International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209982 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

A Secure and Reliable Handoff Authentication Protocol with Batch Verification for Internet of Things Environment

Ramandeep Kaur
M.M. Institute of Computer Technology and Business Management, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India
ramanz2112@yahoo.co.in

Sumit Mittal
M.M. Institute of Computer Technology and Business Management, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India
sumit.mittal@mmumullana.org

Received: 10 July 2021 / Revised: 17 August 2021 / Accepted: 26 August 2021 / Published: 27 October 2021

Abstract – Internet is no longer a mere source of information as the concept of interconnectivity has expanded to connect real things or objects like every kind of machines, cars, homes, hospitals, even our bodies through wearable devices. The concept of interconnectivity of billions of objects (mobile or stationary) providing and exchanging real time data is called Internet of Things (IoT). Myriad IoT applications are touching every aspect of our lives and have the latent to develop the basic quality of life for masses. However, prerequisite for successful implementation of any IoT application is uninterrupted and high-quality network connectivity and handling of huge amounts of personal and sensitive user data which gives rise to the questions of security. A handoff authentication protocol with high security and efficiency is required for enabling secure and seamless handoff of mobile nodes between different access points (AP). However, there are number of challenges in designing a secure handoff protocol for IoT systems like limited power of mobile nodes, computational capability, security and vulnerability of open IoT networks. In this paper, we propose a secure and reliable handoff authentication protocol for such IoT devices. Compared with other well-known similar handoff protocols, the protocol proposed here satisfies all relevant security requirements of handoff such as batch verification, mobile node un-traceability, and anonymity and is unaffected by other attacks like replay attacks and also provides mutual authentication. To demonstrate the security strength (against replay attacks) of our protocol, simulation has been done using AVISPA. Thus, protocol proposed by us is more appropriate for IoT environment compared to the alike protocols.

Index Terms – Batch Verification, Authentication, Security, Reliability, Handoff, IoT, AVISPA.

1. INTRODUCTION

The term Internet of Things (IoT) was given by Kevin Ashton in his presentation in 1999[1]. Since then, the term IoT has evolved to a great extent and these days it is being used for a broad range of ideas and concepts and there exist a number of different interpretations and understandings of the term IoT but we feel that what Kevin originally meant by this term is still relevant and important to understand the concept[1]. Today, internet consists of a vast pool of information and data which is created, captured and inputted by humans, in other words people have provided data about things of the real world on the basis of their observations and ideas. Now if we consider that things of the real world provide data about themselves through RFID and sensor technology to the computers, in such scenario information and real time data on the internet becomes very cost efficient and free of inaccuracies arising due to human involvement.

Thus, IoT is a network of interconnected devices having sensory or actuating capabilities with unique identification that communicate with each other while capturing and sharing data through a Secure Service Layer (SSL). Internet of Things envisages an environment where digital and physical objects are associated using suitable technologies to facilitate various applications. There has been rapid emergence of IoT enabled networks comprising a vast variety of applications catering to the needs of various sectors like healthcare, manufacturing, retailing, home appliances, automobile automation, traffic control, supply chain management, smart cities etc.

IoT has great potential and its smart application can enormously contribute towards enhancing the quality of life of billions of people throughout the world [2]. To fit-in IoT suitably into any field, there are some basic requirements like proper network coverage, Quality of Service (QoS) demands of a particular application, mobility management (seamless

RESEARCH ARTICLE

connectivity), energy efficiency (battery life), security, data privacy, and authentication.

IoT applications require continued optimum and secure connection at all-time catering to the QoS demands of the application which can be limited by the mobility of the mobile node (MN). In order to overcome this issue an effective, efficient and reliable handoff (process of switching connection of MN between two access points (APs) as it moves) authentication protocol is required that is not only able to ensure the seamless mobility management but also takes care of mutual authentication so as to maintain the highest standards of data privacy and network security in a Heterogeneous Wireless Network (HWN) environment. Handoff decision is primarily based on meeting the service demands of a MN while keeping it Always Best Connected (ABC)[3].

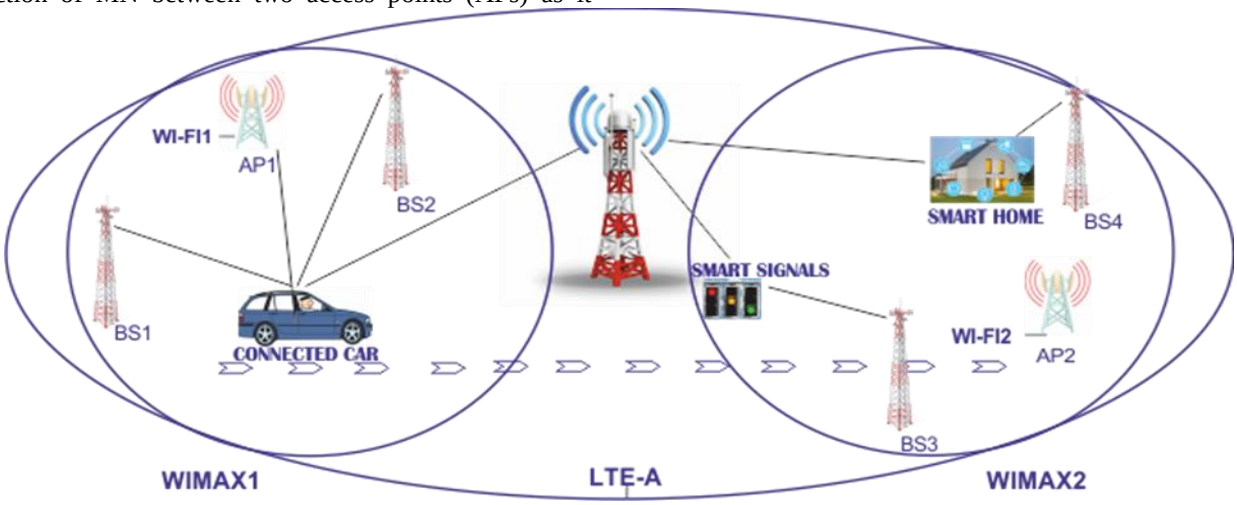

Figure 1 Handoff Scenario in Heterogeneous Network Environment

Figure 1 shows a typical scenario of an internet connected car moving from one region to another while facing a handoff decision of choosing from a number of network options to get connected with the best available while network connected and controlled traffic signals and smart home with various internet connected appliances and devices are also shown. For an efficient handoff management technique to be designed for next-generation wireless networks, following concerns need to be taken care of: (i) Minimise signal overhead and the required power for handling handoff messages, (ii) QoS should be guaranteed, (iii) effective and efficient use of network resources, (iv) robust and reliable handoff mechanism, and (v) the handoff itself must be secure and reliable.

1.1. Our Contributions

In this paper, a new reliable and secure handoff authentication protocol for an IoT environment has been proposed which when compared with other parallel protocols has higher efficiency and less computational complexity. Main offerings of this paper are:

- The proposed scenario is for IoT based environments where handoff takes place between the MN and the AP.
- A new secure and reliable handoff authentication protocol for the proposed IoT scenario which supports batch verification.
- Informal security analysis is done to check the security strength of the protocol against known attacks and functional requirements.
- AVISPA has been used for formal security analysis.

1.2. Organization of the Paper

Section 2 gives the detailed review of literature with respect to IoT and handoff authentication. Section 3 states the system model used for the paper. Section 4 elaborates the different security requirements of the handoff authentication. The proposed system model of the protocol for handoff authentication is given in Section 5. The informal security analysis is covered in Section 6. For a simulated security analysis, AVISPA is given in Section 7. Security comparison with earlier studies is given in Section 8. Lastly, the conclusion of the paper is given in Section 9.

2. RELATED WORK

IoT is one of the fastest growing technology which is being integrated into almost every sphere of life – industries, transportation, smart cities, healthcare, security systems and much more. Healthcare is one of the fields where adaptation and implementation of IoT can provide very promising results, the needs of healthcare services are tailor made for the IoT environment. Next decade is expected to witness wide usage of IoT in healthcare devices and applications. The 2017

RESEARCH ARTICLE

study given by [4] shows that from IoT perspective the economic growth potential is highest in the field of healthcare as compared to manufacturing, agriculture, retail, vehicular technologies etc. which makes IoT healthcare applications a promising area of research.

Incorporating IoT features into medical devices and applications greatly improves not only the quality and efficiency of medical care but also enables doctors to remotely monitor the data concerning the vital parameters of a patient collected from the IoT enabled devices like pacemakers, BP monitors, electronic wristbands, hearing aids, heart-rate monitors, medication management etc. Generally, these healthcare devices are connected to internet through various types of networks as the MN/IoT device (worn by user)roams from place to place it accesses the internet through multiple access points (AP) which are constituent parts of the various types of networks. This type of connectivity poses threat to confidentiality, integrity and authenticity of the users (patients) data.

Considering the diverse aspects of healthcare technologies using IoT, the authors in [5] have discussed various healthcare (IoT-based) network architecture and platforms. Security requirements of such an environment are similar to communication environments like integrity, confidentiality, availability, authentication etc. Various challenges faced while providing Secure IoT healthcare services include memory limitations, energy limitations, mobility, scalability etc. The comprehensive survey done by the authors also includes E-health and IoT policies of various regions.

Emphasizing on security of medical data of patients, the authors [6] have proposed an architecture for authentication and authorization which uses smart E-health gateways. This architecture is not only more secure than delegation-based centralized architecture but also has reduced impact of DoS attacks.

In another attempt to make IoT-based healthcare systems more secure, the authors [7] have designed sensor tags-based communication architecture. The proposed design uses single secure sign-on-based authentication protocol. A strong coexistence protocol has also been developed for multiple sensor tags which may exist at the same place at the same time.

Even though cloud IoT based healthcare services have advantages like centralised storage and easy accessibility of data but at the same time patients data privacy becomes critical issue. Working upon such an issue, the authors [8] use multi-factor authentication protocol (based on ECC) to allow only authorised user to use patient's data which has been stored on the cloud server. AVISPA tool is used to demonstrate the security of the scheme against various attacks like cloud server compromise attack, etc.

2.1. IoT Security Protocols

In 2010, [9] talked about the security and privacy of "connected things", i.e., IoT. As RFID and WSN are the two main sources of collecting data, various security issues arise with them. While RFID suffers from authentication problems, WSN also has issues like integrity and privacy. Though the measures are being developed to take care of such issues in the smart objects, still in the long run infrastructural security, flexibility and privacy (for IoT) should be focused upon.

In 2011, [10] had given a meticulous study on "Trust" in devices particularly in Internet of Things. Defining trust as reliance on integrity of an entity, the author analysed IoT environment for human trust. Software bugs like Trojans, hardware security risks, secure updates or procedures etc. are the few issues mentioned in detail in the paper. Threats in an IoT environment encourage measures for security to be devised and employed. The authors concluded with an optimistic remark of modelling IoT integrated with secure approaches like TNA-SL (Trust Network Analysis-Subjective Logic) so as to ensure the human to devise trust.

In 2012, [11] analysed prevailing methods for authentication and access control and suggested a protocol which was based on ECC along with an access control policy for an IoT network based on Role-Based Access Control (RBAC). The analyses results proved that the said protocol works against attacks like eavesdropping, key control attack, and man-in-the middle attack.

In 2013, [12] established security tasks of the distributed IoT. A comparison of centralized IoT and distributed IoT shows that issues like privacy and governance are less flexible in former and identity and authentication work more widely in the latter environment. Considering the future of IoT's, the authors stressed upon the co-existence of centralized and distributed IoT's.

The authors [13] in 2014 illustrated the ongoing challenges for IoT security. In IoT- object identification, location, authentication, authorization, privacy, software vulnerability etc. are the main challenges discussed by the authors. Although researchers are working on the issues but heterogeneity and complexity of an IoT environment makes it difficult to find a solution.

In such an attempt of securing IoT objects especially using RFID system the authors of [14] have proposed a lightweight cryptography protocol which uses XOR function instead of complex encryption with hash function. The hardware implementation of the same shows enhancement in security of an IoT application.

Working on authentication in distributed IoT applications using WSN's along with key establishment, the authors [15] proposed the protocol namely PAuthKey, which works in two

RESEARCH ARTICLE

phases- registration and authentication phase. The experimental outcomes show that PAuthKey can be used in constrained devices with low performances in WSN's used in distributed IoT Environment.

The survey given by the authors in [16] in 2015, states that authentication, confidentiality and access control are key security requirements of an IoT environment. The detailed literature review done by the authors' shows the work done by the researchers on the security requirements. Other issues like privacy, mobile security, middle ware in IoT security etc. are also reviewed. The conclusion states that although great deal of work is being done in IoT security, suitable solutions needs to be designed and used in IoT systems in real world.

Venturing into the other aspect of security in IoT, the authors [17] reviewed and discussed various layers of IoT with respect to security for each layer. For example, at application layer malicious attacks can bug the application program codes. Similarly at network layer, Denial of Service (DoS) attack or unauthorized access can compromise devices or create network congestion. The authors have mentioned solutions and limitations of attacks on various layers with the respect to the work done by the researchers on it.

Proposing a lightweight key-agreement and multi-factor user authentication model for IoT surroundings, the authors [18] used XOR and hash functions for secure IoT environment. The suggested model is checked for security against various attacks like DOS, impersonation, replay attacks, etc. Simulation in AVISPA tool validates its security whenever it finds an intruder.

In 2018, [19] surveyed IoT frameworks of eight different companies namely AWS IoT, Smart Things, Calvin, Brillo/Weave, Kura, ARMMbed, Home Kit and Azure IoT. On the basis of security mechanisms utilized by them the comparison shows that these frameworks use same standards for communications security but follow different methods for other security features.

The authors [4] discussed various layer wise security issues of IoT architecture. For example, they have mentioned issues like node capture, DoS or DDOS, replay attack etc. at perception layer while data disclosure, eavesdropping, network intrusion at network layer of the IoT architecture. Various security requirements of the IoT protocol stack and available operating systems (like mbed, RIOT etc.) have been mentioned. IoT applications, technologies used with IoT and trust management have been explained in detail. While concluding the authors have stressed over the need of unified vision and solutions for security in the IoT devices.

The authors [20] have talked about QoS parameters with low energy criteria in management models for IoT scenarios. These QoS parameters require reliability, performance and scalability optimization. The authors have analysed various methods used to obtain these conditions. Further, they have discussed various solutions or models in IoT environments to overcome issues occurring from Big Data.

With the advances in mobile technologies, 5G will soon be connecting IoT devices. In [21] the authors have proposed a Slice Specific Authentication and Access Control (SSAAC) method for managing authentication and access control in these 5G enabled IoT devices. A third party will manage these devices thereby reducing load on core network of connectivity provider. Feasibility analysis is done with Open Air Interface (OAI) open source platform. This approach will enable flexibility and better management of AAC credentials in 5G-based IoT devices.

The emergence of the IoT enabled devices has led to a unique set of requirements as these devices need continued seamless connectivity and best quality of service while being mobile in the heterogeneous wireless environments, fool proof handoff authentication is a must for the sanctity of the security and privacy of data.

2.2. Handoff Authentication Protocols

In 2012, [22] proposed PairHand protocol which used efficient batch signature verification method to achieve better efficiency. It was found that PairHand which is pairing-based cryptography protocol, is feasible in real applications as was shown through its implementation on PCs. Later, in the same year, the same authors found an inherent weakness in design in PairHand [23] and at times compromised session key. This improved version of PairHand fixed these problems without losing on strong security and high efficiency.

Proposing a secure handoff protocol, in 2013, the authors [24] used prime-order bilinear pairings. Various security attacks like user linkability, replay attack, user anonymity etc. have been resisted by the proposed protocol. In addition, computational cost of various operations have come out to be negligible as compared to [23] protocol. In 2013, [25] established the user authentication, efficient communication and computation along with user anonymity and untraceability. The authors have stated 12 main requirements like local access service expiration, local AP validation etc for an efficient authentication protocol. For formal analysis of the proposed protocol Handauth, AVISPA has been used and proved that Handauth is more efficient.

In 2014, [26] suggested a Privacy Aware Handover Authentication(PAHA) protocol which has short latency, low overhead and high level of security. PAHA uses Schnorr like signature which uses a pseudo-identity of the user. The proposed protocol shows better results in terms of user privacy with low communication and computation costs in comparison to other protocols. The authors in [27] discussed security authentication of PairHand and improved PairHand protocol. To overcome the security weakness like secure

RESEARCH ARTICLE

authentication for first message transmission, the authors have proposed new handoff authentication protocol which not only has better security in random oracle model but also has better efficiency.

In 2015, [28] have analysed the paper[26] and stated its vulnerability to impersonation attacked at access point. To overcome this problem, [28]have proposed an improved protocol which is robust and ensures users anonymity. The model has been tested on random Oracle model and is said to have achieved low computation costs. In 2015, [29]have defined a software-defined networking enabled model for authenticated handoff and privacy protection in a 5G environment. Using MATLAB simulations of 5G network, they compared authentication delay and 5G network utilization and the proposed SDN enabled model achieves reduced latency. In 2015, the authors [30] reviewed existing hand over authentication protocols and stated that PairHand protocol (proposed by[22]) outperforms other reviewed protocols as it does not release private information and resists DOS attacks. But to overcome shortcomings of PairHand protocol they proposed HashHand protocol. The experimental results show that HashHand removes security related vulnerabilities of PairHand protocol along with providing efficient and updated mechanism.

In 2016, [31] have discussed handoff authentication protocols with respect to their security and privacy requirements. They focused on identity based (ID-based) public key cryptography (PKC) as it is assumed to provide better security. The in-depth study here also included computation and communication costs after the implementation of various lightweight and heavyweight protocols on mobile device. The authors of [32] suggested authentication mechanism which used batch signature and identity-based encryption scheme. It reduced the total computation cost along with eliminating the requirement of storing multiple pseudo-identities.

In 2016, the authors [33] discussed about weaknesses in existing Anonymous Handoff Authentication (AHA) protocols. To overcome these weaknesses, the authors stated various security requirements and proposed a new AHA for mobile wireless networks. The performance analysis using MIRACL library shows that proposed method has lesser running time as compared to existing protocols.

In 2017, [34] reviewed [26] PAHA and stated its deficiencies to finally propose iPAHA (improved PAHA) scheme. Final comparison with PairHand, PAHA and WAS shows that iPAHA provides mutual authentication which is not in PAHA and resists key compromised attack which is missing in PairHand. Overall communication and computation costs are also less when compared with other schemes.

In [35], the authors proposed an anonymous batch handover authentication protocol which uses group signature technique. Contrary to the prevalent practice of protocols, the proposed protocol does not use group signature correlation functions in the handoff authentication phase, thereby giving better results.

Author	Limitations (Attacks not taken care of)
[22]	Session Key compromise problem, Perfect Forward Secrecy, Masquerade Mobile Node Attacks, Replay Attacks
[24]	Not suitable for practical purposes, Non-Traceability, Perfect Forward Secrecy, Conditional Privacy Preservation
[26]	Not secure against impersonation attack
[27]	User Anonymity, Non-traceability, perfect forward secrecy
[31]	Higher common cost, Masquerade Mobile Node Attacks, Batch Verification
[34]	User Anonymity, Replay Attacks and Batch Verification

Table 1 Limitations of Related Work

Table 1 elaborates the limitations of the related works studied above. The proposed protocol overcomes these limitations and provides better security and reliability.

3. SYSTEM MODEL

With the growing integration of heterogeneous wireless environment with IoT devices, it becomes imperative to explore the communication of various IoT devices while moving within such an environment. As stated earlier, IoT has found its application in almost every walk of life like automobiles, industries, home automation, healthcare services [36] etc. The heterogeneity of the wireless networks in which these applications are working, calls for handoff procedure whenever the mobile node (using IoT devices) moves from one network to another. Further, these HWN are openly accessible to intruders which maybe internet operators, peer nodes or even third party technologies. Such an intrusion may lead to security breach of users data leading to illegitimate use of users data as well as exploitation of Quality of Services (QoS) appreciated by the authorized users. This demands a reliable and authenticated handoff mechanism in an IoT environment.

A handoff authentication model typically contains three main entities: Mobile Nodes (MNs), Access Points (APs) and the Authentication Server (AS)[27]. In general, MN is a listed user of AS, who has the right to use its subscribed services through a connection to any AP. An AP works as a patron for assuring for an MN as an authentic subscriber. As the MN moves out of the network area of the present AP (e.g. APc), it tries to establish a connection to a new AP (e.g. APn) (as shown in Figure 2). The APn will initiate handoff authentication process to recognize the MN. Once it is successful, a session key is created between the MN and APn

RESEARCH ARTICLE

to verify the MN's later admittance. Else, the request to access the network will be rejected by APn.

Figure 2 Handoff Authentication for IoT

Based on such crucial requirements, consider the proposed model of healthcare application scenario shown in Figure 3 where a mobile node (MN) such as a smart ambulance vehicle is travelling through different networks and therefore needs to perform handoff. This handoff has to be reliable as well as efficient.

The IoT environment usually consists of constrained wireless devices which suffer from problems like low power, battery life etc. which in turn causes loss of signals. Further, the mobility or movement of these devices around different wireless technologies results in frequent disruption of Internet connectivity thereby draining the battery or the power source of the node. To eradicate the constraint of terrestrial coverage, smooth access services are preferred for IoT networks. Unfortunately, even after great deal of research, to make sure the security, reliability and productivity of this process is still questionable. In recent times, handoff authentication methods have been much talked about seamless access control technology.

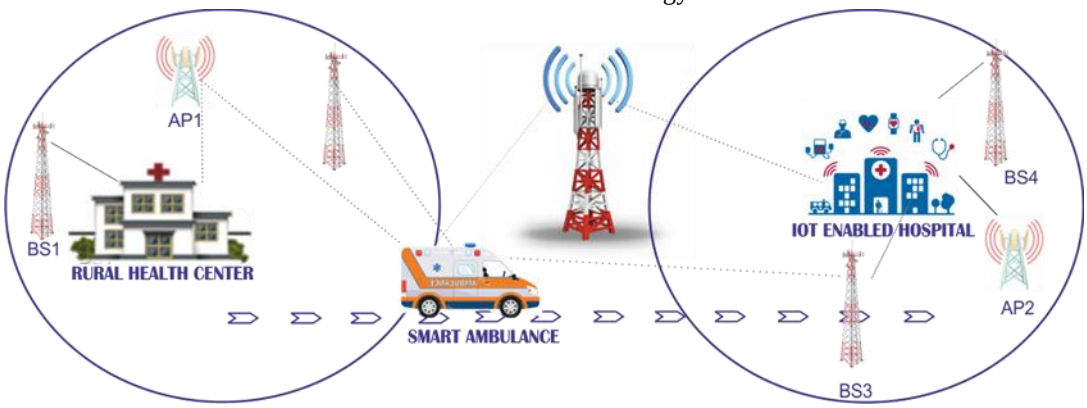

Figure 3 Proposed Scenario

4. SECURITY REQUIREMENTS

In an IoT environment, significant number of devices are working on heterogeneous wireless networking technologies thereby making the wireless communication channel vulnerable to attackers. The attacker can easily control this insecure channel between the MN, AP and the AS. Hence to ensure a secure and reliable mobility management framework, handoff authentication phase must be integrated in the mobility framework. Thus, the handoff authentication protocol must fulfill the following security necessities [37]:

a). **Mutual Authentication:** The Network Handoff Authentication Protocol (NHAP) for an IoT environment must provide mutual authentication amongstMN_i and $AP_j$and assure the access of network services by an authorized user only.

b). **User Anonymity:** The NHAP for an IoT environment should shield the user's privacy when he accesses network services. User anonymity should be maintained and the attacker (including the malevolent user and the malevolent AP) must not be eligible to extract MN_i's actual identity from the captured messages.

c). **Non-Traceability:** A smart attacker can traceMN_i's action simply by keeping an eye on pseudo-identity. Thus, user unrecognizability alone is not sufficient for shielding the user's privacy and therefore, an NHAP should provide non-traceability i.e., the attacker (both for the malevolent MN and malevolent AP) must not be able to trackback MN_i'saction.

d). **Safeguarding Conditional Privacy:** In an IoT environment where there are multiple nodes which are connected to a network, there are high chances of a miscreant (MN_i) trying to connect to these nodes and cause harm. In such situations, the manager (authentication server- AS) of NHAP may have to find the real identity of MN_i so as to penalize him. Therefore,

RESEARCH ARTICLE

AS should locate MN_i's actual identity over the seized messages.

e). **Batch Verification/Authentication:** As the IoT application environment may have increase in the number of users, AP_j will have many login requests concurrently. Thus, for an efficient performance, a NHAP should provide batch verification/ authentication, so that $AP_j$is able to validate received requests simultaneously and considerably reduce the computation cost.

f). **Establishing a Session Key:** Once the handoff is done and the connection is established, the data transmission starts. Hence, to ensure secrecy and integrity, a session key has to be generated beforehand and shared between MN_iandAP_j. Therefore, a NHAP needs to take care of the session key establishment.

g). **Perfect Forward Secrecy:** As stated above, the session key is exchanged between MN_i and $AP_j$and is used to encrypt data exchanged between them. Some of the earlier studies have shown that the intruder/attacker could trace the preceding session key as soon as he retrieves private keys of MN_i and AP_jresulting in a severe security threat to the nodes/users privacy data. To overcome this threat, a NHAP should be able to take care of perfect forward secrecy so that the intruder/attacker is not able to learn about preceding session keys created by MN_iandAP_j, even if he finds the access to the private keys.

h). **Attack Resistance:** Because of the open accessible nature of an IoT atmosphere, the authentication protocol is vulnerable to numerous attacks like the replay attack, the impersonation attack, the man-in-the middle attack, the modification attack etc. To deliver secure communication in such a heterogeneous IoT environment, it is vital that a NHAP is able to withstand such attacks.

5. PROPOSED HANDOFF AUTHENTICATION PROTOCOL

A secure, reliable handoff authentication protocol should ensure that only genuine MN accesses the network without revealing its personal information and sincere AP gives network access service. A handoff authentication protocol provides mutual authentication in MN and AP, along with generation of a session key for securing communication amongst them.

The proposed handoff authentication protocol comprises of following phases:

Phase 1: Initializing the System

Phase 2: Registration Phase

Phase 3: Handoff Authentication Phase

The symbolizations used here in this protocol are given in Table 2.

Notation	Description
G_1, G_2	two groups with the same prime order q
P	a generator of G_1
e	bilinear pairing $G_1 \times G_1 \rightarrow G_2$
h, H	hash functions $h \rightarrow \{0,1\}^* \rightarrow Z_q^*$and $H \rightarrow \{0,1\}^* \rightarrow Z_q^*$
s	$s \in Z_q^*$ as the private key of the system
P_{pub}	system public key $P_{pub} = s.P$
AP_j	Access point j
AS	Authentication Server
MN_i	Mobile node i
ID_{AP_j}	identity of access point AP_j
ID_{MN_i}	identity of mobile node MN_i
S_{AP_j}	private key of Access point AP_j
$pid_{MN_i}^1$	pseudo identity generated by AS to be used by mobile node MN_i
$S_{MN_i}^1$	private key generated by AS for mobile node
$T1, T2, T3, T4$	current timestamp

Table 2 Notations Used

5.1. Phase 1: Initializing the System

Authentication Server (AS) chooses

- G_1, G_2 – two groups with the same prime order q,
- P – a generator of G_1
- e – bilinear pairing $G_1 \times G_1 \rightarrow G_2$
- h, H – two hash functions $h \rightarrow \{0,1\}^* \rightarrow Z_q^*$and $H \rightarrow \{0,1\}^* \rightarrow Z_q^*$
- selects random $s \in Z_q^*$ as the private key of the system, calculates the public key $P_{pub} = s.P$
- AS announces parameters $\{G_1, G_2, q, P, h, H, P_{pub}\}$.

5.2. Phase 2: Registration Phase

- **For Access Point AP_j**
  - Identity of the Access point AP_j is denoted by ID_{AP_j}
  - AS generates private key $S_{AP_j} = s.Q_{AP_j}$, $Q_{AP_j} = H(ID_{AP_j})$
  - Sends the private key of the $AP_j$to the access point via secure channel.
- **For Mobile Node MN_i**
  - Identity of the mobile node MN_i is denoted by ID_{MN_i}

RESEARCH ARTICLE

- AS creates a group of unlinkable pseudo-identities $PID_{MN_i} = \{pid^1_{MN_i}, pid^2_{MN_i} \dots \dots\}$
- AS computes a group of private keys $PK_{MN_i} = \{S^1_{MN_i} = s.Q^1_{MN_i}, S^2_{MN_i} = s.Q^2_{MN_i}, \dots \dots\}$ where $Q^k_{MN_i} = H(pid^k_{MN_i})$
- AS sends the pseudo-identities and private keys to the Mobile node MN_i over secure channel.

MN_i	AP_j
chooses $pid^k_{MN_i}, S^k_{MN_i}$ computes, $A = h(pid^k_{MN_i} \| H(ID_{AP_j}) \| T1)$ $B = A.S^k_{MN_i}$.	
$\{pid^k_{MN_i}, ID_{AP_j}, B, T1\}$ →	
	validates the timestamp If invalid, the process is terminated. else, computes $C = h(pid^k_{MN_i} \| h(ID_{AP_j}) \| T1)$ $Q^k_{MN_i} = H(pid^k_{MN_i})$ checks if $e(B,P)? = e(A.Q^k_{MN_i}.P_{pub})$. If not, login request is rejected otherwise computes $D_{ji} = e\left(Q^k_{MN_i}.S_{AP_j}\right)$ $Auth_{AM} = h(D_{ji} \| pid^k_{MN_i} \| H\left(ID_{AP_j}\right) \| T2)$
← $\{pid^k_{MN_i}, ID_{AP_j}, Auth_{AM}, T2\}$	
computes $Q_{AP_j} = H(ID_{AP_j})$ $D_{ij} = e(S^k_{MN_i}, Q_{AP_j})$ checks if $Auth_{AM} = h(D_{ij} \| pid^k_{MN_i} \| H(ID_{AP_j}) \| T2)?$ holds. If not, then mobile node rejects the session due to invalid access point.	
	sends the message $\{pid^k_{MN_i}, ID_{AP_j}, T1, A)$ to the AS. On receiving this message, AS can fetch the real identity of MN_i from the pseudo-identity included in the message.

Figure 4 Work Flow Diagram for the Proposed Protocol

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209982 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

5.3. Phase 3 Handoff Authentication Phase

When a MN, say i, shifts into the scope of a new AP_n, a handoff authentication process is accomplished amongst MN_i and AP_n as given below:

Step 1: MN_i picks up an unused pseudo-identity $pid^k_{MN_i}$ and equivalent private key $S^k_{MN_i}$. It then computes $A = h(pid^k_{MN_i}||H(ID_{AP_j})||T1)$, where T1 is the present timestamp. It also computes $B = A.S^k_{MN_i}$and directs the login request message to the access point AP_j: $\{pid^k_{MN_i}, ID_{AP_j}, B, T1\}$.

Step 2: The access point AP_j on acceptance of the login request message $\{pid^k_{MN_i}, ID_{AP_j}, B, T1\}$ first validates the timestamp value. If the timestamp is valid, the process lasts else it is terminated. The access point calculates $C = h(pid^k_{MN_i}||h(ID_{AP_j})||T1)$ and $Q^k_{MN_i} = H(pid^k_{MN_i})$. It then checks if $e(B,P)? = e(A.Q^k_{MN_i}.P_{pub})$. If not, then AP_j rejects the request; otherwise it computes the secret parameter $D_{ji} = e(Q^k_{MN_i}.S_{AP_j})$ and the authorisation message for the mobile node $Auth_{AM} = h(D_{ji}||pid^k_{MN_i}||H(ID_{AP_j})||T2)$. Then it transmits the response message to the mobile node MN_i: $\{pid^k_{MN_i}, ID_{AP_j}, Auth_{AM}, T2\}$.

Step 3: The MN_i receives $\{pid^k_{MN_i}, ID_{AP_j}, Auth_{AM}, T2\}$ and the response message computes $Q_{AP_j} = H(ID_{AP_j})$ and $D_{ij} = e(S^k_{MN_i}, Q_{AP_j})$ and checks if $Auth_{AM} = h(D_{ij}||pid^k_{MN_i}||H(ID_{AP_j})||T2)$ holds. If not, then mobile node rejects the session due to invalid access point.

Step 4: Finally, the access point AP_j sends the message $\{pid^k_{MN_i}, ID_{AP_j}, T1, A)$ to the AS. On getting this message, AS can fetch the actual identity of MN_i from the pseudo-identity contained within in the message.

After efficaciously running the handoff protocol, MN_i and AP_2 share a session key, since $D_{ji} = e(Q^k_{MN_i}.S_{AP_j}) = e(S^k_{MN_i}.Q_{AP_j}) = D_{ij}$. Additionally, using a pseudo-ID enables unilateral unidentified authentication for the MN_i, and every session is distinctively recognised by $(pid^k_{MN_i}; ID_{AP_j})$.

Figure 4 shows the work flow diagram for the proposed protocol.

6. INFORMAL SECURITY ANALYSIS

a). Mutual Authentication: *The proposed protocol provides mutual authentication.* Both the mobile node $MN_i$and the access point AP_2mutually authenticate each other's identity and only then the connection is established. The access point computes the authorization message for the mobile node $Auth_{AM} = h(D_{ji}||pid^k_{MN_i}||H(ID_{AP_j})||T2)$ and the mobile node computes $Auth_{MA} = h(D_{ij}||pid^k_{MN_i}||H(ID_{AP_j})||T2)$ for the access point. Using these parameters, both the entities jointly validate each other and calculate the session key $D_{ji} = e(Q^k_{MN_i}.S_{AP_j}) = e(S^k_{MN_i}, Q_{AP_j}) = D_{ij}$.

b). User Anonymity: *The proposed protocol provides user anonymity.* The proposed protocol makes use of unlinkable pseudo-identities $PID_{MN_i} = \{pid^1_{MN_i}, pid^2_{MN_i} \dots\dots\}$ which are pre-generated by the authentication server during the registration process. Hence, the actual identity of the mobile node is never exposed and user anonymity is maintained.

c). Non-Traceability: *The proposed protocol provides non-traceability.* Although the login request message $\{pid^k_{MN_i}, ID_{AP_j}, B, T1\}$consists of the pseudo identity $pid^k_{MN_i}$of the mobile node, however, these pseudo identities are independent of each other. An attacker, which can be a malevolent access point cannot find a connection between two different sessions initiated by the same mobile node, since the mobile node uses a different pseudo identity.

d). Conditional Privacy Preservation: *The proposed protocol provides conditional privacy preservation.* To maintain the secrecy for MN, the authentication server generates a set of pseudo identities for the mobile node and creates associated private keys for each mobile node. Hence, the authentication server knows how to extract real identity from the pseudo identity of a mobile node. Thus, the authentication server can easily fetch the real identity of any MN from any of the intercepted messages in case needed.

e). Batch Verification: *The proposed protocol provides batch verification.* The access points can face a significant bottleneck when a group of signature verifications occurs. Hence, batch verification is a necessary feature, which allows access points to authenticate several signatures at the same time. The advantage of batch verification is the reduced overall computation cost.

$$e(\sum_{i=1}^{n} B_i, P)$$
$$= e\left(\sum_{i=1}^{n}(A.S^k_{MN_i}), P\right)$$
$$= e\left(\sum_{i=1}^{n}(h(pid^k_{MN_i}||H(ID_{AP_j})||T1).S^k_{MN_i}), P\right)$$

RESEARCH ARTICLE

$$= e\left(\sum_{i=1}^{n}(h(pid_{MN_i}^{k}\|H(ID_{AP_j})\|T1).s.Q_{MN_i}^{1}), P\right)$$

$$= e\left(\sum_{i=1}^{n}(h(pid_{MN_i}^{k}\|H(ID_{AP_j})\|T1).s.H(pid_{MN_i}^{k})), P\right)$$

As can be deduced from this equation that the overall computation cost of validating 'n' signatures gets condensed to 'n' point multiplication by using batch verification.

f). Session Key Establishment: *The proposed protocol provides session key establishment.* A session key, $D_{ji} = e(Q_{MN_i}^{k}.S_{AP_j}) = e(S_{MN_i}^{k}, Q_{AP_j}) = D_{ij}$, is established between the communicating entities MN_i and AP_jafter the authentication process. This key is different in each session and cannot be replayed after the session expires.

g). Perfect Forward Secrecy: *The proposed protocol provides perfect forward secrecy.* In the proposed protocol, the session key $D_{ji} = e(Q_{MN_i}^{k}.S_{AP_j}) = e(S_{MN_i}^{k}, Q_{AP_j}) = D_{ij}$ relies on a security hash function which gives a session key as output which is distributed uniformly in $\{0,1\}^k$ and has no relation with other session keys. Thus, revealing one session key will not affect the security of other session keys.

h). Masquerade Mobile Node Attacks: *The proposed protocol prevents masquerade mobile node attacks.* Assume that an attacker tries to access the network through a mobile device. In such a case, the attacker will try to connect his device by sending the {login request message}. The current AP will reject the request as it is an unknown device, since the MN needs to be registered with the AS.

i). Replay Attack: *The proposed protocol resists replay attacks.* Assume that an attacker resends the login request message $\{pid_{MN_i}^{k}, ID_{AP_j}, B, T1\}$ of a mobile node MN, the access point AP will first check the timestamp. If the timestamp is not fresh, the AP rejects the login request message $\{pid_{MN_i}^{k}, ID_{AP_j}, B, T1'\}$. If the attacker revises the timestamp value in the login request message, still it will not be able to succeed as the timestamp value $T1'$ is embedded in the parameter $A = h(pid_{MN_i}^{k}\|H(ID_{AP_j})\|T1)$ and the verification will fail at the access point.

7. AUTOMATIC FORMAL VERIFICATION USING AVISPA

Automated Validation of Internet Security Protocols and Applications (AVISPA) a web based tool has been used to simulate the proposed protocol[38]. The proposed protocol is written in High Level Protocols Specification Language (HLPSL)[38]. The components of AVISPA tool are shown in Figure 5.

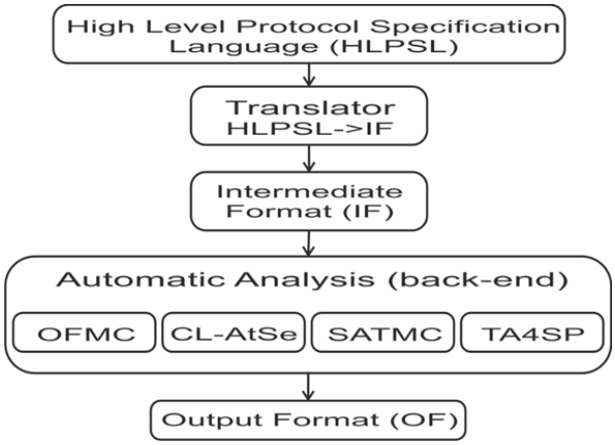

Figure 5 AVISPA Components

7.1. Simulation Results

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web-interface-computation
./tempdir/workfile77qXob.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.10s
visitedNodes: 18 nodes
depth: 4 plies
```

Figure 6 Simulation Results of the Analysis Using OFMC

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/avispa/web-interface-computation/
./tempdir/workfile77qXob.if
GOAL
As Specified
BACKEND
CL- AtSe
STATISTICS
Analysed : 8 states
Reachable : 8 states
Translation: 0.02 seconds
Computation: 0.01 seconds
```

Figure 7 Simulation Results of the Analysis Using CL-AtSe

RESEARCH ARTICLE

The proposed protocol has been simulated on the two backends OFMC and CL-AtSe. In order to check against replay attacks in the protocol, both the back-ends check for a passive intruder. Both the back-ends give the attackers information of valid sessions. The back-ends also check for Man-In-the-Middle attacks. The simulation results have been shown in Figure 6 and Figure 7. The results evidently show that the proposed protocol is secure and safe against the replay and man in the middle attacks.

8. SECURITY COMPARISON

This section gives the security comparisons between the four existing protocols and proposed handoff authentication protocol (Table 3). As can be seen, there are few conditions which are not fulfilled by other protocols but the proposed protocol fulfills.

Properties	[26]	[32]	[34]	[35]	Proposed Protocol
Mutual authentication	No	Yes	Yes	Yes	Yes
User anonymity	Yes	Yes	No	Yes	Yes
Non-traceability	Yes	Yes	No	Yes	Yes
Conditional privacy preservation	No	No	Yes	No	Yes
Perfect forward secrecy	No	No	Yes	No	Yes
Masquerade mobile node attacks	No	No	No	Yes	Yes
Replay attack	Yes	Yes	No	Yes	Yes
Batch verification	No	Yes	No	Yes	Yes
Session key establishment	Yes	No	Yes	Yes	Yes

Table 3 The Proposed Protocol Security Comparison with the Existing Protocols

For example, mutual authentication is not fulfilled by Li et al., mobile node anonymity is not satisfied by Xie et al, Wang & Hu perfect forward secrecy and masquerade mobile node attacks are not resisted. Similarly, batch verification is not done by Li et al. and Xie et al. protocols. The proposed protocol fulfils all security and privacy necessities and thus proves to be reliable and efficient.

9. CONCLUSION

Prospective growth of the IoT based applications to the levels they are capable of is dependent on the faith of users which can only be attained by addressing the concerns regarding the privacy and security of user data in addition to the performance levels and their reliability and efficiency. A handoff authentication protocol with high security and efficiency is of paramount importance in order to facilitate mobile nodes with seamless and secure handoff to different access points and to address the concerns mentioned above. Computational capability and limited power of mobile nodes, vulnerabilities related to security in open IoT networks are key challenges in designing a secure handoff protocol for IoT systems. In this paper, we have proposed a handoff authentication protocol for IoT devices which is secure, reliable and efficient in comparison to the similar handoff protocols proposed in other papers. The handoff authentication protocol proposed here provides mutual authentication and satisfies all major security requirements of handoff like batch verification, mobile node anonymity while providing resistance to several kinds of prospective attacks like replay attacks, masquerade attacks. Results of the simulation done using AVISPA prove the security strength of the proposed protocol against replay attacks. Thus, our proposed protocol is more appropriate for IoT networks than the similar protocols. In future, we can use some advanced techniques like hyper elliptic curves to further strengthen the security of the suggested protocol along with the techniques which may help in reducing the delay in handoff.

REFERENCES

[1] Kevin Asthon, “That ’ Internet of Things ’ Thing,” RFID Journal, p. 4986, 2010.
[2] Y. Ibrar and Ahmed Ejaz et al, “Internet of Things Architecture : Recent Advances , Taxonomy , Requirements , and Open Challenges,” IEEE Wireless Communication, no. June, pp. 10–16, 2017.
[3] R. Kaur and S. Mittal, “Enhanced Handoff Decision Making for Application-Aware Environment by Using Blended Approach,” International Journal of Intelligent Engneering Systems, vol. 14, no. 1, pp. 433–443, 2020.
[4] A. Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Generation Computer Systems, vol. 108, pp. 909–920, 2020.
[5] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, “The internet of things for health care: A comprehensive survey,” IEEE

RESEARCH ARTICLE

Access, vol. 3, pp. 678–708, 2015.
[6] S. R. Moosavi et al., "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," Procedia Computer Science, vol. 52, no. 1, pp. 452–459, 2015.
[7] J. L. Hou and K. H. Yeh, "Novel Authentication Schemes for IoT Based Healthcare Systems," Int. J. Distrib. Sens. Networks, vol. 2015, no. ii, 2015.
[8] P. K. Dhillon and S. Kalra, "A secure multi-factor ECC based authentication scheme for Cloud-IoT based healthcare services," Journal of Ambient Intelligent Smart Environment, vol. 11, pp. 149–164, 2019.
[9] S. A. Medaglia, Carlo Maria, "An Overview of Privacy and Security Issues in the Internet of Things," Giusto D., Iera A., Morabito G., Atzori L. Internet Things. Springer, New York, NY, pp. 367–373, 2010.
[10] G. M. Køien, "Reflections on trust in devices: An informal survey of human trust in an Internet-of-Things context," Wireless Personal Communications, vol. 61, no. 3, pp. 495–510, 2011.
[11] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and access control in the Internet of things," Proc. - 32nd IEEE International Conference on Distributed Computing Systems Workshops ICDCSW 2012, pp. 588–592, 2012.
[12] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
[13] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," Proc. - IEEE 7th International Conference on service-oriented computing and applications SOCA 2014, pp. 230–234, 2014.
[14] F. L. Ţiplea, "A lightweight authentication protocol for RFID," International Conference on Cryptography and Security Systems, pp. 110-121. Springer, Berlin, Heidelberg, 2014.
[15] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," International Journal of Distributed Sensor Networks, vol. 2014, 2014.
[16] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[17] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," Proceedings Annual Hawaii International Conference on System Sciences, vol. 2016-March, pp. 5772–5781, 2016.
[18] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments," International Journal of Communication Systems, vol. 30, no. 16, pp. 1–20, 2017.
[19] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
[20] A. Luntovskyy and L. Globa, "Performance, Reliability and Scalability for IoT," Proceedings International Conference on Information and Digital Technologies 2019, IDT 2019, pp. 316–321, 2019.
[21] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," Future Generation Computer Systems, vol. 108, pp. 46–61, 2020.
[22] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," IEEE Transactions on Wireless Communications, vol. 11, no. 1, pp. 48–53, 2012.
[23] D. He, C. Chen, S. Chan, and J. Bu, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," IEEE Communications Letters, vol. 16, no. 8, pp. 1270–1273, 2012.
[24] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure handover authentication protocol based on bilinear pairings," Wireless Personal Communications, vol. 73, no. 3, pp. 1037–1047, 2013.
[25] D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authentication with conditional privacy for wireless networks," IEEE Transactions on Computers, vol. 62, no. 3, pp. 616–622, 2013.
[26] G. Li, Q. Jiang, F. Wei, and C. Ma, "A New Privacy-Aware Handover Authentication Scheme for Wireless Networks," Wireless Personal Communications, vol. 80, no. 2, pp. 581–589, 2014.
[27] W. Wang and L. Hu, "A secure and effcient handover authentication protocol for wireless networks," Sensors (Switzerland), vol. 14, no. 7, pp. 11379–11394, 2014.
[28] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. H. Islam, and T. Shon, "A Robust and Efficient Privacy Aware Handover Authentication Scheme for Wireless Networks," Wireless Personal Communications, vol. 93, no. 2, pp. 311–335, 2017.
[29] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," IEEE Communication Magazine, vol. 53, no. 4, pp. 28–35, 2015.
[30] D. He, S. Chan, and M. Guizani, "Handover authentication for mobile networks: Security and efficiency aspects," IEEE Networks, vol. 29, no. 3, pp. 96–103, 2015.
[31] D. He, S. Zeadally, L. Wu, and H. Wang, "Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography," Computer Networks, vol. 128, pp. 154–163, 2017.
[32] J. L. Tsai and N. W. Lo, "Provably secure anonymous authentication with batch verification for mobile roaming services," Ad Hoc Networks, vol. 44, pp. 19–31, 2016.
[33] D. He, D. Wang, Q. Xie, and K. Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," Science China Information Sciences, vol. 60, no. 5, pp. 1–17, 2017.
[34] Y. Xie, L. Wu, N. Kumar, and J. Shen, "Analysis and Improvement of a Privacy-Aware Handover Authentication Scheme for Wireless Network," Wireless Personal Commununications, vol. 93, no. 2, pp. 523–541, 2017.
[35] D. Wang, L. Xu, F. Wang, and Q. Xu, "An anonymous batch handover authentication protocol for big flow wireless mesh networks," Eurasip Journal Wireless Communication Networks, vol. 2018, no. 1, 2018.
[36] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," Proceedings - 10th International Conference on frontiers of Information Technology FIT 2012, pp. 257–260, 2012.
[37] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255–270, 2017.
[38] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, and L. Compagna, "The AVISPA Tool for the Automated Validation," Computer Aided Verification, vol. 3576, pp. 281–285, 2005.

Authors

Ramandeep Kaur is a Ph.D. Research Scholar of M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India. Her area of interests include Wireless communications, Internet of Things and Networks. She has 20 years of teaching experience.

Dr. Sumit Mittal is Professor at M.M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala, Haryana, India. He has more than 45 papers published in reputed journals/conferences. His areas of interest include Cloud Computing, Wireless Communications and Computer Architecture. He is active member of reputed Computer Societies like CSI.

RESEARCH ARTICLE

How to cite this article:

Ramandeep Kaur, Sumit Mittal, "A Secure and Reliable Handoff Authentication Protocol with Batch Verification for Internet of Things Environment", International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 477-489, 2021, DOI: 10.22247/ijcna/2021/209982.