International Journal of Engineering & Technology, 7 (1.9) (2018) 34-40

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Conditional privacy-preserving authentication with access likability for roaming service over internet of things

P. S Uma Priyadarsini [1] *, P. Sriramya [2]

[1] Assistant Professor Research Scholar, Department of Computer Science and Engineering, Saveetha University Department of Computer Science and Engineering, Saveetha School of Engineering Saveetha University, Thandalam, Chennai, Tamil Nadu
[2] Associate Professor Research Scholar, Department of Computer Science and Engineering, Saveetha University Department of Computer Science and Engineering, Saveetha School of Engineering Saveetha University, Thandalam, Chennai, Tamil Nadu
**Corresponding author E-mail: umaps2014@gmail.com*

Abstract

Today the mobile subscribers can access the internet service whenever they want or wherever they are because of the roaming service. The necessity of accessing pervasively for the developing paradigm of networking such as the Internet of Things (IoT) is accomplished through this facility. In order to provide universal roaming service which is secure and privacy preserving at the multilevel, this paper proposes a privacy-preserving validation which is conditional with access likability called CPAL for roaming service. By utilizing a method of group signature it provides linking function of an anonymous user. This method has the capability to keep the identity of the users concealed and makes the authorized bodies possible to connect all the access information of the same user even without knowing the user's real identity. In order to connect the access information from the user for enhancing the service, the foreign operators who are authorized or the service providers particularly uses the master linking key possessed by the trust linking server. In order to examine user's likings, the individual access information is used but user's identity is not disclosed. Subscribers can further make use of this functionality to probe the service usage without being identified. The proposed method also has the efficiency to simultaneously revoke a group of users. Comprehensive analysis of CPAL demonstrates that it can withstand many security threats and more adjustable in privacy preservation as compared to the other techniques. Assessment of its performance further proves the efficiency of CPAL with regards to communication and computation overhead. Future work would include the extension of CPAL scheme to effectively withstand internal attackers and design the lightweight secure and privacy-preserving scheme that will support IoT devices of large group.

Keywords: *Conditional Privacy-Preserving, Internet of Things; Wireless Networks.*

1. Introduction

Wireless networks and mobile devices are pervasive computing technologies that has tremendously improved the digital information availability and also transformed the landscape of the way we access and use them. The Internet of Things is yet another technology that extends digital resources to the real world. Today many applications implement mobile interaction with tagged objects for various services.

There is an unprecedented development of wireless technologies paving way for pervasive network accesses via smartphone, laptop PC and vehicle. Accessing network-based applications such as e-commerce, e-learning and social-networking has become highly convenient. Nevertheless, such technology advancement also raises many security and privacy concerns such as unwarranted revelation of sensitive information by users who are not watchful or not experienced, ease of wireless signal interruption to the growing complexity of devices in surveillance field. The utmost concern in deploying wireless access networks is achieving security, privacy, efficiency and liability. The nature of wireless access network is open and distributed. Hence, the network access control is implemented to deal with the free riders and malicious attacks. The second serious concern is to ensure user privacy particularly in banking, commercial transactions, and e-healthcare. It does not only mean hiding the true identity of the user but it also involves connecting amongst the transactions of the same anonymous user. Thirdly, it is important to examine and determine fraudulent users and insider attacks under due consent of the law authority in order to provide user accountability. Lastly, the efficiency of each access point (AP) should be such that it is able to validate many requests at the appropriate time and manner. This will ensure that the connections of roaming users are not ceased.

Most of the prior security research on wireless access networks deduced that there is a trusted third party which controls all keying materials. And secured information and privacy details are disclosed through this. However, the trusted third party has a limitation wherein the security network has to face the problem of key escrow and single point of failure. By conceding the trusted third party, the security measures of the whole system can be broken by the opponent. Because of this fact the security and privacy preservation must be accomplished devoid of any trusted third party.

Most often users connect to the wireless access networks under different environments and characters. For example, a patrol car that belongs to a police station can be driven by a policeman or an employee of a hospital can drive an ambulance etc. So depending upon the user's roles in the society their identity can be defined as the collective attribute. Essential and non-essential attributes are the two types of user identity information. The essential attributes consists of social security number that would be unique and the nonessential attributes consists of information associated with different social roles as mentioned in the example earlier. Wireless

access network is based on the idea of user group existence. So the grouping could be any type of organization such as a company, government agency etc.

The role of user group manager is to manage a group of network users and subscription to network services is done on behalf of its group members. Complete exposure of the user happens if their essential attributes are revealed. But revealing of non-essential attribute does not display the identity of the user. From NO's point of view, the user's nonessential attribute information is adequate with regards to billing and accountability. Therefore taking into account all these above factors, the necessities for an efficient authentication framework which is privacy-preserving and accountable is furnished below:

1) Security: It plays a vital role between users and APs by achieving a common explicit authentication and key establishment. This helps in preventing free riders and adversaries from accessing the network illegally.
2) Anonymity and non-linkability: One sided and simultaneous anonymous authentication between users and APs is achieved through this factor. In this communication link the user identity information is not revealed except the authenticity of a network user. No two different communication sessions can be connected to the same particular user. It should also not be possible for adversary, other users, NO and the user group manager to link a communication connection to the corresponding and genuine user.
3) Complete privacy and accountability of user: In the course of maintaining accountability, the information of the users disclosed is very minimum. Hence it is essential that a given communication link for NO should be credited only to the role information of the user. And the complete identity information of the user is not revealed. The equivalent nonessential attribute information for billing and user accountability purposes can be retrieved by NO provided that a communication connection is given. Also it is possible for the law authority to connect the corresponding responsible network user with the assistance from NO and user group manager.
4) Efficiency: The efficiency of each AP is expected to be aptly able to validate many access requests.
5) Dynamic participation: Addition of new users and elimination of undermined users must be allowed.
6) No trusted third party: The framework can evade single point of failure since there is a limitation for all entities.

2. Literature survey

The air interface of fixed broadband wireless access (BWA) systems are detailed in this standard. It assists multimedia services and allows rapid worldwide deployment of highly developed multivendor BWA products. Essentially, the medium access control layer (MAC) assists a point-to-multipoint structure with a possible mesh topology. It supports multiple physical layer (PHY) specifications, each of which is matched to specific operational surroundings. This standard is a coherent whole since it reviews and integrates IEEE Std 802.16-2001, IEEE Std 802.16a™-2003, and IEEE Std 802.16c™-2002 [1].

Based on NovaGenesis (NG) this work proposes a concept and operation of a Future Internet of things. Taking into account the present developments, the key contributions of this paper are proposal of a novel service-defined architecture where the arrangement of device is a reflex of the real service needs, ICN benefits integration with named-services, Identifying IoT devices, services, and data continuously by using self-verifiable naming. It also demonstrates the feasibility NovaGenesis as an option for the existing IoT architectures [2].

In order to communicate between various communications devices in vehicular ad hoc systems, this paper initially identifies the needs of specific design. And based on group signature and methods of identity (ID)-based signature, it proposes a secure and privacy-preserving protocol. Besides guarantee the needs of security and privacy, the proposed protocol provide the desired traceability of each vehicle whenever there is a dispute and the ID of the message sender has to be disclosed by the authority. In order to validate the competency of the proposed protocol in a range of application circumstances under different road systems, comprehensive simulation is conducted [3].

In order to overcome the problem on anonymous authentication for safety messages with authority traceability, this paper proposes an efficient conditional privacy preservation (ECPP) protocol in vehicular ad hoc networks (VANETs). It is distinguished by the production of on-the-fly short-time anonymous keys between On-Board Units (OBUs) and Roadside Units (RSUs), which can provide unknown authentication and privacy tracking very quickly. In this process it reduces the required storage for short-time anonymous keys. Extensive examination proves the advantages of the proposed protocol [4].

This paper investigates mobile communication with attached everyday objects and related information which are based on the Internet of Things and its technologies. Perci architecture has three components. Communication of mobile devices with attached physical objects that are associated with Web services and provide information for their invocation. Interaction with tagged objects and associated services are handled by the modules of the generic universal client on mobile devices. The interaction proxy not only manages the communication between Web services and mobile clients but also keeps them independent from each other [5].

This paper delves into the present scenario of the Internet of Things and then examines the possible integration of many "Intranets" of Things into a more heterogeneous network. This paper also highlights the key technical problems associated with wireless- and mobility and then discusses in a nutshell of how some of these challenges can be overcome. Subsequently, this will facilitate the advancement of IoT's and its acceptance in the next few years. Further, this paper also explains a case study on the IoT protocol architecture [6].

With an aim to concurrently accomplish security, privacy, accountability and competency without involvement of any trusted third party for wireless access networks, this paper presents a novel authentication framework named APEA. Integration of new key management protocol, an adapted construction of short group signature and batch verification helps APEA to accomplish the key goals devoid of any trusted third party. The implementation and performance results prove that a large number of access requests can be verified judiciously with the help of APEA [7].

This paper presents an analysis of PBNFCP and its drawbacks. So in order to overcome these security issues such as failure to thwart the claimed security properties, this paper proposes a secure and highly competent authentication protocol (SEAP) for NFC applications. It utilizes the lifetime-based pseudonyms and is simulated for the formal security verification using the widely-accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. In contrast to the existing authentication protocols, simulation results prove that SEAP is secure and efficient for NFC applications [8].

A lightweight secure and privacy preserving V2G connection System is proposed in this paper. It not only thwarts EVs from acting maliciously but also assures the financial profits of the grid. By generating their own pseudonym identities the EVs protect their private information. The lightweight overhead reduces the messages that are exchanged during (dis)charging sessions and subsequently provides all security requirements. Results prove that the total communication and computation load for V2G connection, especially for EVs are considerably reduced with the help of the proposed scheme [9].

With an aim to reveal the limitations in designing a practical authentication system for mobile devices, this paper employs three schemes namely Truong et al.'s scheme, Li et al.'s scheme, and Zhang et al.'s Scheme as case studies. So this study shows that Truong et al.'s scheme fails to accomplish some key security goals such as failure to defend against known session-specific temporary information attack, failure to endure main compromise impersona-

tion attack and poor usability. Li et al.'s privacy-preserving scheme has serious limitations making it virtually impossible for any practical use. Zhang et al. scheme is vulnerable to collusion and replay attack. Therefore, this study further examines the essential causes for these limitations and outlines enhancement over Truong et al.'s scheme [10].

This paper proposes a protocol with an order of pseudonyms depending on the time period of their usage. In contrast to other protocols, the proposed protocol merely anticipates a truthful-but-curious behavior from otherwise fully trusted authorities. User's privacy is completely protected to the point of time the protocol is honestly followed by the user. The user's identity is disclosed to the concerned authorities in the event of harmful acts. CRL maintenance is not essential in this protocol and the authenticity and safety of the message and corresponding pseudonym for the receiver are assured by the inherent mechanism. The proposed protocol proves its resilience against various attacks. In addition, the protocol is simulated for examining the network performance which proves its feasibility with regards to end-to-end delay and packet delivery ratio [11].

The existing validation techniques for privacy protection usually necessitate powerful devices such as smartphones and smart watches. This paper delves into the performance evaluation of cryptographic and math methods on the smart devices. In addition, this study also shows that the validation system for privacy protection with smart devices can be efficient and provide user privacy and security and can be implemented on smart devices. Future work would involve analysis of optimization tricks for pairing-based schemes that run on smart devices [12].

A trust and privacy preserving handover authentication protocol for wireless networks is presented in this paper. In the process of handover authentication, the new protocol accomplishes the user anonymity, untraceability and trust authentication. This is possible using the advantages of mechanism of pseudo identity and elliptic curve cryptography. Evaluation of security and performance proves that the new protocol is capable of universality, robust security and also enhanced performance in comparison to other protocols [13].

In order to improve security and privacy for V2V communications in intelligent transportation network, this paper proposes a novel authentication scheme (PPDAS). Independent of an additional key management, PPDAS exploits the advantage of bilinear pairing to compute encryption key. This will enable vehicles to establish session key by protecting their privacy. The dual verification uses the identity and behaviour authentication in order to enhance accuracy in decision-making. By treating the identity as an element of entity in order to understand fine-grained authorization and access control, the proposed scheme can also be a comprehensive element based key agreement protocol [14].

This paper proposes an approach that helps the user to protect their privacy when they avail the location based services. The protocol is built by employing a deniable authentication in such a way that the user privacy is not compromised when submitting the accurate location information to SP. This highly enhances the service quality of SP. The requirement of privacy is becoming paramount and keeping this in mind, the privacy-enhanced version maintains the user identity and location unknown even to SP [15].

This paper analyses the security drawbacks of PBNFCP in checking the claimed security properties. With an aim to solve these limitations, this paper utilizes lifetime-based pseudonyms to provide an authentication protocol (SEAP) which is highly safe and efficient for NFC applications. The simulation of SEAP using AVISPA (Automated Validation of Internet Security Protocols and Applications) tool proves the efficiency and security of the system [16].

This paper is a survey of the most significant aspects of the IoT. It concentrates on the developments that have progressed so far and challenges that calls for further research. The outcome of confluence of activities carried out in different fields of knowledge can only impact towards the development of the Internet of Things. Since it involves highly integrated network of work, this survey is primarily conducted for those willing to approach such intricate discipline and help in its advancement. The most relevant challenges that will be faced by the research community are discussed elaborately [17].

A new architecture that efficiently works for the emergency tetra network in the Italian Emilia-Romagna region is presented in this paper. A migration plan that guarantees a switching off wholly transparent from the standpoint of the user is further discussed in the paper. There are close to five hundred radio terminals (users) and five BTS sites at Ferrara province and the process of migration would commence from there. Having a complete distributed architecture even in a network with significantly high BTS nodes is considered as the key contribution of this work [18].

This paper provides an overview of the EPS network architecture. It comprises of the functionalities provided by the E-UTRAN access network and the evolved packet core network. The EPS bearer's concept and their related quality of service attributes can be a potential tool for different kinds of services to the end user. The EPS can make available multiple data flows with different QoSs based upon the type of the application. Therefore, a UE can be engaged in a VoIP call that necessitates assured delay and bit rate simultaneously as browsing the web with a best effort QoS [19].

Considering the complex connection of the surviving multi-vendor resources and the use of the emergency portable EDFAs, this paper introduces an emergency optical network design problem. In disaster recovery, the first available resources are the surviving multi-vendor optical nodes and fiber links. To model an emergency network planning for this design problem, an Integer linear programming (ILP) formulation is used. The selection of emergency interconnection location of the multi-vendor networks and positioning of the portable EDFAs are done optimally. Estimations and assessments are performed which proves the credibility of the proposed approach and the use of emergency portable EDFAs [20].

3. Proposed work

The proposed work comprises of five key modules. MS acts as a medium of data transfer. VAS provides the authentication of remote mobile nodes. HAS provides mobile nodes authentication of local subscribers and all requested nodes gets the secret key from HAS.

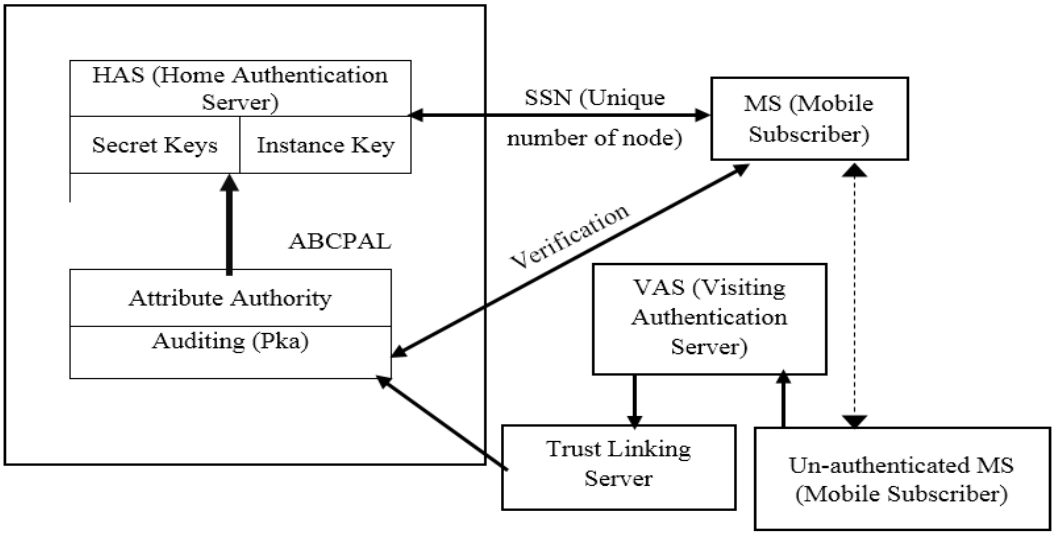

Fig. 1: Proposed Architecture Modules of ABCPAL.

TLS collates the truthful data from VAS which is already collected from MS. Using secret key and Recommendation from TLS, AA gives permission for accessing a particular data to the requested node.

The five important modules are described in Fig.1 and they are as follows:

1) MS- Mobile Subscriber
2) VAS – Visiting Authentication Server
3) HAS – Home Authentication Server
4) TLS- Trust Linking Server
5) AA- Attribute Authenticator

MS- Mobile Subscriber: In this module each node has one channel for data transfer and this act as a medium of data transfer. The type of transfer discussed here is of Remote medium so different types subscriber are present.

VAS – Visiting Authentication Server: It is specifically designed for giving the authentication of remote mobile nodes. The truthful information from MS is collated when node gives request to VAS. Subsequently the information is send to TLS where positive information is extracted from the data collected.

Further it is send for recommendation to AA. Whenever VAS receives any request from the client, it sends the authentication message in encrypted form.

HAS – Home Authentication Server: It is specifically designed for giving the mobile nodes authentication of local subscribers. A request message is send to HAS by node from local MS. Subsequently, as HAS receive request from any client the authentication message is send in encrypted form.

TLS- Trust Linking Server: Its role is to collate the truthful data from VAS which is already collected from MS. In order to extract positive truthful data it is processed. Then, ABCPAL algorithm is utilized for recommending to AA for the purpose of authentication. It also attempts to detect the malicious node.

AA: Attribute Authentication: The permission for accessing a particular data to the requested node is given by AA.It utilizes secret key and Recommendation from TLS in order to accomplish this.

4. Deployment of abcpal

Secret key Generation (SKG) operation is detailed below:

The operation set up:

1) Generate group G1(Current),G2(Roaming) of some prime order q and an admissible pairing

$$\hat{e} : G1XG2 \rightarrow G2;$$

2) Choose an arbitrary generator $P \in G1$.
3) Choose cryptography hash functions $H_1 : \{0,1\}^* \rightarrow G1, H_2 : \{0,1\}^n$ for some n;
4) Pick a random and set $\alpha \in Z_q^*$

$$Q_0 = \alpha P, \quad P_0 = H_1(DN_0), \quad S_0 = \alpha P_0.$$

$< G_1, G_2, \hat{e}, Q_0, P, P_0, H_1, H_2 >$The root SKG's master key is S_0 and the system parameters are

a) Basic Setup:

1) m nodes are supposed in the level-1. The root SKG act as follows for each node (Let X be an arbitrary node in the m nodes:
2) Compute the Secret Key of node X:Px= H1(IDX), where IDX=DN0 || DNX;
3) Pick the secret point for node $\rho \in \mathbb{Z}_q^*$ X. ρ_x is only know by node X and its parent node;
4) Set the secret key of node X:SX = S0 + ρ_xPX;
5) Define the Q-Value; QIDX = ρ_xP.QIDXis secret.

Subsequently, all nodes in the level-1 get the secret key and secret points. It is then securely kept.

The public key and the Q-value are publicized.

Steps (2-5) are repeated by each node in the level-1.

b) Encryption:

Encryption: In the IOT environment let us assume E1 and E2 as two mobile subscriber. The identity of E_2 is ID_{E2}= $DN_0||DN_1||DN_2$. In order to encrypt message m with ID_{E2}, E_1acts as follows:

1) Compute

P1=H1 (DN0||DN1) (1)

P2=H1 (DN0||DN1||||DN2) (2)

2) Choose a random $r \in \mathbb{Z}_q^*$
3) output the cypher text

$$C =< rP, rP_1, rP_2, H_2(g^r) \bigoplus m > \quad (3)$$

Where $g = \hat{e}(Q_0, P_0)$ which can be pre-computed.

c) Decryption:

By using its secret key, entity E_2 can decrypt C subsequent to receiving the cipher text C=<U_0, U1, U2, V>,

S_{E2}=S0 +$\rho_1$$P_1$+$\rho_2$$P_2$, where $\rho_1$the secret point of node DN0||DN1 is, ρ_2 is the secret point of node $DN_0||DN_1||DN_2$:

$$d = \frac{\hat{e}(\cup_0, S_{E2})}{\prod_{i=1}^{2} \hat{e}(Q_{IDE2^{Ui}}, \cup_i)}$$

$$Q_{ID_{E_2}l1} = \rho_1 P, Q_{ID_{E_2}l2} = \rho_2 P;$$

$$m = H_2(d) \bigoplus V.$$

Attribute based Identity-Based Signature:

Signature: To sign message m, entity E2 act as follows:

1) Compute Pm=H1(DN_0||DN_1||DN_2|| m);
2) Compute δ=S_{E2} + ρ_2 is the secret point of Entity E_2;
3) Output the signature

$$< \delta, P_m, Q_{ID_{E_2}l1}, Q_{ID_{E_2}l2} >,$$

Verification: other Entities can verify the AA signature by acting as follows: Confirm

$$\hat{e}(P, \delta) = \hat{e}(P, \rho_2 P_m) \prod_{i=1}^{2} \hat{e}(Q_{ID_{E_2}li}, P_i)$$

Signature is validated provided the equation is true.

d) ABCPAL based authentication for IOT

1) C -> S: MobilenodeHello (n_C,ID,Specification$_C$)

MobilenodeHello

2) S-> C:TLServerHello(nS,ID,SpecificationS)

Server Key Exchange (E_{PC} [F_{CS}])

Identity verify (Sig_{Ss}, [m]) ServerHello Done

3) C->S: Client Finished.

Where

NC and ns are random node number

ID: session identifier

C- Data transmitting mobile node (client)

S- TLS node (give authentication)

F_{CS}– secret key

E_{PC} [F_{CS}] = attribute based authentication key

M- Message (including hand shake)

Sig_{Ss} [M] – signature message

5. Result and implementation

The probable co estimation is accomplished through simulation since network topologies are unlimited. Built-in OLSR module is utilized in the network simulator NS2. The simulation value was set and ran ~1,000 times and the movement was 1.5-2 m/s (5.4-7.2 km/h) wherever appropriate. In order to examine the success of ABCPAL against node isolation attacks the first set of simulation was designed. Without movement and with movement are the two types of simulations ran for this. And 40 nodes are used by each of the first two simulations in random topology in an area of 750 - 1,000 m. The victim, the attacker and a sender are the three predefined nodes additionally used for sending messages to the victim. At an arbitrary distance of at least three hops to each other the victim and the sender were placed. It was designed in such a way for the attacker to follow the victim. The transmission range was about 250 meters using 40 nodes in the attack simulation. Eight of the forty were predefined attackers located at equal distances from each other to make sure that the area was covered by at least one attacker. The remaining nodes had the liberty to move with similar restrictions for the other simulations. The same topology and seed was used for each of the simulation round.

Fig.2 shows that Initialize the parameter, All the requested node gets the secret key from Home Authentication Server (HAS) which inturn gets the identification from the client node. Subsequently, the secret key for all requested node is created by HAS. Each dedicated node has a role such as Node 1 act as the source, Node 2 act as TLS (Trust Lining Layer), Node 9 act as attribute authentication and Node 8 act as visiting node Authentication Layer. Apart from these nodes all other nodes are ordinary data transfer node.

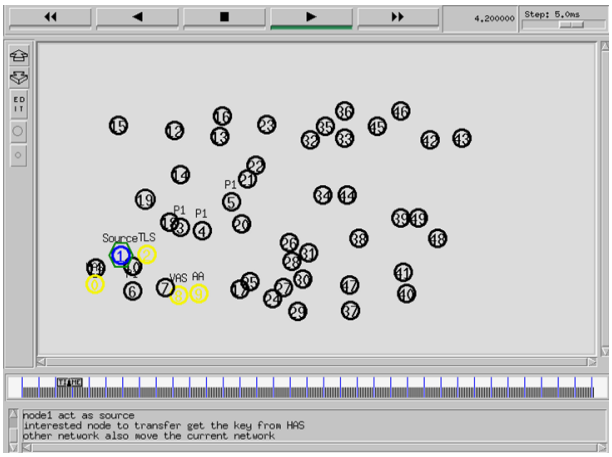

Fig. 2: Initialize the Parameter.

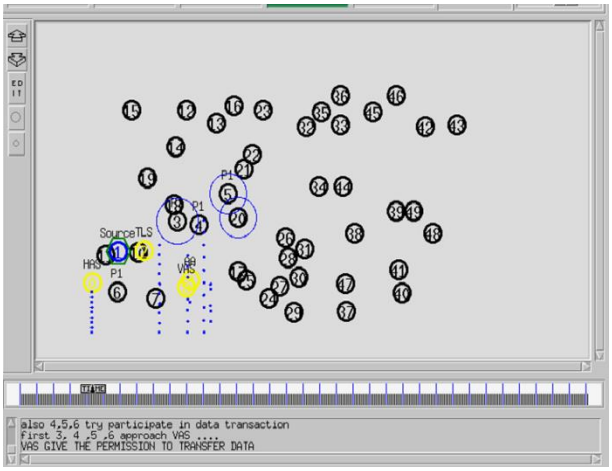

Fig. 3: Node Authentication with HAS.

Fig 3 describes Node authentication with HAS, there is movement of few nodes from one network to another. The remote network node ask permission from VAS. The transfer of data is not accepted by the remote node prior to authentication. Because of this there is a high loss of data. Normal transaction commences only after this.

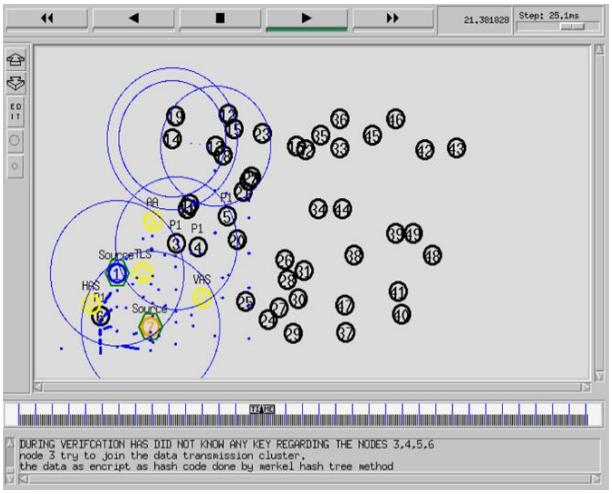

Fig. 4: Nodes Try to Get Instance Key from VAS.

Fig.4 shows Nodes try to get Instance Key from VAS, the HAS verify all node 3,4,5,6 ...prior to data transaction but no active instance key for that nodes although node3 attempts to join the cluster. Utilizing merkel hash tree method the encryption of transmitted data with hash code technique is done. Node 3 attempts to get the data devoid of instance key. Therefore node 3 is assumed to be a malicious node.

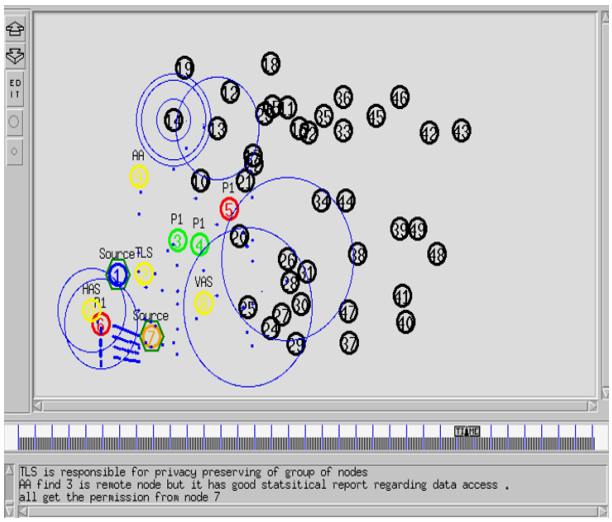

Fig. 5: AA Identifies Legal Node.

The malicious nodes are assumed to be 3,4,5,6. The malicious node behaviour of preceding history is verified by AA and TLS provides the data. So according to the transfer history, the statistical report of node 3 is good and instance key of node 4 expired just then. Based on this AA recommends node 3 and 4 to be a dynamic member. These two nodes approach to VAS to get instance key. Fig.5 noticed AA identifies legal node.

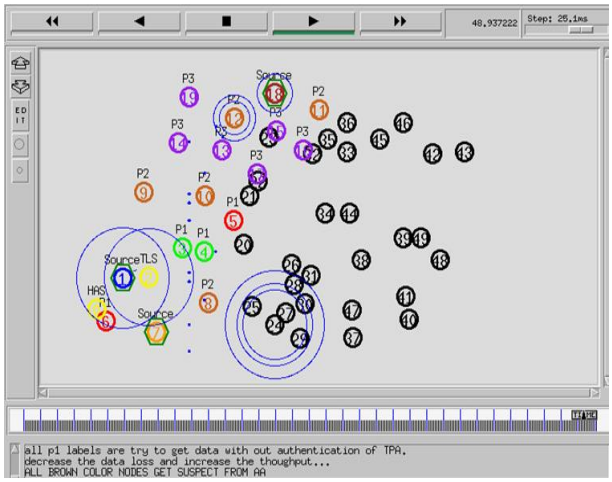

Fig. 6: AA Identifies Illegal Node.

Fig.6 describes AA identifies illegal node; those nodes in brown colour have poor and irregular behaviour and are suspected to be malicious.

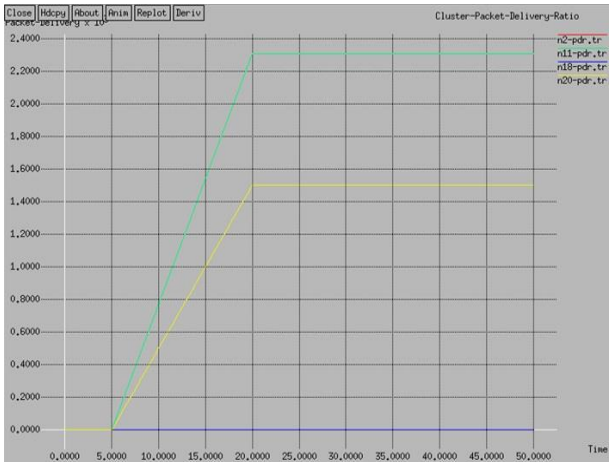

Fig. 7: Packet Delivery Ratio after Applying ABCPAL Authentication.

Packet delivery ratio= No. of packet received / No. of packet send

Fig.7 describes Packet Delivery Ratio after Applying ABCPAL Authentication, The packet delivery ratio before and after applying the proposed algorithm is shown in the plot. The line in green colour is after applying the proposed algorithm and yellow color line is before the proposed algorithm is applied. The x axis in the plot represents the simulation time and y-axis represents the no of packet delivered.

6. Conclusion

Through this study we understand that there is tremendous transformation in the area of accessing digital information. Unprecedented development in wireless networks and mobile devices plays a vital role. The Internet of Things is yet another technology that extends digital resources to the real world. Today many applications implement mobile interaction with tagged objects for various services. The privacy-preserving validation which is conditional with access likability called CPAL for roaming service provides secure universal roaming service. By utilizing a method of group signature it provides linking function of an anonymous user. This method has the capability to keep the identity of the users concealed and makes the authorized bodies possible to connect all the access information of the same user even without knowing the user's real identity. Therefore comprehensive analysis of CPAL demonstrates that it can withstand many security threats and more adjustable in privacy preservation as compared to the other techniques. Assessment of its performance further proves the efficiency of CPAL with regards to communication and computation overhead. Future work would include the extension of CPAL scheme to effectively withstand internal attackers and design the lightweight secure and privacy-preserving scheme that will support IoT devices of large group.

References

[1] IEEE 802.16 Working Group. "Part 16: Air interface for fixed broad-band wireless access systems-Amendment 2: Medium access control modifications and additional physical layer specifications for 211 GHz." *IEEE Std. 802.16 a* (2003).

[2] Alberti, Antonio M., Gabriel D. Scarpioni, Vaner J. Magalhaes, S. Arismar Cerqueira, Joel JPC Rodrigues, and Rodrigo da R. Righi. "Advancing NovaGenesis Architecture towards Future Internet of Things." *IEEE Internet of Things Journal* (2017).

[3] Lin, X., Sun, X., Ho, P. H., & Shen, X. (2007). GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on vehicular technology*, *56*(6), 3442-3456. https://doi.org/10.1109/TVT.2007.906878.

[4] Lu, Rongxing, Xiaodong Lin, Haojin Zhu, P-H. Ho, and Xuemin Shen. "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications." In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pp. 1229-1237. IEEE, 2008.

[5] Broll, Gregor, Enrico Rukzio, Massimo Paolucci, Matthias Wagner, Albrecht Schmidt, and Heinrich Hussmann. "Perci: Pervasive service interaction with the internet of things." *IEEE Internet Computing* 13, no. 6 (2009): 74-81. https://doi.org/10.1109/MIC.2009.120.

[6] Zorzi, Michele, Alexander Gluhak, Sebastian Lange, and Alessandro Bassi. "From today's intranet of things to a future internet of things: a wireless-and mobility-related view." *IEEE Wireless Communications* 17, no. 6 (2010). https://doi.org/10.1109/MWC.2010.5675777.

[7] He, D., Chan, S., & Guizani, M. (2016). An Accountable, Privacy-Preserving, and Efficient Authentication Framework for Wireless Access Networks. *IEEE Transactions on Vehicular Technology*, *65*(3), 1605-1614. https://doi.org/10.1109/TVT.2015.2406671.

[8] Odelu, V., Das, A. K., & Goswami, A. (2016). SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms. *IEEE Transactions on Consumer Electronics*, *62*(1), 30-38. https://doi.org/10.1109/TCE.2016.7448560.

[9] Abdallah, Asmaa, and Xuemin Sherman Shen. "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections." *IEEE Transactions on Vehicular Technology* 66, no. 3 (2017): 2615-2629. https://doi.org/10.1109/TVT.2016.2577018.

[10] Wang, Ding, Haibo Cheng, Debiao He, and Ping Wang. "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices." *IEEE Systems Journal* (2016). https://doi.org/10.1109/JSYST.2016.2585681.

[11] Rajput, Ubaidullah, Fizza Abbas, and Heekuck Oh. "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET." *IEEE Access* 4 (2016): 7770-7784. https://doi.org/10.1109/ACCESS.2016.2620999.

[12] Malina, Lukas, Jan Hajny, and Zdenek Martinasek. "Privacy-preserving authentication systems using smart devices." In *Telecommunications and Signal Processing (TSP), 2016 39th International Conference on*, pp. 11-14. IEEE, 2016. https://doi.org/10.1109/TSP.2016.7760820.

[13] Yang, X., Zhang, Y., Liu, J. K., & Zeng, Y. (2016, August). A Trust and Privacy Preserving Handover Authentication Protocol for Wireless Networks. In *Trustcom/BigDataSE/ISPA, 2016 IEEE* (pp. 138-143). IEEE.

[14] Liu, Yanbing, Yuhang Wang, and Guanghui Chang. "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm." *IEEE Transactions on Intelligent Transportation Systems* (2017). https://doi.org/10.1109/TITS.2017.2657649.

[15] Zeng, Shengke, Shuangquan Tan, Yong Chen, Mingxing He, Meichen Xia, and Xiao Li. "Privacy-preserving location-based service based on deniable authentication." In *Proceedings of the 9th International Conference on Utility and Cloud Computing*, pp. 276-281. ACM, 2016. https://doi.org/10.1145/2996890.3007872.

[16] Odelu, Vanga, Ashok Kumar Das, and Adrijit Goswami. "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms." *IEEE Transactions on Consumer Electronics* 62, no. 1 (2016): 30-38. https://doi.org/10.1109/TCE.2016.7448560.

[17] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54, no. 15 (2010): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010.

[18] Taddia, Chiara, F. Marcheselli, and Gianluca Mazzini. "Architecture improvements for an efficient emergency network." In *Software, Telecommunications and Computer Networks (SoftCOM), 2015 23rd International Conference on*, pp. 259-263. IEEE, 2015.

[19] Sesia, S., Baker, M., & Toufik, I. (2011). *LTE-the UMTS long term evolution: from theory to practice*. John Wiley & Sons. https://doi.org/10.1002/9780470978504.

[20] Xu, Sugang, Noboru Yoshikane, Masaki Shiraiwa, Takehiro Tsuritani, Hiroaki Harai, Yoshinari Awaji, and Naoya Wada. "Multi-vendor interconnection-based emergency optical networks design with optimal placement of portable EDFAs in disaster recovery." In *Design of Reliable Communication Networks (DRCN), 2016 12th International Conference on the*, pp. 55-61. IEEE, 2016. https://doi.org/10.1109/DRCN.2016.7470835.