Computers, Materials & Continua
DOI:10.32604/cmc.2021.014967
Article

Tech Science Press

An Intelligent Hybrid Mutual Authentication Scheme for Industrial Internet of Thing Networks

Muhammad Adil[1], Jehad Ali[2], Muhammad Sajjad Khan[3], Junsu Kim[3], Ryan Alturki[4], Mohammad Zakarya[4], Mukhtaj Khan[4], Rahim Khan[4] and Su Min Kim[3,*]

[1]Department of Computer Science, Virtual University of Pakistan, Lahore, 54000, Pakistan
[2]Department of Computer Engineering, Department of AI Convergence Network, Ajou University, Suwon, 16499, South Korea
[3]Department of Electronics Engineering, Korea Polytechnic University, Slheung, South Korea
[4]Department of Computer Science, Abdul Wali Khan University Mardan, 23200, Pakistan
[*]Corresponding Author: Su Min Kim. Email: suminkim@kpu.ac.kr
Received: 29 October 2020; Accepted: 30 November 2020

Abstract: Internet of Things (IoT) network used for industrial management is vulnerable to different security threats due to its unstructured deployment, and dynamic communication behavior. In literature various mechanisms addressed the security issue of Industrial IoT networks, but proper maintenance of the performance reliability is among the common challenges. In this paper, we proposed an intelligent mutual authentication scheme leveraging authentication aware node (AAN) and base station (BS) to identify routing attacks in Industrial IoT networks. The AAN and BS uses the communication parameter such as a route request (RREQ), node-ID, received signal strength (RSS), and round-trip time (RTT) information to identify malicious devices and routes in the deployed network. The feasibility of the proposed model is validated in the simulation environment, where OMNeT++ was used as a simulation tool. We compare the results of the proposed model with existing field-proven schemes in terms of routing attacks detection, communication cost, latency, computational cost, and throughput. The results show that our proposed scheme surpasses the previous schemes regarding these performance parameters with the attack detection rate of 97.7 %.

Keywords: Security; industrial Internet of Things; routing attacks; routing protocols; base station; authentication aware nodes

1 Introduction

The utilization of Internet of Things (IoT) in industry is a revolutionary technology for data acquisition and processing, which bring many benefits to the lives of human beings utilizing different applications. Sensor devices collect data from human inaccessible areas by interconnecting hundreds and thousands of wireless nodes to form a heterogeneous network over the Internet [1]. Internet of Things had a wide range of applications, which includes industrial automation,

forest monitoring, flood monitoring, military, agriculture, healthcare, smart homes, smart cities, automobile, and smart grids, etc. [2,3].

Wireless sensors have limited resources in terms of On-board battery power, memory, transmission, and computation, etc. Therefore, they need efficient utilization in the deployment phase to maximize network output by accurate results [4,5]. Generally, Industrial IoT collects data with the help of deployed sensor nodes, which consists of sensitive and confidential information to be exchanged in the network. In addition, this information is transmitted over a transmission medium to a central location, i.e., gateway, cluster head or Edge node, through either direct or multi-hop communication infrastructure in the network [6]. Industrial IoT are deployed in an open area, due to its distributed nature with information collection and monitoring capabilities. Therefore, they are susceptible to various internal and external security threats, due to their open communication behavior [7]. Authentication of sensor nodes in an operational network is a primitive process, which is used to authenticate the participating nodes i.e., both sender and receiver modules in the network [8].

In addition, routing protocols have an important role in Industrial IoT to disseminate information in an efficient way. Due to the limited resources of sensor devices, lightweight routing protocols have been given preference to achieve better results with minimal resources [9]. Routing protocol low power (RPL) was specially designed for low power hardware devices, lossless links, low bandwidth, and limited resources networks. The RPL protocol is worked on the basis of the shortest path selection in the network to transmit data from source to destination. RPL is also helpful to create a loop-free wireless network topology just like spanning tree protocol (*STP*) in wired networks [10]. The vulnerability threats to Industrial IoT in terms of routing attacks include the Sinkhole attack, Sybil attack, Black hole attacks, Selective forwarding attack, Wormhole attack, Denial of service attacks (DoS), Eavesdropping attack and Jamming attacks, etc. [11–13]. Selective forwarding is another type of routing attack, where the intruder traps the legitimate traffic of the network by forwarding fake route request messages [14].

The literature of Industrial IoT routing attacks is comprehensively over-viewed in this paper to evaluate the pros and cons to address the associated issues. Although, some of the existing literature plays remarkably well to combat the routing attacks in Industrial IoT, but at some stage, they are complex in their implementation or specific to the system or operation. Therefore, a lightweight authentication scheme is needed for Industrial IoT to counter routing attacks with efficient resource utilization.

In this paper, we propose an intelligent mutual authentication scheme for Industrial IoT networks to identify and prevent routing attacks. The proposed model is very effective against routing attacks i.e., sinkhole attack and wormhole attack. Besides, the proposed mutual authentication scheme uses two functions such as Authentication Aware Node (AAN) and BS, which back-up each other to identify malicious activities in the network. The AAN and BS use the communication parameters such as route request (RREQ), received signal strength (RSS), round trip time (RRT), and node-ID to verify the legitimacy of participating nodes and network traffic. To elaborate, we individually define both functions as below:

a. Authentication Aware Nodes (AAN)
b. Base Station/Gateway Authentication Phase

The AAN and BS support each other in the backup to ensure the security of deployed Industrial IoT networks. Besides that, different communication parameters are considered to verify the performance reliability of the metrics of the network. The AAN node deployed in the network

at different locations uses the information of incoming packets such as RREQ, RTT, RSS, and nodes-ID to verify the legitimacy of network traffic in their proximity. Let assume that the legitimate nodes (*Li*) node-ID, distance (RSS), and time (RTT) parameters are set in AAN to verify the legitimacy of incoming RREQ/RREP by matching its values with defined values. In the initial phase, AAN node broadcasts a RREQ packet in the network and all nodes in their vicinity respond with a route reply (RREP).

Once, the AAN node receives the RREP the of vicinity node, then, AAN nodes match the information responding node such as node-ID, distance (RSS), and time (RTT) with defined configuration. If it satisfies the defined parameters, then the AAN allows the responding node for communication in the network. Otherwise, an alarm message is generated by AAN to acknowledge the existence of malicious activity in the network. Moreover, those ordinary nodes, they are close to the BS and send their data directly to the BS. In this case, the BS in the back-up scenario checks the defined parameters such as considered for AAN to verify the legitimacy of requesting nodes. The backup scenario assessment process of the proposed model is very efficient, because if function 1 fails to detect malicious activity. Then, function 2 also carried out the security check against defined security parameters for incoming packet

The rest of the paper is organized as Section 2 of the paper contains the related work followed by Section 3, which contain the contribution of this research work. Section 4 of the paper comprehensively overviews the proposed methodology, followed by Section 5, which represents the formal security analysis of proposed model with rival schemes. The implementation and result statistics in terms of comparative analysis are further discussed in Section 6. Section 7 summarizes and concludes the paper with future work.

2 Related Works

Industrial Internet of Things (IoT) is an effective tool to gather information from inaccessible areas, where human access is not possible. Security of these networks is a challenging issue for the research community to devise new methodologies and techniques, which should be prone to security threats. The literature given below contains some latest techniques adopted to counter routing attacks in Industrial IoT.

Parmar et al. [15] proposed the *Ad hoc* on-demand Multipath Distance Vector (AOMDV) routing protocol with the incorporation of RTT time to combat routing attacks in IoT networks. Del et al. [16] proposed the Connected and Extended Mechanism-based technique to counter link attacks in IoT networks. The proposed model uses performance reliability parameters of communication in the designated network infrastructure to identify transmission attacks. The intrusion detection system (IDS) framework was proposed by Granjal et al. [17]. This model was specifically against one system, which minimizes its use in the real deployment.

Khan et al. [18] suggest the signature-based security technique to identify malicious nodes in the deployed network. In this technique, the authors used special nodes to detect assailant nodes in the deployed WSNs based on signature matching. However, the signature-based security identification mechanism in the Industrial IoT network increases the communication costs and network overhead in the heterogeneous environment. The Markle tree-based hash algorithm scheme was proposed by Idris et al. [19]. They used the hash function to verify the legitimacy of participating sensor nodes. The limitation of the proposed model was complex implementation, high cost, end to end delay (E-2-E) and network overhead. The multi-level authentication scheme was proposed by Vo et al. [20]. In this model, the authors used a three-phase hop authentication

technique, where the adjacent node uses the control information to authenticate legitimate packets and segregate abnormal packets from legitimate traffic in the network. The limitation of the proposed scheme was its complex implementation and extra energy consumption during the authentication process.

Yifeng et al. [21] proposed the received signal strength (RSS) based technique for the detection of wormhole attacks in WSNs. In the proposed model, the authors used RSS information for paired nodes to verify the legitimacy of participating nodes. However, the implementation and authentication mechanism of the proposed model was very simple, which allow the attacker to adjust intruder nodes in the network with the same RSS. Therefore, this model was not reliable as far as security concerns of WSNs. Rezaei et al. [22] proposed the different route discovery scheme to identify wormhole and sinkhole attacks in IoT. The author's used hop count information of adjacent nodes to verify the authenticity of participating nodes in the proposed model. To address, the authentication problem in IoT networks, a time interval-based technique was proposed by Kaur et al. [23]. In the proposed technique, the author's used E-2-E delay information between paired nodes to identify malicious routes in the network. However, the proposed model was effective for the closed and small WSNs, where the external interferences such as fidelity and attenuation do not affect the transmission medium. Mukherjee et al. [24] used the round-trip time (RTT) information in their model to verify the authenticity of the participating nodes and network traffic. Besides that, they used the RTT comparison for the paired nodes authentication.

Adil et al. [25] proposed the MAC-AODV mutual authentication scheme for constraint-oriented networks. The proposed model was very effective for small WSNs, due to its high throughput, low latency and least packet lost ratio. The limitation of the proposed model was deployment in a specific area such as a homogeneous environment. Obaidat et al. [26] proposed the Software-defined networking (SDN) infrastructure for wireless networks to avoid man-in-the-middle attacks. They used a central program hub named 'SDN Controller which controls the communication and authentication process in the network. Shigeyasu et al. [27] was proposed the novel distributed algorithm, which is derived from the Collusive Interest Flooding Attack (CIFA) to address the security problem in IoT networks. The Theil index-based security scheme was suggested for vampire attacks countermeasure by Cong et al. [28]. A comprehensive review of security issues associated with IoT networks was presented by Georgios et al. [29]. Ali et al. [30] proposed the decentralized approach for a peer-to-peer authentication scheme for WSNs. Adil et al. [31] proposed an anonymous channel categorization scheme for constraint-oriented networks to resolve the security issue.

3 Contribution of the Proposed Approach

The contribution of the proposed model is the development of a lightweight hybrid mutual authentication scheme to identify routing attacks in deployed Industrial IoT networks. Moreover, the proposed scheme uses the communication parameters to identify routing attacks in the deployed Industrial IoT networks, which not only minimizes network overhead, but also improve the overall lifetime of wireless nodes. Therefore, the proposed scheme is very effective for resources limited network, because it not only focuses on the security aspect of Industrial IoT networks, but it also considers the communication aspects of deployed Industrial IoT networks to achieve better results for end-to-end delay, throughput, packet lost ratio with minimum energy consumption and network overhead. Steps to be followed in the proposed model:

a. To interconnect all legitimate nodes in the network topological order

b. To develop a secure routing infrastructure, where legitimate nodes share information with
c. Development of two functions authentication scheme to verify the confidentiality and integrity of data
d. To identify routing attacks and malicious nodes in an operational network
e. Authentication of legitimate nodes in an operational network in terms of back-up scenario
f. The feasibility of the proposed model is checked in the simulation environment to verify the performance reliability in terms of comparative results with rival schemes.

4 Proposed Methodology: Mutual Authentication Scheme

In this paper a hybrid mutual authentication scheme for Industrial IoT networks is proposed combat routing attacks. The proposed model uses two functions, which back up each other during assessment of network traffic to identify malicious activities in the network. The function 1 of the proposed scheme is known as AAN, which initiates a RREQ message in the network, the ordinary nodes in the vicinity responds with a RREP message. The AAN node uses communication parameters such as node-ID, RSS and RTT to verify the legitimacy of incoming RREP packet. Likewise, if any node in the network is missed by an AAN node during the assessment process and this node make direct communication request with the BS. Then in the backup BS will assess its traffic as function 2 by comparing the aforementioned communication parameters to verify the legitimacy of incoming RREQ/RREP. If the incoming RREQ/RREP satisfies the defined communication parameters, then the BS allows it for communication in the network. If the defined communication parameters of requesting or responding node do not match in the BS, then the BS denied it's RREQ/RREP for further processing in the network. Once the incoming RREQ/RREO packet is denied by BS or AAN node, then an alarm message is generated to acknowledge the existence of malicious activity in the network. Moreover, in the proposed model, both the functions worked independently of each other, but they ensure the security of the network in composition. This is the advantage of our proposed model, where both the functions are working in backup order to minimize the chance of an attacker node to participate in the operational Industrial IoT network.

Herein, we explain the concept of our proposed model with an example to clarify the working steps. Let assume, an AAN (Ai) generates an RREQ packet in the network, a sensor node (Si) $\in (Sn-1)$ in the vicinity respond with an RREP message. The Ai node checks the incoming RREP of $Si \in (Sn-1)$ for its defined security parameters, if Si RREP verifies the defined security parameters, then Ai will allow it for communication in the network. In case, if Si RREP does not verify the defined security parameters of Ai, then Ai broadcast an alarm message in the network to acknowledge the existence of a malicious node in the network. Moreover, if Ai node fails to detect the fake RREP/RREQ in their proximity, and the same attacker node directly approaches to the BS for communication. In this case, the BS in the backup scenario checks the RREQ with the defined security parameters as mentioned for the Ai node to verify the legitimacy of the requesting node. After security assessment, the incoming packet is allowed or denied for communication in the network.

The basic diagram of our proposed scheme is shown in Fig. 1. The legitimate nodes in the network are shown with green color, AAN nodes with blue color and directly connected nodes with BS are shown with pink color. AAN verifies the legitimacy of participating nodes by generating an RREQ message in the network, which is shown with yellow color in the diagram. Similarly, the AAN nodes receive RREPs against generated RREQ in the close vicinity as shown with yellow arrows in Fig. 1. Moreover, the Pink nodes shown in the diagram are directly connected with BS, where the BS checks their legitimacy by comparing its RREQ or

RREP information with defined security parameters. The legitimacy verification process of BS and directly connected nodes are shown with the Blue line in the diagram. Similarly, the network topological connectivity of the proposed model is shown with dark green lines in Fig. 1, where the legitimate nodes send their collected data from source to destination node via hop count selection in the network. Fig. 1 of the paper verifies that AAN and BS work independently to identify malicious activity in the network. The back-up support of the two functions maintains a high standard of security in deployed WSNs.

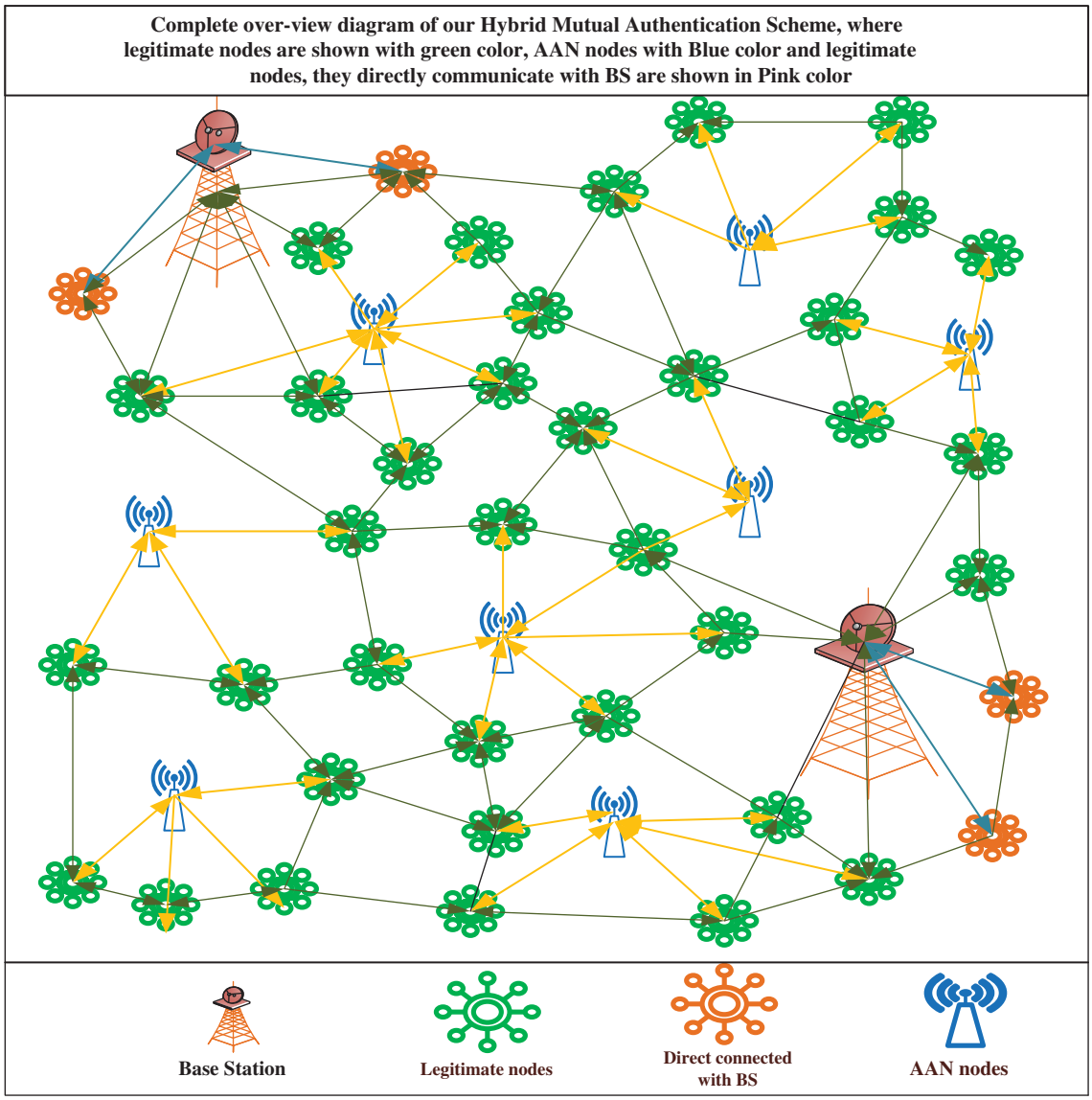

Figure 1: The detail overview of proposed scheme, where AAN and base station independently monitor network traffic

The stepwise authentication mechanism of the proposed model is elaborated as follows: The AAN nodes are used with ordinary nodes during the deployment of network architecture. The AAN are special nodes, which have high storage, computation, and transmission capabilities. Moreover, these nodes use their built-in configuration to verify the legitimacy of network traffic and participating nodes. The behaviors of these special nodes are different from other legitimate nodes in the network because the functionality and tasked assigned to these nodes are completely different. The AAN assesses the network traffic in their nearest proximity in terms of communication parameters, such as node-ID, RTT and RSS to identify malicious activity in the deployed WSN. The parameters used by AAN node in the following manner to verify the legitimacy of network traffic and participating nodes.

4.1 Authentication of Legitimate Nodes through Device-ID, RTT and RSS: AAN Nodes

The AAN nodes assessment phases: The AAN nodes use communication parameters such as nod-ID, RTT and RSS to verify the security of the deployed network. In the first phase, an AAN node matches the responding node-ID with its routing table to verify the legitimacy of the network traffic. The AAN node Ai generates an RREQ message, all the $Si \in Sn\text{-}1$ in proximity respond with a RREP packet. After reception of $Si \in Sn\text{-}1$ nodes RREPs messages, the AAN node compares the responding nodes node-ID(s) with its routing table. If the $Si\,\text{node} - \text{ID} \in Ai$ routing table, then Si fulfills the defined criteria, and the packet is forwarded for the next assessment parameter to ensure the legitimacy. Likewise, the process is continuous to verify the legitimacy of the participating nodes and network traffic throughout the life of deployed WSN.

4.2 Round Trip Time (RTT) Model: AAN Nodes

The RTT of a message is very sensitive, because its value is affected by communication metrics such as medium, congestion and contention in the network. Therefore, in the proposed model sufficient attention has be given to this issue to utilize the RRR of a message in an operational environment effectively. Moreover, in simulation environment links parameters was kept constant for ordinary communication. However, the value of RTT was considered infinity or higher than its estimated value if there is a fault communication in the communication medium. Likewise, these nodes are identified by comparing their RTT values with their estimated values to identify them accurately.

The RTT time mostly depends upon the numbers of wireless nodes they are present in the source and destination node. The efficiency of RTT can be improved by minimizing the distance between communicating nodes. Therefore, in this work, we used the AAN nodes to verify 96% to 98 % RTT of participating nodes with one-hop communication, because RTT calculation was the responsibility of AAN.

$$\text{RTT} = \text{queuing time source} + \text{propagation delay} + \text{buffer time at destination node} \tag{1}$$

In the proposed model, let assume that the minimum RTT is λRTT with one sensor node is given by:

$$\lambda\text{RTT} = \lambda 1 + \lambda 2 \tag{2}$$

In Eq. (2), $\lambda 1$ and $\lambda 2$ represents the delay time for AAN node and responding legitimate node. The network topology for proposed consideration is shown in Fig. 1, where the paired node is at a distance of one hop or λ from AAN. Therefore, the defined threshold value for all participating nodes should be the same in terms of RTT time.

Hence, λ be the uniform delay time or RTT for allpaired nodes, then $\lambda = \lambda 1 = \lambda 2 = \lambda 3 \ldots = \lambda n - 1$ for N number of nodes. Then,

$$\mathrm{RTT}\lambda = \lambda 1 = \lambda 2 = \lambda 3 = \lambda 4 \ldots = \lambda n - 1 \tag{3}$$

This is the minimum RTT time a node takes to send a message from source to destination with the help of hop count. So we can define their RTT through Eq. (4):

$$\mathrm{RTT}\lambda = \lambda 1 + \lambda 2 + \lambda 3 + \lambda 4 + \ldots \lambda n - 1 \tag{4}$$

4.3 Received Signal Strength (RSS) Assessment Model: AAN Nodes

The RSS of signal/received packet plays a vital role in the authentication process of our proposed scheme because the RSS confirms the distance range parameters defined for legitimate nodes by AAN. AAN nodes in the network continuously measure the values of RSS parameters for all incoming RREP to identify routing attacks, such as wormhole and sinkhole attack. The calculation of RSS is made based on the following formula:

$$\mathrm{RSS} = \mathrm{Antenna\ Gain} + \mathrm{Transmission\ Power} - \mathrm{Path\ loss} \tag{5}$$

The value of transmission power and antenna gain is kept constant for fixed transmitter (Tx) and receiver (Rx). The AAN Ai broadcast an RREQ message packet in the network, the ordinary nodes $Si \in Sn - 1$ in the proximity respond with a RREP message, which contains node-ID, RTT and RSS information. After the reception of Si RREP, the assessment of the incoming packet is started for node-ID, RTT and RSS. In the case of RSS, the packet threshold value for RSS is set about 80 m. Likewise, all incoming RREPs go-through this process to verify the legitimacy of network traffic, before initialization of the communication process in the network. If any packet, who's RSS, is (>) 80 m, then the requesting node traffic is denied for communication in the network and an alarm is generated to acknowledge the existence of malicious packet in the network. Moreover, during the operational network, the verification process is continuous throughout the entire lifetime of the network. The AAN nodes Ai broadcasts RREQ packets in the network after a defined interval of time and receive RREP from close vicinity Si nodes $\in Sn - 1$ to verify the legitimacy of network traffic and maintain high-quality security in the network.

In Fig. 2, the legitimate node is denoted by Si, where Tx is used for transmission and Rx for reception of a packet. Fig. 2 of the paper briefly overviews the authentication process of an AAN node to verify the legitimacy of network traffic. AAN node (Ai) initiates RREQ message and broadcast it in the network. All participating node $Si \in Sn - 1$ in close vicinity receives Ai RREQ and responds with RREP packet, which contains information of Si node such as source node-ID, RTT, RSS and Destination node-ID. The Ai node checks the received RREP packet of responding node to measure the value of RSS. If the RSS value of responding nodes is $\leq$80 m, then AAN verifies its legitimacy in the network. Hence, the authentication and verification process of an AAN complete successfully.

Theorem-1: An authentication aware node Ai generates a RREQ with $Si \in Sn - 1$, if Si–RSS $\leq$ 80 m $\rightarrow$ Accept.

Proof of Theorem 1: Let us suppose that, the AAN (Ai) generates RREQ with $Si \in Sn - 1$. The Ai RREQ message is received by proximity $Si \in Sn - 1$ nodes. The Si node responds with a RREP messages to Ai RREQ, which contain node-ID, RTT and RSS. By, following the authentication

process, Ai checks node-ID, RTT and RSS of responding RREP, the RSS of $Si \in Sn-1 > 80$ m. Hence, Ai denied the RREP of Si because it did not satisfy the define security parameters.

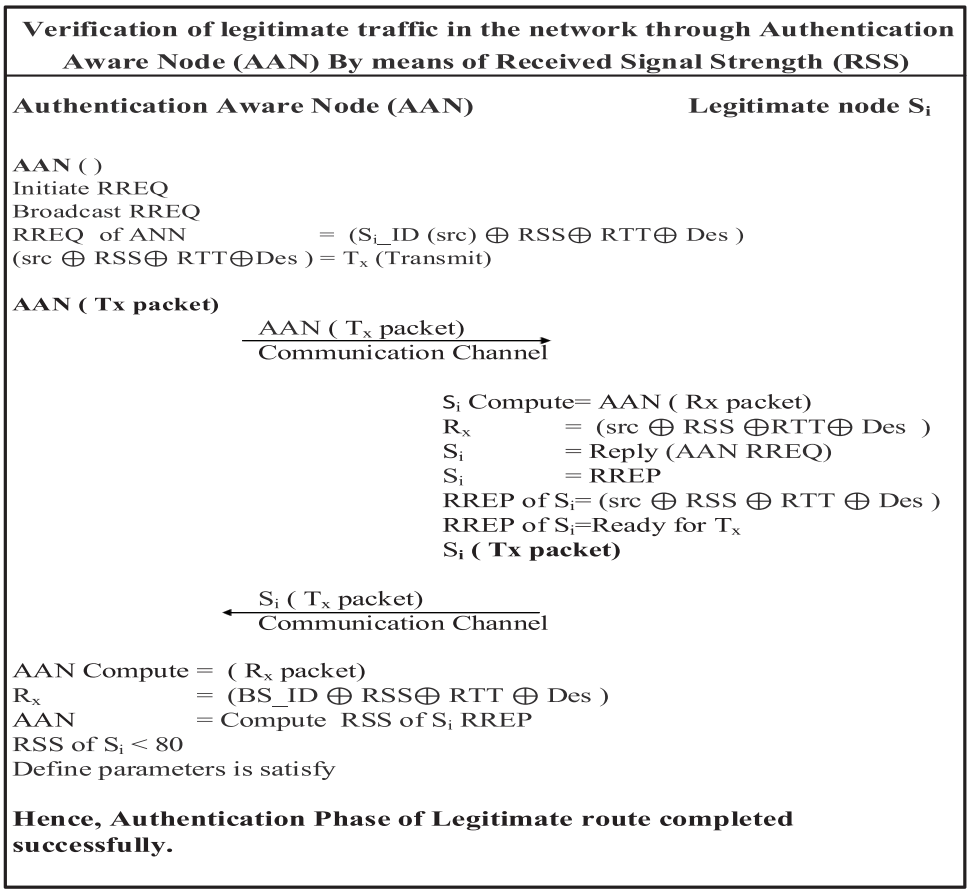

Figure 2: Detail overview diagram of authentication aware nodes (AAN) to verify legitimate route in the network

Conversely, if an authentication aware node (Ai) of the network generates a RREQ request with $Si \in Sn-1$. Likewise, the $Si \in Sn-1$ responds with an RREP packet. Ai verifies the security parameters of Si by comparing node-ID, RTT and RSS of RREP. The RSS of responding node $Si \in Sn-1$ node RREP is < 80 m as check by AAN. Hence, the RREP information of Si will be authenticated successfully by AAN. Hence, the aforesaid theorem verifies that only legitimate node $Si \in Sn-1$ having RSS $\leq$ to 80 m can be authenticated in the network.

However, the role of $Si \in Sn-1$ is to collect information according to their deployment requirement and process them for further analysis in the network, after the security check of AAN. The communication of legitimate nodes in the proposed scheme is based on point to point and point to multi-point with respect to AAN and BS.

4.4 Base Station (BS): Authentication Mechanism

Base Station (BS) plays the role of a junction for all traffic in the network because all traffic passes through the BS in the homogeneous and heterogeneous network infrastructure. Fig. 1 of the paper shows the importance of BS that how the legitimate nodes send their collected data to destination location via BS. Moreover, in our proposed model the connectivity of BS is point-to-point and point to multi-points in the deployed network. Similarly, the legitimacy of incoming packets is confirmed by matching its nodes ID, RTT and RSS in the AAN nodes and BS.

Algorithm 1: Authentication Aware node verification Phase of malicious routes and nodes

Require: To allow legitimate node and route for communication in the network.
Ensure: Security of participating nodes based on RSS, node-ID and RTT:
Start
2: $AAN(Ai) \rightarrow$ Generates RREQ packet
3: $Ai \leftarrow 0$
4: $Si \in Sn-1 \leftarrow$ Receives Ai RREQ
5: Si Respond with $\leftarrow$ RREP
6: Si RREP contains $\leftarrow$ node − ID, RSS, RTT
7: For (i = 0; I < n − 1; I++)
8: $SiRREP \leftarrow Ai$
9: $Ai \leftarrow$ verifies Si–node-ID & RTT
10: **If**
11: RSS of Si RREP $\leftarrow \leq 80$ Meters
12: **Accept**
13: **Else**
14: Reject
15: $Ai \leftarrow$ broadcast an alarm message (in case of reject)
16: **(End If)**
17: $Si \in Sn-1 \leftarrow$ Accept acknowledge and update
18: **(End For)**
19: **Return Updated legitimated node information**

4.5 BS Authentication Process: Round Trip Time (RTT) Verification Mechanism

Base station authenticates the directly connected nodes through incoming traffic such as RREQ/RREP packets. The legitimate nodes of the network $Si \in Sn-1$, which are not in the vicinity of AAN, they directly communicate with BS. Likewise, the directly connected nodes share their collected information through concerned BS. However, once the legitimate nodes $Si\text{–} \in Si-1$ generate a RREQ with BS. The BS verifies its security in terms of comparing or measuring its node-ID, RTT and RSS of the incoming packet. The BS match node-ID RSS and RTT of requesting node, if all security parameters are satisfied, then the BS allows the requesting node for communication in the network. Else BS denied the incoming RREQ/RREP packet for communication in the network. According to Eq. (1) RTT is the time that a message needs to reach from source to destination. Similarly, the minimum RTT set for BS is equal to λRTT in our case and the distance parameters are set for BS according to Eq. (2), where

$$\mathrm{RTT}\lambda = \lambda 1 + \lambda 2 \tag{6}$$

In Eq. (6) λ1 and λ2 is the delay time between BS and requesting node for one-hop distance in the proposed model to maintain accurate RTT between paired nodes. The parameters of Eq. (3) are considered for one-hop distance communication between BS and requesting node. Likewise, the BS checks the value of RTT time to verify the legitimacy of the requesting node in the network.

Base Station Authentication Phase of legitimate traffic in the network through neighbor Nodes by means of Device ID and Received Signal Strength (RSS)

Wireless node S_i	**Base station (BS)**
S_i () Start Authentication Request Si Broadcast RREQ RREQ of S_i = (S_i_ID ⊕ RSS⊕ RTT⊕ Des) (Si_ID ⊕ RSS⊕ RTT ⊕ Des) = T_x (Transmit) **S_i (T_x packet)**	
	S_i (T_x packet) Communication Channel
	BS Compute= S_i (R_x packet) R_x = (S_i_ID ⊕ RSS ⊕ RTT⊕Des) BS = Check S_i_ID ⊕ RTT⊕RSS BS = S_i_ID ⊕ RTT⊕RSS ∈ BS list BS Compute= S_i (RSS) RTT = S_i ∈ BS RSS = S_i (RSS) ≤ 80 M BS = RREQ S_i ∈ BS BS = RREP to RREQ of S_i RREP (BS) = (BS_ID ⊕ RSS⊕ RTT⊕ Des) Ready Pkt = (T_x packet)
	BS (T_x packet) Communication Channel
S_i Compute = (R_x packet) R_x = (BS_ID ⊕ RSS⊕ RTT ⊕ Des) S_i = Store RREP information	
Hence, Authentication Phase of Legitimate route completed successfully.	

Figure 3: Detail overview of BS authentication phase to verify legitimate route in industrial IoT networks

4.6 Base Station (BS): Received Signal Strength (RSS) Model

Let assume that a legitimate node of the network $Si \in Sn-1$ generates a RREQ message with concerned BS. The *Si* RREQ packet contains information such as (src-ID ⊕ des-ID ⊕ RTT ⊕ RSS). After the reception of *Si* node RREQ, the BS checks the security parameters such as node-ID, RTT and RSS. The RSS value of incoming RREQ is compared with the defined threshold value of RSS in BS, which is <80 m. Moreover, the BS uses Eq. (5) to calculate the RSS value of incoming RREQ message, where the values of transmission power and antenna gain are kept constant for fixed transmitter (*Tx*) and receiver (*Rx*). After the calculation of RSS value, the verification process is started, where the value of RSS is matched in the BS. If the value of RSS is < 80 m, then the incoming RREQ message RSS is matched in BS. Similarly, the BS after this verification check allows the requesting node for communication in the network. In case, if the

value of RSS does not match in the BS, then the BS denied the RREQ message and broadcast an alarm message in the network to acknowledge the existence of malicious activity in the network.

The paper illustrates the authentication process of legitimate nodes $Si \in Sn-1$ RREQ with concerned BS in Fig. 3. The legitimate node *Si*– generates a RREQ with concerned BS, which contains information such as (src-ID $\oplus$ RTT $\oplus$ RSS $\oplus$ des-ID). After reception of *Si* RREQ, the BS checks the node-ID, RTT and RSS. Likewise, in the verification process, the BS calculates the values of the incoming RREQ packet for RSS. After that the BS matches the values of RSS with the defined threshold value, which is $\leq$ 80 Meters, if the RSS belongs to this defined category, then the BS station allows the same node or route for communication in the network. If the value of incoming RREQ does not satisfy the security parameters condition of BS, then the BS denied the incoming RREQ packet for communication and generates an alarm message in the network to acknowledge the existence of malicious activity in the network. The steps adopted during the authentication phase for a legitimate node $Si– \in Si-1$ with BS are shown in Algorithm 2.

Algorithm 2: Base station authentication Phase of routes and nodes

Require: Allow legitimate traffic for further processing or information exchange in the network.
Ensure: Security of route and participating nodes

Start $Si \leftarrow 0$
Si initiates $\rightarrow$ communication request
$Si \leftarrow$ RREQ with BS
BS receives $\leftarrow$ *Si* RREQ
BS $\leftarrow$ Matches *Si* security parameters
    If
    $Si \leftarrow \text{RREQ}(\text{node}-\text{ID}\ \&\ RTT) \in \text{BS}$
    Next Step
    BS $\leftarrow$ Measure RSS threshold value (80 M)
        If
        RSS Distance $\leftarrow \leq$ 80 Meters
        Accept
        Else
        Si RSS $\notin$ BS $\leftarrow$ BS Denies *Si* RREQ
        End if else
    deny *Si*– RREQ and blacklist
    End If
    BS $\leftarrow$ allows $Si \in Sn-1$ for communication in the network
End for
Return List of legitimate nodes communicating with path information

Theorem-2: A Legitimate node *Si*–generates a RREQ with *BS* if *Si* ID, RRT and RSS $\in$ (BS).

Proof of Theorem 2: Let's suppose that an assailant node *Bi* generate a RREQ with concerned BS. The BS receives *Bi* RREQ. After the reception of *Bi* RREQ, the BS verifies the security

parameters of *Bi*. Likewise, the BS starts the authentication process and matches the *Bi* RREQ node-ID, RTT and RSS with defined parameters, where *Bi* security parameters $\notin$ BS list.

Hence, *Bi* RREQ will be denied by concerned BS.

Conversely, if a legitimate node *Si* generates a RREQ request with concerning base station (BS). The BS checks *Si* RREQ request with define security parameters. The *Si* node packet satisfies the security parameter of BS. Thus, the RREQ request information of *Si* will be matched successfully, because $Si \in membersBS$. Therefore, the aforesaid theorem verifies that only legitimate node *Si* $\in$ member (BS) generates RREQ in the network to process data.

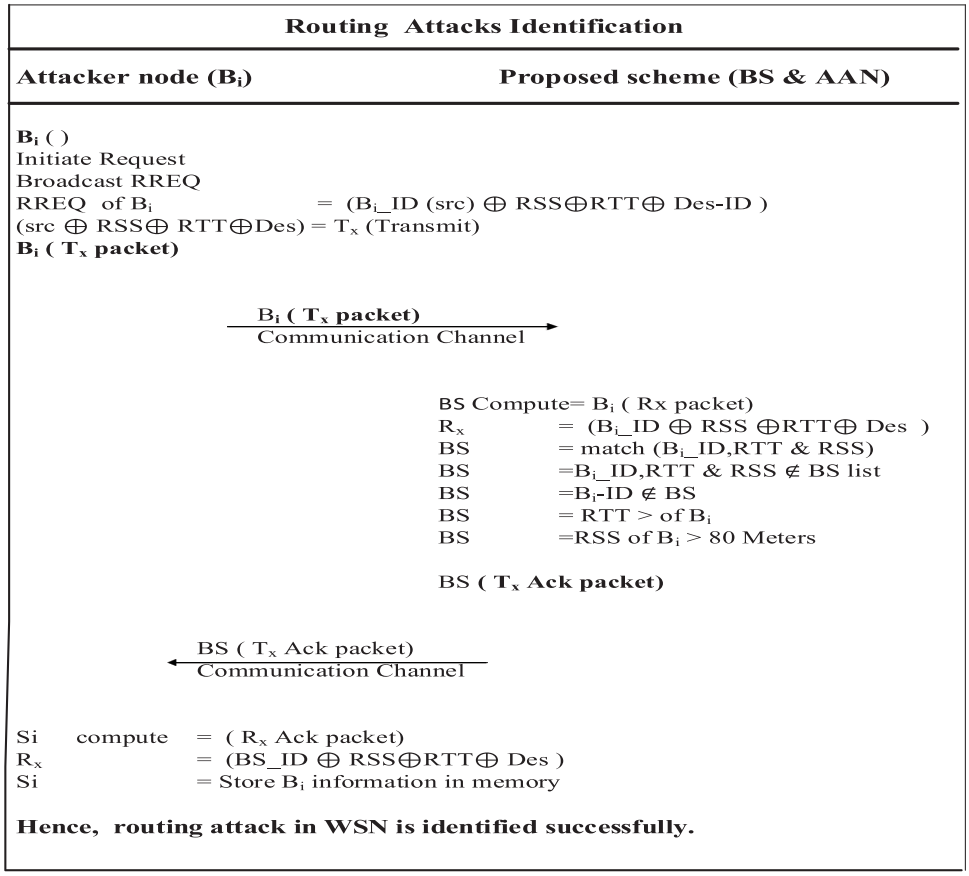

Figure 4: Detailed step by step authentication process of routing attacks in deployed Industrial IoT networks

4.7 Authentication of Fake Route RREQ: Routing Attacks

The functions of the proposed model back up each other to identify routing attacks and malicious nodes in the network. However, both the function works independently, which minimizes the chance of attacks in designated WSNs. Once, one function fails to identify fake RREQ, then function two in the backup carried out the same security check to verify the legitimacy of the network traffic by applying security parameters. The AAN node and BS use the node-ID, RTT and RSS information to verify the authenticity and integrity of data in the network.

The AAN node continuously generates RREQ messages in the network to verify the legitimacy of participating nodes and network traffic in their vicinity. However, in the case, when an ordinary node, which is not in the vicinity of AAN node and it launches a direct communication request with the concerned base station. Then the BS checks the security parameters of incoming RREQ with its defined security parameters to verify the legitimacy of requesting node.

Likewise, an attacker node *Bi* generates an authentication request with *Ai* or BS. The *Bi* RREQ contains (src-ID $\oplus$ RTT $\oplus$ RSS $\oplus$ des-ID) information. The *Ai* or BS matches *Bi* RREQ information with their defined security parameters. The *Bi* node-ID, RTT and RSS $\in$ *Ai* or BS security defined parameters. Therefore, *Ai* or BS denies *Bi* RREQ and broadcasts an alarm message in the network to acknowledge the existence of an attacker node. The detailed overview of attacker node detection is shown in Fig. 4.

The malicious RREQ authentication mechanism is shown in Fig. 4, of the paper. The malicious node *Bi* generates RREQ with BS or *Ai* nodes by advertising fake RREQ in the network. After reception of *Bi* RREQ BS or *Ai* applies the security check parameters such as node-ID, RTT and RSS. The BS or *Ai* matches the above-mentioned parameters of the requesting *Bi* node. The *Bi* node-ID $\notin$BS or *Ai* registered list. Likewise, the RTT and RSS of *Bi*(>) the defined values of security parameters in BS or *Ai*. Therefore, the BS or *Ai* node denies *Bi* RREQ and broadcast an alarm message in the network.

The attacker node *Bi* is identified in the above-mentioned scenario of Fig. 4 successfully by comparing conditional security parameters. Our proposed scheme plays exceptionally well to combat routing attacks in industrial IoT networks. Moreover, the effectiveness of our scheme was seen for different types of attacks, such as Eavesdropping, Man-in-Middle attack, Server-side attack, Client-Side attacks, Insider, and Anonymity based attacks on deployed IoT networks.

5 Formal Security Analysis of Our Mutual Authentication Scheme

In this section, the proposed model was evaluated for well-known security threats to WSNs, which can be launched on an operational network. The comprehensive overview and adopted measures are discussed as follows.

5.1 Client Impersonate Attacks

Let us assume that an attacker node (*Bi*) generates RREQ with neighbor's nodes. For this, *Bi* broadcast its RREQ packet in the network, which should be received by concerned BS or AAN node. After, the reception of attacker node B_i RREQ packet, the BS and AAN nodes checks the security parameter such as node-ID, RTT and RSS. The BS and AAN (*Ai*) node calculate and verifies the defined security parameters for the incoming packet of *Bi*. The *Bi* RREQ packet does not verify the BS and *Ai* security parameters. Therefore, the BS or AAN node broadcast an alarm message in the network to acknowledge the presence of a malicious node in the network.

5.2 Eavesdropping Attacks

In this type of attacks, the attacker hijacks the transmission channel and attracts the network traffic in term of an insecure communication channel. In our proposed model, an attacker node *Bi* generates a fake route RREQ in the network, which aims to advertise the shortest path to the destination node. The broadcasted RREQ message of *Bi* is received by AAN and BS. The BS and AAN nodes apply the security check parameters to verify the legitimacy of the incoming RREQ packet. Once, the security check is carried out, then, the *Bi* RREQ does not fulfill the security parameters of our proposed model. Therefore, malicious RREQ is easily identified by our

parametric hybrid scheme and acknowledges the existence of malicious activity in the network by broadcasting an acknowledgment message. Hence, our proposed model is very effective against eavesdropping attacks in WSNs environment.

5.3 Server-Side Attacks

Let suppose that an adversary node *Bi* generates an authentication RREQ with BS. Once the BS receives *Bi* RREQ, it checks the security parameters like node-ID, RTT and RSS. In the parameter matching process, *Bi* RREQ does not verify the defined parameters of BS. Therefore, *Bi* fake authentication RREQ is successfully identified and denied by concerned BS in our proposed model.

5.4 Off-Line Phase Guessing Password Attacks

Let assume that an adversary *Bi* guesses the authentication scheme and authenticate in polynomial time to communicate as a legitimate node *Si* in the network. In this case, the adversary *Bi* needs to fulfill all the security parameters like node-ID, RTT and RSS. Once the calculation has been carried out the RTT and RSS of requesting *Bi* node does not match in AAN or BS. Therefore, the off-line guessing password attack fails against our scheme, due to RTT and RSS value calculation.

5.5 Sensing Node Capture Attacks

Let assume that an adversary *Bi* hijack one legitimate node of the network and attract it is all security parameters and traffic information. In this case, the adversary node did not know about the AAN and BS, where the communication parameters of broadcasted RREQ/RREP messages are continuously checking. Let assume that node-ID of adversary *Bi* matches in BS or *Ai*, but their RTT and RSS information does not match. Hence, our scheme is also effective against sensing node capture attacks, because of communication parameters checking. The formal security analyses are shown in Tab. 1 of the paper.

Table 1: Formal security analysis of our proposed model with competitor schemes

Attacks name	Rezaei et al. [22]	Kaur et al. [23]	Vo et al. [20]	Amish et al. [15]	Hayajneh et al. [26]	Our scheme
Client impersonate attacks	Yes	Yes	No	Yes	No	Yes
Eavesdropping attacks	No	Yes	No	No	No	Yes
Server-side attacks	No	No	Yes	No	Yes	Yes
Off-line guess password	Yes	No	Yes	Yes	No	Yes
Anonymity attacks	Yes	No	Yes	Yes	Yes	Yes

6 Experiment Results Analysis

The Proposed hybrid mutual authentication scheme was implemented in the simulation environment, where OMNeT++ was used as a simulation tool. OMNeT++ simulation tool has the

capability to develop real-time IoT, WSNs and *ad hoc* networks in the simulation environment. The proposed model was implemented by specifying network area with distribution of AAN nodes, ordinary nodes and BS(s) in the network topological order. The authentication parameters were set in the AAN and BS with communication connectivity with ordinary nodes. Moreover, the role assigned to BS and AAN node to identify malicious activity in the network such as victim nodes and routing attacks by the assessment of communication parameters such as RSS, RTT and node-ID. The parameters set-up used in the proposed model are briefly shown in Tab. 2.

Table 2: Data set of parameters taken for the proposed scheme implementation

Type of parameter	Definition of parameter
Simulation tool	OMNeT++
Simulation environment	800×800
Number of wireless nodes L_i	200, 400, 700, 1000
Number of BS(s)	5
Number of AAN	2, 10, 20, 40, 50
Initial energy of nodes (E_i)	60,000 mAh
Energy consumed during T_x of packet	85.6 mW
Energy consumption during normal state	1.5 mW
Energy consumption during sleep mode	0.9 μW
Transmission range	180 M
Packet size	256 Kbps
Network traffic type	UDP and CBR
Transmission interval of AAN	40 Sec
Transmission of legitimate nodes time interval	10 Sec
Network topology deployment	Random/Dynamic

The parameters shown in Tab. 2 were used in the topology and infrastructure development of our proposed scheme. Moreover, the simulation environment was developed through the composition of theses parameters to capture results for our scheme. In addition, the extracted results of our proposed scheme were compared with its rival schemes based on routing attack detection rate, average throughput, latency and communication cost. Moreover, energy consumption and performance reliability were also seen to evaluate the overall structure of the proposed scheme.

6.1 Communication Cost

The communication cost of our proposed scheme was compared with existing schemes to address the issue of routing attacks in WSNs such as wormhole and sinkhole attack. Furthermore, the communication cost was observed for the proposed scheme during a simulation environment, which has better results statistics than its rival schemes, except Vo et al. [20] scheme. The communications session was established between legitimate nodes of the network with proper monitoring to verify the legitimacy of network traffic. The results extracted during simulation are shown in Tab. 3 with a comparison ratio to its competitor schemes.

Table 3: Communication cost comparison table of our scheme with competitor schemes

Proposed scheme name	The number of messages sent	Total numbers of bits
Kaur et al. [23]	16	20,248
Rezaei et al. [22]	10	32,768
Vo et al. [20]	8	15,960
Parmar et al. [15]	12	49,152
Hayajneh et al. [26]	7	28,672
Our scheme	12	24,576

6.2 Results Analysis of AAN Based on RTT Assessment

The results of our proposed model were seen for routing attacks during the simulation environment. The simulation statistics for both functions AAN and BS were individually observed to verify the performance reliability of the proposed model in terms of routing attacks detection. The results statistic seen for routing attack detection and adversary node identification through BS and AAN node was found quite consistent and remarkable. In the phase, the AAN was considered for evaluation, where an adversary node advertises fake RREQ in the network. The adversary node advertised fake shortest path information to the destination node by a broadcast packet in the network. Similarly, this RREQ was also received by AAN node. The AAN node carried out the necessary security verification process to match the RREQ RRT time with its defined values. The adversary node was observed that it does not verify the security condition of RRT by matching its value. Similarly, after the assessment, the AAN node generates an alarm message to acknowledge the existence of an adversary node in the network.

The simulation result verifies that AAN node successfully identified an adversary node in the network. This verifies that the AAN node detection rate of routing attacks based on RTT assessment was quite accurate in the operational network against fake RREQ packet. Subsequently, the number of adversary nodes was increased in the deployed WSN infrastructure to verify performance reliability with a high number of fake RREQ, which was also found quite exceptional for AAN node. The AAN aware node detects the maximum number of fake RREQ in their vicinity, whose statistics are shown in Fig. 5.

6.3 Results Analysis of AAN Based on RSS Assessment

The results of our proposed model have also seen for RSS based assessment of AAN, where adversary nodes were used in the operational network to advertise fake RREQ and hijack network security. The node-ID and RTT time in fake RREQ was kept similar to legitimate nodes RTT and node-ID, where the RSS was different for all introduced adversary nodes. During the simulation, the AAN nodes were closely observed for assessment of RSS of fake RREQ of an adversary node, which was found quite remarkable by assessing maximum RREQ in the close vicinity. Moreover, the statistical analysis observed during the simulation for an AAN node based on RSS is shown in Fig. 6, where the adversary node RREP(s) assessment and detection % are shown in graphical form as captured during the simulation.

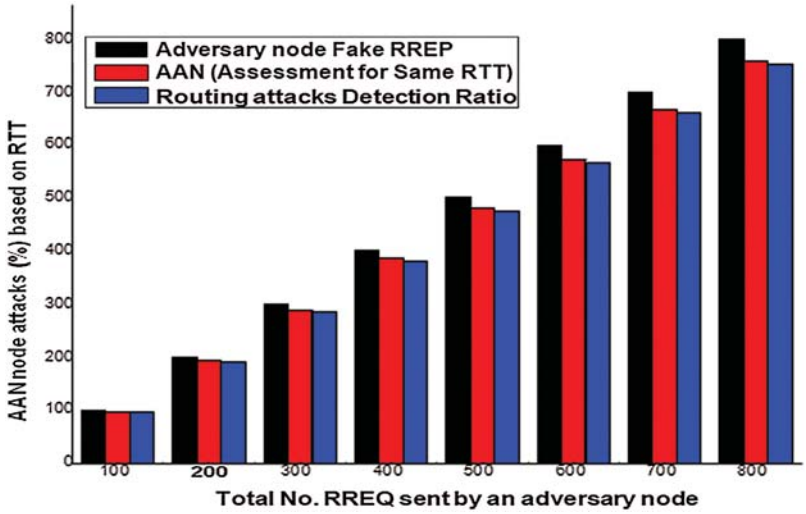

Figure 5: AAN results analysis to detect fake RREQ in deployed Industrial IoT networks

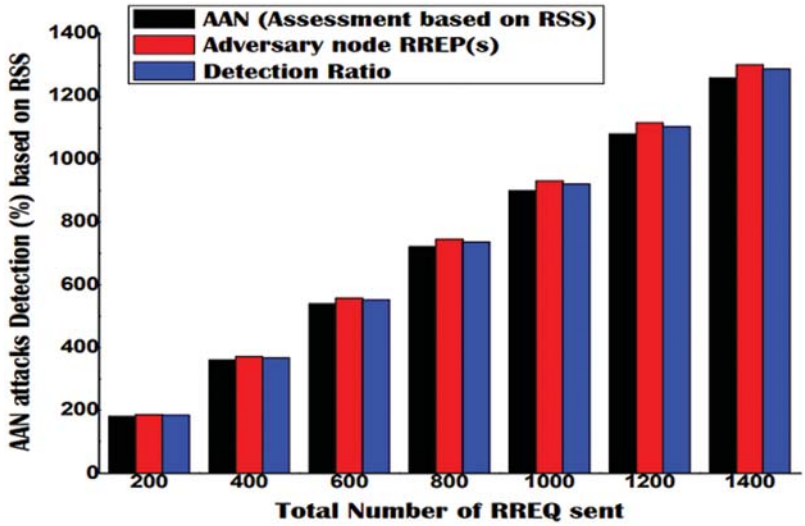

Figure 6: AAN results analysis to detect fake RREQ in Industrial IoT based on incoming packet RSS assessment

6.4 Results Analysis of AAN Based on RSS and RTT Assessment

AAN node's results were also seen for fake RREQ(s), where both the values of RTT and RSS were different from other legitimate nodes of the network. The legitimate nodes and adversary node in the operational were closely seen in term of authentication of RTT and RSS for incoming RREQ/RREP to ANN. The ANN nodes were found quite consistent in identifying adversary nodes; they have fake RREQ(s) in the network. Moreover, the performance reliability of the network was also seen during the existence of adversary nodes with legitimate nodes in the network. The statistical analysis observed during the simulation assessment of AAN node to detect fake RREQ with the help of RSS and RTT are shown in Fig. 7.

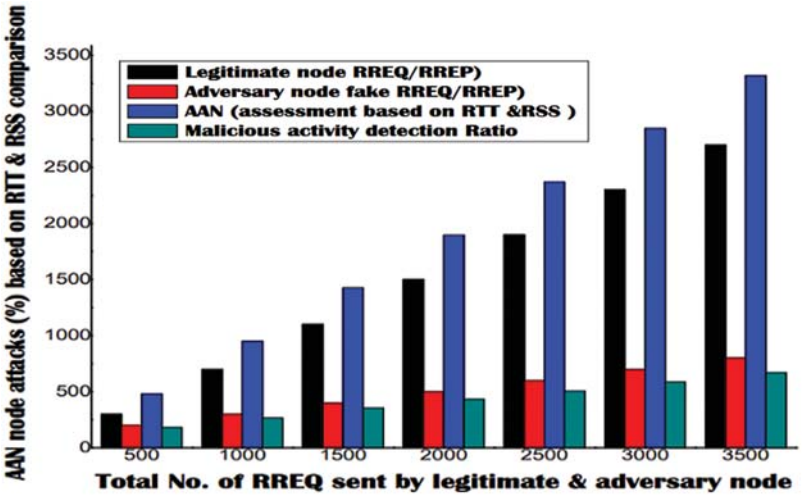

Figure 7: AAN results analysis to detect fake RREQ in Industrial IoT-based on both RTT and RSS assessment

6.5 BS Fake RREQ Results Analysis Based on RTT and RSS

The BS results were also seen for the detection of fake RREQ(s) during the operational network, where the legitimate nodes were communicating with BS. The statistical analysis extracted from the simulation tool is shown in Fig. 8, where both adversary and legitimate nodes broadcast RREQ/RREP packets in the network. However, those fake RREQ, which were received by BS directly from adversary nodes are assessed for security check. The statistical results analysis for fake RREQ/RREP of adversary nodes, which were captured during simulation, is shown in Fig. 8.

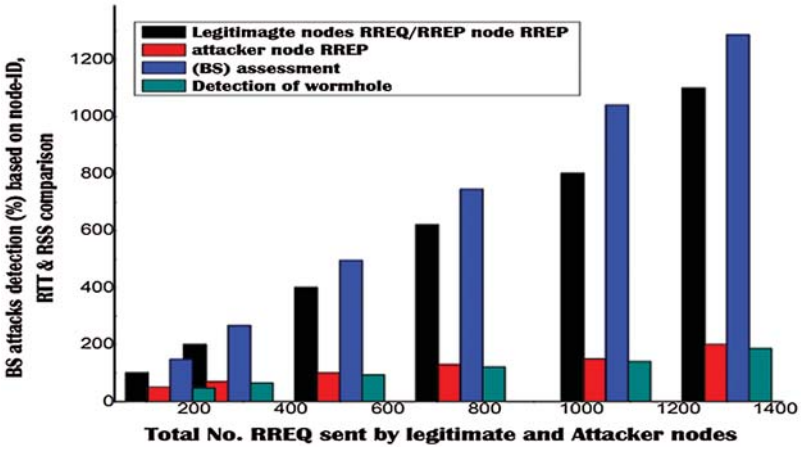

Figure 8: BS fake RREQ detection statistical analysis, based on both RTT and RSS assessment

6.6 BS and ANN Node Combined Statistical Analysis for Fake RREQ/RREP(s)

The simulation of the proposed model was continued to see the overall detection rate of our hybrid scheme for AAN node and BS. Moreover, the fake RREQ/RREP(s) was sent to AAN node and BS. Similarly, the malicious nodes they were not in the vicinity of AAN node was successfully detected by concerned BS. The combine results observed for BS and AAN node in terms of fake RREQ and RREP(s) packet was about 97.7%, which is far better than its rival schemes. Although, the detection rate of our proposed scheme was 97.7%, but it is better than the existing by means of energy consumption, communication cost, computation costs and communication metrics, because all the authentication process is performed by AAN and BS, which improves the overall network communication infrastructure. The results statistic captured during the simulation for our hybrid mutual authentication scheme is shown in Fig. 9, where 95.7% fake RREQ was identified successfully.

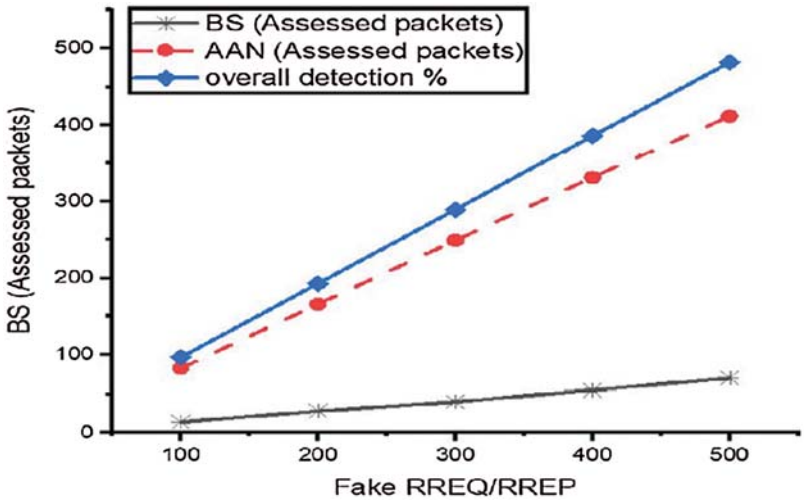

Figure 9: Statistical analysis of our scheme to detect fake RREQ/RREP(s) in operational network

6.7 Routing Attacks Results Analysis of Our Proposed Model with Rival Schemes

The proposed model was evaluated for each function, where different parameters of adversary nodes were disturbed to identify routing attacks or fake RREQ/RREP(s) packets in the network based on parameter assessments. The detection rate of fake RREQ/RREP(s) of the proposed model was quite excellent individually. Similarly, the fake RREQ/RREP(s) assessment of adversary nodes was also carried out in a combination of BS and AAN, which shows a high detection ratio, and the statistics are shown in Fig. 9. Moreover, after individual and combine results statistic the proposed scheme was compared with its competitor's scheme based on accurate routing attacks detection, which was found promising in the presence of field-proven schemes. The malicious activities in the network were successfully identified with the help proposed model. Moreover, the proposed model is not only effective against routing, but also helpful to identify some network attacks, which is shown in the formal security analysis. The results statistics for proposed model with its rival schemes are shown in Fig. 10.

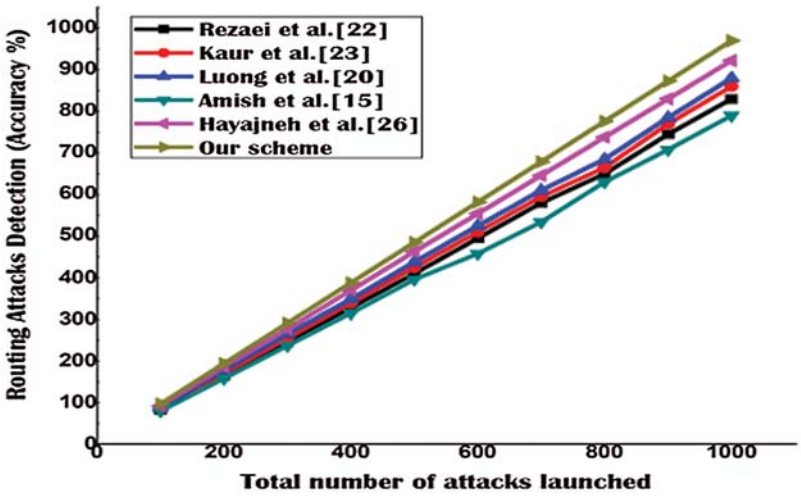

Figure 10: Routing attacks statistical analysis of our proposed model with its rival schemes

6.8 Statistical Analysis of Our Proposed Scheme with Rival Scheme for Latency

The proposed model was also observed for latency during the communication process to verify the performance reliability of packet exchange based on the delay time. During the experiment analysis, the latency observed for the proposed model was exceptional, due to several BS(s) in the deployed area of Industrial IoT networks. The latency of the proposed model was compared with the field-proven scheme, which was found remarkable well in their presence. The statistical analysis of the latency for our proposed model and its competitor's schemes are shown in Fig. 11.

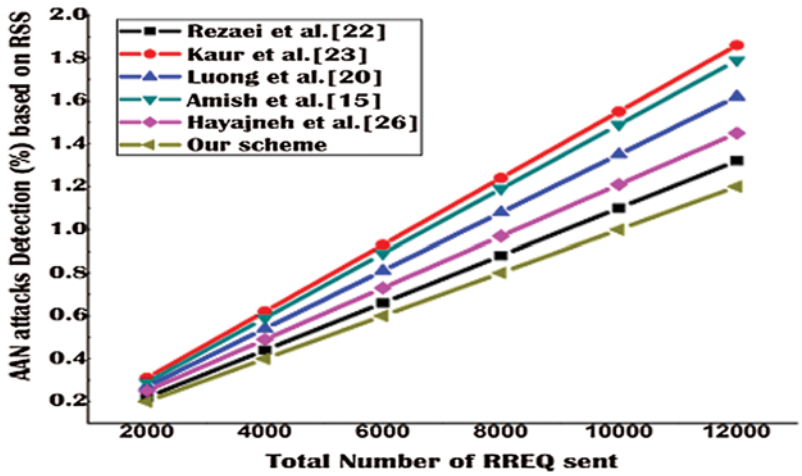

Figure 11: Latency statistical analysis of our proposed model with its competitor schemes

6.9 Throughput Statistical Analysis of Our Proposed Scheme with Competitor's Scheme

The results statistic of our parametric hybrid mutual authentication scheme was also checked for network throughput, which was found convincing during the simulation. The network traffic was observed in terms of throughput to check the reliability of proposed scheme. The accurate

detection of routing attacks in an operational network minimizes congestion, contention and network overhead, which improves the overall communication environment of the network. Therefore, the result observed for throughput in our scheme during simulation environment was significant, which shows the reliability of our hybrid scheme. Moreover, the utilization of several BS(s) in the deployed Industrial IoT minimizes the network overhead up-to a great extent, which maximizes network throughput. The results statistic captured for our scheme during simulation is shown in Fig. 12 in comparison with its competitor's schemes.

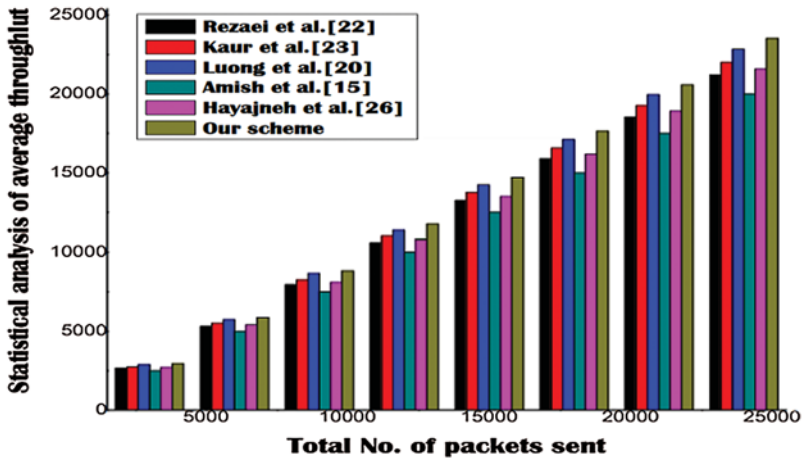

Figure 12: Throughput statistical analysis of our proposed model with rival schemes

7 Conclusions

In this paper, we proposed a hybrid mutual authentication scheme for Industrial IoT networks to combat routing attacks. The proposed model uses two functions in the back-up scenario to ensure the legitimacy of network traffic in Industrial IoT networks. In addition, both the functions work independently, but the authentication mechanism back-up each other to identify routing attacks with significant results. In the initial phase, the AAN node initiates RREQ with the nearest proximity nodes in the network. The nodes nearby AAN respond with a RREP packet. Once, the AAN node receives RREP from nearby nodes, they match security parameters such as node-ID, RTT, and RSS to ensure the legitimacy of the incoming packet. Likewise, if the incoming RREP fulfills the defined security parameters, then the authentication mechanism completes successfully. Likewise, the BS works as function 2 in the proposed model, if any RREQ/RREP misses by an AAN, and the same RREQ/RREP approach directly to the BS. Then, the BS carries out the same security check mechanism of AAN to verify the legitimacy of requesting packet. The performance reliability of the proposed model was checked based on attack detection, communication cost, computational cost, latency, and throughput in the presence of its competitor's schemes, which showed an overall improvement. Besides that, the attacks detection percentage observed for the proposed model was 97.7%, which surpasses the existing schemes by an average 13% improvement.

Funding Statement: This research was supported by the MSIT (Ministry of Science and ICT), Korea under the ITRC (Information Technology Research Center) support program (IITP-2020-2018-0-01426) supervised by IITP (Institute for Information and Communication Technology

Planning & Evaluation) and in part by the National Research Foundation (NRF) funded by the Korea government (MSIT) (No. 2019R1F1A1059125).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. C. Chien, C. F. Lai, M. S. Hossain and G. Muhammad, "Heterogeneous space and terrestrial integrated networks for IoT: Architecture and challenges," *IEEE Network*, vol. 33, no. 1, pp. 15–21, 2019.

[2] M. Adil, R. Khan, J. Ali, B. H. Roh, Q. T. H. Ta *et al.,* "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment," *IEEE Access*, vol. 8, pp. 163209–163224, 2020.

[3] M. Adil, R. Khan and M. A. N. Ul-Ghani, "Preventive techniques of phishing attacks in networks," in *2020 3rd Int. Conf. on Advancements in Computational Sciences*, University of Lahore, Pakistan, pp. 1–8, 2020.

[4] C. Hennebert and J. D. Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 384–398, 2014.

[5] W. Trappe, R. Howard and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 14–21, 2015.

[6] G. Ankur, M. Tripathi, T. J. Shaikh and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Computer Networks*, vol. 14, no. 9, pp. 29–42, 2019.

[7] M. Adil, M. A. Almaiah, A. O. Alsayed and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, pp. 2311, 2020.

[8] P. Gope, A. K. Das, N. Kumar and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.

[9] R. Elnaz, "Energy efficient RPL routing protocol in smart buildings," Master's thesis, University of Waterloo, 2014.

[10] W. Linus, S. Raza and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 794326, 2013.

[11] D. Mazzei, G. Baldi, G. Fantoni, G. Montelisciani, A. Pitasi *et al.,* "A blockchain tokenizer for industrial IOT trustless applications," *Future Generation Computer Systems*, vol. 105, pp. 432–445, 2020.

[12] M. Ophilipp, S. Mattejat, Z. Benenson, C. Muller and F. Armknecht, "Insecure to the touch: Attacking zig bee 3.0 via touch link commissioning," in *Proc. of the 10th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, Boston University, USA, pp. 230–240, 2017.

[13] A. U. Rehman, S. U. Rehman and H. Raheem, "Sinkhole attacks in wireless sensor networks: A survey," *Wireless Personal Communications*, vol. 106, no. 4, pp. 2291–2313, 2019.

[14] C. Youngho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 205920, 2013.

[15] A. Parmar and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Computer Science*, vol. 79, pp. 700–707, 2016.

[16] C. Del-Valle-Soto, C. Mex-Perera, I. Aldaya, F. Lezama, J. A. Nolazco-Flores *et al.,* "New detection paradigms to improve wireless sensor network performance under jamming attacks," *Sensors*, vol. 19, no. 11, pp. 2489, 2019.

[17] J. Granjal, J. M. Silva and N. Lourenço, "Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection," *Sensors*, vol. 18, no. 8, pp. 2445, 2018.

[18] F. A. Khan, M. Imran, H. Abbas and M. H. Durad, "A detection and prevention system against collaborative attacks in mobile ad hoc networks," *Future Generation Computer Systems*, vol. 68, pp. 416–427, 2017.

[19] F. Idris Khan, T. Shon, T. Lee and K. H. Kim, "Merkle tree-based wormhole attack avoidance mechanism in low power and lossy network based networks," *Security and Communication Networks*, vol. 7, no. 8, pp. 1292–1309, 2014.

[20] T. T. Vo, N. T. Luong and D. Hoang, "MLAMAN: A novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network," *Wireless Networks*, vol. 25, no. 7, pp. 4115–4132, 2019.

[21] Z. Yifeng, L. Lamont and L. Li, "Wormhole attack detection based on distance verification and the use of hypothesis testing for wireless ad hoc networks," in *MILCOM 2009-2009 IEEE Military Communications Conf.*, pp. 1–7, 2009.

[22] F. Rezaei and A. Zahedi, "Dealing with wormhole attacks in wireless sensor networks through discovering separate routes between nodes," *Engineering Technology & Applied Science Research*, vol. 7, no. 4, pp. 1771–1774, 2017.

[23] P. Kaur, D. Kaur and R. Mahajan, "Wormhole attack detection technique in mobile ad hoc networks," *Wireless Personal Communications*, vol. 97, no. 2, pp. 2939–2950, 2017.

[24] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay and P. Kar, "Wormhole detection based on ordinal MDS using RTT in wireless sensor network," *Journal of Computer Networks and Communications*, vol. 2016, no. 10, pp. 1–15, 2016.

[25] M. Adil, R. Khan, M. A. Almaiah, M. A. Zahrani, M. Zakarya *et al.,* "MAC-AODV based mutual authentication scheme for constraint oriented networks," *IEEE Access*, vol. 8, pp. 44459–44469, 2020.

[26] M. A. Obaidat, S. Obeidat, J. Holst, A. A. Hayajneh and J. Brown, "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," *Computers*, vol. 9, no. 2, pp. 44, 2020.

[27] T. Shigeyasu and A. Sonoda, "Detection and mitigation of collusive interest flooding attack on content centric networking," *International Journal of Grid and Utility Computing*, vol. 11, no. 1, pp. 21–29, 2020.

[28] P. Cong, J. Brown and L. Carpenter, "A theil index-Based countermeasure against advanced vampire attack in internet of things," in *2020 IEEE 21st Int. Conf. on High Performance Switching and Routing*, New Jersey Institute of Technology in Newark, USA, pp. 1–6, 2020.

[29] K. Georgios, C. Kolias, D. Geneiatakis, G. Karopoulos, G. M. Makrakis *et al.,* "A state-of-the-art review on the security of mainstream IoT wireless PAN protocol stacks," *Symmetry*, vol. 12, no. 4, 2020.

[30] M. S. Ali, M. Vecchio, G. D. Putra, S. S. Kanhere and F. Antonelli, "A decentralized peer-to-peer remote health monitoring system," *Sensors*, vol. 20, no. 6, pp. 1656, 2020.

[31] M. Adil, M. A. Almaiah, A. Omar Alsayed and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, pp. 2311, 2020.