International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

A Secured Dynamic Lightweight Authenticity Mechanism For Iot Assisted WSN

Vino.T[1], Srinivasan S[2], Suma Sira Jacob[3], Dr.G.Manikandan[4], Dilavar Basha K[5]

[1]*Assistant Professor, Dept of ECE, Sathyabama Institute of Science and Technology, Chennai, Tamilnadu, India*
[2]*Assistant Professor, Dept of ECE, Hindustan Institute of Technology and Science, Chennai, Tamilnadu, India.*
[3]*Assistant Professor, Dept of CSE, Christian Engineering College & Technology, Dindigul, Tamilnadu, India.*
[4]*Assistant Professor, Dept of ECE, Dr.M.G.R Educational and Research Institute, Maduravoyal, Chennai, Tamilnadu, India.*
[5]*Assistant Professor, Dept of EEE, RMK College of Engineering and Technology, Chennai, Tamilnadu, India.*

Email id: [1]vinodhevan@gmail.com , [2]ssrinivasan@hindustanuniv.ac.in, [3]sumasarajacob@gmail.com , [4]mrg.manikandan@gmail.com, [5]dilavarbashaeee@rmkcet.ac.in

Abstract: ***There is an exponential growth in the field of Internet of Things (IoT) assisted WSN with respect to the user credentials. Providing security is the first step process for efficient client-service association. Dynamic lightweight authenticity mechanism is proposed that utilizes the polynomial bivariate based key authentication for providing security. In this proposed scheme each node is assigned with polynomial bivariate keys. The link is generated after the verification of shared keys. By evaluating the polynomial shared keys the relay nodes are selected for the transmission. If both the sending and receiving nodes have the matching shared keys then the source node broadcast its random key. Authentication is carried out between the nodes through this polynomial key sharing system and hence the communication key is used for authentication.***

Keywords: Bivariate Polynomial Key; Key Sharing; Key Pre-distribution; Wireless Sensor Networks; Internet of Things.

1. INTRODUCTION

Internet of Things (IoT) is widely applicable for different scenarios in day to day life and it is included in the smart applications like smart cities, smart homes, smart industries, smart hospitality system, smart agriculture, etc [1]-[2]. Wireless Sensor Networks (WSN) is the main contribution for IoT in order to activate the smart devices, caching and data transmission resources with restricted resources [3]. Heterogeneous IoT (HetIoT) [4] seems to be the future development for the computation of mobile services and to resolve the issues caused due to the usage large number of sensors in the field monitoring purpose. The group of sensors can be managed through the machine learning operations which was developed using Stacked Extreme Learning Machine (SELM) operations [5].

A secured and key managing operation for IoT [6] seems to be a mandatory and a difficult process in order to protect the system from security attacks. Therefore data transmission is done confidentially by integrating the data with implicit certificates in order to maintain the authenticity. The main requirements of secured network are user verification and managing keys among them in order to protect the data from eavesdropping. Confidential data is collected from the patients through their wearable and medical sensors since it is directly linked with human life.

Anonymity is said to be user identity protection that un-reveal the location based services from any of the third parties [7]. Authentication is a mechanism in which the credentials provides by the communicating entity and it is compared with the existing database in order to verify that only the authenticated entity is participating in the communication process.

2. RELATED WORKS

Topological Key Hierarchy (TKH) scheme was proposed with the topology based key-tree in order to manage the process of rekeying however the cost of communication and computations gets increased with the group size [8]. A lightweight scheme and least mean scheme was proposed for Group Key Management (GKM) and intelligent data analysis in dynamic IoT scenarios [9-10]. Here one node can participate in multiple groups and be a member of multiple groups simultaneously. Therefore creation of multiple keys can protect the sensitive information from the malignant users. Forward and backward secrecy also ensured by using this scheme as well as preventing collision attacks.

Efficient Multi-Group Keying (EMGK) for IoT was projected for ensuring the backward and forward secrecy. Variety of co-existences of similar services in same region is ensured along with certain security metrics [11]. Two fundamental boundaries [12] were found in this WSN based health monitoring scheme such as (i) μ TESLA calls for synchronization of nodes (difficult in achieving gain) and (ii) lack of details for the performance of authentication process also results in high communication overheads. GKM protocol includes the logical Key Encryption Key (KEK) tree here each and every root node should be capable of computing tree secret keys from the leaf node.

For each and every parental node the weight is computed through its connected nodes, weight of the link (count of chain connected nodes) and node value. The node weight is measured uniquely since it is the key affiliation to identify the predescence member node towards the cluster head or group head. To reduce the excessive rekeying problem Logical Tree based Secure Mobility Management (LTSMM) scheme was proposed [14]. The smart devices setup is done through the group registration since the group head is registered with the BS. Group deployment, moving node joining and migration was also used with chaotic map based one-way hash functions for ensuring the message integrity.

3. PROPOSED WORK

Polynomial Bivariate Key Generation scheme is utilized for the proposed protocol named Dynamic Lightweight Authenticity Mechanism (DLAM) to provide authentication and security for the IoT assisted wireless sensor network. In this DLAM scheme each node is assigned with polynomial bivariate keys. Therefore the link is generated dynamically by analyzing the key values. The polynomial keys are shared among the relay and destination

nodes. If both the sending and receiving nodes have the same polynomial then the source node broadcast its random key.

The polynomial keys are generated for each node to share the secret message from one end to other end. Each node holds a variable to generate a polynomial key and two positive integers $\{a,b\} \in K_n$ is used to generate a key variable K_n. The random polynomial key is generated for the sender node with the positive integers. $f_1(x)_{>0} \in K(N_1) \rightarrow K_1$ is the generated polynomial key for the sender node then this key is shared with the relay node. The polynomial key K_1 generated by the sender node is given in equation 1.

$$K_{12} = f_1(a) * aK_2(f_1(b)) \quad (1)$$

The key K_1 is shared with their neighbour relay node and the relay node is generated with polynomial bivariate key using the two positive integers. On the basis of received key K_1 the relay node is generated with the polynomial keys of function $f_2(x)_{>0} \in K(N_2) \rightarrow K_2$. The generated polynomial key by the relay node is given in equation 2.

$$K_{23} = f_2(a) * aK_3(f_2(b)) \quad (2)$$

Now by receiving the keys K_1 and K_{21} from the sender and relay nodes the receiver node generates the polynomial bivariate key. The functional polynomial key $f_3(x)_{>0} \in K(N_3) \rightarrow K_3$ for the receiver node is generated by assisting two positive integers and the created bivariate polynomial functional key is given in equation 3.

$$K_{31} = f_3(a) * aK_{12}(f_3(b)) * aK_{23}(f_3(b)) \quad (3)$$

The correctness of the PBKPS is proved by validating the shared polynomial keys from one node to the other. Let K_1 be the key generated by the source node, K_2 be the relay node which is used to carry forward the data sent by the source node to the receiver and K_3 is the node which receives the data from the source node and it should be an authenticated and trustable data. Therefore the functional bivariate polynomial keys that are shared between the nodes are verified to be the same. If the node sends and receives the same polynomial key shares then the nodes are to be validated as secured nodes. The generated node keys $K_1(N_1)$, $K_2(N_2)$ and $K_3(N_3)$ from the assigned variables (a, b) are checked for their correctness and the validating equations are given in 4, 5 and 6 respectively.

$$\begin{aligned} K_1(N_1) &= f_1(a) * aK_2(f_1(b))^n \\ &= f_1(a) * aK_{23}(f_1(b))^2 \\ &= f_1(a) * aK_2(f_1(b)) * aK_3(f_1(b)) \\ &= f_1(a) * aK_2(f_1(b)) * aK_3(f_1(b)) \\ &= f_1(a) * f_2(a) * f_3(a) * aK_2(f_1(b)) * aK_3(f_1(b)) * aK_1(f_1(b)) \end{aligned} \quad (4)$$

$$
\begin{aligned}
K_2(N_2) &= f_1(a) * aK_{31}(f_1(b))^n \\
&= f_1(a) * aK_{23}(f_1(b))^2 * aK_{31}(f_1(b))^2 \\
&= f_1(a) * aK_2(f_1(b)) * aK_3(f_1(b)) * aK_3(f_1(b))^2 * aK_1(f_1(b))^2 \\
&= f_1(a) * f_2(a) * aK_2(f_1(b)) * aK_3(f_1(b)) * aK_1(f_1(b)) \\
&= f_1(a) * f_2(a) * f_3(a) * aK_2(f_1(b)) * aK_3(f_1(b)) * aK_1(f_1(b))
\end{aligned} \tag{5}
$$

$$
\begin{aligned}
K_3(N_3) &= f_1(a) * aK_{31}(f_1(b))^n \\
&= f_1(a) * aK_{12}(f_1(b))^2 * aK_{23}(f_1(b))^2 \\
&= f_1(a) * aK_1(f_1(b)) * aK_2(f_1(b)) * aK_2(f_1(b))^2 * aK_3(f_1(b))^2 \\
&= f_1(a) * f_3(a) * aK_1(f_1(b)) * aK_3(f_1(b)) * aK_2(f_1(b)) * f_2(a) \\
&= f_1(a) * f_2(a) * f_3(a) * aK_2(f_1(b)) * aK_3(f_1(b)) * aK_1(f_1(b))
\end{aligned} \tag{6}
$$

Therefore the proposed protocol key sharing process is evaluated mathematically and the shared polynomial key for the communicating nodes is derived and it is given in equation 7.

$$
\begin{aligned}
&K(N_1) = f_1(a) * aK_{12}(f_1(b))^n \\
&K(N_2) = (f_2(b)) * aK_{23}(f_2(b))^n \\
&K(N_3) = (f_3(b)) * aK_{31}(f_3(b))^n \\
&Hence \\
&Shared\_Key \Rightarrow K(N_1) \Leftrightarrow K(N_2) \Leftrightarrow K(N_3)
\end{aligned} \tag{7}
$$

4. RESULTS AND DISCUSSION

The simulation analysis is carried out for both the proposed DLAM scheme and the conventional LTSMM method and the comparative analysis is done. The simulator tool called Network Simulator of version 2.35 is used to simulate the proposed test system. The node density is considered for the simulation is 125 and the simulation area is 1100X900 m^2. Constant Bit Rate (CBR) is the traffic model considered here for the generation of data packets. The metrics used for the analysis of both DLAM and LTSMM are packet delivered rate, false node detection rate and key matching ratio.

a. Packet Delivered Rate (PDR)

The data packets that received successfully at the destination node or sink node is said to be the rate of packets delivered. The efficiency of the network can be evaluated by their effective delivery of data packets. Packet delivered rate is determined through the equation 8 shown below, where ‘n’ denotes the node density that includes during routing process.

$$PDR = \sum_{0}^{n} \{Pkts\ Sent / PktsRcvd\} \quad (8)$$

Figure 1 shows the graphical representation of PDR values that is obtained for both the proposed DLAM and conventional method LTSMM. The proposed scheme DLAM achieves better delivery rate compared to the conventional scheme.

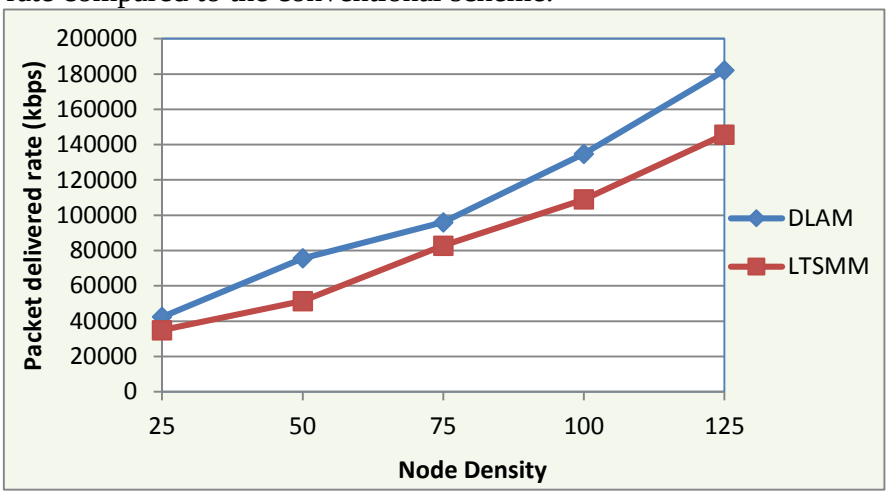

Figure 1: Packet Delivered Rate

b. False Node Detection Ratio (FNDR)

The ratio of detecting the false nodes from the routing process is said to be false node detection ratio.

This detection of false nodes from the routes and elimination of false nodes from the routing process leads a successful routing that improves the system performance and makes the routes as a trustable path. The figure 2 gives the graphical representation of FNDR for both DLAM and conventional method LTSMM. Proposed scheme achieves better FNDR rate compared to the existing LTSMM model.

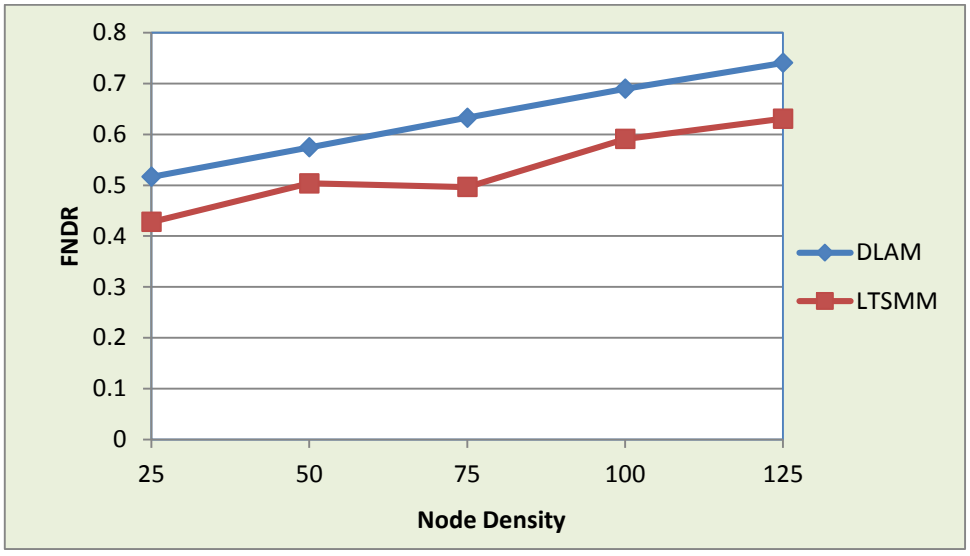

Figure 2: FNDR

c. Key Matching Ratio

The node key matching rates are determined to identify the reputed nodes in order to process the data transmission via trustable nodes. The secret keys are generated with respect to their source node variable and assigned positive integers. If the nodes are authenticated with the same keys then the keys are matched and the data transmission process is carried out.

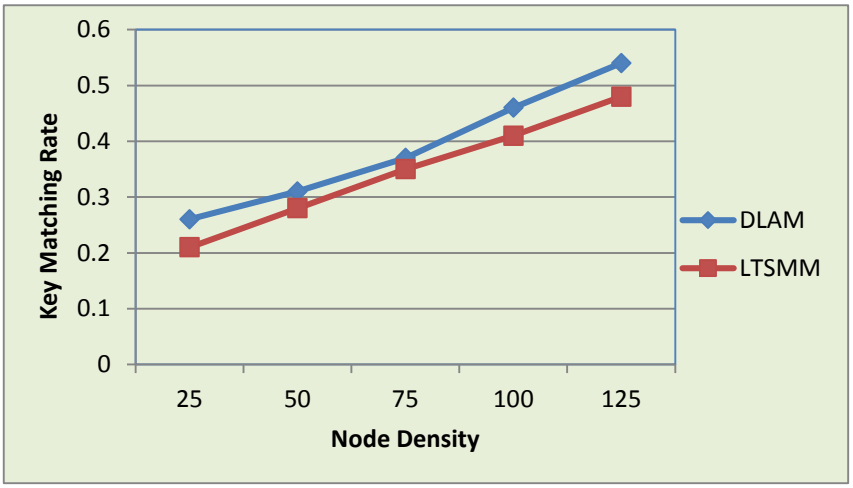

Figure 3: key Matching Rate

The proposed scheme obtains the average key matching ratio of 0.388 while the LTSMM model obtains 0.346 respectively. Hence the proposed DLAM scheme achieves high key matching rates compared conventional model and it is shown in figure 3.

5. CONCLUSION

Dynamic lightweight authenticity mechanism is proposed that utilizes the polynomial bivariate based key authentication for providing security. In this DLAM scheme each node is assigned with polynomial bivariate keys. Link will be generated dynamically by analyzing the key values. The polynomial keys generated through the variables or positive integers generates the keys and this key share is done among the routing nodes. If both the sending and receiving nodes have the same polynomial then the source node broadcast its random key. Thereby the communication keys is computed and validated for the process of node authentication.

6. REFERENCES

[1] Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144, 17-39.
[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
[3] Lazarescu, M. T. (2013). Design of a WSN platform for long-term environmental monitoring for IoT applications. IEEE Journal on emerging and selected topics in circuits and systems, 3(1), 45-54.

[4] Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How can heterogeneous internet of things build our future: A survey. IEEE Communications Surveys & Tutorials, 20(3), 2011-2027.
[5] Luo, X., Xu, Y., Wang, W., Yuan, M., Ban, X., Zhu, Y., & Zhao, W. (2018). Towards enhancing stacked extreme learning machine with sparse autoencoder by correntropy. Journal of The Franklin Institute, 355(4), 1945-1966.
[6] Sciancalepore, S., Capossele, A., Piro, G., Boggia, G., & Bianchi, G. (2015). Key management protocol with implicit certificates for IoT systems. In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems (pp. 37-42).
[7] Nam, J., Choo, K. K. R., Han, S., Kim, M., Paik, J., & Won, D. (2015). Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation. Plos one, 10(4), e0116709.
[8] Son, J. H., Lee, J. S., & Seo, S. W. (2010). Topological key hierarchy for energy-efficient group key management in wireless sensor networks. Wireless personal communications, 52(2), 359-382.
[9] Kung, Y. H., & Hsiao, H. C. (2018). GroupIt: Lightweight group key management for dynamic IoT environments. IEEE Internet of Things Journal, 5(6), 5155-5165.
[10] Luo, X., Deng, J., Liu, J., Wang, W., Ban, X., & Wang, J. H. (2017). A quantized kernel least mean square scheme with entropy-guided learning for intelligent data analysis. China Communications, 14(7), 1-10.
[11] Kandi, M. A., Lakhlef, H., Bouabdallah, A., & Challal, Y. (2018). An efficient multi-group key management protocol for Internet of Things. In 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-6). IEEE.
[12] Zhou, G. D., & Yi, T. H. (2013). Recent developments on wireless sensor networks technology for bridge health monitoring. Mathematical Problems in Engineering, 2013.
[13] Kung, Y. H., & Hsiao, H. C. (2018). GroupIt: Lightweight group key management for dynamic IoT environments. IEEE Internet of Things Journal, 5(6), 5155-5165.
[14] Mughal, M. A., Shi, P., Ullah, A., Mahmood, K., Abid, M., & Luo, X. (2019). Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN. IEEE Access, 7, 76699-76711.