International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.1 (2025) pp. 280-290
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

A dynamic integrity and data confidentiality based wireless N2N data communication and security protocol on large networks

Seshagiri Rao Ganta[1,2]*, Naga Malleswara Rao Nallamothu[3]

[1]Research Scholar, Department of Computer Science and Engineering, University College of Engineering, Acharya Nagarjuna University, Guntur, India, AP, India
[2]Lecturer in Computer Engineering, Government Polytechnic for Women, Kakinada, Department of Technical Education, Andhra Pradesh, India
***Corresponding Author Email:** seshagiri.ganta@gmail.com - **ORCID:** 0009-0001-3140-7933

[3]Professor and Head of the Department, Department of CSE-IoT, RVR & JC College of Engineering (A), Guntur, India
Email: nnmrao@rvrjc.ac.in - **ORCID:** 0000-0002-1360-1150

Article Info:

DOI: 10.22399/ijcesen.720
Received : 02 November 2024
Accepted : 05 December 2024

Keywords

Security,
integrity,
VANET,
data confidentiality.

Abstract:

WANET is a network built in an ad hoc network where various connecting devices and moving wireless nodes make connection with the exchange valuable information and wireless medium to one another. As the size of the wireless networks and internet architectures are increasing, there is an exponential demand for data processing and sharing resources in the WANETs. Most of the traditional node authentication models in WANET's require high computational memory and resource constraints for data security and node authentication. In order to overcome these problems in the traditional models, a novel non-linear integrity-based intrusion detection models is designed and implemented in WANETs. In this work, a hybrid security protocol is designed and developed for the node-to-node communication system. In the proposed security protocol, a hybrid integrity approach and encryption framework is implemented on N2N communication process. Experimental results show that the present security protocol has better improvement on different metrics over traditional security approaches.

1. Introduction

Most traditional wireless systems have limited energy, speed of calculation and uncertain communication. To optimize the security model against unregistered access, numerous research projects are undertaken in the wireless networks. In WANETs, each wireless node client is initialized to check its neighbour's authentication against different types of malicious such as Active attacks, Passive attacks and message distraction. Only authorized nodes can access the network for data sharing on the communication channel. Before accessing the communication channel and its resources, all nodes must be authenticated. This work aims at providing novel integrity verification algorithm on variable size data against DOS attack in WANET's . Experimental study show that the present approach has high efficiency hash variation, variable key size and less runtime compared to the existing approaches. The wireless service protocols provide resourceful and pioneering solutions to acquire the objectives of smart transport systems [1]. It is a system to resolve the road traffic issues to avoid congestion, accidents and environmental issues.

The WANET architecture consists of many components such as intelligent wireless nodes fixed with receivers, transceivers, on board units, roadside units, workstations, servers etc. The mobile unit domain, infrastructure domain and management domain are the various modules in WANET architecture. In the mobile unit domain, wireless nodes are fixed with smart devices for communication between wireless node to wireless node and wireless node to infrastructure. In the infrastructure domain, the roadside units and other transceivers maintain the wireless node communication. Wireless node to infrastructure model of communication is performed in this domain.

The WANET security challenge is considered based on the WANET architecture and the security protocols. Many security attacks and threats are faced by WANETs. The network attack is given high priority as the entire network is unsafe. A single network attack affects the entire network. Denial of service attack happens when the wireless node's resource is attacked or when there is a jam in the communication channel, which prevents the critical information. A Sybil attack happens when the attacker acts as if traffic jam had occurred and forces to take alternate routes that affect hundreds of wireless nodes. In the application attack, the attacker manipulates the application content. The actual message is altered or suppressed or changed with false content to harm the other wireless nodes. In the fabrication attack, the false information is transmitted into the network. The messages, warnings, certificates and identities are fabricated. In the alteration attack, the existing data is altered, delayed and transmitted. Social attack happens by sending an emotional message to create problems in the network and to affect the activities of road users. The tunnel attack happens by inserting false information when the GPS signal disappears in the tunnel. The attacker exploits the temporary loss of location information. In the monitoring attack, the attacker silently monitors and tracks the key information by eavesdropping in the network layer. The attacker secretly obtains private conversations, passwords and other confidential data. Every node in the wireless node to wireless node communication model should be authenticated efficiently in order to establish a fair network communication among the nodes. In N2N communication architecture each node is responsible to transfer the messages to the other nodes. In that case each node should be trust worthy. The nodes should not misbehave and should not be malicious. If any of the node is malicious it will collapse the communication performance. In order to ensure that each node is reliable all the nodes must be authenticated at the regular periodical interval.

Some effective authentication algorithms must be developed to ensure the trust worthy of the nodes in the network topology. If the nodes are not authenticated effectively, it is possible to get malicious nodes in the network architecture. Once the malicious nodes are entered into the network, the communication may be collapsed. When a node receives a message from the other node it should forward the message to the next node. If the node is malicious, it may drop the message without forwarding the message to the other node. On the other hand, sometimes, the malicious node may duplicate the data by changing the original data. Similarly, the malicious node may broadcast the unwanted messages to the other nodes to collapse the communication process [2]. Access control has a primary goal, which is to save the usage of network services and system resources by those without authorization. This control attributed to authentication. Generally, access control is one of the most widely required services for network communications as well as individual computer systems. Cryptography has strong ties to mathematics as well as number theory. Hence, the creation of a new design with composite cryptographic techniques is difficult in the absence of sound security analysis, and this usually based on cryptographic reasoning [3].

One method to reach this goal is by learning from others through a review of existing MANET security plans and also the insight of the network for further understanding the techniques of cryptography combined with MANETs for providing a security service that has reasonable features. Various methods can evaluate security design. The primary goal is the provision of proper perspectives by using cryptographic techniques and study basic techniques related to cryptography when they are applied to trust factors. Further study would is required of several of the most common methods of cryptography to see how they are used for dealing with various tasks and for balancing security as well as performance. One of the conventional approaches these days exploitation package engineering style patterns in illustrating the look of object-oriented programming, Similarly, within the security and performance of MANETs, crypto strategies used with success at totally various stages of the packet communication, network bootstrap, and alternative factors that should evaluate.

In RSU communication model entire communication process is carried out by the RSU. In that case securing the RSU will make communication performance better. However, in N2N communication model, each wireless node is responsible to carry out the communication process. In that case, all the nodes must be secure enough ultimately. They represented that effective security mechanism must be applied to all the nodes and all the nodes must be monitored at the regular periodical interval time. Each and every node must be authenticated for its trust worthy. The overhead of adopting high security mechanism will be high [4].

It was discussed about the vertical hand off techniques in VANET [5]. The hand off occurs when the wireless node shifts from one network coverage area to another network coverage area, that is, when there is a change in the access points. The two kinds of hand off algorithm such as handoff execution algorithm and handoff decision algorithm are discussed. The comparison of various handoff execution algorithm related to the scheme, addressing, layers concerned in handover, the network area detection and the technology used are analysed. The comparison of various handoff decision algorithm related to the scheme, parameter evaluation, hand off decision, unnecessary handoff, handoff delay and the limitations are also analysed.

To ensure quality of service of the network, unnecessary handoff and other drawbacks are taken care by the hand off algorithms. Parameters such as handoff delay, hand off decision, the technology used and packet drop rate are validated to maintain the quality of service. The possibility of occurrence of network failure is not considered in this algorithm. When the handoff call dropping probability is measured, it will be easy to keep track of the probability of rejection and this process leads to the improvement of the handoff algorithm. It was presented a survey about WANET security and communication [6]. Research is performed on the message forwarding problems and authentication. The malicious nodes may attack the network, so these attacks should be avoided by some measures.

The WANET authentication parameters are the speed of authentication and confidentiality preservation. Two types of cryptography techniques such as adaptive elliptic curve and enhanced elliptic curve are presented in this study. The key generation phase creates the key with different sizes. The key size range is small, medium and large. There are extra parameters for data transmission such as wireless node identification, from location of the wireless node to the roadside units and the other wireless nodes.

Key and trust management is the critical schemes utilization for external attacks, which those concerning internal attacks are secure routing protocols. The science and art of changing a message into a hidden version which can be read-only by an authorized person, though it can be taken out in its pure form from before encryption by the person intended as the recipient is applied to as message encryption. Keys, small quanta of information used in cryptographic algorithms, are the primary forces that govern over the processes or encryption and decryption.

Encryption techniques are primarily of two types. In symmetric-key cryptosystems, the hidden key utilized for encrypting of a message, while the asymmetric key cryptosystems make use of two distinct keys. Of this, one public key is used to encrypt a message while another key, known as the private key used for decryption. The keys are public or private; they synced in a manner where simply the former one can encrypt texts, and similarly, just the respective latter key can be put to use for decrypting the same message. It is quite not possible to, in any way, reduce the private key even if an attacker were to use a private key. Such key algorithms are quick. In comparison to the asymmetric key algorithms, symmetric ones are usually much faster in the electronic execution.

The process of encryption is mainly vital for ensuring the confidentiality of the message being forwarded. Several methods could be used for the performance of this activity, which has different amounts of initial configuration, communication, and computation. In this approach, the cored idea divided among the certification authorities (CAs [7]. Each CA encompass public and personal try of keys where its open secret's famous to each node, and authorize public keys to nodes when on the QT valedictory their credibleness. The sure CA is requiring staying on-line for reflection of these bindings that modification over time: such keys must be revoked in cases wherever the owner node cannot be sure any longer or isn't any longer a part of the network. The node could refresh its essential try sporadically to make sure the reduction of any probability of a brute-force attack being in turn on its connected personal key.

2. Related works

It has been surveyed the possible attacks to enhance security mechanisms [8]. Various literatures related to attack detection technique have been discussed. By there the various security challenges such as scalability, privacy, mobility, cooperativeness hard delay constraints were discussed. The internet of things techniques is applied to the WANET technology. The various attacks related to internet of things such as inter-wireless node attacks and intra-wireless node attacks are discussed in detail. The types of attacks in the WANET such as Sybil attack, denial of service attack, flooding attack, black hole attack, wormhole attack, bogus information attack, false position information, sensor tampering, illusion attacks, GPS spoofing, replay attack and passive eavesdropping attack are presented in this study. Solutions to multiple behaviour detection are also provided. It has been performed a survey on the trust management in WANETs [9]. This study discusses about the various challenges in trust management due to the dynamic infrastructure, vast, open and decentralized data. The comparative study of the existing models in the trust management in WANETs, the vital issues and the various properties related to the solutions were discussed. The trust models in WANET are entity oriented, data oriented and combination of the entity and data-oriented trust models are presented. The properties such as decentralization, coping with sparsity, scalable, event and location specific, integrated confidence measure, system level security, sensitive to privacy and robustness were also discussed.

It was presented a survey on the authentication schemes for protected communication in WANETs [10]. According to him, the authentication schemes are divided into digital signature, cryptography and message verification techniques. Its taxonomy, pros and cons of the scheme are presented in the paper. The cryptography schemes are asymmetric, symmetric and identity-based cryptography. The asymmetric is classified into public key infrastructure and elliptic curve digital signature algorithm. The symmetric is classified into MAC, hash function and time efficient stream loss tolerant and the signature scheme is classified into single user and group. Finally, the verification scheme is classified into batch and cooperative. A ring signature scheme which is based on the ElGamal signature scheme concept is developed [11].

The actual user identity in this scheme is not disclosed to the neighbor wireless nodes. Also the authors have proved that this scheme provides security against attacks of random adaptive message. The major constraint of this scheme is that the verifier could not know the member who actually generated the signature. The dual RSA algorithm, introduced and it is an upgraded RSA variant [12]. In this technique, they have created two key pairs with the identical private and public exponent. This dual RSA algorithm adds to the computational complexity when it comes to key generation. A proxy re-encryption mechanism was suggested by them.

To construct a secure distributed storage system, and a decentralized code were combined[13]. The user can use this technique to send data from the WANET storage servers to other servers or users without having to download the data. Encoding and forwarding activities over encrypted messages are supported by this proxy re-encryption technology. This strategy, however, incurs additional expense in terms of encoding and forwarding procedures. It was proposed a retrievable data perturbation approach to protect the privacy of WANET outsourced data outsourcing [14]. This method entails four steps: using an upgraded random generator to generate accurate "noise," using an algorithm to disturb the original data by adding noise, using an algorithm for information retrieval to generate the original data from the disturbed data, and finally combining the disturbance method with the access control procedure to ensure access.

They have proposed a Cooperative System for Intelligent Road Safety (COOPERS) to create telematics applications. A cooperative traffic organization between the wireless nodes and infrastructure was developed for vehicular communication systems. System was proposed for drivers' safety and convenience with the advanced driver support system to deal with the independent lane change system. The route tracking and route planning issues are described in the polynomial technique.

It was proposed an integrated project, named safe spot that aims to assist the cooperative system approach for road safety improvements[15]. Wireless node to wireless node communication and wireless node to infrastructure approaches were compared with the wireless node centred applications to analyse the benefits of this integrated approach. A cooperative approach with the goal to enhance the intelligent wireless node and road safety for the drivers was included. Then paper discusses the real time technology assisted the drivers to improve the interaction between the wireless node and the infrastructure. They have presented a solution for green environment in vehicular networks for safe communication. All these communications were happening in wireless infrastructure so there was a need to minimize the total power utilization and emission of other gases.

It was surveyed on vehicular networking related to road safety, infotainment and the road efficiency [16]. The overview of the characteristics, requirements and the challenges of the proposed solutions related to the protocol and the network architecture were emphasised. It was proposed an innovative transport management system for smart cities using different technologies [17]. This study aimed for the security threats, highlighted the advances in the smart transportation for the smart cities and presented with the vision and various challenges to build a forceful transport management system. It was come up with a network architecture with multi-cluster and multi- hop packet radio network [18].

The author proposed a distributed clustering algorithm to deal with the multimedia traffic which assisted to organize the nodes into various clusters. The cluster head are selected and channel scheduling and the allocation of virtual bandwidths to the circuits were presented. The scalability issues of the network were also handled in the proposed system. Simulations were performed in the static as well as in the mobile infrastructure. They have presented adaptive clustering algorithm based on the distributed group mobility for MANETs. This technique derived the linear distance of the node movement based on the node speed and the node direction. Clustering approach aimed to create a stable cluster with an increase in the lifetime of the cluster by minimizing the iterations of the cluster in the dynamic infrastructure. The results showed that the clustering approach gave better results in terms of the cluster head selection, lifetime of the cluster, the average number of clusters and the changes in the cluster heads. They have created a hierarchical organization by presenting a clustering algorithm, for extending the lifetime of the clustering structure. The scheme was constructed which predicts the node mobility and the strength of the neighbourhood nodes based on the over time. A cluster was formed from the hosts and the information about the clusters were highly mobile based on the dynamic topology. This study dealt with the creation of the cluster and maintenance. The selection of cluster heads, mobility patterns, probability of the neighbourhood nodes, clustering structure and the repeated topology variations were considered in the proposed technique [19].

The communication range were calculated for all pair of nodes in every case due to the wireless node obstacles. Here relative forces were applied to the wireless nodes and the movement of the wireless nodes were assessed in the same direction and also in the opposite direction. The modelling of wireless nodes and buildings in the cluster was in the rectangle dimension. The geographical information and the size of the obstacles of the spring clustering enhanced the communication reliability. They have developed a clustering algorithm based on distributed multi-hop cluster system to generate cluster heads through the neighbourhood trail of the wireless nodes. Neighbourhood follow technique was used for one-hop neighbours to update the neighbourhood information. Simultaneously clusters were created and maintained in the disseminated way. Location based service were not provided in this clustering technique due to topology changes. This technique worked with the assumptions to identify the wireless node and the suitable cluster head and then nodes were able to select the cluster head for the stable wireless nodes. Simulation experiments validate the above clustering algorithm[20]. A unique security approach was implemented to address the problem of wormhole-free routing attacks in WANETs [21]. In small WANETs, this strategy is effective at preventing DoS attacks. This model is only suitable for a static wireless network with a small number of wireless node clients.

A safe integrity verification approach for QoS-aware wireless networks was implemented [22]. The major goal of this model is to build a security model for wireless networks that are cognizant of QoS. To check the message integrity in WANETs, they created and implemented an expanded version of the MD5 method. However, to achieve extended security on dynamic WANETs, this approach requires a novel chaotic map function. In tiny wireless networks, author presented a novel handoff wireless node client authentication mechanism [23]. To increase the authentication between the wireless nodes, they devised a novel Wireless node Scan technique. Traditional handoff delays, on the other hand, do not apply to dynamic WANETs.

To overcome the problem of randomization in static and dynamic WANETs, a novel non-linear chaotic map is required. Author, implemented an efficient attack detection technique on limited WANETs [24]. It is very difficult to check the malicious behaviour of the nodes in the wireless network. In this method, all the wireless nodes are authenticated during the network initialization process. This model is used to trace the malicious attacks using the integrity verification approach. These security models result in communication overhead due to high computational time and memory constraints. These models are not at all used for large wireless networks. Traditional integrity verification and authentication models require high computational time and memory on dynamic WANETs.

Traditional integrity verification models in WANETs have low sensitivity and it is limited to small size data and fixed hash size. In order to overcome these limitations, a novel non-linear integrity verification algorithm is designed and implemented on dynamic WANETs. It was implemented an IDS model in the wireless networks to find an attack using the network traffic [25]. This model is not appropriate to the large WANETs due to high computational memory, localization problem and high computational time. Most of the traditional IDS techniques are based on encryption techniques and hash functions to overcome the limitations of localization attacks [26]. As the size of the wireless network increases, these models require high computational time. In dynamic WANETs, chaotic linear functions are not strong to detect and prevent the attack. In this paper, a novel integrity verification model is designed and implemented to detect and prevent the malicious attacks in dynamic WANETs. Proposed IDS model is used to prevent the malicious attacks that occurs at different positions in the WANETs.

In their paper have presented “an extensive survey for WANETs and their related challenges and issues [27]. The key challenges include parameters like signal fading, connectivity, security and privacy, proper routing protocols etc. Signal fading occurs due to static and moving objects between two wireless nodes. The impact of various obstacles ultimately increases the signal fading. As WANET has limited bandwidth, channel congestion occurs in highly dense environment. Further rapidly changing topology may result in frequent disconnections. Increase in transmission power can slightly accomplish the problem”.

It has been given “overview of a concept for mobility models and a network simulator [28,29]. With the help of such a simulation environment, the impacts of wireless node to-wireless node communication on traffic can be explored in details. This is essential for evaluation of the benefits for traffic safety and throughput. The simulation environment set up is a big step forward to a realistic representation of different scenarios. The focus in the research paper is on the routing performance in vehicular ad hoc networks along with an extensive simulation study to compare the routing protocols: AODV, DSR and TORA, using a variety of highway scenarios, characterized by the mobility and size of the networks. The results indicate the reactive routing protocols performance, which is suitable for WANET scenarios in terms of packet delivery ratio, routing load, and end-to-end delay DSR in simulation experiment show overall best performance”.

3. Proposed Model

Most of the WANETs are vulnerable to different kinds of attacks such as Brute force attacks, cloning nodes, and malicious nodes. In WANETs, the authentication and security of the communication among wireless nodes and communication among the Roadside Units (RSUs) are essential to validate the performance of the network. In the traditional hash-based models, the size of the integrity verification code is limited to 512- or 1024-bit size due to computational time and WANET size. In the large WANETs, these models need to enhance with >1024 bit-size as node integrity verification. In this paper, a novel entity authentication model for WANETs is computed to each wireless node as integrity verification. In the malicious WANETs, the suggested entity-based integrity verification approach is employed to create a dynamic-sized hash value for each communication message. Many cars and routes are examined in the proposed model for wireless node identity verification against malicious wireless nodes. The nodes are dynamic and dispersed across a vast area. Wireless nodes communicate with one another through a broadcast technique in this concept. Each wireless node in the dynamic network has a neighbour list with its position, unique identifier, data, and credentials in this model. The fundamental goal of this approach is to ensure that each wireless node's integrity is maintained during data communication.

The CRL validation process is fully bypassed when the proposed hash technique is used. By evaluating the integrity of nodes, this technique can discover malicious and invalid message generating nodes. As a result, the proposed approach increased the batch authentication process' efficiency. In this section, the implementation of proposed integrity verification and signature verification algorithms are discussed with pseudo codes. In the pseudo code, wireless network is initialized with wireless node parameters such as number of wireless node clients, malicious attack nodes and number of iterations for wireless node client communication. In simulation, each wireless node is communicated with its neighbour nodes for data communication.

During the data communication, each wireless node client and its neighbour nodes are checked against integrity verification process. In the integrity computation process, initially wireless node client data is converted into byte array as input message to integrity algorithm. Here, Hash size S is taken as input parameter to the proposed integrity algorithm. If the input data size exceeds the hash size then append the bit sequence 1000…00 to the input data for block processing. Here, the block processing is repeated until S/8 times. Each block is partitioned into sub-blocks of 4 byes each. To each sub-block, a set of mathematical operations such as Cauchy polynomial and non-linear transformations are applied on the sub-block data. This process is repeated to all the blocks. Finally, all the hash values of the block are integrated to form the final integrity value for wireless node client verification. This computed integrity verification value is used in signature verification process for malicious attack detection. To each neighbour node in the data communication, initially integrity value of the node is verified. If the integrity value of the neighbour node is same as the pre-computed integrity value, then the node is tested for signature verification. In the signature verification process, each node’s signature is tested using the bilinear mapping function.

3.1 Improved trust-based ACO for optimal path construction

The mathematical steps for computing the trust probability using ACO in wireless sensor networks.

ACO, or Ant Colony Optimization, is a metaheuristic algorithm inspired by the foraging behaviour of ants. It works by mimicking the way ants search for the shortest path between their nest and a food source. Ants leave pheromone trails as they move, and these pheromones attract other ants to follow the same path. The more ants that travel along a particular path, the stronger the pheromone trail becomes, making it more attractive to other ants.

In the context of wireless sensor networks, ACO can be used to optimize the routing of data packets between nodes. Each node in the network acts as an "ant" and leaves pheromone trails on the paths it takes to communicate with other nodes. The trust probability for each node is computed based on the amount of pheromone it has received from its neighbours, as well as its own inherent "heuristic" value. This trust probability determines the likelihood that a particular node will be selected as the next hop in the data packet's route. To maintain network security, nodes are rewarded or penalized based on their trust value. If a node's trust value falls below a certain threshold, it is considered malicious and removed from the network. By using ACO with a trust-based routing algorithm, wireless sensor networks can achieve both optimal performance and enhanced security.

Finally, nodes are labelled with malicious and non-malicious based on the verification of node signature. In this section, a hybrid heterogeneous integrity checking approach is developed in order to compute the unique hash value for the data encoding and decoding process. In this algorithm, a sequence of non-linear mathematical transformation steps is performed on the input data types for hash value computation as shown below.

Description: In the step 1, input data is converted in to byte array using the medical user ID as S_id and its corresponding record as S.data. This step is repeated to each multi-user data in the given transactions list. In the step 2, input data M is partitioned into k blocks with each size 8bits. In the step 3, padding operation is performed on the input data if the message_size exceeds the block size. In the step 4, each block in the k blocks is partitioned into subblocks of each 32bits. In the step 5, a sequence of mathematical transformations is applied on the subblock partition for hash computation. In the step 6, all the subblock hash values are concatenated as final hash value.

3.2 Encryption model

Phase1:

In this step, each user's attributes and their access policies are used to compute the master key and public key for the data security in the WANET framework. In this step, a randomized hash key-based policies are constructed for the key generation process. G_1, G_2, Z_p represents the cyclic group elements for the data security initialization process.

In this step process, a hybrid vehicle policy-based master-key and public-key are generated using the randomized cyclic group elements. The vehicle master and public key elements of the setup process are constructed based on the bilinear pairing elements.

Phase2:

In this phase, a multi-user initialization parameter such as attributes list, integrity-based policies are used to generate cipher text for the WANET communication. In this phase, CP-ABE access tree policy is used to encode the data based on the policies list.

$$GeoDist(x) = x(1-x)^{p}, \quad p = 0,1,2,\ldots$$

$$UniDist(m) = m/(d1-d2) \quad \text{for } d1 \le m \le d2$$

Let Zr, G1, G2 are multi-user access control based cyclic group elements.

$$\alpha = bilinear\_map(Zr, \mu_{GeoDist(x)});$$

$$Mult\_PubK(g) = bilinear\_map(G1(), max\{\mu_{UniDist(x)}, \mu_{GeoDist(x)});$$

$$Mult\_PubK(gp) = bilinear\_map(G2(), \sigma_{GeoDist(x)});$$

$$Multi\_MasK(\beta) = bilinear\_map(G2(), \sigma_{UniDist(x)});$$

$$Multi\_MasK(g\_\alpha) = bilinear\_map(Mult\_PubK(gp), (\alpha)^{Zr});$$

$$Mult\_PubK(h) = bilinear\_map((Multi\_MasK(\beta))^{Zr}, Mult\_PubK(g));$$

$$Mult\_PubK(g\_\alpha) = bilinear\_map(Multi\_MasK(g\_\alpha), Mult\_PubK(g));$$

$$Multi\_User\_PublicKey = \{g\_\alpha, Mult\_PubK(g), Mult\_PubK(gp), Mult\_PubK(h), Mult\_PubK(g\_\alpha)\}$$

$$Multi\_User\_MasterKey = \{Multi\_MasK(\beta), Multi\_MasK(g\_\alpha)\}$$

Phase 3:

In this phase, wireless node secret key is generated using the master key.

Phase 4:

In the decryption phase, cipher text, secret key, access tree, policies are used to decode the input data.

4. Experimental Results

Experimental results are executed in the NetBeans IDE tool using Java environment by integrating WANET Simulator. In this experimental study, different scenarios are created as per requirement. WANET Simulator is an open-source simulator used for simulating WANET security mechanisms, following simulation parameters are set for simulating proposed mechanisms. Figure 1 is simulation view for the authentication process and figure 2 is packet delivery ratio of SESAF Vs Existing schemes.

Packet Delivery Ratio:

The below graph depicts the packet delivery ratio for the proposed SESAF model over the existing models like LESPP , Handoff Auth , LVAP, and MLAS. On the x-axis proposed and existing models are represented and on the y-axis, PDR (packet delivery

Table 1. *Simulation parameters*

Parameters	Settings
Simulation area	1000 * 1000 m
No of Vehicle	1- 100
No of RSU's	1-25
Transmission range	250 m
Data size	512 bytes
Mac Protocol	IEEE 802.11p
Real-time maps	Open street maps
Simulator	VANET Simulator

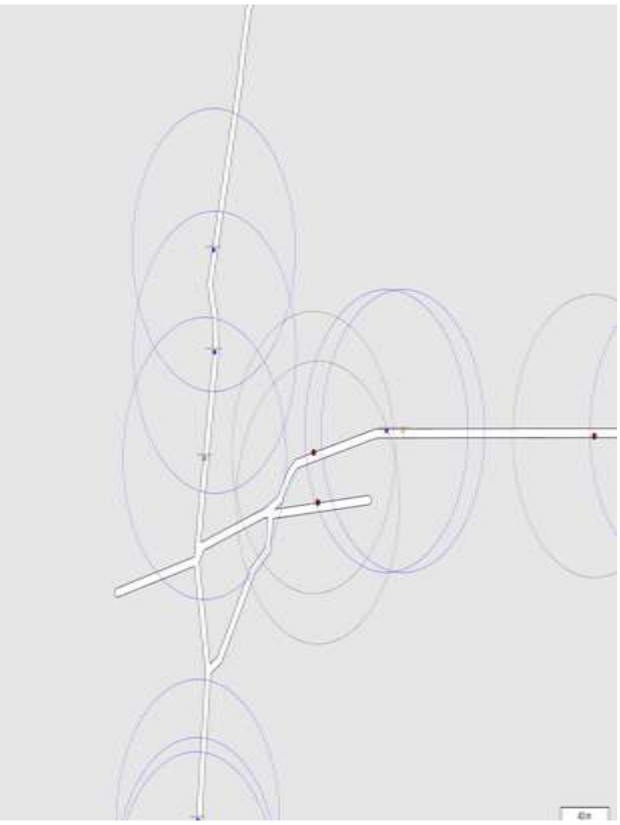

Figure 1 *Simulation view for the authentication process*

ratio) is mentioned. As per the graph, it is observed that the proposed SESAF model has a better packet delivery ratio compared to existing schemes.

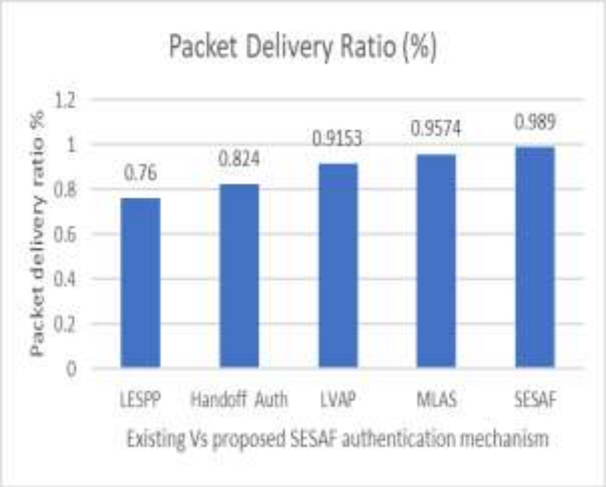

Figure 2. *Packet delivery ratio of SESAF Vs Existing schemes*

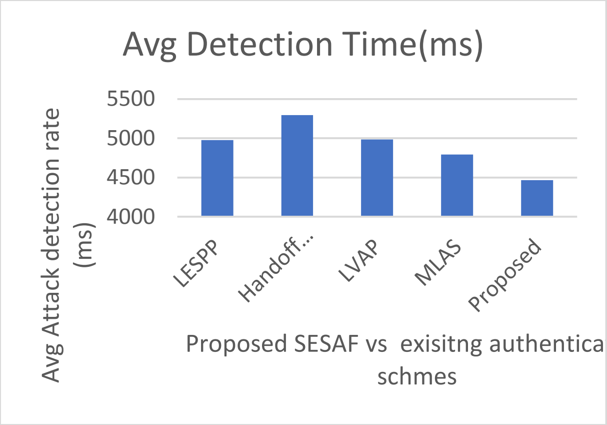

Figure 3. *Average attack detection rate of SESAF Vs Existing schemes*

Average Attack detection rate:

The below graph depicts the Average Attack detection rate of malicious attacks (clone attack) for the proposed SESAF model over the existing models like LESPP, Handoff Authentication, LVAP, and MLAS. On the x-axis proposed and existing models are represented and on the y-axis attack detection rate is mentioned. As per the graph, it is observed that the proposed SESAF model has a better detection rate compared to existing schemes (figure 3).

Average Authentication time:

The below graph depicts the Average Authentication time for the proposed SESAF model over the existing models like LESPP , Handoff Authentication, LVAP, and MLAS.. On the x-axis proposed and existing models are represented and on the y-axis, the Average authentication time is mentioned. As per the graph, it is observed that the proposed SESAF model has a better detection rate compared to existing schemes (figure 4).

Scenario 1: In this scenario simulation is performed to measure the average runtime and attack detection time is taken for the proposed model and existing

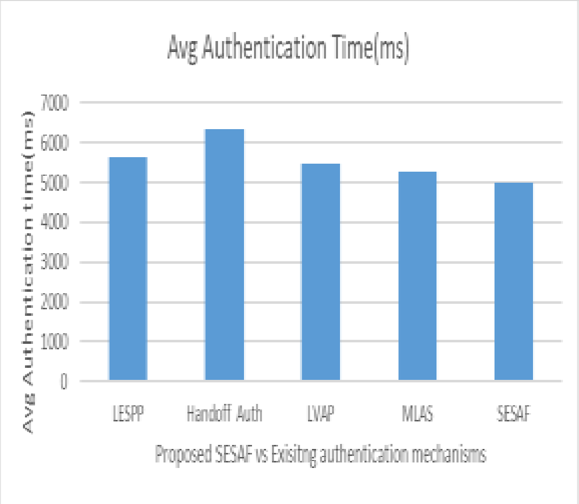

Figure 4. *Average authentication time of SESAF Vs Existing schemes*

integrity verification models like MD5, SHA-512, Whirlpool, and linear chaotic Hash functions. We had considered variable no of wireless nodes 25,30,35,40 and 50 respectively and recorded the average runtime in milliseconds(ms) to verify the integrity of nodes.

Average runtime for Integrity verification:
Figure 5 illustrates the performance of the proposed Hash model to the existing Hash models for integrity verification in terms of Average runtime (ms). As per the graph proposed model has low Avg runtime for integrity verification during WANET communication.

Message Integrity: In our scheme, whenever a wireless node broadcasts a message a hash value of 2048, 4096 will be generated and appended with the message, the same received at the end of the receiver side. The receiver OBU will regenerate the hash value of the received message and compare it with the hash value appended in the received message if an adversary node has altered the message, then a change in hash value is noticed and such messages are discarded. Otherwise, if the hash value is like the hash generated at the source the messages are accepted. Hence the message integrity is achieved in our scheme (figure 6).

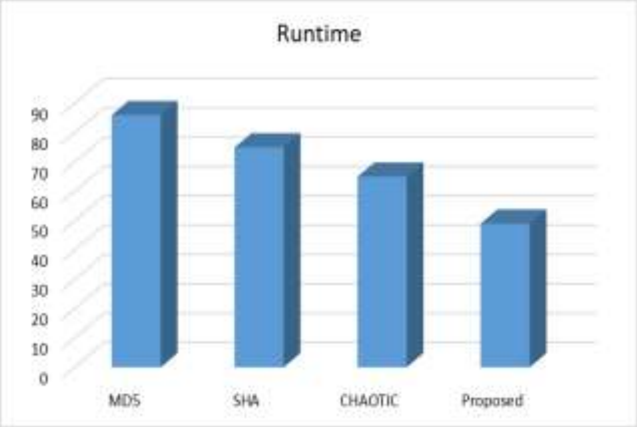

Figure 5. *Comparison of proposed integrity model to existing integrity models*

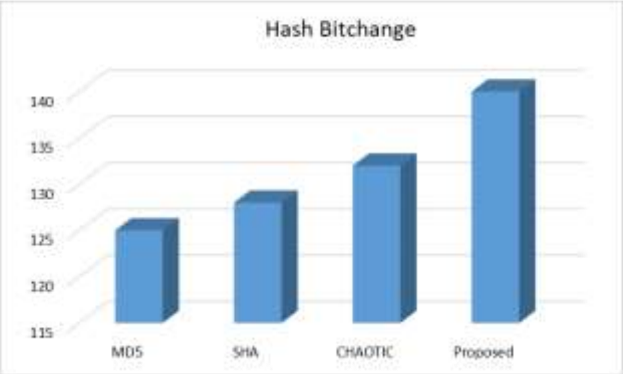

Figure 6. *Comparison of proposed integrity model to existing integrity models for hash bitchange*

5. Conclusion

In this paper, a hybrid security framework is developed to improve the overall data confidentiality of the WANET communication process. Since, most of the conventional approaches are difficult to provide the security during the WANET communication process due to high computation time and delay. Most of the traditional node authentication models in WANET's require high computational memory and resource constraints for data security and node authentication. In order to overcome these problems in the traditional models, a novel non-linear integrity-based intrusion detection models is designed and implemented in WANETs. In this work, a hybrid security protocol is designed and developed for the node-to-node communication system. In the proposed security protocol, a hybrid integrity approach and encryption framework is implemented on N2N communication process. Experimental results show that the present security protocol has better improvement on different metrics over traditional security approaches. Similar works done and reported in the literature [30-43].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]H. Abualola, H. Otrok, R. Mizouni, and S. Singh, (2022). A N2N charging allocation protocol for electric wireless nodes in VANET, *Vehicular*

Communications, 33;100427, doi: 10.1016/j.vehcom.2021.100427.

[2]B. Alaya, (2021). Efficient privacy-preservation scheme for securing urban P2P WANET networks, *Egyptian Informatics Journal*, 22(3);317–328, doi: 10.1016/j.eij.2020.12.002.

[3]B. Alaya and L. Sellami, (2021). Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban WANET networks, *Journal of Information Security and Applications*, 58;102779, doi: 10.1016/j.jisa.2021.102779.

[4]I. Ali, A. Hassan, and F. Li, (2019) Authentication and privacy schemes for vehicular ad hoc networks (WANETs): A survey, *Vehicular Communications,* 16;45–61, doi: 10.1016/j.vehcom.2019.02.002.

[5]B. Amar Bensaber, C. G. Pereira Diaz, and Y. Lahrouni, (2020). Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET, *Journal of Computational Science*, 47;101234, doi: 10.1016/j.jocs.2020.101234.

[6]R. Amin, I. Pali, and V. Sureshkumar, (2021). Software-Defined Network enabled Wireless node to Wireless node secured data transmission protocol in WANETs, *Journal of Information Security and Applications,* 58;102729, doi: 10.1016/j.jisa.2020.102729.

[7]D. Antolino Rivas, J. M. Barceló-Ordinas, M. Guerrero Zapata, and J. D. Morillo-Pozo, (2011). Security on WANETs: Privacy, misbehaving nodes, false information and secure data aggregation, *Journal of Network and Computer Applications*, 34(6);1942–1955, doi: 10.1016/j.jnca.2011.07.006.

[8]M. Arif, G. Wang, V. E. Balas, O. Geman, A. Castiglione, and J. Chen, (2020). SDN based communications privacy-preserving architecture for WANETs using fog computing, *Vehicular Communications*, 26;100265, doi: 10.1016/j.vehcom.2020.100265.

[9]M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, (2019). A survey on security attacks in WANETs: Communication, applications and challenges, *Vehicular Communications*, 19;100179, doi: 10.1016/j.vehcom.2019.100179.

[10]H. Bangui, M. Ge, and B. Buhnova, (2021). A Hybrid Data-driven Model for Intrusion Detection in VANET, *Procedia Computer Science*, 184;516–523, doi: 10.1016/j.procs.2021.03.065.

[11]B. Baruah and S. Dhal, (2021). A secure road condition monitoring scheme in cloud based VANET, *Computer Communications*, 174;131–142, doi: 10.1016/j.comcom.2021.04.027.

[12]W. Ben Jaballah, M. Conti, and C. Lal, (2020). Security and design requirements for software-defined WANETs, *Computer Networks,* 169;107099, doi: 10.1016/j.comnet.2020.107099.

[13]S. Bouakkaz and F. Semchedine, (2020). A certificateless ring signature scheme with batch verification for applications in VANET, *Journal of Information Security and Applications*, 55;102669, doi: 10.1016/j.jisa.2020.102669.

[14]K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, (2019). Effect of security and trustworthiness for a fuzzy cluster management system in WANETs, *Cognitive Systems Research*, 55;153–163, doi: 10.1016/j.cogsys.2019.01.008.

[15]X. Chen, T. Zhang, S. Shen, T. Zhu, and P. Xiong, (2021). An optimized differential privacy scheme with reinforcement learning in VANET, *Computers & Security,* 110;102446, doi: 10.1016/j.cose.2021.102446.

[16]Y. Chen, J. Yuan, and Y. Zhang, (2021). An improved password-authenticated key exchange protocol for VANET, *Vehicular Communications,* 27;100286, doi: 10.1016/j.vehcom.2020.100286.

[17]G. S. Chirayil and A. Thomas, (2016). A Study on Cost Effectiveness and Security of WANET Technologies for Future Enhancement, *Procedia Technology*, 25;356–363, doi: 10.1016/j.protcy.2016.08.118.

[18]E. Diallo, O. Dib, and K. Al Agha, (2022). A scalable blockchain-based scheme for traffic-related data sharing in WANETs, *Blockchain: Research and Applications*, 100087, doi: 10.1016/j.bcra.2022.100087.

[19]R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, (2014). WANET security surveys," *Computer Communications,* 44;1–13, doi: 10.1016/j.comcom.2014.02.020.

[20]X. Feng, Q. Shi, Q. Xie, and L. Liu, (2021). An Efficient Privacy-preserving Authentication Model based on blockchain for WANETs, *Journal of Systems Architecture,* 117;102158, doi: 10.1016/j.sysarc.2021.102158.

[21]S. Goudarzi et al., (2022). A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET, *Ad Hoc Networks*, 128,102782, doi: 10.1016/j.adhoc.2022.102782.

[22]J. Grover, (2022). Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review, *Vehicular Communications*, 34;100458, doi: 10.1016/j.vehcom.2022.100458.

[23]H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, (2017). WANET security challenges and solutions: A survey, *Vehicular Communications*, 7; 7–20, doi: 10.1016/j.vehcom.2017.01.002.

[24]R. Hussain, F. Hussain, and S. Zeadally, (2019). Integration of WANET and 5G Security: A review of design and implementation issues, *Future Generation Computer Systems*, 101,843–864, doi: 10.1016/j.future.2019.07.006.

[25]Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, (2021). Blockchain-based distributed management system for trust in VANET, *Vehicular Communications,* 30,100350, doi: 10.1016/j.vehcom.2021.100350.

[26]M. H. Junejo, A. A.-H. Ab Rahman, R. A. Shaikh, K. M. Yusof, D. Kumar, and I. Memon, (2021). Lightweight Trust Model with Machine Learning scheme for secure privacy in VANET, *Procedia Computer Science,* 194,45–59, doi: 10.1016/j.procs.2021.10.058.

[27]M. H. Junejo, A. A.-H. Ab Rahman, R. A. Shaikh, and K. M. Yusof, (2021). Location Closeness Model for WANETs with Integration of 5G, *Procedia*

Computer Science, 182,71–79, doi: 10.1016/j.procs.2021.02.010.

[28]R. Kaur, R. K. Ramachandran, R. Doss, and L. Pan, (2021). The importance of selecting clustering parameters in WANETs: A survey, *Computer Science Review*, 40,100392, doi: 10.1016/j.cosrev.2021.100392.

[29]S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, (2021). Towards secure and practical consensus for blockchain based VANET, *Information Sciences*, 545,170–187, doi: 10.1016/j.ins.2020.07.060.

[30]A. Jeneba Mary, K. Kuppusamy, & A. Senthilrajan. (2025). Multi-layer access control for cloud data using improved DBSCAN, AES, homomorphic encryption, and RMAAC for text, image, and video. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.837

[31]N. Vidhya, & C. Meenakshi. (2025). Blockchain-Enabled Secure Data Aggregation Routing (BSDAR) Protocol for IoT-Integrated Next-Generation Sensor Networks for Enhanced Security. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.722

[32]MOHAMED, N. N., Yulianta SIREGAR, Nur Arzilawati MD YUNUS, & Fazlina MOHD ALI. (2024). Modelling the Hybrid Security Approach for Secure Data Exchange: A Proof of Concept. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.344

[33]Sushma Polasi, & Hara Gopal Venkata Vajjha. (2024). Secure Drone Communications using MQTT protocol. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.685

[34]Rahul SHANDILYA, & R.K. SHARMA. (2024). ProTECT: A Programmable Threat Evaluation and Control Unit for Zero Trust Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.673

[35]M. Swetha, & G. Appa Rao. (2024). Hybrid Ensemble Lightweight Cryptosystem for Internet of Medical Things Security. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.625

[36]Guven, M. (2024). A Comprehensive Review of Large Language Models in Cyber Security. *International Journal of Computational and Experimental Science and Engineering*, 10(3). https://doi.org/10.22399/ijcesen.469

[37]Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.417

[38]Vutukuru, S. R., & Srinivasa Chakravarthi Lade. (2025). CoralMatrix: A Scalable and Robust Secure Framework for Enhancing IoT Cybersecurity. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.825

[39]V. Ananthakrishna, & Chandra Shekhar Yadav. (2025). QP-ChainSZKP: A Quantum-Proof Blockchain Framework for Scalable and Secure Cloud Applications. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.718

[40]OZER, E., & AYDOS, H. (2024). Performance and Security of AES, DES, and RSA in Hybrid Systems: An Empirical Analysis of Triple Encryption. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.694

[41]Kosaraju Chaitanya, & Gnanasekaran Dhanabalan. (2024). Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.613

[42]Godavarthi, S., & G., D. V. R. (2024). Federated Learning's Dynamic Defense Against Byzantine Attacks: Integrating SIFT-Wavelet and Differential Privacy for Byzantine Grade Levels Detection. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.538

[43]guven, mesut. (2024). Dynamic Malware Analysis Using a Sandbox Environment, Network Traffic Logs, and Artificial Intelligence. *International Journal of Computational and Experimental Science and Engineering*, 10(3). https://doi.org/10.22399/ijcesen.460