MIDDLEWARE BASED NODE AUTHENTICATION FRAMEWORK FOR IOT NETWORK

[1]Abdul Malik Ansari
[1]M.Tech Research Scholar
[1]Dept. of Computer Science and Engineering,
[1]Central University of Rajasthan, Ajmer, India

Abstract:* Security and protection are among the most squeezing worries that have developed with the Internet. As systems extended and turned out to be more open, security hones moved to guarantee insurance of the consistently developing Internet, its clients, and information. Today, the Internet of Things (IoT) is rising as another sort of system that associates everything to everybody, all over. Subsequently, the edge of resistance for security and protection moves toward becoming smaller on the grounds that a break may prompt vast scale irreversible harm. One element that eases the security concerns is validation. While diverse confirmation plans are utilized as a part of vertical system storehouses, a typical personality and validation plot is expected to address the heterogeneity in IoT and to coordinate the distinctive conventions exhibit in IoT. In this paper, a light weight secure framework for authentication, identity management, and a flexible trust management for secure and compatible communication channel among IoT devices is proposed.

***Keywords* - security, authentication, network, internet of things.**

I. Introduction

Wireless sensor networks (WSNs) are progressive ad hoc networks that are made out of a considerable amount of asset compelled sensor hubs that are arbitrarily conveyed over the objective district. Such systems give financially savvy keys to an extent of observing issues, for example, military front lines, medicinal services administrations, brilliant matrix systems, and omnipresent processing situations. Besides, the propelled advances in the field of WSNs that a sensor joined to a gadget speaks with other encompassing sensors are empowering to open the IoT condition. Therefore, WSNs have been broadly examined, both in the scholarly and modern fields [1].

The Internet of Things (IoT) presents a few difficulties that prevent its wide arrangement. By and by, the innovation is advancing with several billions of things will be associated with the Internet by 2020. IoT will traverse an extensive variety of unmistakable correspondence advancements utilized as a part of the diverse islands of systems of things, and will likewise bring about a lot of information alluded to as "IoT Big Data". In IoT, the worry identified with Big Data isn't especially identified with the extent of the information, but instead to the heterogeneity of the information as far as configuration, sort, and semantics. Security and protection are likewise extra concerns and constitute fundamental IoT impediments. Applying security conspires in IoT requires watchful thought since the prerequisites and gadget capacities are not quite the same as in customary systems. In addition, these plans must be versatile with a specific end goal to traverse the several billions of things; along these lines another administration worldview should be conjured [2]. WSNs are ending up always various and interconnected with the IOT, in this way showing new openings yet in addition challenges which should be tended to. A case of such would be a remote client who needs to get to a specific sensor hub of the WSN. Such a client should be approved and, if done decidedly, permitted to accumulate information from or send summons to the sensor hub. Since the most essential and particular normal for WSNs is their asset obliged engineering (i.e., constrained computational and communicational abilities), a lightweight security arrangement is required, in this manner encouraging the security configuration to be more judicious. A key test is the way to empower the foundation of a mutual cryptographic key in a safe and lightweight way, between the sensor hub and the client outside the system [3].

II. Related work

In this area different studies have been done on the different techniques. Jung et al. [1] portray how these assaults function, and propose an improved unknown client validation and key assentation plot in light of a symmetric cryptosystem in WSNs to address the greater part of the previously mentioned vulnerabilities. The examination demonstrates that the proposed plot enhances the level of security, and is additionally more effective with respect to other related plans.

Salman et al. [2] proposed an personality based verification plot for heterogeneous IoT. The rightness of the proposed plot is tried with the AVISPA instrument and results demonstrated that our plan is safe to disguise, man-in-the-center, and replay assaults. Turkanovic et al. [3] concentrated on such a situation and proposes a novel client verification and key assentation plot for heterogeneous impromptu remote sensor systems. The proposed conspire empowers a remote client to safely arrange a session key with a general sensor hub, utilizing a lightweight key understanding convention. The proposed plot guarantees shared validation between the client, sensor hub, and the door hub (GWN), in spite of the fact that the GWN is never reached by the client. The proposed plot has been adjusted to the asset obliged design of the WSN, along these lines it utilizes just basic hash and XOR calculations. The proposed conspire handles these dangers and the difficulties postured by the IOT, by guaranteeing high security and execution highlights.

Ferrag et al. [4] exhibited an extensive overview of verification conventions for Internet of Things (IoT). Particularly in excess of forty validation conventions produced for or connected with regards to the IoT are chosen and analyzed in detail. These conventions are sorted in view of the objective condition: (1) Machine to Machine Communications (M2M), (2) Internet of Vehicles (IoV), (3) Internet of Energy (IoE), and (4) Internet of Sensors (IoS). Danger models, countermeasures, and formal security check procedures utilized as a part of validation conventions for the IoT are displayed. Likewise a scientific classification and correlation of validation conventions that are created for the IoT as far as system display, particular security objectives, principle forms, calculation multifaceted nature, and correspondence overhead are given. In view of the ebb and flow review, open issues are recognized and future research bearings are proposed.

Wazid et al. [5] proposed a new decentralized lightweight verification and key understanding plan for VANETs. In the proposed conspire, there are three kinds of common validations: 1) between vehicles; 2) amongst vehicles and their individual group heads; and 3) between bunch heads and their particular roadside units. Aside from these verifications, the proposed conspire additionally keeps up mystery keys between roadside units for their protected correspondences.

The thorough formal and casual security examination demonstrates that the proposed plot is competent to shield different malevolent assaults. Besides, the ns-2 reproduction exhibits the practicability of the proposed plot in VANET condition.

Bu et al. [6] considered disseminated joined confirmation and interruption location with information combination in such MANETs. Multimodal biometrics are sent to work with interruption identification frameworks (IDSs) to mitigate the weaknesses of unimodal biometric frameworks. Since every gadget in the system has estimation and estimation restrictions, in excess of one gadget should be picked, and perceptions can be melded to build perception precision utilizing Dempster– Shafer hypothesis for information combination. The framework chooses whether client validation (or IDS input) is required and which biosensors (or IDSs) ought to be picked, contingent upon the security act. The choices are made in a completely dispersed way by every confirmation gadget and IDS. Recreation comes about are displayed to demonstrate the adequacy of the proposed conspire.

Xiao et al. [7] introduced a biometric verification model to upgrade data security in specially appointed systems. Utilizing this model, an associate is verified with biometrics when joining a current gathering even without the nearness of a confirmation server. Hashmi et al. [8] examined the adequacy of ebb and flow confirmation instrument for MANETs in adapting to the Sybil assault, the framework necessity postured by these systems and materialness of these components to various types of specially appointed systems and distinguished open research issues that should be tended to by the up and coming age of validation components for MANETs.

Sanzgiri et al. [9] portrayed these dangers, particularly demonstrating their consequences for specially appointed on-request remove vector and dynamic source directing. This convention, named verified directing for impromptu systems (ARAN), utilizes open key cryptographic components to overcome every single distinguished assault. Sarvabhatla et al. [10] proposed an enhanced validation plot which opposes all major cryptographic assaults, with less calculation cost contrasted with A.K Das et al., and other comparative plans.

III. Proposed Framework

Some of the current IoT devices are not even able to make use of current authentication techniques due to heterogeneous in nature. To design or improve a light weight secure framework for authentication, identity management, and a flexible trust management for secure and compatible communication channel among IoT devices.

- In the proposed mechanism a resourceful middleware has been introduced for authentication purpose.
- This middleware works as a gateway between IoT devices and provides user authentication along with the node authentication.
- When a user or a node wants to access a node in network, it is authenticated via middleware by using authentication mechanism.
- This middleware framework is able to handle heterogeneous network messages.
- These messages are converted and sent to the intended receiver in the network.
- By implementing this proposed framework, Problem of interoperability among IoT networks can be solved.
-

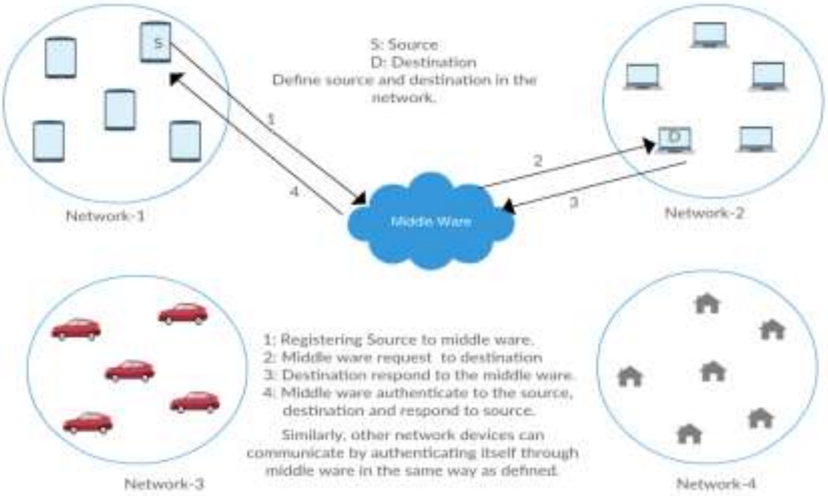

S
S: Source
D: Destination
Define source and destination in the network.
1
2
3
4
D
Network-1
Middle Ware
Network-2
1: Registering Source to middle ware.
2: Middle ware request to destination
3: Destination respond to the middle ware.
4: Middle ware authenticate to the source, destination and respond to source.
Similarly, other network devices can communicate by authenticating itself through middle ware in the same way as defined.
Network-3
Network-4

Fig. 1 Authentication model of the proposed framework

This proposed mechanism consists of following three phases:

1. **Registration phase-** The aim of this phase is to register the user and node with middleware framework. The registration is done by using some identity based registration technique.
2. **Authentication phase-**This scheme is developed to adapt the IoT notion, the user sends the authentication message to a desired sensor node of the network via middleware framework. The aim of this phase is to negotiate a key between the user and the sensor node in a way that both will individually contribute to the secret key. After successfully negotiating the key, they can use it to securely communicate in any encrypted matter. In order to achieve the secure key negotiation, a lightweight key agreement method is used which involves mutual authentication between all parties.
3. **Node addition phase-** Node can stop working due to battery life, hardware failure and can be physically destroyed or stolen. In such type of cases nodes to be replaced so that network functionality can be maintained. Moreover some additional nodes can be added as per requirement. Every node to be added in the network, node registration is required. Our proposed scheme enables nodes to be simply and dynamically added to the network without causing any changes in the established security states of the current entities within the network.

IV. FLOW CHART OF PROPOSED FRAMEWORK

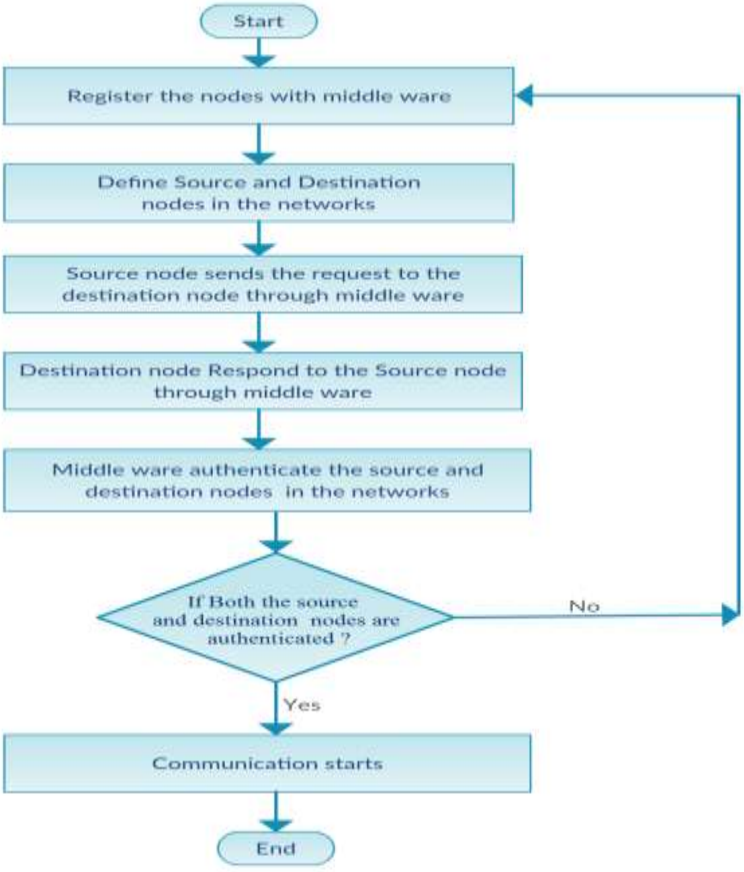

Start
Register the nodes with middle ware
Define Source and Destination nodes in the networks
Source node sends the request to the destination node through middle ware
Destination node Respond to the Source node through middle ware
Middle ware authenticate the source and destination nodes in the networks
If Both the source and destination nodes are authenticated ?
No
Yes
Communication starts
End

Fig.2. Flow Chart of Proposed Technique

V. IMPLEMENTATION OF PROPOSED TECHNIQUE

The methodology of the proposed work is given in the below section with description;

Step 1: The proposed methodology is described for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things. First we will design the wireless sensor network with fixed height and width. We will design the area of propose work with given formula;

$$\boldsymbol{Area\ of\ Network = Height\ X\ Width}$$

After the network area developments, define some nodes in the network area and also define the source node and the destination node for the simulation of proposed work. Then set the coverage area for each node for discovering the route in the wireless sensor network. When source nodes with the destination node are defined then we initialized the network middleware for the authentication of nodes within the network and define a main middleware. Define the x coordinates and y coordinates of N number of nodes using the given algorithm and considers a node as a source and destination.

Network deployment algorithm

```
Define height = 1000
Define width = 1000
Define N number of nodes for the simulation of network
For i = 1 to N
        Plot_node(i)=coordinate(X, Y)
        Define node name = N(i)
        Source_Node = random(N)
        Destination_Node = random(N)
        If Source_Node == Destination_Node
                Source_Node = rand(N)
                Destination_Node = rand(N)
        Else
        Source_Node = Source_Node
        Destination_Node = Destination_Node
        End
        Define Source_Node as source
        Define Destination_Node as destination
End
```

Step 2: After the first step we register the all node using the node number and generate a key for the authentication purpose. When the registration process done then we define the coverpaage set, and then find distance between nodes. After the calculation of distance we create the route using the given algorithms,

Coverage area creation algorithm and routing algorithm

```
$Define\ Coverage\_set = \frac{20 * width\ of\ network}{100}$
For i = 1 to N
    Cov_set(i) = Coverage_set(N)
    Cov_list(N, i) = Cov_set(i)
End
For i = 1 to N
    Route(i) = Source_Node
    Route(i) = Source_Node(Cov_se(N))
    If Cov_set(Source_Node) == empty
        Next_node = random
    End
    Repeat while destination is not found
    Route(last) = Destination_Node
End
```

Step 3: After the route generation, network middleware check the authentication of source node and destination node using the authentication process of IoT system. To verify the node registration we use the infrastructure as an authentication service to authenticate the node ID during communication.

Step 4: If attackers are founded then we analyze the network and calculate the QoS performance metrics like Throughput, Delay, Bit Error Rate, Execution time and Storage Consumption on the basis of iteration. So the proposed work is simulated on iteration based technique so we can calculate the best efficiency of the proposed work.

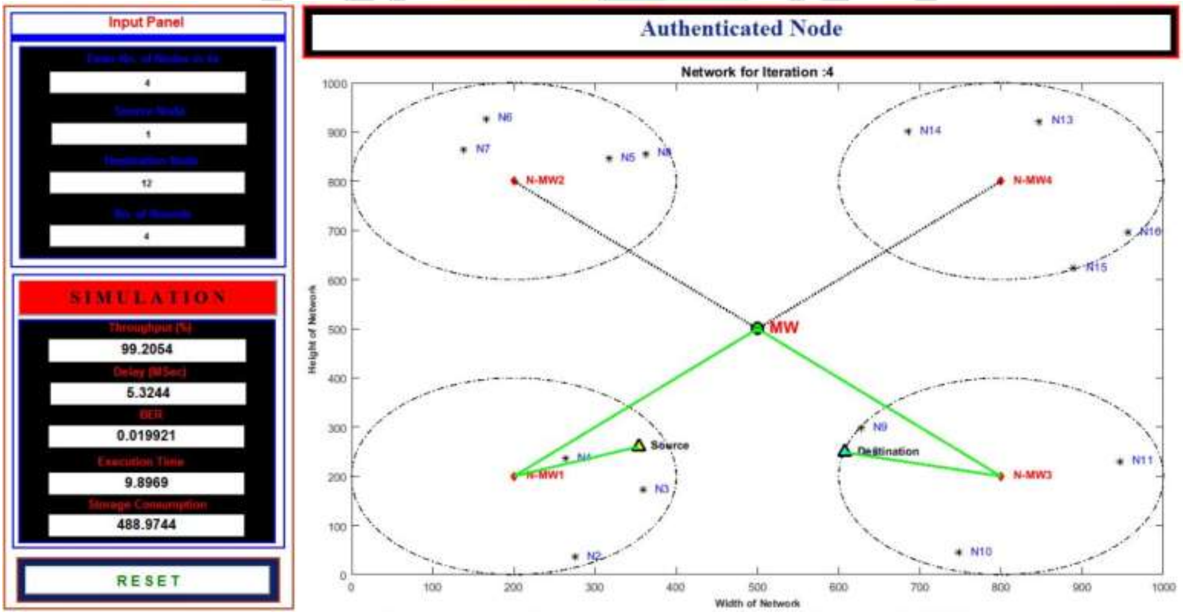
VI. Results

This section presents results of the proposed algorithm. Various parameters are used for implementation of the proposed technique. These are defined as follows:

Table 1: Parameters of Proposed Technique

Parameters	Proposed Work	Base Paper Work
Number of packets	1000	700
Average Memory Storage (Bytes)	462	132
Number of Nodes	20 - 100	50
Authentication	4 Step Authentication	4 Step Authentication

Above table shows the parameters like number of packets, average memory storage, number of nodes, and authentication for the proposed technique.



Input Panel

Enter No. of Nodes in Itr: 4

Source Node: 1

Destination Node: 12

No. of Rounds: 4

SIMULATION

Throughput (%): 99.2054

Delay (MSec): 5.3244

BER: 0.019921

Execution Time: 9.8969

Storage Consumption: 488.9744

Fig.2 Simulation of Proposed Technique

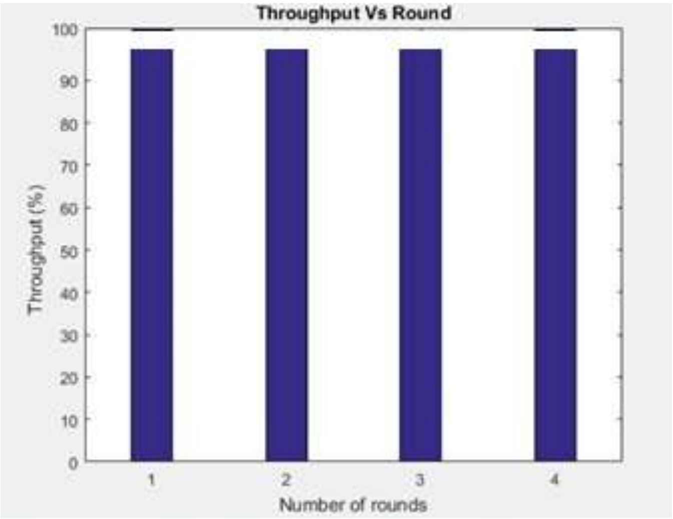


Fig.3. Throughput Comparison with Round

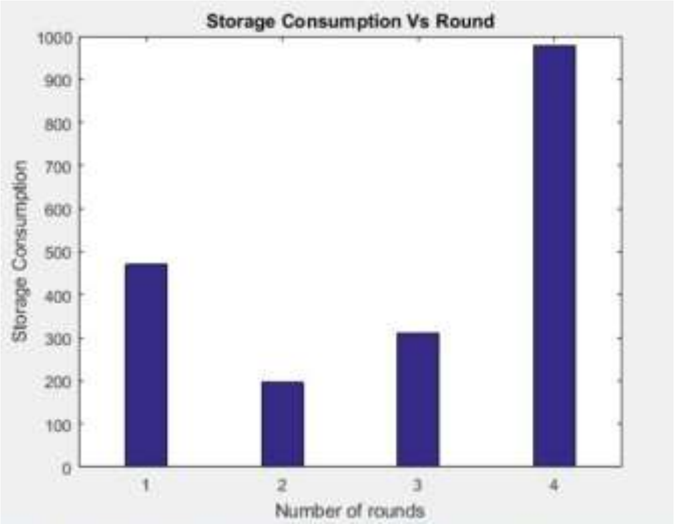


Fig. 4. Storage Consumption Comparison with Round (Bytes)

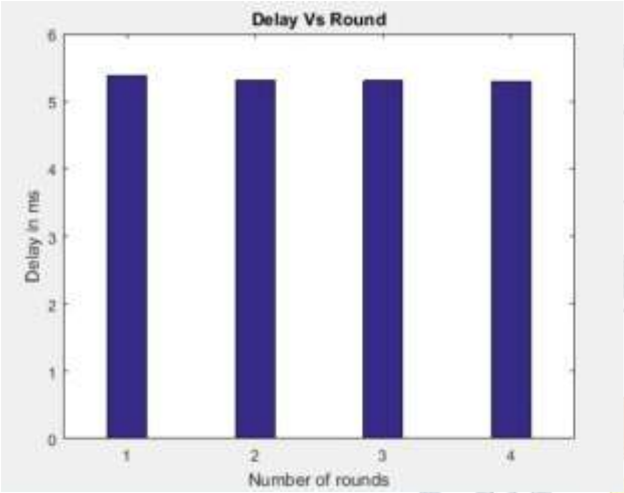


Fig. 5. Delay Comparison with Round

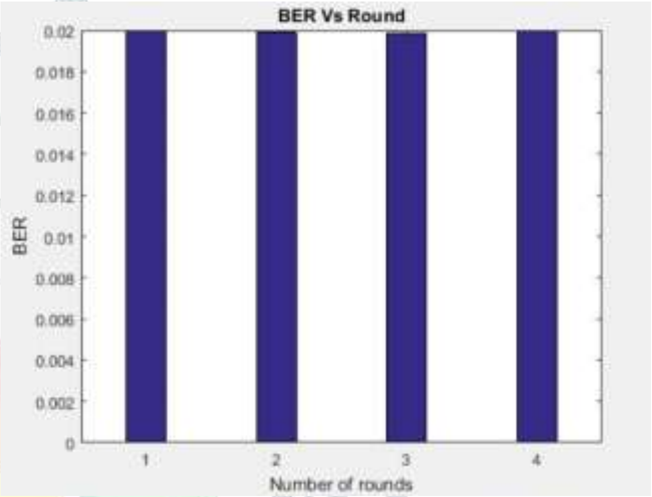


Fig. 6. BER Comparison with Round

Above figures shows simulation of the proposed technique and its comparison in terms of throughput, delay, bit error rate, and storage consumption.

Table 2: Comparison of proposed work on the basis of storage parameters

S No.	Before Reg. Phase 0	Before Reg. Phase 1	Before Reg. Phase 2	After Reg. Phase 0	Authentication Phase 0	Authentication Phase 1	Authentication Phase 2	Authentication Phase 3	After Authentication Phase 0
1	430	449	438	462	474	472	482	487	469
2	28	98	67	56	152	196	193	324	76
3	29	79	85	51	51	51	149	266	68
4	29	29	29	29	29	29	67	100	26
5	29	29	29	29	29	29	73	102	26
6	29	29	29	29	29	29	77	118	26
7	29	29	29	29	29	29	64	98	26
8	29	29	29	29	29	29	62	97	26
9	29	29	29	29	29	29	66	94	26
10	26	26	26	26	26	26	26	26	26

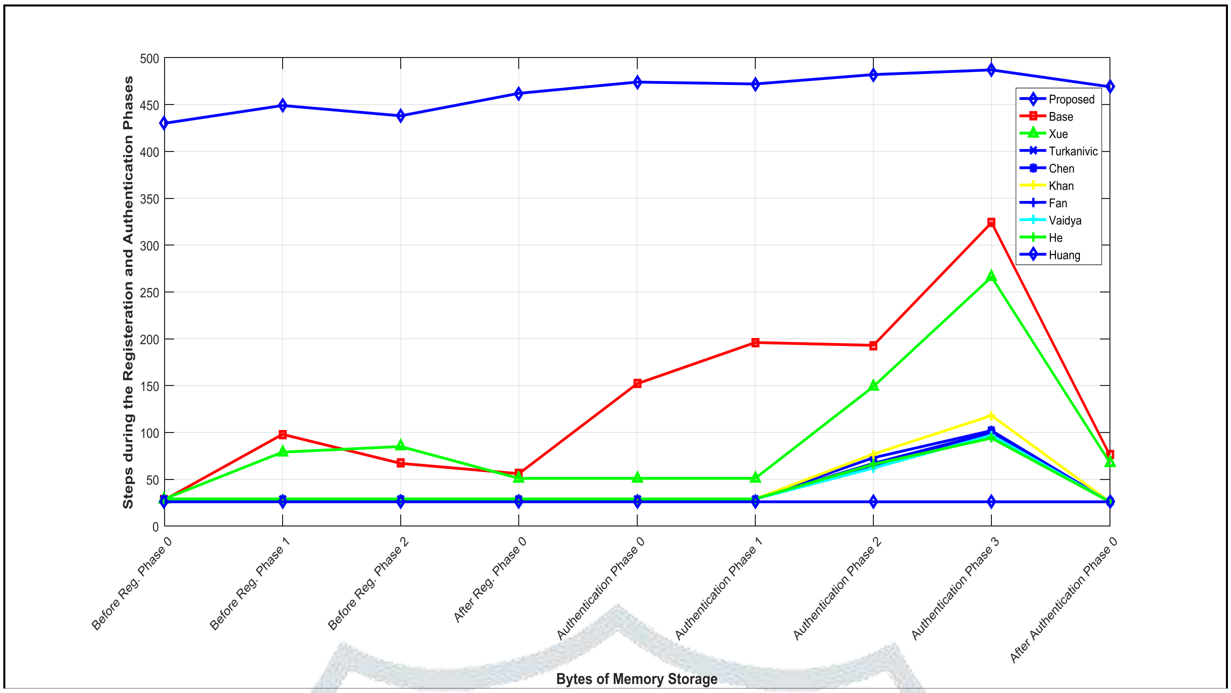


Fig. 7. Parameter Comparison of Proposed Technique

Above table and figure represents the comparison of proposed work and existing work on the basis of memory storage. From the figure, it is clear that the memory storage of proposed work is better than already existing work and the maximum memory storage is mark as 487 bytes for proposed work. The average memory storage of proposed work is 462 bytes and base paper work is 132 bytes.

VII. CONCLUSION

Security is a crucial concern in networks. In particular, with IoT, security implications are even more pronounced since the impact of attacks is more drastic, mainly because IoT includes a wide range of applications from simple location awareness to very critical healthcare uses. In this paper, a light weight secure framework for authentication, identity management, and a flexible trust management for secure and compatible communication channel among IoT devices is proposed. Various parameters like number of packets, average memory storage, number of nodes, and authentication are used to implement proposed technique. To evaluate and compare the results parameters like throughput, delay, bit error rate, and storage consumption are used. Experimental Results demonstrate that the proposed technique works efficiently. In future we may further refine the proposed framework and its functionality.

REFERENCES

[1] Jaewook Jung, Jiye Kim, Younsung Choi, Dongho Won, "An Anonymous User Authentication and Key Agreement Scheme Based on a Symmetric Cryptosystem in Wireless Sensor Networks", 2016, pp. 1-30.

[2] Ola Salman Sarah Abdallah Imad H. Elhajj Ali Chehab Ayman Kayssi, "Identity-Based Authentication Scheme for the Internet of Things", IEEE Symposium on Computers and Communication, 2016.

[3] Muhamed Turkanovic, Boštjan Brumen, Marko Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion", 2014, pp. 96–112.

[4] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, Lei Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey", Security and Communication Networks, 2017, pp. 1-41.

[5] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Vanga Odelu, Vanga Odelu, Kisung Park, YoungHo Park, "Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks, IEEE, 2017, pp. 1-15.

[6] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang, "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks", IEEE, Transactions on Vehicular Technology, Vol. 60, No. 3, MARCH 2011, pp. 1025-1036.

[7] Qinghan Xiao, "A Biometric Authentication Approach for High Security Ad-Hoc Networks", IEEE, 2004, pp. 250-256.

[8] Sarosh Hashmi, John Brooke, "Authentication Mechanisms for Mobile Ad-hoc Networks and Resistance to Sybil Attack", IEEE, International Conference on Emerging Security Information, Systems and Technologies, 2008, pp. 120-126.

[9] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, "Authenticated Routing for Ad Hoc Networks", IEEE, Journal on Selected Areas in Communications, Vol. 23, No. 3, March 2005, pp. 598-610.

[10] Mrudula Sarvabhatla, Chandra Sekhar Vorugunti, "A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN", IEEE, International Conference of Emerging Applications of Information Technology, 2014, pp. 367-372.