Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.057848

ARTICLE

Combined Architecture of Destination Sequence Distance Vector (DSDV) Routing with Software Defined Networking (SDN) and Blockchain in Cyber-Physical Systems

Jawad Ahmad Ansari[1], **Mohamad Khairi Ishak**[2,*] **and Khalid Ammar**[2]

[1]School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, Nibong Tebal, Pulau Pinang, 11800, Malaysia

[2]Department of Electrical and Computer Engineering, College of Engineering and Information Technology, Ajman University, Ajman, 346, United Arab Emirates

*Corresponding Author: Mohamad Khairi Ishak. Email: m.ishak@ajman.ac.ae

Received: 29 August 2024; Accepted: 09 December 2024; Published: 17 February 2025

ABSTRACT: Cyber-Physical System (CPS) devices are increasing exponentially. Lacking confidentiality creates a vulnerable network. Thus, demanding the overall system with the latest and robust solutions for the defence mechanisms with low computation cost, increased integrity, and surveillance. The proposal of a mechanism that utilizes the features of authenticity measures using the Destination Sequence Distance Vector (DSDV) routing protocol which applies to the multi-WSN (Wireless Sensor Network) of IoT devices in CPS which is developed for the Device-to-Device (D2D) authentication developed from the local-chain and public chain respectively combined with the Software Defined Networking (SDN) control and monitoring system using switches and controllers that will route the packets through the network, identify any false nodes, take preventive measures against them and preventing them for any future problems. Next, the system is powered by Blockchain cryptographic features by utilizing the TrustChain features to create a private, secure, and temper-free ledger of the transactions performed inside the network. Results are achieved in the legitimate devices connecting to the network, transferring their packets to their destination under supervision, reporting whenever a false node is causing hurdles, and recording the transactions for temper-proof records. Evaluation results based on 1000+ transactions illustrate that the proposed mechanism not only outshines most aspects of Cyber-Physical systems but also consumes less computation power with a low latency of 0.1 seconds only.

KEYWORDS: DSDV; intelligent authentication; SDN; control & monitoring; blockchain; recording of transactions

1 Introduction

Emerging technologies such as the Internet of Things (IoT) greatly influence our daily lives. Depending on such systems makes our lives easier, faster, and more productive. Utilizing such systems enhances efficiency, speed, and productivity in daily activities. Appropriate implementation of technology ensures the secure usage of devices. This principle applies to various real-world applications, including smart farming, healthcare, disaster management, military surveillance, and industrial automation [1–3]. To ensure smoothness in the system, establishing robust security solutions for our systems is a priority, particularly for sensor devices.

The centralized Device-to-Device (D2D) approach relies on third parties, thus increasing the likelihood of failure and indicating that the legitimacy of sensor devices still needs to be fulfilled for the requirement.

To address the issue, Device-to-Device (D2D) authentication without the presence of any centralized source offers a promising solution. To resolve this problem, Device-to-Device (D2D) authentication without the presence of any centralized source positively serves the purpose. In [4], researchers have suggested a lightweight DSDV routing protocol which takes advantage of the MAC addresses of the devices, utilizes the HASH algorithm, and verifies the legitimacy of the devices indicating that the described protocol ensures no false nodes are in the network, clearing ways for the DSDV routing. Consequently, authentication is achieved.

SDN facilitates accountability and feasibility of detection within the network, enabling device monitoring through switches and controllers. Utilizing these helps manage control and flow motion inside the network. With this in mind, the computational cost, low latency, and a record of devices. Acquiring such information helps in the detection rate; faster detection ensures that the response time to any vulnerability is identified. Low latency will help in decision-making for routing packets from the source to the destination. Rapid decision-making and network responsiveness enable the identification of optimal routing paths.

Blockchain technology, with its cryptographic features, enhances record-keeping through its temper-free ledger system. This helps record the transactions occurring between the devices. Using the TrustChain capabilities as described in [5] creates a permission-less-temper-proof record that serves the purpose of tracking and storing data of the contributors acting as agents. This means that whenever an agent serves its purpose by give and take policy, it is then identified as an accepted activity. In the reverse scenario, free agents will be detected as favouring refusal of service. Hence data structure is irrefutable compared to the Bitcoin structure, and its long-lasting nature makes this Blockchain applicable to most scenarios.

1.1 Research Contributions

This paper proposes the framework of HASH-based DSDV routing architecture for the multi-WSNs, SDN monitor and action features for detection and Blockchain ledger-based system in CPS for IoT devices. Fig. 1 shows the network infrastructure for this purpose constituting multi-WSNs interconnected with the components such as sensor devices, Base Station (BS) and clustered (CH). Next comes the SDN which has its controllers, switches, user database, Authentication, Authorization and Accounting (AAA) server and Modify management. Continuing, Blockchain comes with its local chain features and ledger systems combined making a trustworthy network. The system first utilizes the HASH mechanisms for the encryption and decryption techniques in the initial phases of communication which is then carried out by the DSDV router which then creates the pathway for the packets to send and receive.

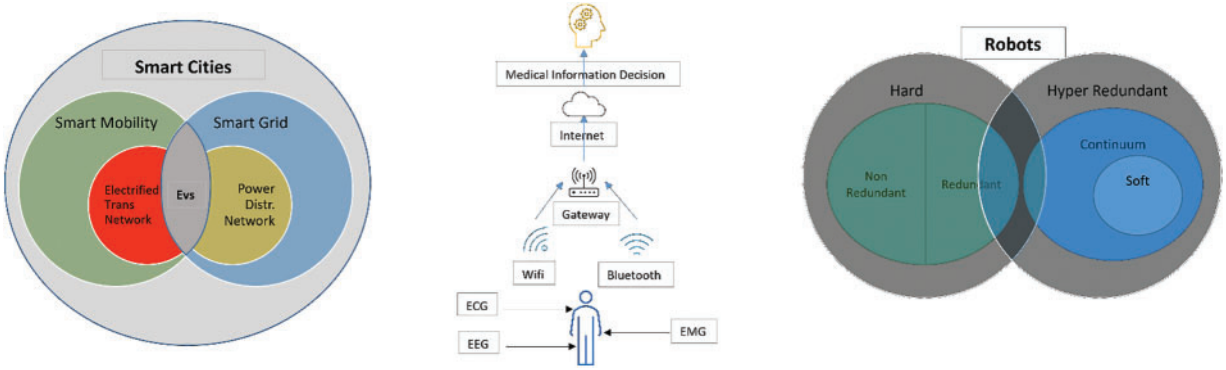

Figure 1: Background of the desired application of proposed system

Now, the SDN is responsible for optimising the processing pipeline of the traffic and continuously watches each data packet being sent for any unauthorized access and actions taken accordingly. As a result, the network middle point is much more viable for continuous processes, improves reliability by lowering latency, and requires less computing. Blockchain records the transaction from the beginning till the end, compiles the data and records it in the ledger, multiple recordings make a chain reaction and the process.

When continued further, creates an infinite length of TrustChain blockchain which becomes temper-proof.

The major contributions of this study are as follows:

1. The CH and BS nodes are responsible for advertising the route by utilising the power and resources sufficient for them to perform. This continuous process ensures with the help of DSDV that only the devices with the correct HASH authentication keys are allowed into the network.
2. SDN utilizes its controller and switches to recognize the incoming and outgoing communications using the switch which aids in developing the most suitable pathway for packet transfer. The controller then acts as the supervisor in this scenario and it helps to direct the correct procedures to be accounted for whenever a possible node is causing hurdles, is stated as a malicious node action and actions are taken immediately to block such node.
3. Blockchain will take the lead from here and utilize its cryptographic data structure, which helps in continuous, independent resource creation of records and is much more suitable than the Bitcoin structure. This chain will then make the structure Sybil-proof, increasing its trustworthiness. The strength of this structure is exponentially beneficial to that of Bitcoin, which has limited capabilities.
4. The result becomes encrypted, directed, authorized data packets of communication from source to destination secured within a chain.

2 Literature Review

Discussion in the literature review has the goal of devising a solution for the challenges in terms of security barriers in Cyber-Physical Systems. These studies have distinct features addressing a certain scenario or use case. Using such methods is useful for a certain time and hence a long-term method must be devised for a better lifespan. These studies apply to Cyber-Physical Systems enhancing their robustness, enhancing stability and control and improving the effectiveness overall. Many researchers have suggested solutions for wireless sensor networks (WSNs) on the Internet of Things (IoT), SDN-controlled networks with their distinctive features, and Blockchain distributed systems on multiple sectors of application with limited capabilities and future scope.

2.1 Authentication

Adil et al. [4] devised a solution for a mutual authentication process, the HASH-MAC-DSDV protocol which enables the network to authenticate the sensor network devices intelligently, and this is done using the MD5 algorithm which allows the devices to have their routing tables for sending information from source to destination. The procedure helps reduce the latency and energy while increasing the attack detection rate and PLR. Ma et al. [6] proposed a two-stage solution for the problem of bandwidth utilization and improving signal acceptance can be addressed. Both issues are solved using the two different stages when one stage solves the problem of bandwidth then the second layer solves the problem of accepting high signal acceptance hence better overall performance. This is done using the CAN-FD message packing method and it proved to be more secure for intelligent ACPS. In the future, this can be theoretically proved so that the deadline can be met. Yuan et al. [7] investigated that when data eavesdropping is faced then the transmission strategy, data security, and transmission stability cannot be guaranteed when it's the case of an IoT network

causing very much harm to the services. Using the k-n approach allows the secrets to be transmitted through different routes hence making the attack nearly impossible to obtain the information until and unless the attacker compromises a huge number of large and that is very costly as a system and hence almost impossible. Wang et al. [8] discussed that effectively reducing the network bandwidth and computational load of the cloud server, an emerging ecosystem known as MEC is used. Efficient security measures are required which have low complexity and hence MEC needs to adapt accordingly. For this purpose, an SDN-based authentication system for MEC is introduced which will not only mutually authenticate but secretly keep the key confidential. This scheme is simulated using the NS-3 denoting that the proposed scheme has high efficiency. Wang et al. [9] proposed that with the joint optimization of the communication and computation resource allocation for the blockchain-enabled SD-CPS framework using the actor-critic (A3C) algorithm for the balance of cloud/edge resource allocation with best strategies. Also using reinforcement learning helps reduce the latency problem compared with the other algorithms.

2.2 Software Defined Networking

Zarca et al. [10] proposed the Anastacia security management architecture presented in the paper to deal with security and privacy in NFV/SDN-enabled IoT scenarios. Different scenarios have been tested in this case one is the Mobile edge computing, and the other is IoT-enabled Critical infrastructure. The proposed solution has the feasibility of automatically monitoring, detecting, reacting, and mitigating IoT cyber-attacks, which helps maintain the strength of the network, reducing latency, and eliminating delays in IoT networks. Future works support extendibility in cyber threat detection and mitigation using VNF orchestration and deployment on the IoT network. Wu et al. [11] discussed in their paper that for increasing the lifetime of the Software-defined CPS, comes the proposal of a novel virtual and dynamic control architecture. Using the NFV technique, sleep mode is a topology control to be introduced which increases the lifespan of the CPS and hence delivers better results. Simulation results have proved that both the NFV and the SDN, if utilized together get better efficiency and are energy efficient.

2.3 Blockchain

Mollah et al. [12] proposed that the Internet of Vehicles (IOV) is another great challenge faced nowadays because as more and more cars are shifting towards centrally controlled environments, they become more vulnerable as they lack the security measures needed to tackle the situation. Blockchain enables distributed resource management capabilities but is still not up to the standard to make the system reliable for every case. Ahmad et al. [13] proposed a novel trust model named MARINE which increases network security. This is done by detecting and revoking dishonest vehicles and their generated content, and this is done very quickly. Because outsider attacks can be easily detected by insider attacks and are likely to be detected very difficultly hence the conclusion from the simulations shows that the model has proved itself to be very efficient and can efficiently detect all MiTM attacks and clear the pollution. Zhao et al. [14] explained in their article how beneficial conceivably the integration of blockchain-enabled CPS is. Next, they explained nine basic operations that can be done with the help of integration and how they are challenging too. All the aspects of new possibilities were discovered along with their benefits and drawbacks. Hu et al. [15] proposed that edge computing plays a vital role in the SDN integrated security mechanisms as they can optimize the block size, reduce the latency of the network and enable smart contracts which will help in preventing hurdles that can disturb the whole network performance and hence the reliability is also compromised. Egala et al. [16] proposed that the Internet of Medical Things (IoMT) is used in the smart healthcare sector where it uses the blockchain, DDSS and hybrid computing to perform medical procedures with minimal human involvement. SRAC and cryptography are the major key factors contributing to security concerns.

This procedure technique can be enhanced more when AI/ML is involved. Plus, low latency will ensure the procedure is performed accurately and error-free.

2.4 Cyber-Physical System

Jahromi et al. [17] proposed a two-stage ensemble novel deep learning-based attack detection using its deep representation learning that maps the samples to the new dimensional space and detects the attack sample using DT. The model forms a complex DNN which accurately attributes cyber-attacks. In future, cyber-threat design with its hunting components will help facilitate invisible intrusion attacks and maintain a normal profile for the entire system. Moness et al. [18] investigated that wind energy is a source of energy and is pollution-less hence producing clean energy. Expected technological advancements in computation, control, communications, and physical components of WECS have massive plans for farms with better strategies. This energy results in the Internet of Energy (IoE). But these components require the implementation of sensors with health monitoring as well resulting in a more sustainable power source. Omoniwa et al. [19] proposed the FECIoT with its potential by adding value to the existing IoT systems by providing storage, and computational services as well as enabling real-time response resulting in a distributed manner to the IoT end-devices. This framework, while eliminating costly bandwidth additions, also provides more responsiveness to the core network. This framework has a bright future, and it can surely benefit the service of the IoT devices and be called the Internet of the future. This framework is expected to be the prime focus for researchers in the next decade. Hatzivasilis et al. [20] worked on the Presentation of SCOTRES which is a trust system for secure routing. With the evaluation of six different routing schemes in an NS2 simulator, the results came out as the SCOTRES being the best performing in the best energy and load-balancing behaviour as well as the provision of the highest level of security thus proving to be the best performer in all the six routing schemes. When SCOTRES are applied in rural CPS communications providing low overhead of the trust system and hence the node longevity is preserved.

3 Proposed Methodologies

The proposed methodology comprises Authentication measures + Control features + a Distributed ledger system. The integration of these techniques makes them capable of distinguishing between the legitimate node and the false node.

CPS has sensor nodes within the architecture that help to communicate and manipulate the data. The starting point is dealt with in the DSDV router. It consists of CH and BS which have their memory and processing power for broadcasting the existence of a node within the network. Upon verification, the CH is triggered which increases the lifetime of the sensor devices. Then it transmits the data to the BS which also has the computational power and capability to influence the lifetime of the sensor devices.

The nature of the transaction being used in this study comprises a combined scenario which integrates traditional network routing with blockchain transactions. Data packets would be routed through the network using DSDV and SDN, while Trustchain handles secure transactions and data storage on the blockchain ledger. This helps in daily transactions such as the ongoing activities using our Mobile Phones, our Cars, our Machines etc. All these devices exchange data packets, which are further processed for verification and clarification. Having such a traditional network with this defence mechanism concludes that the system is overall capable of using in daily driven activities and also in scientific activities. The tested network includes such devices in the simulation environment and network conditions are set according to standard protocols of communication and speeds.

Fig. 2 represents the architecture for the authentication mechanism of our proposed system. The illustration shows that the sensor devices within are connected via a local chain and it defines that the cluster head is a verified source. Black lines represent the cluster head of each local chain. These cluster heads are connected to the CH which is responsible for the advertisement of the devices across the network and BS is contributing to the interconnectivity.

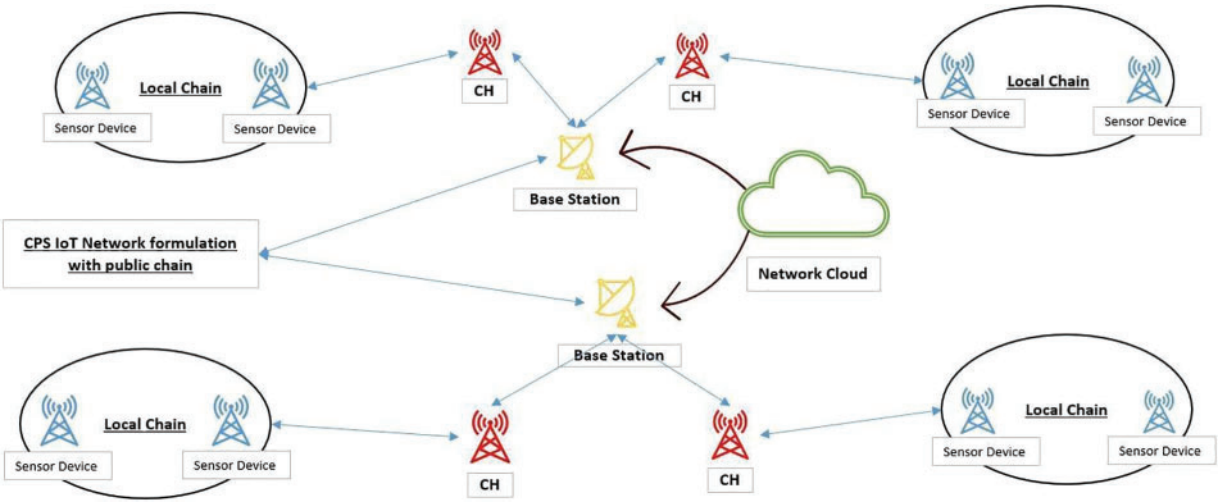

Figure 2: Authentication mechanism of our scheme

3.1 Authentication Mechanism

The proposed authentication model consists of the MD5 hash algorithm which persists in the effective working for the uniqueness of the sensor devices. It uses the phenomena of matching the keys stored within to verify it with the concerned devices so that the identification can be completed. Whenever a new sensor device is trying to connect to the network, it first defines its identity, for example by denoting it by i = (1, 2, 3, 4, . . . , n) and this is investigated in terms of D2D communication so, if Di device is attempting to communicate, it first need to generate its identification key to pass the verification with the attempt to provoke a request message such that Di ∈ D n − 1. The key factor here is that the authentication key must be legitimate to proceed from the checkpoint. As soon the initial process is done, it will move towards the authentication phase and be carried on. CH will then take responsibility for distributing information such that if one sensor node attempts to connect with another sensor node, it can be verified. CH has its table of information which stores the information necessary to process the existence of a node. The next step is the route generator request which is done by RREQ. It helps generate route plans which can be carried out by the data packets in the network. If for example there is an attacker device Ak which is attempting to establish a connection request and communicate to release false information or cause harm to the network, the hash algorithm identifies the node with its key which is confirmed to be non-existent inside the list of sensor devices table information and is prevented from being executed. Proceeding with the registration and verification phase, the DSDV router performs the route generation upon request from RREQ which results in the end-to-end encrypted communication from source to destination.

Attempt to detect the attacker node Ak is done at each stage whether it's between D2D communication, Device to CH communication, Device to BS communication or Device to other Device communication. This helps prevent any possible attacks in each stage, and it greatly increases the network integrity and boosts

the overall performance. It checks whether the sensor node Di ∈ (Local Chain) the offline verification and D2D communication, BS is kicked in when attempting to communicate with for the other CH nodes in the network. Hence the network has multiple checkpoints for the Attacker node Ak to be identified and its effects are eliminated.

3.2 Control and Monitor

Fig. 3 shows the SDN control and monitor architecture developed for our proposed system which is responsible for keeping the authentication key secret, effectively optimising the traffic flow for data packets and troubleshooting the network if any error occurs. The network is based on 5G interconnectivity and traditional Wi-Fi, considering the IoT devices in daily usage such as Laptops, Appliances, Transportation, Medical, etc., also act as a fog environment in the architecture.

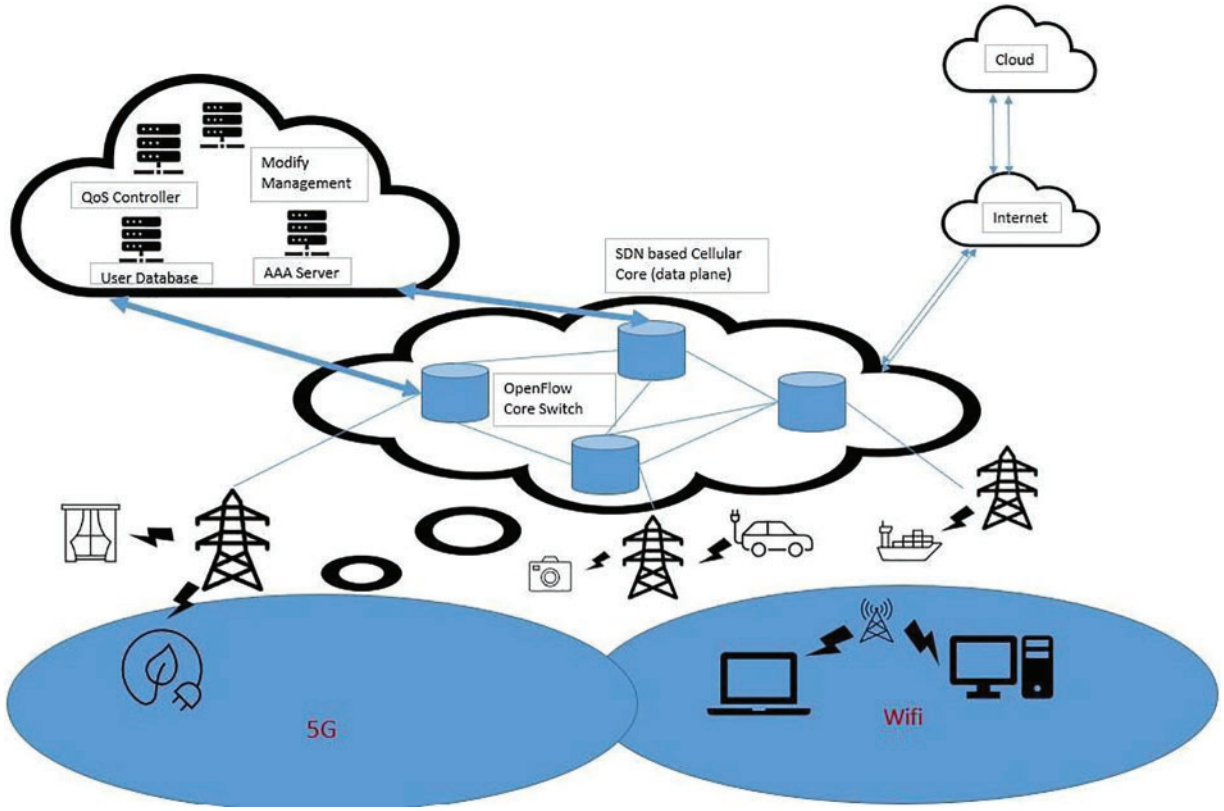

Figure 3: SDN architecture of proposed system

Building on the authentication process, where the secret is generated and the connection is established, SDN (Software-Defined Networking) utilizes several controllers, including the QoS Controller, and components such as the OpenFlow Core Switch, AAA server, and User Database. Once traffic is generated within the network, it must be managed within a controlled environment by SDN. The OpenFlow Controller determines how traffic should flow throughout the network. Doing so results in the encrypted and verified packet being transferred to the designated pathway. Suppose a packet a exists inside the network and it wants to communicate to its destination point d. As soon as the route is identified by the open flow controller, it commands the SDN switch which handles the network data to divert the traffic. This information is directed according to the flow tables which contain the information of the diversion of each data packet within the

route. If a second packet b is attempting to cross through the controller, it must wait in the queue until packet a is transferred and once the process is done then process b is allowed. This ensures that there is no overloading in the system and computational power is kept optimal. QoS controller manages the power delivery for the job. It controls the latency, throughput, and network bandwidth necessary for the process flow. When the process is allocated network bandwidth, the latency and throughput requirements are adjusted accordingly. This process continues and is carried further for processes b, c, . . ., n number of processes. QoS triggers the Hierarchical Token Bucket (HTB) which ensures that all the processes in the queue have allocated bandwidth to them by controlling their inbound and outbound bandwidth settings [21]. OpenvSwitch then supports traffic shaping by policing and shaping the ingressing and egressing traffic from the switch. It depends on the rate-limiting using qdisc by queues or priority based on the network link using HTB [22]. Authentication, Authorization and Accounting (AAA) server is used to authorize access for verifying their authentication from previous explained processes, allowing their traffic to the internet and keep track of it. The policy-based tracking of traffic will make sure that the inbound and outbound activities are ful-filling the policies defined in the QoS controller. Suspicious activities will be immediately reported and handled accordingly. User Database is responsible for recording all the session-wide data being performed. This ensures that the session details are stored in a secure location for tracking sessions whenever necessary.

3.3 Distributed Ledger System

Algorithm 1 describes the complex procedure starting from the RREQ generators of the legitimate device Di, OpenvSwitch traffic ingressing/esgressing, QoS controller mechanism, user Database registration and the formation of the TrustChain ledger system. The process starts from the Di key generation for uniqueness. OpenvSwitch directs the traffic to avoid overflow after the key is verified. AAA server will authorize the traffic and constantly monitor it for any unusual activity. Next, the user database will record the information such as session ID. TrustChain then kicks in and records the transaction within its ledger system making it Sybil-proof.

Blockchain plays a vital role in the proposed system as it consists of distributed ledger systems which are useful in our case. This helps record the transactions among the sensor devices from the beginning till the end and keeps track of it in a chain of records. This makes it temper-proof and almost impossible to alter any transaction record. TrustChain is a Sybil-resistant scalable blockchain making it capable of creating separate blocks of each participating node due to its inherently parallel data structure. This enables the creation of an immutable chain of transactions for each node. Which shows the strength of this architecture which is much more resilient than the Bitcoin data structure and has a limited timespan of transactions. The process starts with the consignment of both nodes. In Fig. 4, suppose process p1 proceeds to be done between A and B points. They both must mutually sign the digital agreement to agree to participate. This process is done after the verification, authorization and route assignment are done from the previously mentioned. After the pact is made between both parties, p1 will transmit data and it is then stored in the TrustChain ledger. The processes are stored in sequence form, and they have their distinctive blocks for existence. Each block observes other blocks for an increase in the TrustChain level for increased integrity. Sybil attacks are hence prevented in this regard and the defense level of the architecture is highly durable from attacks. This process is highly scalable and future-proof in terms of its robustness.

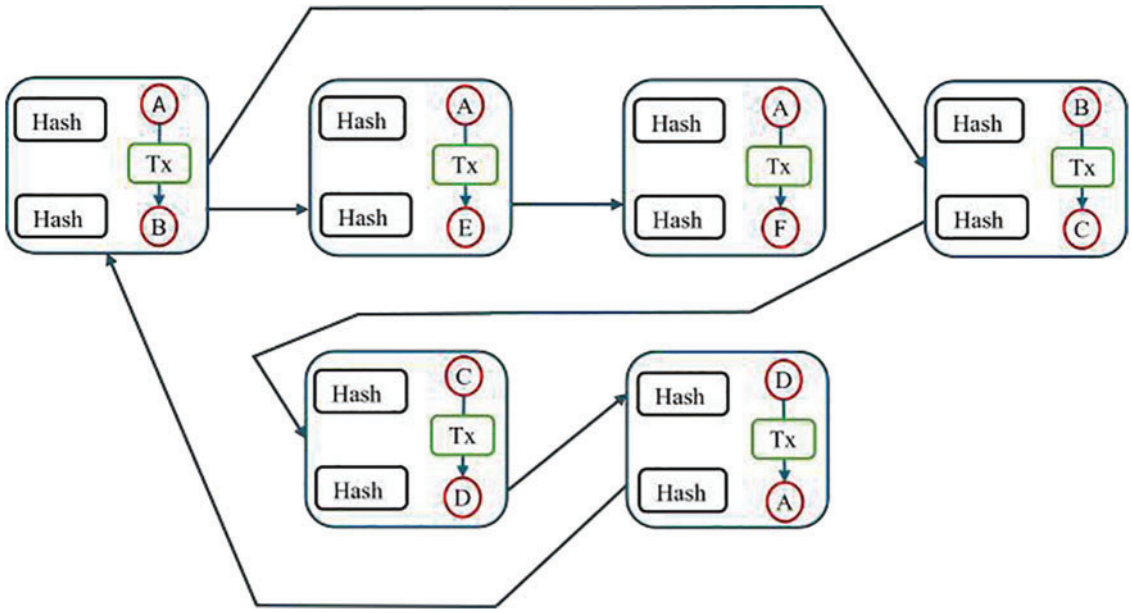

Figure 4: Blockchain model

Algorithm 1: Authentication of devices Di, along with SDN integration and recording in distributed ledger.

Require: Authentication of *Di*, control and flow, and involvement of Blockchain.
Ensure: Verification of *Di*, apply supervision and record using TrustChain.
1: *Di* generate registration RREQ with *Dj*
2: *Di* forward registration RREQ through CH
3: *Dj* Receives *Di* RREQ through CH, where i = 1, 2, 3. . .n − 1
4: **for** (i = 0; i = n, i++)
5: *Dj* check local chain (CH) of *Di*
6: **if**
7: *Di* RREQ ∈ local chain of *Dj*
8: **then,**
9: *Dj* checks hash unique key generated by CH
10: **If**
11: *Di* hash key ∈ hash table of CH
12: **then,**
13: **if**
14: OpenvSwitch check the nature of traffic *Di*
15: *Di* ∈ AAA (authorization)
16: **then,**
17: user database registers *Di* session data
18: Tx creates a unique block of data in the ledger system
19: **Else**
20: *Di* is denied access and considered false node
21: **Else**
22: *Di* is declared attacker node

(Continued)

Algorithm 1 (continued)

23: **Else**
24: *Di* is declared attacker node
25: **end if**
26: Tx register block of node in the ledger
27: CH ← Local chain has shared information from public chain
28: According to *Dj*, devices will update their routing table
29: **return**: verified chain of *Di* devices transactions

4 Evaluation

To evaluate our proposed system, the development was made for a network based on Omnet++ simulation environment which is used to build C++ simulations for networks. This will help us identify the computation power and examine the security analysis of the proposed system. These results are an approximation of how our system would behave in a real-world scenario and conclusions can be drawn from them. Table 1 includes all the abbreviations used in this study for clarification which are also discussed in the later stages.

Table 1: List of abbreviations

Abbreviation	Full form
DSDV	Destination Sequence Distance Vector
WSN	Wireless Sensor Network
CPS	Cyber Physical System
D2D	Device to Device
SDN	Software Defined Networking
BS	Base Station
CH	Cluster Head
PLR	Packet Loss Rate
RREQ	Route Request Packet
QoS	Quality of Service
AAA	Authentication, Authorization and Accounting
HT	Hierarchical Token Bucket

4.1 Analysis of Authentication

In this section, the evaluation of our proposed authentication mechanism is presented. The analysis will consist of the number of sensor devices being authenticated to be verified. In this case, the observation of the computational cost of the multiple stages of the authentication process is covered. This computation cost is considered very important because it can either have positive effects or negative effects on the performance of the system. Determining how the system will behave in such conditions results in a better overall system, less consumption of power and increased efficiency. The model consists of following parameters:

1. MD5 hash function for the key generation along with message digest.
2. Generation of time stamp which is shared via CH and BS.

3. Authentication procedure.

The process which starts from registration and authentication being used in our proposed system minimizes the computational cost which overrides the previous study [4] excluding the processing of the MAC addresses generated by the sensor devices. This processing of a unique key generated by the hash function directly and being processed by the DSDV router results in an effective mechanism and the results shown in Fig. 5 illustrates how our proposed system will behave.

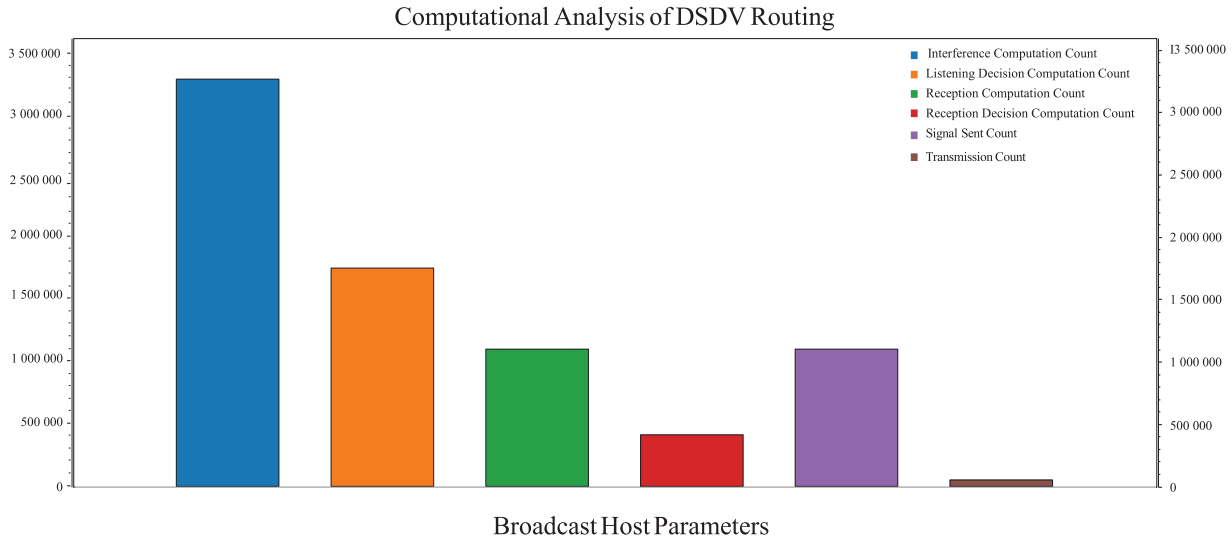

Figure 5: Performance of the proposed authentication method

Various parameters are involved in the performance evaluation for the proposed authentication mechanism starting from the Interference Computational Cost which occurs when signals from different nodes overlap or conflict against themselves. Here, our system behaves proactively in this case. The computational cost of interference in a routing protocol encompasses factors such as collision detection and avoidance, as outlined in the previously mentioned protocol, which incorporates mechanisms to detect and prevent collisions between data packets transmitted by different nodes. Dynamic Channel Allocation, used to mitigate interference, involves computational processes for dynamically allocating communication channels to nodes, avoiding congested or noisy channels. Frequency Hopping or Spread Spectrum Techniques Usage where frequency hopping or spread spectrum techniques help to spread the signal across multiple frequencies, reducing the likelihood of interference. This involves computational processes to manage the frequency assignments. Interference-aware routing is where the routing protocol considers the interference levels when making routing decisions. This involves additional computational steps to evaluate and select routes that minimize interference.

When discussing the Listening Decision computational cost. Consideration of following procedures is kept in mind such as Neighbor Discovery and Maintenance, like many other routing protocols relies on maintaining information about neighboring nodes. The decision to listen to a particular neighbour involves periodic communication to discover and update the status of neighbouring nodes. The proposed system incurs low computational costs associated with processing incoming neighbour advertisements and maintaining a current list of neighbours. Topology Maintenance maintains a routing table that reflects the network's topology. The listening decision involves staying aware of changes in the network topology, such as link breakages or node mobility. Computational costs arise from updating and propagating topology changes

throughout the network. Sequence Number Management while utilizing the sequence numbers to order route updates and avoid inconsistencies. The decision to listen involves managing and comparing sequence numbers to determine the freshness and reliability of received routing information. Computational costs are associated with sequence number comparison and maintenance. Route Computation and Maintenance in DSDV to calculate and maintain routes based on the information received from neighbouring nodes. The listening decision includes processing route updates and recomputing routes when changes occur. Computational costs are incurred during route calculations and updates.

To process the reception computational count, the following measures have to be followed to achieve the desired outcome such as Packet Processing where the reception decision involves processing incoming packets or messages containing routing information. This includes parsing the received data, extracting relevant routing information, and making decisions based on the content of the received packets. Neighbour validation, like other routing protocols, relies on information from neighbouring nodes. The reception decision may involve validating the authenticity and correctness of the received information to ensure that it comes from legitimate neighbours. This includes checking source addresses and sequence numbers. Route Table Updates, upon receiving routing information from neighbours, DSDV needs to update its routing table. This involves decisions on whether to accept or discard the received information and whether it represents a better or worse path to a particular destination. Sequence Number Comparison uses sequence numbers to order route updates and avoid inconsistencies. The reception decision might include comparing the sequence numbers of received updates with the ones already known to the node. This helps determine the freshness and reliability of the received routing information. In a proactive routing protocol such as DSDV, the routing information that is received must be propagated to other nodes within the network. The decision on when and how to propagate this information involves computational costs related to message generation and transmission.

Likewise, the reception decision computational count features and parameters to be followed. These are Packet Processing—Upon receiving routing information from neighbouring nodes, DSDV routers process the incoming packets. This involves parsing the received data, extracting relevant routing information, and making decisions based on the content of the packets. Validation and Verification—The reception process may involve validating the authenticity and correctness of the received information. This includes checking the source of the packets to ensure they are from legitimate neighbouring nodes. Additionally, sequence number verification might be performed to ensure the freshness and reliability of the received routing information. Route Table Update maintains a routing table that reflects the network topology. The reception decision updates the routing table based on the received packets. The computational cost is associated with updating, verifying, and maintaining consistency in the routing table. Sequence Number Comparison uses sequence numbers to order and timestamp routing updates. During the reception decision, a sequence number comparison is performed to determine whether the received update is more recent than the current information in the routing table. Propagation Decisions, depending on the protocol's design, reception decisions may involve determining when and how to propagate the received routing information to other nodes in the network. This process incurs computational costs related to message generation and transmission.

Following are the parameters of the signal send count for the proposed system such as route advertisement where the DSDV router is used as a proactive routing protocol, meaning that nodes periodically advertise their routing information to their neighbours. The count of signal transmitted could refer to the number of times a node sends out route advertisements to update its neighbours about its routing table. Control Packet Transmission uses control packets or messages to convey routing information and update neighbouring nodes. The term "signal send count" is associated with the number of control packets

transmitted by a node within a certain time frame. Network Topology changes in a dynamic *ad-hoc* network due to node mobility or other factors. The signal send count is related to how often a node sends signalling messages in response to changes in the network topology.

Last, the transmission count is responsible for the number of times a node initiates the transmission of routing information or control packets. Route Update Transmission is a proactive routing protocol, and nodes periodically broadcast route updates to their neighbours. The transmission count represents how often a node has broadcasted its routing information to inform neighbouring nodes. Periodic Advertisement Count nodes send periodic advertisements to update their neighbours about the current state of their routing tables. The transmission count could indicate how often these periodic advertisements have been sent. Control Packet Transmission uses control packets or messages to convey routing information and update neighbouring nodes. The transmission count relates to the number of control packets a node sends. Response to Topology Changes in dynamic *ad hoc* networks, topology changes can trigger the need for route updates. The transmission count is associated with the number of times a node transmits route updates in response to changes in the network topology.

Fig. 6 illustrates the performance of the hash functions included in the authentication feature provided by the DSDV router and incorporated in this study for evaluation. This clearly shows that the proposed mechanism is robust as latency and practical application can be expected from this result.

Experiment	Module	Name	Value
TicTocNet	TicTocNet.network1.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network2.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network3.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network4.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network5.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network6.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network7.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network8.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network9.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network10.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network11.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network12.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network13.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network14.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network15.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network16.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network17.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network18.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network19.tictocout.channel	delay	0.1s
TicTocNet	TicTocNet.network20.tictocout.channel	delay	0.1s

Figure 6: Latency table

4.2 Control and Monitoring Analysis

In the evaluation results, the usage of multiple SDN switches, hence, increased the number of controllers. Hop count is considered as the parameter for the simulation environment under examination. The results

generated show that as the number of SDN controllers increases in the network, the hop count is greatly influenced positively. Keeping in mind the requirement of the network topology, these switches can be utilized accordingly. Optimal usage of these will have a huge impact on the network and the results are shown in Fig. 7, which shows that the expected application of our proposed scheme is seamlessly effective in terms of Hop Count.

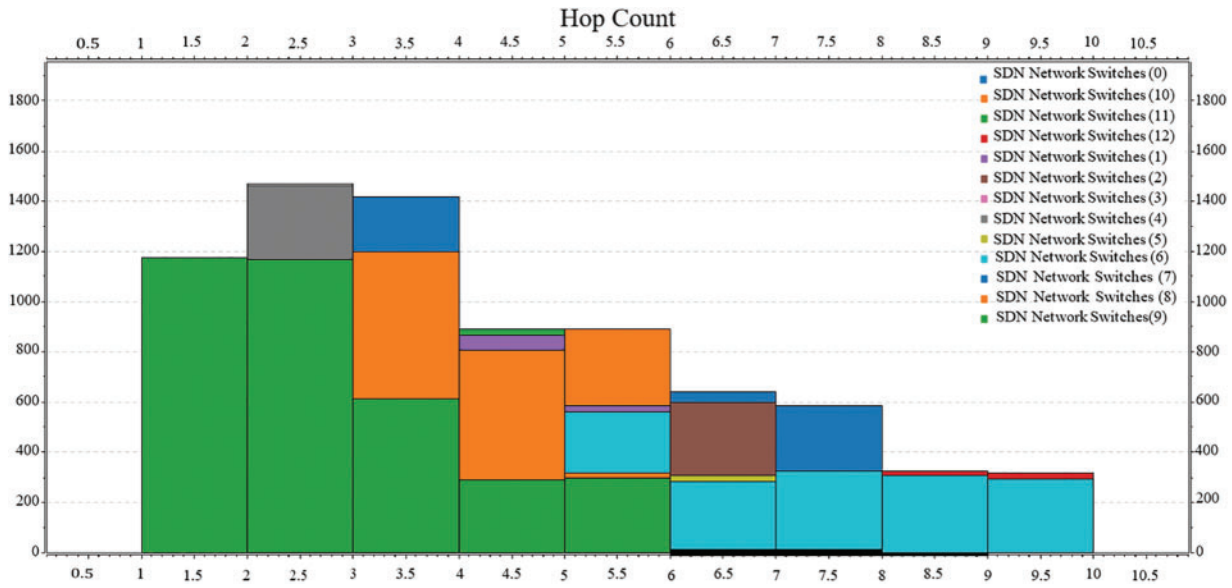

Figure 7: Hop count for SDN

SDN usage is based on the source, which starts from 0 up to 11, which is the destination. The generation of the AAA server mechanism starts from the switch, then the controller, and then comes the AAA server authorization and accountability process and User Database recording procedure.

4.3 Blockchain Performance Analysis

To evaluate the cryptographic features, both participating parties must first be digitally signed to proceed with the correct policies for consignment. This results in the ability to create a TrustChain to track, record and secure the transactions occurring in the network. The proposed system is running the desired blockchain with more than 530 transactions between multiple nodes in the network. Each node is directed towards its distinctive destinations and is unique in nature. Each transaction can run through limited resources which constitute 2 GB RAM, dual-core processing power allocated. This means that less processing power is to be consumed with the evaluation for the architecture and this can be applied in real-world scenarios as well. The latency as mentioned earlier is limited to 0.1 s and that indicates the performance overview of the system for responsiveness.

The results shown in Fig. 8 clearly show the end-to-end delay of packets arriving from one node to another node and the inclusion of the distributed ledger system. The time used here is in milliseconds and the maximum time consumed for the architecture is around 5 ms. The End-to-End delay of arrived packets is denoted by $1e - 1, 2e - 1, \ldots, ne - 1$.

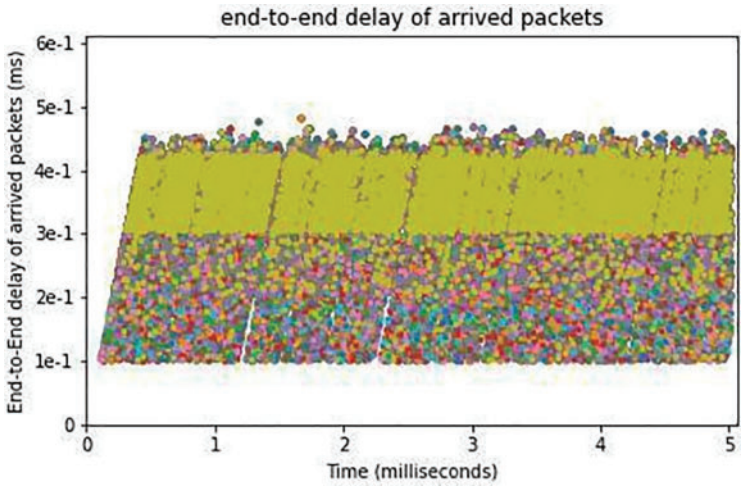

Figure 8: TrustChain time computation in milliseconds

4.4 Security Analysis

The security analysis depends on the number of devices connected to the Internet and through which mechanisms they transfer data. Therefore, the proposed technology can be used to assess the system and determine whether it is sufficiently robust to withstand such attacks.

Various Attack scenarios are created in this manner and their activity has been observed accordingly. Each scenario has its impact and effects accordingly. The ranking of these attacks is based on their severity and thus more complex scenarios can be tested in terms of system capability.

Quantitative evaluation is used here to determine the effects to be assessed, the impacts on the network, and the applications. Thus, any changes can be observed, and performance metrics can be set accordingly, allowing the proposed system to be challenged. There will also be an attack-free case, which will help as a comparative baseline. By following this methodology, the analysis can be performed and investigated.

4.4.1 Attack Injection Denial of Service Attack

Examining, our system starts receiving packets at t = 90 s, the clients are sending and receiving data are denoted as Cn, and the servers are denoted as Sn. DSDV and SDN act as defence barriers against such attacks at the specified attacks. Each attack has a different perspective, more packets received from a client mean an intense attack and as these packets get lower, so is the strength of that attack. In case of the attacks being received with an enormous number of attack packets, the system with its well-tuned design and capabilities always detects those malicious packets from causing hindrance in the flow of working and maintaining a secure environment. Since state-action-reward-state-action (SARSA) routing techniques have been used in this study, they provide a powerful tool to optimize route selection under uncertain GSI and electromagnetic interference. The system effectively detects the malicious packets and even though the attack is much stronger, the attack is always detected at t = 120 s. Fig. 9 shows the evaluation results captured from such scenario.

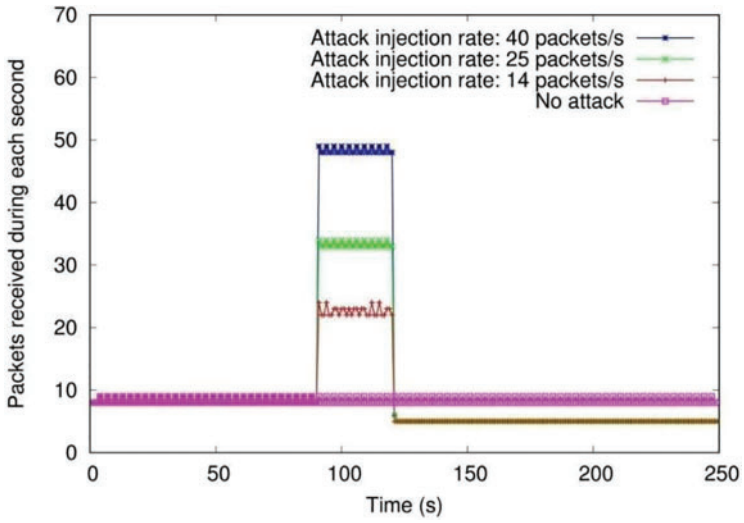

Figure 9: Attack injection denial of service detection

4.4.2 Static Collection Denial of Service Attack

Using anomaly detection rate, here presents the examination of Entropy-based with a fixed threshold. This detection system consists of bounded TX/RX rates per node which helps in making anomaly detection much faster. This is done through more frequent collection of data packets which results in the system successfully detecting the Attack. As more and more frequent collections have occurred, the anomaly detection rate is increased as a result, the system not only intensifies the attack success rate as positive but also makes the detection rate much faster for better protection than in the past. Fig. 10 illustrates the observation of the above scenario of Attack and the behaviour of the proposed system.

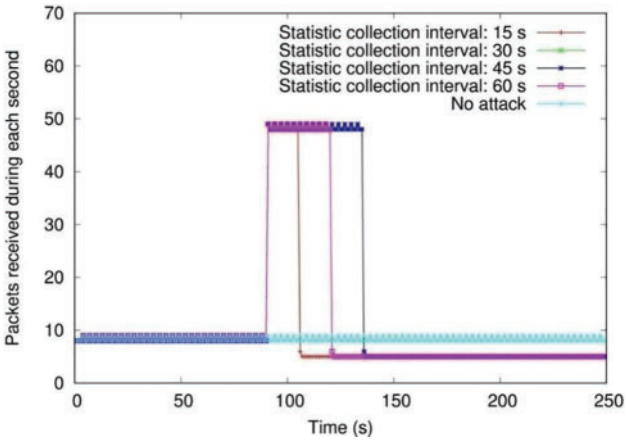

Figure 10: Static collection denial of service detection

4.4.3 Double Spending and Selfish Mining Attack

These types of attacks are examined for the behaviour of our Blockchain model, how it persists and how the performance varies as attacks are more intense. For this purpose, the consensus algorithm when in action is in charge of the block generation and rewarding procedure. Doing so will create a temperless chain

of interconnected blocks. Here, we have the number of nodes denoted by n, and there are multiple points for the hash rate where n is specified. In this experiment, n = 2, 4, 6 for the theoretical values and n = 2, 4, 6 for the simulation were used. The success probability is then observed according to the attacker hash rate and a conclusion can be drawn. The following Figs. 11 and 12 illustrate the Success Probability rate against a Double Spending Attack and the Block Generation rate against a Selfish Mining Attack, respectively.

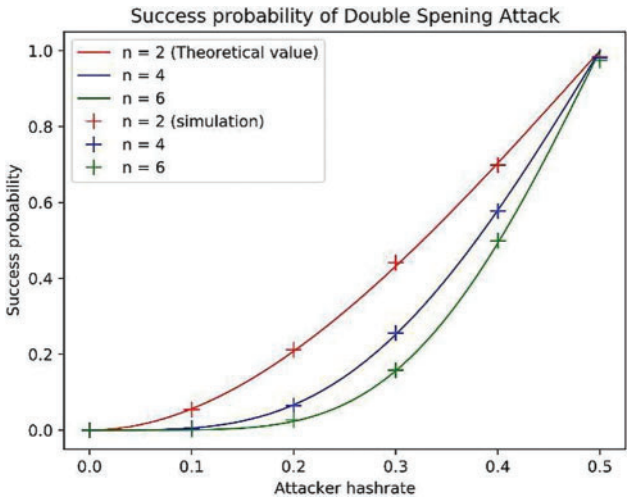

Figure 11: Success probability of double spending attack

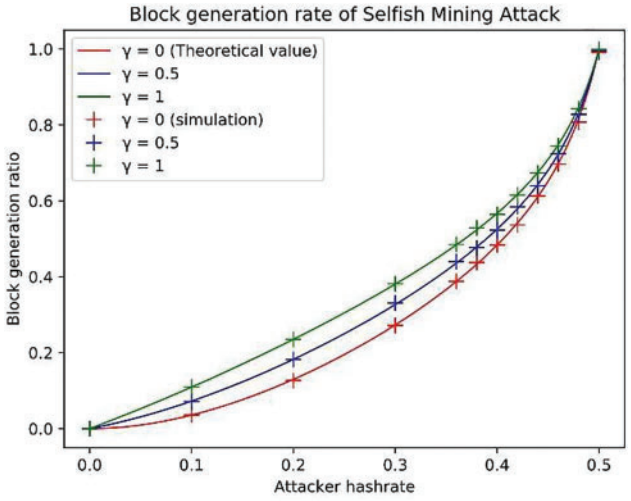

Figure 12: Block generation rate of selfish mining attack

4.5 Real World Scenario

There are various scenarios where the proposed system can be applicable. Mentioning a few of them here, starting with the smart grid system, which consists of the smart energy distribution system. The system can distribute the energy to and from the smart meter system, smart infrastructure and so on. With the help of the proposed system, DSDV combined with SDN can ensure that the smooth flow of energy is ensured. Since it doesn't require any supply chain features hence it can cater for the defence mechanism only.

The second scenario comes from the Industrial Internet of Things (IIoT), which can feature machinery and operating plants. The concept here is that whenever the electrical machinery which is also connected to a central control unit, should be under the umbrella of the security barriers. That ensures the stable performance of the utility and no hindrance is caused. Supply chain management will ensure that the desired outcome can be compared to what is achieved. Hence, the conclusion can be made that the usage of all the machinery is kept secure, while the ingoing and outgoing power consumption usages, target, achieved, and finally, the maintenance can be recorded.

Mentioning these scenarios highlights the potential of this innovation to significantly impact the Internet of Things, particularly in the area of security. When security is considered the most critical aspect of a network, it ensures the technology is robust enough to protect itself and maintain system stability. This, in turn, can be applied to other sensitive domains, such as medicine, surgery, and food safety. This clearly shows the interest in integrating this system for robust solutions with effective results, integrity, and prosperity.

4.6 Emphasis

The proposed system illustrates the indication of performance parameters according to its characteristics. These evaluations will help determine various aspects of the application and its consequences. Similarly, the effectiveness of this architecture makes it robust in Up-to-Date research.

5 Discussion

DSDV routing, SDN packet tracing & Monitoring, and Trustchain hold vast potential for future development. Establishing comprehensive and challenging situations could testify to the model's abilities for endurance, comparing which will contribute to analyzing the setbacks, identifying potential behaviours and improving the system accordingly. This can be made possible with the help of advanced sensor architectures, combined with the discussed security architecture for enhancements in industry standards. Moreover, energy consumption, Latency, and the impact on the system should be the major concerns in this case. Future research should explore optimizing the algorithm according to the advanced network architectures employing sustainability. The ultimate goal is to create an end-to-end secured system that helps contribute to the betterment of the automated industry, ensuring a positive impact on society.

6 Conclusion

In this paper, we proposed a combined architecture of HASH-DSDV, a mutual authentication scheme for CPS connected to form an IoT network. Unique key generators were introduced to ensure the uniqueness of the devices before their routing through DSDV. The MD5 algorithm serves its purpose in forming a local and public chain concerning CH and BS. The SDN switches and controllers work together to direct the pathway using OpenvSwitch, acquire authorization through the AAA server, and followed by the recording of the session data inside the user database for tracking purposes. The integrated TrustChain is a mutually signed distributed ledger system that works on the principles of Blockchain. The ledger system will contribute to the ability to record the transaction from the starting point to the endpoint. All the devices will have distinctive blocks and be mutually connected to form a chain that ensures the transactions are tamper-proof and independent.

The findings are shaped by the scope of the current study, which is restricted to small and medium-sized infrastructure-based architectures. Future work includes implementing the proposed system on a larger scale and in real-world scenarios to evaluate performance, allowing observations to be made accordingly. Furthermore, expanding with AI/ML techniques would enhance the system's reasoning capabilities and improve its detection speed.

Acknowledgment: The authors would like to thank Ajman University, United Arab Emirates for providing the research grant: AU-Funded Research Grant 2023-IRG-ENIT-22.

Funding Statement: This research was funded by Ajman University, AU-Funded Research Grant 2023-IRG-ENIT-22.

Author Contributions: The authors confirm their contribution to the paper as follows: Study conception and design: Jawad Ahmad Ansari, Mohamad Khairi Ishak, and Khalid Ammar; Analysis and interpretation of results: Jawad Ahmad Ansari; Draft manuscript preparation: Jawad Ahmad Ansari, Mohamad Khairi Ishak, and Khalid Ammar. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Ethics Approval: Not applicable.

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

References

1. Ding W, Jing X, Yan Z, Yang LT. A survey on data fusion in internet of things: towards secure and privacy preserving fusion. Inf Fusion. 2019;51:129–44.
2. Jiang Q, Qian Y, Ma J, Ma X, Cheng Q, Wei F. User centric three-factor authentication protocol for cloud assisted wearable devices. Int J Commun Syst. 2019;32(6):e3900.
3. Wang Q, Lin D, Yang P, Zhang Z. An energy efficient compressive sensing-based clustering routing protocol for WSNs. IEEE Sens J. 2019;19(10):3950–60.
4. Adil M, Jan MA, Mastorakis S, Song H, Jadoon MM, Abbas S, et al. Hash-MAC-DSDV: mutual authentication for intelligent iot-based cyber–physical systems. IEEE Internet Things J. 2022;9(22):22173–83. doi:10.1109/JIOT.2021.3083731.
5. Otte P, de Vos M, Pouwelse J. TrustChain: a Sybil-resistant scalable block-chain. Future Gener Comput Syst. 2020;107:770–80. doi:10.1016/j.fu-ture.2017.08.048.
6. Ma W, Liu Y, Xie G, Li R, Yang LT. Security-aware CAN-FD message packing in intelligent automotive cyber-physical systems. IEEE Internet Things J. 2022;9(22):22343–56. doi:10.1109/JIOT.2021.3085422.
7. Yuan B, Lin C, Zhao H, Zou D, Yang LT, Jin H, et al. Secure data transportation with software-defined networking and k-n secret sharing for high-confidence IoT services. IEEE Internet Things J. 2020;7(9):7967–81. doi:10.1109/JIOT.2020.2993587.
8. Wang C, Zhang Y, Chen X, Liang K, Wang Z. SDN-based handover authentication scheme for mobile edge computing in cyber-physical systems. IEEE Internet Things J. 2019;6(5):8692–701. doi:10.1109/JIOT.2019.2922979.
9. Wang D, Zhao N, Song B, Lin P, Yu FR. Resource management for secure computation offloading in softwarized cyber-physical systems. IEEE Internet Things J. 2021;8(11):9294–304. doi:10.1109/JIOT.2021.3057594.
10. Zarca AM, Bernabe JB, Trapero R, Rivera D, Villalobos J, Skarmeta A, et al. Security management architecture for NFV/SDN-aware IoT systems. IEEE Internet Things J. 2019;6(5):8005–20. doi:10.1109/JIOT.2019.2904123.
11. Wu J, Luo S, Wang S, Wang H. NLES: a novel lifetime extension scheme for safety-critical cyber-physical systems using SDN and NFV. IEEE Internet Things J. 2019;6(2):2463–75. doi:10.1109/JIOT.2018.2870294.
12. Mollah MB, Zhao J, Niyato D, Guan Y, Yuen C, Sun S, et al. Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey. IEEE Internet Things J. 2021;8(6):4157–85. doi:10.1109/JIOT.2020.3028368.
13. Ahmad F, Kurugollu F, Adnane A, Hussain R, Hussain F. MARINE: man-in-the-middle attack resistant trust model in connected vehicles. IEEE Internet Things J. 2020;7(4):3310–22. doi:10.1109/JIOT.2020.2967568.
14. Zhao W, Jiang C, Gao H, Yang S, Luo X. Blockchain-enabled cyber–physical systems: a review. IEEE Internet Things J. 2021;8(6):4023–34. doi:10.1109/JIOT.2020.3014864.
15. Hu J, Reed M, Thomos N, AI-Naday MF, Yang K. Securing SDN-controlled IoT networks through edge blockchain. IEEE Internet Things J. 2021;8(4):2102–15. doi:10.1109/JIOT.2020.3017354.

16. Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J. 2021;8(14):11717–31. doi:10.1109/JIOT.2021.3058946.
17. Jahromi AN, Karimipour H, Dehghantanha A, Choo K-KR. Toward detection and attribution of cyber-attacks in IoT-enabled cyber-physical systems. IEEE Internet Things J. 2021;8(17):13712–22. doi:10.1109/JIOT.2021.3067667.
18. Moness M, Moustafa AM. A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy. IEEE Internet Things J. 2016;3(2):134–45. doi:10.1109/JIOT.2015.2478381.
19. Omoniwa B, Hussain R, Javed MA, Bouk SH, Malik SA. Fog/edge computing-based IoT (FECIoT): architecture, applications, and research issues. IEEE Internet Things J. 2019;6(3):4118–49. doi:10.1109/JIOT.2018.2875544.
20. Hatzivasilis G, Papaefstathiou I, Manifavas C. SCOTRES: secure routing for IoT and CPS. IEEE Internet Things J. 2017;4(6):2129–41. doi:10.1109/JIOT.2017.2752801.
21. Devera M. HTB. lartc.org [cited 2017 Apr 11]. Available from: http://lartc.org/manpages/tc-htb.html.
22. OpenvSwitch. Quality of Service (QoS)—Open vSwitch 2.7.90 documentation. The Linux Foun-dation [cited 2017 Apr 20]. Available from: http://docs.openvswitch.org/en/latest/faq/qos/.