah M., Kumari S. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things // IEEE

16. Kung Y.-H., Hsiao H.-C. GroupIt: Lightweight group key management for dynamic IoT environments. *IEEE Internet of Things Journal*, 2018, vol. 5, no. 6, pp. 5155–5165. https://doi.org/10.1109/JIOT.2018.2840321
17. Mughal M.A., Shi P., Ullah A., Mahmood K., Abid M., Luo X. Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN. *IEEE Access*, 2019, vol. 7, pp. 76699–76711. https://doi.org/10.1109/ACCESS.2019.2921999

Transactions on Industrial Informatics. 2018. V. 14. N 8. P. 3599–3609. https://doi.org/10.1109/TII.2017.2773666
16. Kung Y.-H., Hsiao H.-C. GroupIt: Lightweight group key management for dynamic IoT environments // IEEE Internet of Things Journal. 2018. V. 5. N 6. P. 5155–5165. https://doi.org/10.1109/JIOT.2018.2840321
17. Mughal M.A., Shi P., Ullah A., Mahmood K., Abid M., Luo X. Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN // IEEE Access. 2019. V. 7. P. 76699–76711. https://doi.org/10.1109/ACCESS.2019.2921999

Authors

Loganathan Sasirega — PhD, Research Scholar, Vels Institute of Science Technology & Advanced Studies, Chennai, 600117, India, SC 57414859000, https://orcid.org/0000-0003-3771-8959, lsasirega1975@gmail.com
Chandrabose Shanthi — PhD, Assistant Professor, Vels Institute of Science Technology & Advanced Studies (VISTAS), Chennai, 600117, India, SC 57195615646, https://orcid.org/0000-0002-7976-2360, shanc08071978@gmail.com

Авторы

Сасиега Логанатан — PhD, исследователь, Институт науки, технологий и перспективных исследований Велса, Ченнаи, 600117, Индия, SC 57414859000, https://orcid.org/0000-0003-3771-8959, lsasirega1975@gmail.com
Шанти Чандрабос — PhD, доцент, Институт науки, технологий и перспективных Велса исследований Велса, Ченнаи, 600117, Индия, SC 57195615646, https://orcid.org/0000-0002-7976-2360, shanc08071978@gmail.com

Received 17.11.2021
Approved after reviewing 02.03.2022
Accepted 30.03.2022

Статья поступила в редакцию 17.11.2021
Одобрена после рецензирования 02.03.2022
Принята к печати 30.03.2022