УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2021 Том 21 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2021 Vol. 21 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2021-21-6-929-935

Bi-level authentication and mannequin routing for improving security features of WSN-IoT

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

[1,2] Vels Institute of Science Technology and Advanced Studies, Chennai, 600043, India

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

Abstract
Node authentication and key management are the two significant security services employed in Wireless Sensor Networks (WSN). Since the growth of the devices in WSN is rapidly increasing, strong security policies should be employed to save the network from outside invaders. There is a wide range of smart applications developed in various fields such as military, health, agriculture, smart city, and many others. Since most of the applications consist of sensitive data, they should be protected to save the users' privacy. Conventional protocols are more prone to security attacks and therefore the authors propose a secure and reliable protocol named Polynomial Authentication and Mapping Verification based Mannequin Routing (PAMVMR). This scheme involves two main processes such as Bi-level authentication and Information Processing. Bi-level authentication includes node-to-gateway authentication using polynomial key shares and node-to-node verification using mapping function that is processed through a context free grammar. Information processing includes creation of mannequin routes by applying Pascal's triangle method and transmission of data. This makes the network more secure and reliable for data transmission from sensor nodes to a gateway node and from a gateway to users.

Keywords
Bi-level authentication, polynomial token, mapping variables, mannequin route, Pascal's binomial triangle

For citation: Sasirega L., Shanthi Ch. Bi-level authentication and mannequin routing for improving security features of WSN-IoT. *Scientific and Technical Journal of Information Technologies, Mechanics and Optic*s, 2021, vol. 21, no. 6, pp. 929–935. doi: 10.17586/2226-1494-2021-21-6-929-935

УДК 004.056.53

Двухуровневая аутентификация и манекен-маршрутизация для повышения безопасности беспроводных сенсорных сетей интернета вещей

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

[1,2] Институт науки, технологий и перспективных исследований Велса, Ченнаи, 600043, Индия

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

Аннотация
Аутентификация узлов и управление ключами — две важные службы безопасности, используемые в беспроводных сенсорных сетях (Wireless Sensor Networks, WSN). Так как количество устройств в WSN постоянно увеличивается, следует применять строгие политики безопасности, чтобы защитить сеть от внешних угроз. Существует широкий спектр интеллектуальных приложений в различных областях, таких как военная, здравоохранение, сельское хозяйство, системы «умный город» и многие другие. Большинство приложений содержат конфиденциальные данные, и они должны быть защищены для сохранения данных пользователей. Обычные протоколы безопасности активно подвержены атакам, и для их защиты предложен более надежный протокол, называемый полиномиальной аутентификацией и проверкой соответствия на основе манекен-маршрутизации (Polynomial Authentication and Mapping Verification based Mannequin Routing, PAMVMR). Протокол включает два основных процесса, такие как двухуровневая аутентификация и обработка информации. Двухуровневая аутентификация включает аутентификацию от узла к шлюзу с использованием

общих полиномиальных ключей и проверку от узла к узлу с использованием функции сопоставления, которая обрабатывается с помощью правила бесконтекстной грамматики. Обработка информации включает создание манекен-маршрутов с использованием метода треугольника Паскаля и передачу данных. В результате сеть становится защищенной и надежной для передачи данных от узлов датчиков к узлу шлюза и от шлюза к пользователям.

Ключевые слова
двухуровневая аутентификация, полиномиальный токен, отображение переменных, манекено-маршрутизация, биномиальный треугольник Паскаля

Ссылка для цитирования: Сасиега Л., Шанти Ч. Двухуровневая аутентификация и манекен-маршрутизация для повышения безопасности беспроводных сенсорных сетей интернета вещей // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 6. С. 929–935 (на англ. яз.). doi: 10.17586/2226-1494-2021-21-6-929-935

Introduction

Internet of Things (IoT) has become a trending area [1] recently that led to the popularity of technologies related to Wireless Sensor Network (WSN). WSN uses IoT in many fields of network control. WSN is widely implemented in all areas and created popular and huge IoT-related applications [2] and so-called Smart Life. However, this technology development causes the disclosure of personal information that possibly affects the privacy and protection in such WSN in which people tend to enjoy their convenience. Therefore, security issues in WSN-IoT are getting important for improving the quality of service [3].

In WSN, the user authentication scheme is categorized into five different types that offer good guidance for the proposals of novelty of improved user authentication and key agreement protocols [4]. Later an upgraded authentication model was proposed [5], in which sensors act as routers and destinations. In this case, the sensors might be located between a user and gateway, and therefore, it is necessary to forward the authenticated messages to the gateway node.

Related Works

Various kind of authentication protocols were proposed [6–8], for various WSN-IoT related applications and still there are a lot of security related issues. Different kind of security related authentication factors like biometric factor or fingerprint authentication schemes are undertaken to solve these issues. Especially, physiological biometrics based authentication method was implemented in order to perform user authentications, such as fingerprints [9], iris [10], and facial information [11]. But, this kind of authentications requires additional and costly equipment. Therefore two-factor authentication and key agreement schemes were proposed for protecting the real time data access with smart card that are now the most popular and widely used operations. A representative authentication protocol was proposed in a multi-gateway WSN to resolve the node capturing attacks with the intention of detecting a vulnerable authentication protocol in such a WSN. An untraceable two-factor authentication mechanism for WSN was proposed on basis of Elliptical Curve Cryptography (ECC). This scheme comes up with missed security features that are highly required for real life applications by maintaining the desired features of original model in a parallel way. This method also accomplishes the mutual authentication of Burrows-Abadi-Needham (BAN) logic.

Polynomial and Multivariate Mapping-Based Triple-Key (PMMTK) distribution model was proposed in [12]. This mechanism is carried out through the calculation of the node's individual key and common triple-key by evaluating the polynomial coefficients. Lightweight Polynomial-based Key Management (LPKM) was introduced to improve the security features of the distributed WSN [13]. LPKM scheme establishes various key types by the sensors used for bootstrapping the trust and security for multi-type communications. Also the LPKM model can effectively alleviate the most common attacks like node impersonation attacks, clone attacks, etc. Three-factor anonymous authentication scheme was proposed for WSNs in IoT environments [14]. Here a fuzzy model is utilized for handling the user's biometric information that helps significantly to improve the functional security features.

Anonymous Access Authentication model for WSN (AAA-WSN) was proposed in big data environments for achieving the security services [15]. This AAA-WSN mechanism not only provides strong security services like user anonymity and mutual authentication but also performs the perfect forward secrecy feature with better level of efficiency. To prevent a malicious user from guessing the communication period between Home Gateway Node (HGWN) and the sensor, a dynamic contacting model was designed. The Membership Authentication and Key Establishment (MAKE) protocol was proposed for WSNs [16]. This membership authentication mechanism has the complexity O(n), where n is the number of users in a group communication. Another example is one-to-one authentications with complexity O(n^2) which was a different authentication process handled here. An authentication information exchange scheme (AIES) was proposed in WSN [17] to prevent node capture attacks. This model is developed on basis of the association scheme of HGWN and local sensor nodes. HGWN keep contact with all local sensor nodes and also it is responsible for performing an authentication information exchange scheme to resist the security risks.

Proposed Approach

Our work consider cluster-based wireless sensor network since cluster-based environment helps to increases the performance of the network with less delay and increased energy. The sensor node and the gateway node should communicate periodically with each other. The nodes that enter into the network can be represented by a normal node, a possibly compromised node or a fully compromised node. In order to prove the node's original identities from malicious nodes, we propose to carry out the Bi-level authentication process in our method. Fig. 1 shows the example scenario of a user accessing the gateway node through the located sensor nodes.

The Normal Node (NN) will respond to the gateway node periodically and normally about its node state. Therefore the gateway node assumes that the node is normal and records its status as normal in the database. The possibly compromised nodes respond the gateway node with delay latencies and therefore the gateway node sets this node status as possibly compromised but stores in the database as well. If there is no response after a certain time period from the particular node then the node is set as a fully compromised node and hence this node is set as a malicious one and removed from the routing. However this kind of malicious node detection is not effective because the node can go inactive due to the loss of the communication signal or high energy drain rate. Therefore Bi-level authentication process is carried for each node that enters the network. This scheme also consumes less energy for data processing compared to the conventional schemes.

Bi-level Authentication

Bi-level authentication includes two level authentication processes. The first level authentication is the node-to-gateway (GW) authentication, which is carried out using polynomial key shares. The second level authentication is the node-to-node verification, which is carried out using mapping function. Mapping between the nodes is processed through context free grammar rule.

1) **Node-to-GW Authentication.** Once the node enters the network, the Base Station (BS) and the node generates communication keys to process the authorized communication. When a new node enters the network, key generation process will be initiated by the BS and the key will be based on the node's identity. Then this key will be used as a ticket or token to access a resource. The node should share this token whenever the node wants to communicate with the other node so that the node will be authorized to access the resources. The keys are generated using polynomial structure with '*n*' degree of polynomials. The node identity is given as $Id(i) = 1,2,\ldots,n$ that is allotted to each node that enters the network $f(y) = a_n y^n + \ldots + a_1 y + a_0 \mathrm{mod} N$. Therefore the multivariate polynomial can be computed through $F(y_1, y_2, \ldots, y_m) = \prod_{i=1}^{m} f(y_i) \mathrm{mod} N$. If the node enters the network, the polynomial key generator computes the polynomial keys through the following equation:

$$F(Ni) = f(i)\mathrm{mod}N;\ i = 1, 2, \ldots, n.$$

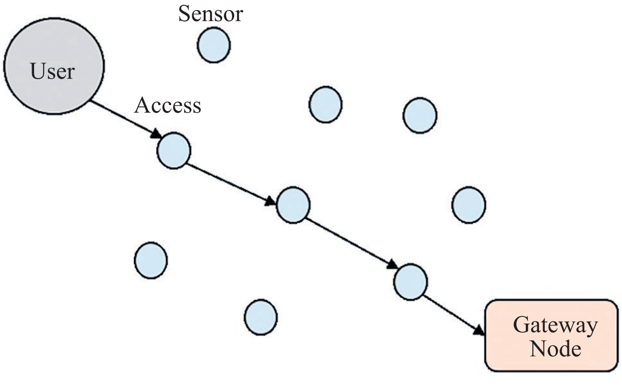

Fig. 1. User access gateway through sensor nodes

The polynomial key tokens are generated for every node *Ni* and secretly stored in the node registration centre. The node registration centre randomly selects the integer to solve the authentication problem by taking $\{f_1(i), f_2(i), \ldots, f_{m-1}(i)\}$, where each integer lies in the key pool. Then the node registration centre generates polynomial key tokens for each node that enters the network. The polynomial token keys are computed as $\{P_{KT1}(Ni), P_{KT2}(Ni), \ldots, P_{KTm-1}(Ni)\}$ for each node. Each node is computed with the polynomial secret key and stored in the gateway node. The polynomial-based authentication mechanism is used in this work. A polynomial key is a ticket that provides permission to access a device that consists of entities such as unique object identifier ID, access rights *Rs*, and a random value *Ri*. The identifier is the name of the device with sensor nodes. The capability will describe the access rights of the device. The random value is generated to prevent forgery. One-way hash function $h(f)$ is used to check the access rights request, when it arrives with the device id. The one-way hash function calculates the output for the given random number and, if it is valid, then the access is granted.

Let us assume that '$N_{i,n}$' is a number of nodes and the gateway node (*GN*) stores $S_{i,n}$ (secret authenticated data) in its authentication database.

Step 1: Each node should broadcast their original identity '*Ni*' to all other nodes that present together.

Step 2: Once the identities '$N_{i,n}$' with random integer 'R_i' is received, each node generates a polynomial token key $\{P_{KT1}(Ni), P_{KT2}(Ni), \ldots, P_{KTm-1}(Ni)\}$ with respect to their random integers 'R_i'.

Step 3: The *GN* node computes an authentication reply (A_{Ri}) by using a hashing key function $A_{Ri} = h\|\{k,(N_1,r_1), (N_2,r_2), \ldots, (N_m,r_m)\}$. The '$A_{Ri}$' is broadcasted to all the respective nodes.

Step 4: The $P_{KT(i)}$ is verified with the key-hash function A_{Ri}. If the computed hash key output matches with the $P_{KT(i)}$ then the verification of the node is determined to be '*NN*'.

Step 5: Continue the process for each set of transmission since the node may be compromised at any time.

This process will be initiated only when a new node wants to communicate with other node in the network. If node *A* wants to communicate with node *B*, both are mutually authenticated first before sharing the data, so that the communication will be secured. Since the key generation for a new node is initially produced, the key management mechanism used in the proposed work avoids rekeying process. Therefore, the proposed work enhances the performance of the network with less energy.

2) **Node-to-Node Verification.** Node-to-node verification process based on a context-free grammar is carried out between the sensors once the node-to-gateway authentication process is done. Each node has its own

mapping variable string by using these node variables (strings), and hence the leftmost and rightmost derivations can be obtained. Source node starts the leftmost derivation with the mapping variable string '*s*' till it reaches the terminal function *D* ('*d*').

Here the source node computes the leftmost derivation and the destination node computes the rightmost derivation. Leftmost derivation follows the top-down approach for derivation of the mapping variables and the rightmost derivation follows bottom-up approach for deriving the mapping variable strings. If the leftmost and rightmost derived mapping strings are equal then the nodes are legitimate and the dummy node id can be generated for each and every node to process the data transmission procedure.

Leftmost and Rightmost mapping derivation. The leftmost and rightmost derivations are obtained on basis of string mapping functions. Every node is assigned with a mapping variable called string. Leftmost non terminals are expanded with leftmost derivation. In the same way rightmost derivations select the rightmost non-terminal variables for expanding till it reaches the terminal node. Fig. 2 shows the example of string mapping function.

Let us assume the example network scenario with n number of nodes and each node holds a mapping variable. The mapping function starts from the source node '*S*' and '*a*' is the mapping variable of node '*S*'. *R* is the random number generated for '*S*'. Similarly the forwarder nodes '*A*' and '*C*' contain the mapping variables '*e*' and '*c*' respectively. Terminal node '*D*' contains the mapping variable '*b*'; therefore the mapping functions can be applied using the context free grammar rule. Now the nodes '*S*', '*A*', '*C*' and '*D*' are considered for the leftmost and rightmost derivations with their respective mapping variables $\{a, e, c, b\}$ for node verifications. The grammar rule is given as per equation:

$$G_{Rule} = (\{S \rightarrow\}, \{a, c, e, b\}R, S).$$

The grammar rule G_R is considered with the production rule given in the equation:

$$G_R = \{S \rightarrow aSSe, S \rightarrow e, S \rightarrow c, S \rightarrow b\}.$$

First, the leftmost derivation is carried out from the source node to the terminal node '*D*' and is calculated by using grammar rule given in the equation:

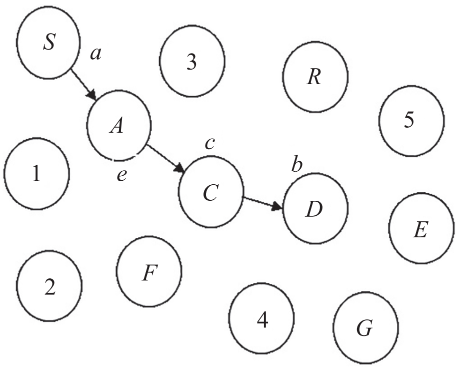

Fig. 2. String mapping function

$$S \overset{LM}{\Rightarrow} aSSe \overset{LM}{\Rightarrow} aeSc \overset{LM}{\Rightarrow} aecSSb \overset{LM}{\Rightarrow} aecSb \overset{LM}{\Rightarrow} \{aecb\}.$$

Then the rightmost derivation is carried out from the terminal node to source node '*S*' using grammar rule given in the equation:

$$D \overset{RM}{\Rightarrow} bSSc \overset{RM}{\Rightarrow} bcSe \overset{RM}{\Rightarrow} bceSSa \overset{RM}{\Rightarrow} bceSa \overset{RM}{\Rightarrow} \{bcea\}.$$

Now the obtained variable is applied with recursive function to check the leftmost derivation output:

$$\{bcea\} \rightleftarrows \{aecb\}.$$

The recursive rightmost output strings are stored in the rightmost deviation. Then the mapping function is done for the leftmost deviation output variables and for the recursive rightmost deviation output variables. The mapping function for nodes '*S*', '*A*', '*C*', '*D*' is given in the equation:

$$\begin{Bmatrix} LM \Rightarrow S \\ a \\ e \\ c \\ b \end{Bmatrix} \xrightarrow[mapping]{} \begin{Bmatrix} RM \Rightarrow D \\ a \\ e \\ c \\ b \end{Bmatrix}.$$

If the mapping variables are the same for both leftmost and rightmost derivation then the nodes are verified to be normal but if the variables are different than said they are assumed to be malicious. The malicious nodes can be removed from the network and the routing table is then updated.

Information Processing. Information processing includes sending the sensed data over the falsely created routes. The falsely created route is a mannequin route that is generated by applying the principle of Pascal's triangle method. By using this mannequin route, the data is transmitted reliably. In order to safeguard the information from malicious nodes, the gateway generates fake route identities for the source node, intermediate data forwarder (relay) nodes and destination nodes. To protect the data from the malicious observer, the source generates a dummy route. The original id is multiplied with Pascal's binomial triangular values to generate the fake identities so that the data are passed through these mannequin node identities. By this way the data can be protected from the malicious observer since the malicious observer cannot identify the real source intermediate and destination nodes.

Therefore the source nodes send the confidential data over the intermediate nodes during the communication and prevent the system from security threats. Fig. 3 shows the example scenario for a mannequin route.

Pascal's binomial triangular function is defined in the equation below:

$$P_{BT} = (A + B)^n.$$

Here '*A*' represents the source node and '*nu*' represents the destination node and '*n*' represents the number of intermediate hop count that exists between them. From the figure source, the node identity is assumed to be 2, the destination identity is assumed to be 1 and the intermediate identities are 5 and 3 respectively. The generation of fake

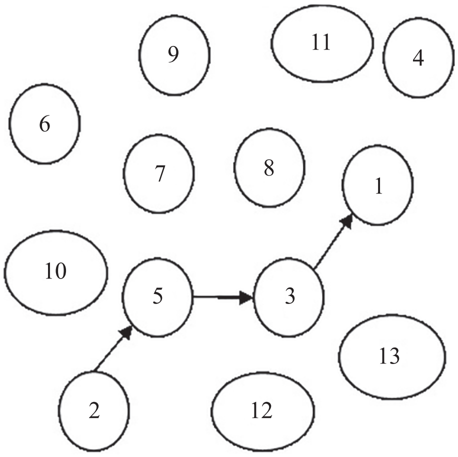

Fig. 3. Mannequin route creation

identities using the Pascal's binomial triangular function is shown below.

Step 1: $(2+1)^3$

Step 2: $(2+1)^3 \rightarrow 2^3 + 3(2^2)(1) + 3(2)(1^2) + 1^3$

Step 3: generated identities → 8+ 12 + 6 + 1

The source original id is 2 but the generated mannequin id is '8', the intermediate real identities are 5 and 3 while their created fake identities are 12 and 6. The destination node identity is the same; however the malicious observer cannot modify the received data in the gateway or destination node. This type of generation of mannequin routes for data transmission makes the network more secured and reliable. Therefore passive type of attacks can be reduced greatly by transmitting the data by this method.

Results and Discussion

Network simulator (version 2.35) is used to simulate the proposed PAMVMR and existing protocols AIES and MAKE respectively. OTCL is the tool command language used in front end. The discrete events are analysed in the network scenario. To analyse the network performance of the proposed protocol, we considered the following: node trust ratio, packet delivered rate, False Node detection ratio, and energy consumption. Other network parameters considered for simulation are given in Table 1. 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.

Table 1. Simulation parameters

Parameter	Value
Channel Type	Wireless channel
Density of nodes	100
Simulation Area	1100 × 900 m^2
Proposed Protocol	PAMVMR
Conventional Schemes	AIES & MAKE
Transmission range	250 m
Data rate	11 Mbps
MAC	IEEE 802.11
Network Interface Type	WirelessPhy

Packet Delivered Rate. Packet delivered rate is estimated for detecting the total number of packets that are sent over the channel successfully from the sender node to the destination including the number of relay hops. The Packet Delivered Rate (P_{DR}) is measured using the total number of the packets received and the total number of packets sent and is given in the equation:

$$P_{DR} = \frac{\sum Total\ Pkts\ Rcvd}{\sum Total\ Pkts\ sent}.$$

The packet delivery rates for the proposed scheme PAMVMR and the existing schemes AIES and MAKE are shown in Fig. 4. The proposed scheme achieves better delivery rates of packets compared to the other conventional security mechanisms. If node density increases then delivery of data packets also gets increased. Packet delivery rates are directly proportional to the network throughput. Therefore the metric P_{DR} achieves better efficiency in delivering the data packets proving the proposed scheme efficiency.

Energy Consumption. The amount of energy that each node consumed for processing and transmitting the data can be defined as energy consumption. The energy that is spent by the node for a set of transmission is calculated with respect to a certain time period. Energy is the main source to keep the entire network to function continuously and hence maintaining the energy level for each node is compulsory. Current energy level can be calculated by taking the remaining energy level of the nodes. The energy consumption for both proposed PAMVMR and conventional schemes AIES and MAKE are shown in Fig. 5.

The proposed scheme PAMVMR consumes low energy for processing and transmission of data compared to the

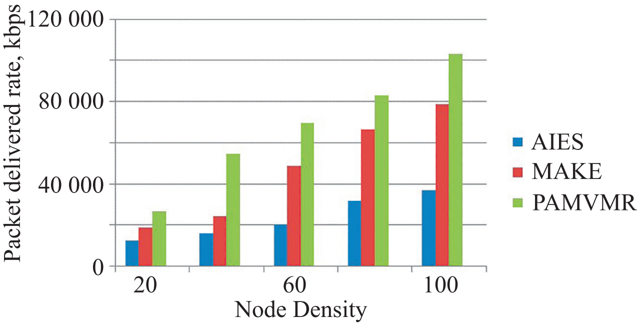

Fig. 4. Packet delivery rates

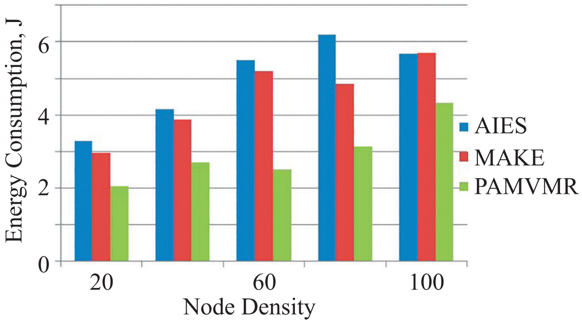

Fig. 5. Energy consumption

conventional schemes. The main reason for less energy is that the proposed scheme allows the nodes to go to sleep state in certain interval during the processing of data which helps to save energy. Another reason for less energy is that it allows only trusted nodes to route process which helps to minimize large number of computational process which saves energy. Therefore the routes selected for data transmission are more reliable and good resource constraint.

False Node Detection Ratio. False Node Detecting Ratio (FNDR) is defined as the ratio between the number of malicious nodes and the number of normal nodes. Based on the node's behaviour, i.e. normal, partially compromised and fully compromised, the FNDR can be determined. Normal nodes forward the packets without any longer delay and packet loss. Whereas compromised nodes forward the false information with delay latencies. Fig. 6 shows the FNDR values for both the proposed and conventional schemes. It is clearly shown that the proposed protocol PAMVMR has FNDR rate compared to the existing scheme such as AIES and MAKE. This leads the network to achieve higher packet rates.

Node Trust Ratio. The ratio of trust values that is obtained for the nodes with respect to their packet forwarding rate is defined as Node Trust Rate (NT_R). By processing the node authentication and verification for each node, the trustable nodes are detected and these nodes are selected for the data transmission process by generating mannequin identities for the respective nodes. NT_R is identified with respect to the normal node that resides in the network.

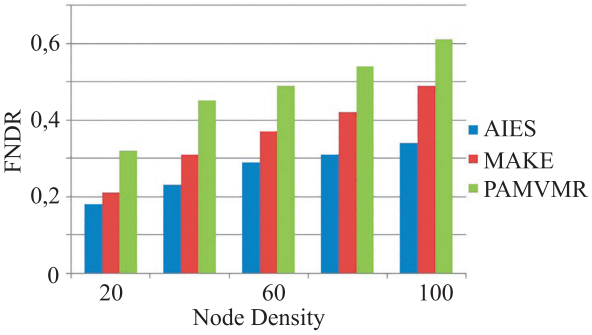

Fig. 6. FNDR

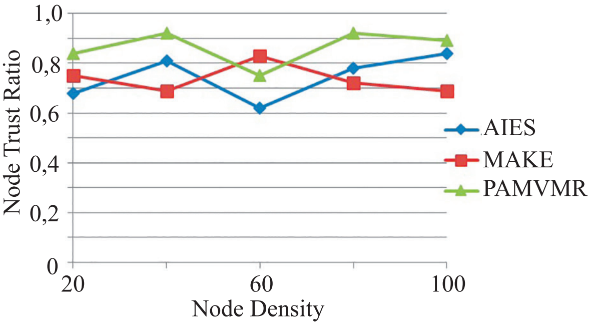

Fig. 7. Node trust ratio

NT_R for both the proposed and existing scheme are shown in Fig. 7. The proposed method PAMVMR has a high trust rate when compared to such schemes as AIES and MAKE. The average NT_R for the proposed scheme PAMVMR is 0.86 and for the conventional scheme the average NT_R is 0.74 and 0.73 respectively. Therefore the proposed Bi-level authentication scheme increases the network trust ratio when compared to the other existing schemes without revealing the nodes original identity during data transmission.

Conclusion

Polynomial Authentication and Mapping Verification based Mannequin Routing scheme is proposed here to improve the security measures. PAMVMR includes two main protection processes such as Bi-level authentication and Information Processing. Bi-level authentication forwards a node to gateway authentication by applying polynomial key shares. Mapping verification of nodes is performed using mapping function which is processed through context free grammar. Later mannequin routes are created by applying Pascal's triangle method for sealing the original identities of the data transmission nodes in order to prevent the nodes from malicious users. Therefore this makes the network more secured and reliable for data transmission from sensor nodes to the gateway node and from gateway to users. Simulation analysis proves the efficiency of the proposed scheme.

References

1. Sharma R., Prakash S., Roy P. Methodology, applications, and challenges of WSN-IoT. *Proc. of the International Conference on Electrical and Electronics Engineering (ICE3)*, 2020, pp. 502–507. https://doi.org/10.1109/ICE348803.2020.9122891
2. Nguyen T.M.C., Hoang D.B., Chaczko Z. Can SDN technology be transported to software-defined WSN/IOT? *Proc. of the 2016 IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom), IEEE Smart Data (SmartData)*, 2016, pp. 234–239. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.63
3. Ezdiani S., Acharyya I.S., Sivakumar S., Al-Anbuky A. An IoT environment for WSN adaptive QoS. *Proc. of the 2015 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS)*, 2015, pp. 586–593. https://doi.org/10.1109/DSDIS.2015.28
4. Xue K., Ma C., Hong P., Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, 2013, vol. 36, no. 1, pp. 316–323. https://doi.org/10.1016/j.jnca.2012.05.010

Литература

1. Sharma R., Prakash S., Roy P. Methodology, applications, and challenges of WSN-IoT // Proc. of the International Conference on Electrical and Electronics Engineering (ICE3). 2020. P. 502–507. https://doi.org/10.1109/ICE348803.2020.9122891
2. Nguyen T.M.C., Hoang D.B., Chaczko Z. Can SDN technology be transported to software-defined WSN/IOT? // Proc. of the 2016 IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom), IEEE Smart Data (SmartData). 2016. P. 234–239. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.63
3. Ezdiani S., Acharyya I.S., Sivakumar S., Al-Anbuky A. An IoT environment for WSN adaptive QoS // Proc. of the 2015 IEEE International Conference on Data Science and Data Intensive Systems (DSDIS). 2015. P. 586–593. https://doi.org/10.1109/DSDIS.2015.28
4. Xue K., Ma C., Hong P., Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks // Journal of Network and Computer Applications. 2013. V. 36. N 1. P. 316–323. https://doi.org/10.1016/j.jnca.2012.05.010

5. Turkanović M., Brumen B., Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, 2014, vol. 20, pp. 96–112. https://doi.org/10.1016/j.adhoc.2014.03.009
6. Amin R., Biswas G.P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, 2016, vol. 36, pp. 58–80. https://doi.org/10.1016/j.adhoc.2015.05.020
7. Wang D., Li W., Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 2018, vol. 14, no. 9, pp. 4081–4092. https://doi.org/10.1109/TII.2018.2834351
8. Jiang Q., Ma J., Wei F., Tian Y., Shen J., Yang Y. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications*, 2016, vol. 76, pp. 37–48. https://doi.org/10.1016/j.jnca.2016.10.001
9. Liu X., Shen Y., Li S., Chen F. A fingerprint-based user authentication protocol with one-time password for wireless sensor networks. *Proc. of 2013 International Conference on Sensor Network Security Technology and Privacy Communication System*, 2013, pp. 9–12. https://doi.org/10.1109/SNS-PCS.2013.6553825
10. Gurabi M.A., Alfandi O., Bochem A., Hogrefe D. Hardware based two-factor user authentication for the Internet of Things. *Proc. of the 14th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2018, pp. 1081–1086. https://doi.org/10.1109/IWCMC.2018.8450397
11. Wang D., Wang P., Wang C. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. *ACM Transactions on Cyber-Physical System*s, 2020, vol. 4, no. 3, pp. 3325130. https://doi.org/10.1145/3325130
12. Selva Reegan S.R.A., Baburaj E. Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks. *Computers and Electrical Engineering*, 2017, vol. 59, pp. 274–290. https://doi.org/10.1016/j.compeleceng.2016.10.018
13. Fan X., Gong G. LPKM: A lightweight polynomial-based key management protocol for distributed wireless sensor networks. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2013, vol. 111, pp. 180–195. https://doi.org/10.1007/978-3-642-36958-2_13
14. Li X., Niu J., Kumari S., Wu F., Sangaiah A.K., Choo K.K.R. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications*, 2018, vol. 103, pp. 194–204. https://doi.org/10.1016/j.jnca.2017.07.001
15. Nashwan S. AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment. *Egyptian Informatics Journal*, 2021, vol. 22, no. 1, pp. 15–26. https://doi.org/10.1016/j.eij.2020.02.005
16. Cheng Q., Hsu C., Xia Z., Harn L. Fast multivariate-polynomial-based membership authentication and key establishment for secure group communications in WSN. *IEEE Access*, 2020, vol. 8, pp. 71833–71839. https://doi.org/10.1109/ACCESS.2020.2987978
17. Yang S.-K., Shiue Y.-M., Su Z.-Y., Liu I.-H., Liu C.-G. An authentication information exchange scheme in WSN for IoT applications. *IEEE Access*, 2020, vol. 8, pp. 9728–9738. https://doi.org/10.1109/ACCESS.2020.2964815

Authors

Loganathan Sasirega — PhD, Research Scholar, Vels Institute of Science Technology and Advanced Studies, Chennai, 600043, India, https://orcid.org/0000-0003-3771-8959, lsasirega1975@gmail.com

Chandrabose Shanthi — PhD, Assistant Professor, Vels Institute of Science Technology and Advanced Studies, Chennai, 600043, India, SC 57191840797, https://orcid.org/0000-0002-7976-2360, shanc08071978@gmail.com

Received 25.08.2021
Approved after reviewing 14.10.2021
Accepted 30.11.2021

5. Turkanović M., Brumen B., Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion // Ad Hoc Networks. 2014. V. 20. P. 96–112. https://doi.org/10.1016/j.adhoc.2014.03.009
6. Amin R., Biswas G.P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks // Ad Hoc Networks. 2016. V. 36. P. 58–80. https://doi.org/10.1016/j.adhoc.2015.05.020
7. Wang D., Li W., Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks // IEEE Transactions on Industrial Informatics. 2018. V. 14. N 9. P. 4081–4092. https://doi.org/10.1109/TII.2018.2834351
8. Jiang Q., Ma J., Wei F., Tian Y., Shen J., Yang Y. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks // Journal of Network and Computer Applications. 2016. V. 76. P. 37–48. https://doi.org/10.1016/j.jnca.2016.10.001
9. Liu X., Shen Y., Li S., Chen F. A fingerprint-based user authentication protocol with one-time password for wireless sensor networks // Proc. of 2013 International Conference on Sensor Network Security Technology and Privacy Communication System. 2013. P. 9–12. https://doi.org/10.1109/SNS-PCS.2013.6553825
10. Gurabi M.A., Alfandi O., Bochem A., Hogrefe D. Hardware based two-factor user authentication for the Internet of Things // Proc. of the 14th International Wireless Communications and Mobile Computing Conference (IWCMC). 2018. P. 1081–1086. https://doi.org/10.1109/IWCMC.2018.8450397
11. Wang D., Wang P., Wang C. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs // ACM Transactions on Cyber-Physical Systems. 2020. V. 4. N 3. P. 3325130. https://doi.org/10.1145/3325130
12. Selva Reegan S.R.A., Baburaj E. Polynomial and multivariate mapping-based triple-key approach for secure key distribution in wireless sensor networks // Computers and Electrical Engineering. 2017. V. 59. P. 274–290. https://doi.org/10.1016/j.compeleceng.2016.10.018
13. Fan X., Gong G. LPKM: A lightweight polynomial-based key management protocol for distributed wireless sensor networks // Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST. 2013. V. 111. P. 180–195. https://doi.org/10.1007/978-3-642-36958-2_13
14. Li X., Niu J., Kumari S., Wu F., Sangaiah A.K., Choo K.K.R. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments // Journal of Network and Computer Applications. 2018. V. 103. P. 194–204. https://doi.org/10.1016/j.jnca.2017.07.001
15. Nashwan S. AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment // Egyptian Informatics Journal. 2021. V. 22. N 1. P. 15–26. https://doi.org/10.1016/j.eij.2020.02.005
16. Cheng Q., Hsu C., Xia Z., Harn L. Fast multivariate-polynomial-based membership authentication and key establishment for secure group communications in WSN // IEEE Access. 2020. V. 8. P. 71833–71839. https://doi.org/10.1109/ACCESS.2020.2987978
17. Yang S.-K., Shiue Y.-M., Su Z.-Y., Liu I.-H., Liu C.-G. An authentication information exchange scheme in WSN for IoT applications // IEEE Access. 2020. V. 8. P. 9728–9738. https://doi.org/10.1109/ACCESS.2020.2964815

Авторы

Логанатан Сасиега — PhD, исследователь, Институт науки, технологий и перспективных исследований Велса, Ченнаи, 600043, Индия, https://orcid.org/0000-0003-3771-8959, lsasirega1975@gmail.com

Чандрабос Шанти — PhD, доцент, Институт науки, технологий и перспективных исследований Велса, Ченнаи, 600043, Индия, SC 57191840797, https://orcid.org/0000-0002-7976-2360, shanc08071978@gmail.com

Статья поступила в редакцию 25.08.2021
Одобрена после рецензирования 14.10.2021
Принята к печати 30.11.2021