Received: August 3, 2020. Revised: October 14, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Trust-Based Framework and Deep Learning-Based Attack Detection for Smart Grid Home Area Network

Divya Mohandas Menon[1]* **N. Radhika[1]**

[1]*Amrita School of Engineering, Coimbatore, India*
* Corresponding author's Email: dmmatmec@gmail.com

Abstract: The Internet of things (IoT) can be used in our daily life. Home area network (HAN) is one of the applications of loT. The Smart Grid is an intelligent power network featured by its two-way flows of electricity and information. The integrated communication infrastructure allows Smart Grid systems to manage the operation of all connected components to provide reliable and sustainable electricity supplies. The Home Area Network is a dedicated network connecting devices in the home, as well as electrical vehicles. The HAN market is now emerging within the smart grid sector to serve home with different solutions. However, at the same time, due to the dependence on information technology and the deep integration of electrical components and computing information in cyber space, the system might become increasingly vulnerable to cyber-attacks. Cyber-attacks have led to numerous incidents and have been concerned by both power system operators and users. They can undermine or even completely disrupt the control system of the power grid. This paper presents an approach to modelling and validating the secure HAN network. Here a novel Trust-Based Iterative Energy-Efficient Routing Protocol (TBIEERP) is suggested with a data encryption scheme for secured data transmission in HAN. The Honeypot algorithm for encryption and decryption of data is employed. Finally, to detect the intrusion a deep auto encoder was used for attack detection and to protect HAN against cyber-attacks. The whole experimentation was carried out under Matlab environment. Thus, the techniques proposed produce the most promising outcome over attack detection. The proposed method obtained better detection accuracy compared to the existing methods.

Keywords: Smart grid (SG), Home area networks (HAN), Trust-based - iterative energy-efficient routing protocol (TBIEERP), Honeypot algorithm, Deep auto-encoders.

1. Introduction

The smart electrical networks with the combination of information and interaction technologies are termed Smart Grid (SG). The SG enables the observability and controllability of the electrical grid. Smart household appliances, electric vehicles, real-time data on power utilization for consumers, and intelligent electrical appliances are just a few examples of SG technology uses. A smart grid is a communicative and unified platform that comprises consumers, creation, transfer, propagation, functions, and service providers having various utilizations and assistances. The systems in SG are interconnected with one another in diverse communication area networks that facilitate several utilizations. The framework of communication in diverse area networks is classified into Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN). Home area network focuses on the consumer area, whereas NAN focuses on local area networks [1].

The physical and the cyber interaction networks are integrated into the traditional grids to execute the Smart Grid. The communication is improved and the features of the power network are controlled by the Smart Grid. The SG enables double-way flow of power and interaction and hence it is a significant contribution to the electrical systems. The main purpose of Smart Grid is to offer a communication channel for safe, stable, and effective data transmission. The prerequisites and characteristics of Smart Grid portrayal are provided below: [2]

- Maximized utilization of digital data and regulates technology to enhance safety, stability, and efficacy of the electric grid.
- Effective enhancement of grid functions and sources, with complete cyber-security.
- Combination of smart devices and consumer gadgets.
- Developing benchmarks for interaction and interoperability of devices and tools linked to the electric grid.
- Distribution and combination of propagated sources and creation, involving renewable sources.
- Identifying and minimizing unwanted impediments to the use of SG methodologies.

An SG is an electrical grid that consists of different dynamic energy resources including smart meters, smart devices, and sustainable energy resources. A smart grid collects real-time data. The fundamental characteristics by which the networks in smart grids are described include authenticity, amalgamation, scalability, and safety. These networks are responsible for data processing, data routing, observation of the nodes, etc. An SG is an accumulation of several networks that utilizes a range of interaction methodologies for secure interactions. It allows the transfer of data in two directions between the smart meters and AMI. There are three layers in which the SG communication takes place. The primary layer is the HAN. A Home Area Network comprises household appliances included in pricing. Usually, HAN encloses an area of 1-100 m.

The two major factors that promote the forthcoming economy and smart cities are electrical energy and telecommunications. In addition, the evolution of smart grids can create a remarkable probability to provide multiple assuring mobile applications that comprise of Advanced Metering Infrastructure (AMI), Demand Response, Vehicle-to-Grid, and Smart Homes. In the current world, the power networks are transformed to an inventive grid with the help of Smart Grid (SG), by completely altering how the production, transmission, or consumption of electricity takes place, and by assisting double-way electricity and data flow between the grids and the consumers. Particularly, SG requires the development of communication frameworks for the transmission of data between them and the consumers. To satisfy this, Advanced Metering Infrastructures were set up that establishes double-way interaction links between the end-users and the utility. It allows effective and automated load regulation. Anyhow, AMI maximizes the intrusion area for the grids making them highly prone to cyber-attacks from vicious users. Such attacks may result in the damage of electricity infrastructures, collapses, and also may cause economic loss for the utility or the consumer [3, 4].

The progression of smart grids has provoked several investigation efforts for securing the grid efficiently. To protect the smart grids in the field of Home Area Networks, the methods should possess minimum computational intricacies to be feasible. The main reason for this is that the computational sources present in the Advanced Metering Infrastructures (AMI) of smart grids are restricted. If the smart grids are prone to cyber-attacks, the consequences will be much destructive. Hence, the detection of attacks in the smart grids has attained more attention concerning the safety of the smart grids [5].

Hence, in this article, a novel trust-dependent iterative energy-efficient routing protocol (TBIEERP) is suggested for transmitting data in home area networks securely. The further portion of the article is structured as shown: Section II provides the literary works associated with our method and the problem statement. Section III explains the flow of the suggested method. Section IV examines the performance of the suggested method. And finally, section V concludes the overall idea of the paper.

2. Related work

[6] discusses a comprehensive explanation of the major functions, which smart meters should offer, together with the examination of conventional resolutions that utilizes smart meters for SGs. Furthermore, open issues in the field are found out and reviewed. This review offers a comprehensive perspective of the potentials previously provided by smart meters and the ones they shall have available to solve the threats smart grids provide. The main disadvantage of the methods is the usage of smart meters which were not clearly illustrated. It could drive up anxiety with elderly or low-income households if they're constantly reminded of what they're spending. This could lead to people depriving themselves of adequate heating or lights.

[7] proposed an improved framework operating efficiently for several users depending on their necessities. Depending on their needs, the users can select the kind of scheduling method. Such needs comprise of minimization of cost and maximization of user satisfaction for excellent power usage and attaining a stable system. They proposed various bio-inspired computing-dependent scheduling algorithms. Moreover, they offer a comparative analysis of such scheduling methods incorporated in the smart grid framework. The major goal of these algorithms is

scheduling load, minimizing electricity bills, and maximizing user satisfaction based on user demands. The process is simple but with less execution time suffer i.e. waiting time is often quite long.

[8] proposed a fuzzy logic trust design to identify the nodes that are not trusted in the networks of SGs. The proposed model is contrasted with the conventional models to reveal its benefits. The suggested design improved the efficacy of routing and the rate of identification for every type of malignant attack. When compared with the conventional lightweight and reliable trust design, the suggested design enhances the drop rate of the packets by up to 90% when the rate of malignant nodes is lower than 25%, as authenticated by simulation methods. The suggested technique shows efficient traffic less routing but the packet drop was higher. Hence the latency seems to be high.

[9] suggested a situation-aware method for effective device verification in Smart Grid-HAN. The suggested method uses the safety risk data evaluated by the intelligent home systems with a situation-aware characteristic. Depending on the evaluated safety risk degree, a relevant verification protocol with sufficient safety protection as well as computation and interaction intricacy is chosen. They also presented a protocol model of the suggested method taking into account two safety risk degrees. The safety of the model is authenticated by utilizing formal and informal authentication. The behavioural examination demonstrated that the suggested method is effective concerning computation and interaction costs. Here the device verification of the security algorithm which was not illustrated seems to be a greater disadvantage.

[10] proposed a technique that offers for grouping and analysis of the devices in a Home Area Network (HAN) to detect the malignant devices effectively. With this, the smart grid HAN may attain a greater degree of fine-grained responsibility. The results of the experiments reveal that the technique is efficient and has a good scheme. But the time taken by the suggested methodology was high over detecting the malignant devices.

[11] proposed a safe and lightweight verification method for resource-limited smart meters that offers trust, obscurity, and shared verification with minimal energy, communication, and computation overhead. The proposed method permits a secure establishment and verification of the trust between the two interacting users. The dominance of the modeled protocol over the conventional protocols is validated using an extensive behavioral analysis. The proposed method has maximum safety features with lesser computation and communication overheads. The attained outcomes further reflected that the suggested protocol is relevant for the execution of resource-limited smart meters since it results in minimum energy usage. The suggested methodology was hard to access but the performance was good.

[12] suggested a unique trust evaluation architecture, which uses a Water Cycle Algorithm for automated adjustment of the ruleset and membership operation for the decision parameter to direct the packets flexibly. The packet flexibility was high but the rule generation process was not clear. They considered distance, link reliability, and node trust for validation utilizing this algorithm. The simulation was carried out in NS-2 for evaluating the behavior of the suggested design.

[13] presented a unique and safe message verification method that offers mutual verification and key formation for smart grids. The method is further modeled to safeguard the integrities of the gateway at the time of transfer of messages. They also proved the safety of the technique, authenticated the safety features utilizing Proverif, and illustrated the advantages of the method employing the simulation techniques. It must protect the integrity of records and of information transactions. The main drawbacks are processing and interpreting the data

[14] proposed an effective data aggregation method dependent on elliptic curves for maintaining confidentiality in the smart grids. Here, the encrypted data is authenticated by smart meters and transferred to the aggregators. These data are verified by the aggregator and aggregated. Hence there is no need for decryption of the data obtained from the smart meters. The aggregated messages are then signed by the aggregator and transferred to the center of operation, where the data are authenticated. The proposed protocol provided effective computation cost and satisfied the safety needs of the smart grid data. But the packet drop was high.

[15] provided the history of the communication prototypes in smart grids and a detailed review of the significant threats associated with the frameworks, the fundamental methodologies, and the needs of the smart grid interaction framework. They also discussed the function of cloud computing and IoT in smart grids. At last, the normalization, possible utilization, and forthcoming investigation threats of the interaction frameworks of the smart grids are categorized and reviewed. Here the integration framework was not clear.

[16] provided a detailed survey of the artificial intelligence methods to assist several utilizations in the smart grid distribution system. Particularly, they discussed the manners by which these methods are employed to assist the management of the smart grids

Received: August 3, 2020. Revised: October 14, 2021.

and how they aid to maximize the entire public welfare of the grids. At last, they provided additional investigation threats for huge-scale integration of automatically distributed appliances to recognize a truly SG. The survey was deeply illustrated but the recent deep or machine learning methodology was not discussed clearly.

[17] investigated the entire perspective of utilizing the technology of the system of smart grids with unique interaction methods and appliances. Further, they suggested the utilization of a hybrid or private cloud for safety, categorizing, and storage of data, which is attained from the power grids.

[18] face up security and availability issues in smart homes and propose an edge-of-things solution that focuses on putting the management of the home at the edge. The management is controlled by the network operator in a similar way as occurs with current set-top-boxes for multimedia streaming at home. They propose an architecture for this system, implement the necessary modules and test it from the point of view of security and availability.

[19] proposed a new secure routing algorithm called energy aware trust based secure routing algorithm which is proposed in this paper. where the trust score evaluation is used to detect the malicious users effectively in WSN and spatio-temporal constraints are used with decision tree algorithm for selecting the best route.

[20] proposed a Robust Deep Autoencoder (RDA)". Further, they present generalizations of our results to grouped sparsity norms which allow one to distinguish random anomalies from other types of structured corruptions, such as a collection of features being corrupted across many instances or a collection of instances having more corruptions than their fellows. Such "Group Robust Deep Autoencoders (GRDA)" give rise to novel anomaly detection approaches whose superior performance we demonstrate on a selection of benchmark problems.

[21] propose a new routing protocol called Secured Quality of Service (QoS) aware Energy Efficient Routing Protocol in this paper which is designed based on trust and energy modelling for enhancing the security of WSN and also to optimize the energy utilization. In the proposed work, the trust modelling uses an authentication technique with a key based security mechanism for providing trust scores. Moreover, three types of trust scores namely direct, indirect and overall trust scores are calculated in this work for enhancing the security of communication. In addition, a cluster based secure routing algorithm is proposed in this work in which the cluster head has been selected based on QoS metrics and trust scores to perform cluster based secure routing. Finally, the final path has been selected based on path-trust, energy and hop count to efficiently carry out the secure routing process. The proposed work has been assessed by simulations carried out using NS2 simulator.

[22] in which a Deep belief Network has been deployed to identify the anomalies in the Smart Grid data traffic thereby detecting intrusion. Support Vector Machine has been used for intrusion classification after creating the Deep Belief Network Model. Using SVM model with deep belief networks has helped in reduction of data

[23] proposes a Real Time Data Collection Unit (RTDCU) to be used in the distribution side of a smart grid for real time data collection. The RTDCU unit uses Discrete Fourier Transform (DFT) based approach to compute the voltage and current phasors and frequency of the power system signals

Here in the literature survey several methods have been proposed each method focuses on cryptographic technique our method focuses on classifier for predicting attacks.

3. Problem statement

Home Area Network has proved to be a popular technique which is a combination of Wireless technology and sensor network on a smart home service. It can also be used for monitoring real-time data from a remote distance. The main issues are the scale of the network, security, result accuracy, node density, power supply, mobility, data rate, Energy consumption, QoS, and real-time communication. Security and privacy are the major interests while creating resolutions for smart grids. Therefore, it is very significant to detect every type of deficiency and to focus on issues, which can result in unauthenticated entry to the maintenance of the Smart Grid system. Much as a human expert, the precise motive for creating an expert system for predicting the attack can be a high research gap in this field. In an expert system, machine learning and deep learning play a major role in creating a system that can determine its own decision over attack prediction. Hence a novel trust-based iterative energy-efficient routing protocol (TBIEERP) is proposed for secured data transmission for home area networks (HAN) in smart grids. Also, deep learning-dependent attack detection is developed for detecting the attacks in the system.

4. Proposed work

This section explains the flow of the proposed method. Fig. 1 displays the entire workflow.

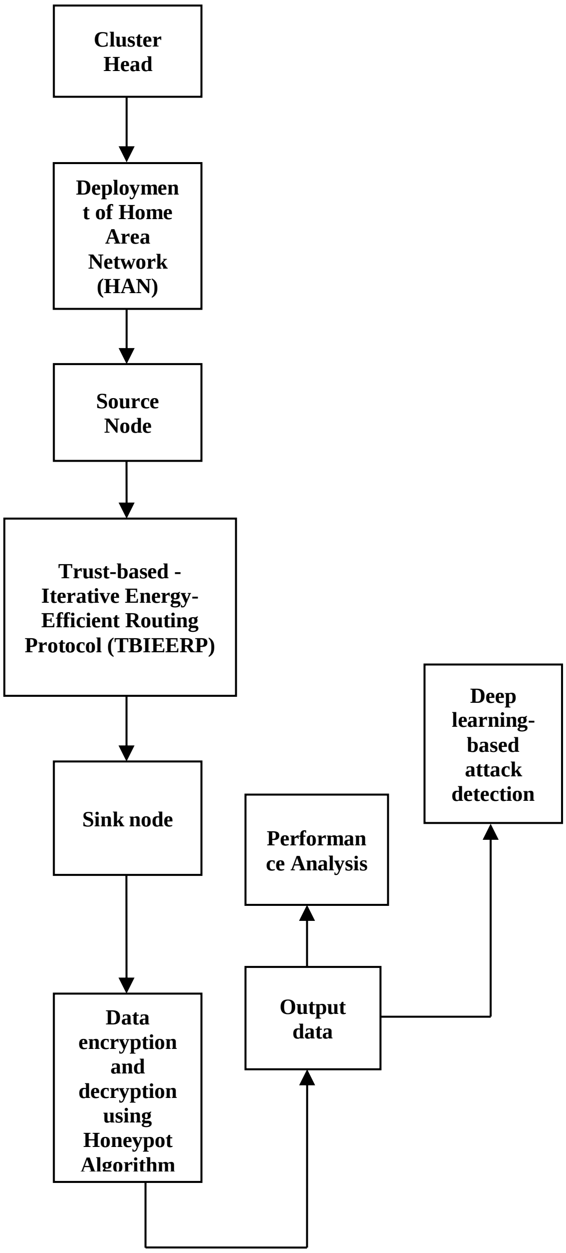
Cluster Head
Deployment of Home Area Network (HAN)
Source Node
Trust-based - Iterative Energy-Efficient Routing Protocol (TBIEERP)
Sink node
Data encryption and decryption using Honeypot Algorithm
Output data
Performance Analysis
Deep learning-based attack detection

Figure. 1 Schematic representation of the proposed methodology

4.1 Deployment of home area networks (HAN)

In this model, there are no controllers, in that the sensors and actuators have integrated the controller features and thus can communicate directly with each other. With sensors having some processing ability, they can analyze the data they receive before reporting the findings to the actuators.

This model is well suited to wireless communication systems, because the devices (sensors or actuators) can be far apart and still communicated with each other. In this case, all sensors/actuators of the network are able to forward messages that reach them, and thus ensure that communication is possible between all devices on the network, regardless of the distance that exists between them. The benefit of redundancy is also achieved, because if a device fails, another can take over its task. In this model, there would be a controller for the user to program and supervise the system. The cluster head can get selected.

4.2 Trust-based iterative energy-efficient routing protocol (TBIEERP)

Following the formation of the clusters, the suggested routing algorithm is presented. It consists of two stages such as trusted node selection and perfect route selection. In the initial stage, the suggested algorithm identifies the safest path depending on trust scores.

For evaluating the nodal trust, the wireless condition with fifteen nodes is developed and at first the trust value is assumed as zero. The TBIEERP is utilized for data transfer in our work. The trust score for a particular node is evaluated depending on the succeeding two factors. Initially, nodes that authentically send their acknowledgment to neighbor nodes whenever they obtained the packet are considered as the initial group. Trust value will be calculated based on different routing parameters (rreq, rply, err, etc) or routing metrics (bandwidth, cost, etc). The nodes that released several packets are then classified as group 2 nodes. Then first trust value is evaluated utilizing Eq. (1), which depicts the rate of authentic acknowledgment.

$$\mathrm{TR}_{(1,j)} = \frac{\left[\mathrm{G1}\times\left(\frac{\mathrm{ACK}}{\mathrm{NP}}\times 100\right)+\mathrm{G2}\times\mathrm{Temp}_{\mathrm{score}}\mathrm{G3}\times\mathrm{Spatial}_{\mathrm{score}}\right]}{[\mathrm{G1}+\mathrm{G2}+\mathrm{G3}]} \tag{1}$$

In which G1, G2, and G3 denote the weights provided to the various trust values, $\mathrm{TR}_{(1,j)}$ denotes the initial trust value in ratio for jth node, ACK represents the count of acknowledgment transferred to the neighbor nodes and NP denotes the packet count attained from neighbor nodes.

The next trust score is evaluated utilizing Eq. (2) that estimates the released packet.

$$\mathrm{TR}_{(2,j)} = 100 - \left(\left(\frac{\mathrm{DRP}}{\mathrm{TDRP}}\right)\times 100\right), \mathrm{t1} < \mathrm{t} < \mathrm{t2} \tag{2}$$

in which $\mathrm{TR}_{(2,j)}$ denotes the second trust value in ratio for jth node, DRP presents the packet count released and TDRP denotes the entire packet count released in the network and t represents the temporal restraint to verify the time bounds t_1 and t_2 for minimum and maximum restrictions of the time gap.

At last, the entire trust value of the specific node j is estimated by utilizing the Eq. (3).

$$\mathrm{TR_j} = \frac{(\mathrm{TR_{(1,j)}} + \mathrm{TR_{(2,j)}})}{2} + \text{Recommendation score} \quad (3)$$

in which $\mathrm{TR_j}$ denotes the entire nodal trust score, $\mathrm{TR_{(1,j)}}$ denotes the initial trust score and $\mathrm{TR_{(2,j)}}$ represents the second trust value for node j.

After selecting the trusted node, the trusted path can get selected. Therefore, the dynamic values are more suitable for prefixes than the static value. With our method, the routing events can be clustered by the signal strength of the nodes in HAN decreases with distance, d. The Eq. (4) is employed to estimate the energy utilized to transfer k bits depending on the distance between two nodes. Therefore, we think the dynamic **values** are more suitable **for** prefixes than the static value. With our method, the routing events can be clustered by using the equation,

$$\mathrm{En_{tx}(k, d)} = \mathrm{k} \times \mathrm{En_{elec}} + \mathrm{k} \times \varepsilon \times \mathrm{d^m} \quad (4)$$

in which $\mathrm{En_{tx}}$ indicates the energy utilized, $\mathrm{En_{elec}}$ denotes the broadcasting circuit loss. m acquires the value of 2 or 4 based on multipath fading. ε represents the energy needed by electricity amplification.

The average values of the complete trust value for every node available in the network condition are used to determine a threshold in this article. Initially, identify the average values utilizing the entire trust value by employing the Eq. (5).

$$\mathrm{TRM} = \sum_{\mathrm{j=1}}^{\mathrm{m}} \frac{\mathrm{TR_j}}{\mathrm{m}} \quad (5)$$

Here TRM indicates the average value of the trust, $\mathrm{TR_j}$ represents the trust score aggregation and m denotes the count of nodes. TRM stands for a threshold that can be used to distinguish a malicious node from the rest of the network.

4.3 Data encryption and decryption using honeypot algorithm

The data in the HAN may be vulnerable to attacks and hence it is needed to secure them. Hence the Honeypot algorithm is employed for the encryption and decryption of the data. The data that is to be secured is encrypted for safety purposes once the identification of intrusion is authenticated. For the process of encryption, Honeypot cryptographic algorithm is employed. The key authentication is processed when the user asks for the available data that is secured in the cloud to authenticate the encrypted code. This assists in the safety and confidentiality preservation of data or information and prevents the utilization of data by attackers. is a block cypher algorithm that transforms plain text in 64-bit blocks to cypher text using 48-bit keys. The number of rounds in honeypot is 16. Using a key-scheduling method, the 64-bit key is utilized to produce 16 keys, each of 48 bits, for each round. It's a symmetric key algorithm, which means it encrypts and decrypts data with the same key. The sequence may now be divided into equal bases. Then each split sequence may be decrypted in its own round. This can help to save both time and money. The honeypot algorithm's security is predicated on the (supposed) difficulty of calculating discrete logs in a high prime modulus. When the data owner requests the file, the cloud server is in charge of creating a key and verifying it with the user for authentication.

For the purpose of key generation parameter can gets chosen.

1. Choose an integer K
2. Compute Round=$(G^k mod\ P)$
3. Compute Length=$(K^{-1}(H(m) + X(r))$
4. It is used for creating the per message or key

Honeypot Algorithm for data encryption and decryption

```
Input: HAN data $H_{data}$ (key, test data)
Output: encrypted data $enc_{msg}$ ,$enc_{key}$
    • read the input $H_{data}$ from the cluster data
    • initialize the data key length $L_{len}$ and N=10
    • bin message =dec2bin(raw_message, $L_{len}$)
    • chipper_message$\phi_{ch}$ = randi(2,size($L_{len}$))<2
 for j=1 :size($L_{len}$,1)
 for k=1:size($L_{len}$,2)
 bin message $\alpha_{msg}$(j,k)=str2num($L_{len}$(I,k))
 end
 end
encode €= mod($\phi_{ch}$ + $\alpha_{msg}$ ,2)
 €=€(:)’
Ndilute μ=round((1+randj)*N)*length(€(:))
Dilute_message ∀=randj(2,1, μ)<2
Pre_Message=[€, ∀] //preview message
Shuffled message=sort(Pre_Message)
 encode €=[];
for j=1:length(Shuffled message(:))
encode_message ω=cat(1, encode €,num2str (Shuffled message(i)))
end
$enc_{key}$ =num2str(key)
$enc_{msg}$ =length(encode_message ω)
```

Received: August 3, 2020. Revised: October 14, 2021.

When the user asks for the data that is secured in the cloud, then one hash key is created and is to be authenticated by the user for verification purposes. If the hash is authenticated, then the data is decrypted and is accessible to the user.

4.4 Deep learning-based attack detection

HAN is practically insecure because it is situated in the public domain. The ease with which attackers can access HAN devices makes them easier targets. Meanwhile, due to the restricted resources and processing power of HAN equipment, implementing strong safety procedures is a difficult task. Sensor nodes in devices, for instance, may not be capable of supporting computationally intensive cryptographic algorithms [24]. Other privacy problem arises from using wireless technologies for HAN. Wireless networks, by virtue of their shared media, are intrinsically more prone to hostile activities like eavesdropping and disruption than wired networks. HAN devices are sensor nodes with restricted computing and processing resources, which distinguishes them from computer systems. HAN devices, unlike computer networks, offer a limited number of protocols and applications. HAN further differs from several previous sensor networks in that it deploys a high number of sensor nodes throughout a broad hostile area.The deep autoencoder is a kind of Deep Neural Network (DNN) that builds a symmetrical network with an input unit, an output unit, and numerous hidden units to simulate relations between all input variables. The process for building the deep autoencoder framework, comprising the encoding and decoding procedures, is shown in Fig. 2. The input y is initially modified in the encoding phase to provide a range of attributes for layer-wisemodifications that build the first portion of the symmetrical networks. Ultimately, through the encoding procedure, code z is generated. The code z is repeatedly translated back to the initial input space through RBM during the decoding stage, and a rebuild of y, ŷ, is obtained. The framework is handled as a feed-forward neural network with many hidden units trained using the back-propagation approach to minimize the difference between y and ŷ.

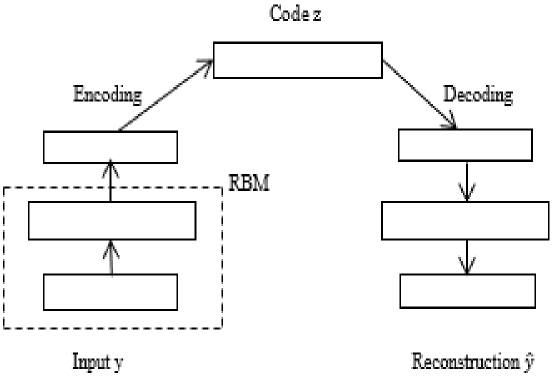

Figure. 2 Model of deep autoencoder

In the deep autoencoder framework, Connections between concealed and exposed elements are included is used to convert the actual input into binary representation, and is used to build hidden units. Because the input variables are periodic, the first hidden layer is trained. To set the weight and bias of each hidden units, this technique is performed several times.

A deep autoencoder is a multiple-layer feed-forward neural network whose required outcome is the source itself. On the sight, this strategy appears to be insignificant because the identity mapping would not have any reconstructive errors. In either case, autoencoders turn non-negligible when the identity map is forbidden, either through regularization or, significantly for the present expression, by using hidden units that are a minimum-dimension, non-linear depiction of the input information.

Autoencoders, in specific, use a combination of encoding and decoding steps to develop a map from the input to itself.

$$\overline{\mathrm{Y}} = \mathrm{D}\big(\mathrm{E}(\mathrm{Y})\big) \tag{6}$$

where Y represents the input data, The encoding map from the data input to the hidden units is E, the decoding map from the hidden units to the output units is D, and the restored form of the input data is $\overline{\mathrm{Y}}$. The goal is to teach E and D how to reduce the variation between Y and $\overline{\mathrm{Y}}$.

Specifically, an auto encoder shall be observed as a resolution to determine the attack issues:

Table 1. Simulation specifications setting [19]

Specifications	Values
Simulator	NS 2.35
Area (m^2)	(200 x 200)m
Count of nodes	100
Simulation Time	60 s
Routing Protocols	Existing and TBIEERP (Proposed)
Node energy	2 Joules
Starting energy	0.5 Joules
Size of the packet	1024 bits
En_{elec}	50 nJ/bit
Portability design	Random waypoint
Portability speed	(10-50) m/s

$$\min(D, E)\ \|Y - D(E(Y))\| \qquad (7)$$

Generally, an autoencoder with greater than a single hidden unit is termed a deep autoencoder and every extra hidden unit needs an extra pair of encoder E(•) and decoder D(•). By permitting several units of encoders and decoders, a deep autoencoder shall efficiently denote attack across the input Y.

5. Performance analysis

5.1 Simulation settings

An NS2 simulator is used in this study to examine and contrast the behavior of the suggested protocol with the conventional protocols. The specifications of the simulation are represented in Table 1.

5.2 Performance metrics

For comparison with existing protocols, various network behavior parameters are considered. These metrics are employed to examine and analyze the behavior of the proposed method.

5.2.1. Packet delivery ratio (PDR)

It is the percentage of data packets transferred to the receiver to those produced by the sender. The performance of the protocol is decreased when the packet loss is maximized. It is estimated as shown:

$$\text{PDR}\ (\%) = \frac{\sum \text{No of packet received}}{\sum \text{No of packet sent}} \times 100 \qquad (8)$$

Fig. 3 displays the comparison of PDR in percentage for the existing and the proposed technique. From the graph, it is clear that the suggested method has a finer PDR when compared with the existing methods.

5.2.2. Average throughput (TP)

It is the number of packets transmitted from source nodes to destination nodes, through the network at a particular time. Generally, it is estimated concerning packets per second or bits per second. To attain better performance, the throughput must be comparably high. The value of throughput is estimated by the Eq. (9).

$$\text{TP} = \frac{\text{Packets received}}{\text{Final packet} - \text{Initial packet}} \qquad (9)$$

Fig. 4 reveals the comparative analysis of throughput in k bit per second for the existing and the proposed method. From the graph, it is proved that our suggested method has a finer throughput when compared with the existing protocols.

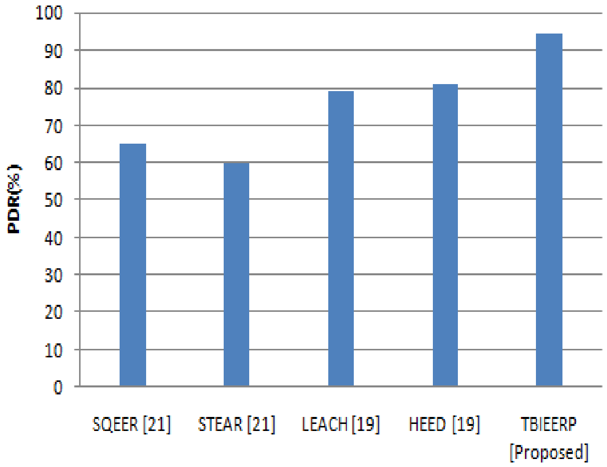

Figure. 3 Comparative analysis of PDR (%) for the existing and proposed method

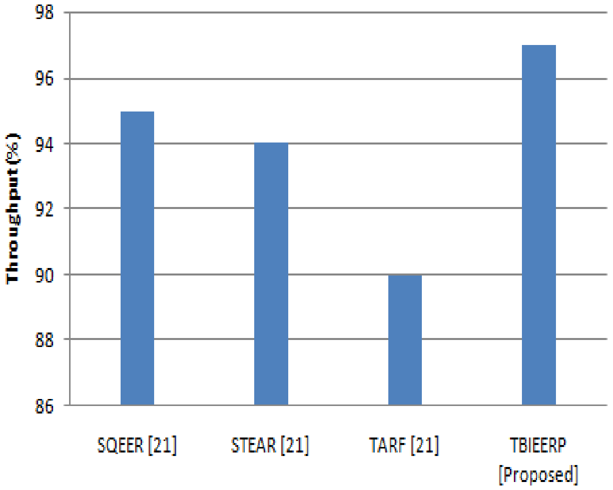

Figure. 4 Comparative analysis of throughput (%) for the existing and proposed method

5.2.3. End-to-end delay (e2e delay):

It is the meantime of the successfully transferred data packet over the network from the sender to the receiver. It consists of the sum of processing delay, queuing delay and distribution delay, etc. It is estimated in seconds. It is estimated as shown in Eq. (10):

$$\text{e2e delay} = \frac{\sum \text{arrive time} - \text{send time}}{\sum \text{number of connection}} \qquad (10)$$

Fig. 5 displays the comparative analysis of e2e delay in milliseconds for the existing and the suggested method. It is evident from the graph that the delay in data transmission is less in our proposed protocol when compared with the existing protocols.

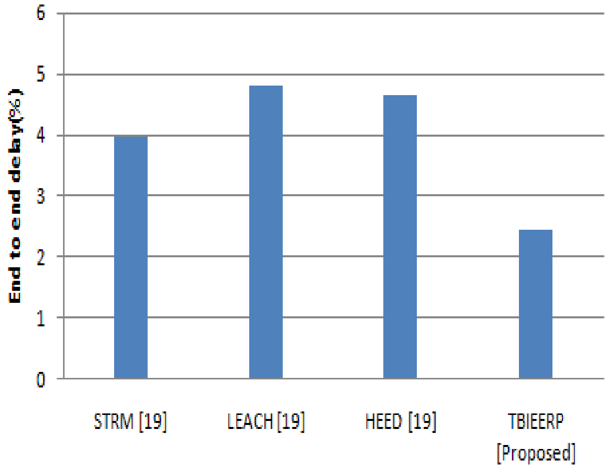

Figure. 5 Comparative analysis of end-to-end delay (ms) for the existing and proposed method

5.2.4. Energy utilization

The total energy utilization is the amount of energy or force devoured by every node in the HAN network to transferring and gathering of information packets throughout the recreation time. This parameter is significant as it decides the general lifetime of the network. The energy utilization of a node depends on data transmission, processing, and communication. The energy utilization for a node is determined by,

$$\mathrm{Eng_c} = \mathrm{Eng_i} - \mathrm{Eng_r} \qquad (11)$$

where $\mathrm{Eng_c}$ represents the energy consumed by the node, $\mathrm{Eng_i}$ denotes the starting nodal energy and $\mathrm{Eng_r}$ is the residual energy present in the node. Figure 6 shows that the proposed method effectively consumed a small quantity of energy due to the minimum amount of deterioration paths and an ideal choice of multiple paths when contrasted to the existing protocols.

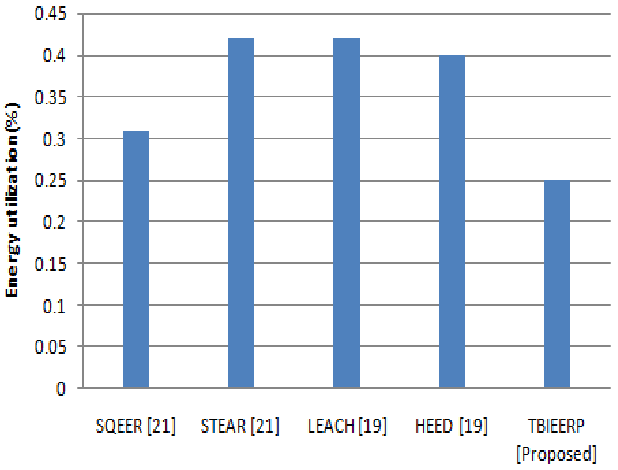

Figure. 6 Comparative analysis of energy utilization (J) for the existing and proposed method

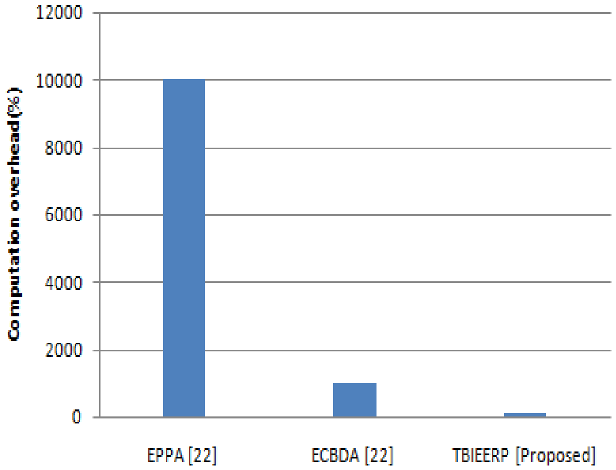

Figure. 7 Comparative analysis of computation overhead (ms) for the existing and proposed method

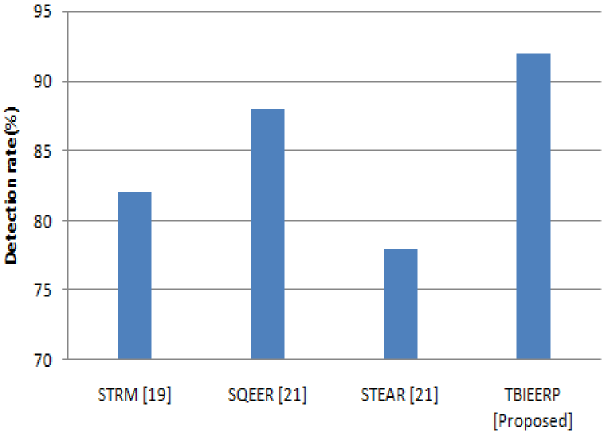

Figure. 8 Comparative analysis of detection rate (%) for the existing and proposed method

5.2.5. Computation overhead

It is the time needed for the HAN nodes to compute the necessary functions that are employed in the data transmission process. Fig. 7 displays the comparison of computation overhead in seconds for the existing and the proposed method. It is evident from the graph that our proposed method has minimum computation time for the data transmission when compared with the existing protocols.

5.2.6. Detection ratio

Fig. 8 displays the intrusion detection ratio for the existing and the proposed method. The suggested technique has a maximum detection rate than the conventional techniques.

6. Conclusion

A novel trust-based iterative energy-efficient routing protocol (TBIEERP) is proposed for transmitting data in home area networks securely.

The TBIEERP algorithm is employed over the HAN network and the QoS metrics were analyzed. Also, deep autoencoders are employed for the attack detection in the HAN networks, and a honeypot algorithm is used for enhancing the security of the data transmission in the HAN networks. In this approach, for efficient secure HAN communication technology is presented over common clustering protocol. Simulation outcomes illustrate that this process makes the greatest choice and identifies the best and the most appropriate route proficiently to send messages to the destination node, and in turn enhances the performance of routing, enhances number of delivered messages, and reduces the delay in delivery on comparing other existing techniques. Thus, the proposed technique is better in offering better security thereby tolerating delay in the network system. In the future attack mitigation scheme was implemented to prevent the network over different attacks.

List of notations

Y - input data,
E- hidden units
D-Output units
E(•)-Encoder
D(•)- Decoder
G- trust value
e2e-end to end delay
Y-Mapped input
E-Amplification
En-Energy

Conflicts of Interest

The authors declare no conflict of interest

Author Contributions

References

[1] M. Maduranga and Y. Weerasinghe, “Survey on Communication Technologies for Home Area Network (HAN) in Smart Grids”, *International Journal of Advanced Scientific Research and Management*, Vol. 2, Issue 9, 2017.

[2] E. Kabalci and Y. Kabalci, “Introduction to smart grid architecture”, *Smart Grids and Their Communication Systems*, pp. 3-45, 2019.

[3] F. B. Saghezchi, G. Mantas, J. Ribeiro, M. A. Rawi, S. Mumtaz, and J. Rodriguez, “Towards a secure network architecture for smart grids in 5G era”, In: *Proc. of 2017 13th International Wireless Communications and Mobile Computing Conference*, 2017, pp. 121-126.

[4] K. Deepa and M. S. Khurana, “Optimization of Routing in Smart Grids Using Intelligent Techniques”, In: *Proc. of 3rd International Conference on Internet of Things and Connected Technologies*, pp. 26-27, 2018.

[5] B. Chatfield and R. J. Haddad, “RSSI-based spoofing detection in smart grid IEEE 802.11 home area networks”, In: *Proc. of 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference*, pp. 1-5, 2017.

[6] D. B. Avancini, J. J. Rodrigues, S. G. Martins, R. A. Rabêlo, J. A. Muhtadi, and P. Solic, “Energy meters evolution in smart grids: A review”, *Journal of Cleaner Production*, Vol. 217, pp. 702-715, 2019.

[7] Z. Amjad, M. A. Shah, C. Maple, H. A. Khattak, Z. Ameer, and M. N. Asghar, “Towards energy efficient smart grids using bio-inspired scheduling techniques”, *IEEE Access*, Vol. 8, pp. 158947-158960, 2020.

[8] A. Alnasser and H. Sun, “A fuzzy logic trust model for secure routing in smart grid networks”, *IEEE Access*, Vol. 5, pp. 17896-17903, 2017.

[9] A. Xiang and J. Zheng, “A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks”, *Electronics*, Vol. 9, p. 989, 2020.

[10] E. McCary and Y. Xiao, “Malicious device inspection home area network in smart grids”, *International Journal of Sensor Networks*, Vol. 25, pp. 45-62, 2017.

[11] S. Garg, K. Kaur, G. Kaddoum, J. J. Rodrigues, and M. Guizani, “Secure and lightweight authentication scheme for smart metering infrastructure in smart grid”, *IEEE Transactions on Industrial Informatics*, Vol. 16, pp. 3548-3557, 2019.

[12] D. Velusamy and G. Pugalendhi, “Water cycle algorithm tuned fuzzy expert system for trusted routing in smart grid communication network”, *IEEE Transactions on Fuzzy Systems*, Vol. 28, pp. 1167-1177, 2020.

[13] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K. K. R. Choo, “A provably secure and anonymous message authentication scheme for smart grids”, *Journal of Parallel and Distributed Computing*, Vol. 132, pp. 242-249, 2019.

[14] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, “A secure ECC-based privacy preserving data aggregation scheme for smart grids”, *Computer Networks*, Vol. 129, pp. 28-36, 2017.

[15] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi, and P. Siano, “Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures”,

IEEE Systems Journal, Vol. 13, pp. 4001-4014, 2019.

[16] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: A review", *Electronics*, Vol. 9, p. 1030, 2020.

[17] M. Talaat, A. S. Alsayyari, A. Alblawi, and A. Hatata, "Hybrid-cloud-based data processing for power system monitoring in smart grids", *Sustainable Cities and Society*, Vol. 55, p. 102049, 2020.

[18] J. M. Batalla and F. Gonciarz, "Deployment of smart home management system at the edge: mechanisms and protocols", *Neural Computing and Applications*, Vol. 31, pp. 1301-1315, 2019.

[19] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks", *Wireless Personal Communications*, Vol. 105, pp. 1475-1490, 2019.

[20] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders", In: *Proc. of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 665-674, 2017.

[21] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", *Wireless Personal Communications*, Vol. 110, pp. 1637-1658, 2020.

[22] D. M. Menon and N. Radhika, "A secure deep belief network architecture for intrusion detection in smart grid home area network", *IIOAB Journal*, Vol. 7, pp. 479-483, 2016.

[23] S. Nithin, P. Sivraj, K. Sasi, and R. Lagerstöm, "Development of a Real Time Data Collection Unit for distribution network in a smart grid environment", In: *Proc. of 2014 Power and Energy Systems: Towards Sustainable Energy*, pp. 1-5, 2014.