International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2022, Vol. 18(10)

DOI: 10.1177/15501329221126609
journals.sagepub.com/home/dsn
SAGE

Survey on authentication and security protocols and schemes over 5G networks

Yahya Tashtoush[1], Dirar Darweesh[1], Ola Karajeh[2], Omar Darwish[3], Majdi Maabreh[4], Safa' Swedat[1], Rawan Koraysh[1], Omar Almousa[1] and Nasser Alsaedi[5]

Abstract

The emergence of fifth generation networks opens the doors for Internet of Things environment to spread widely. The number of connected devices to fifth generation networks is expected to increase to more than 1.7 billion users by 2025. Each year, millions of modern devices go online at the beginning of the school year and after the holidays, and you can even notice the publicity of Internet of Things devices swinging with the seasons. Nowadays, these devices are considered to be very important to our daily life. That is because they provide power to our homes, organize our work operations and let communications more suitable. As a result of the increasing number of connected devices to fifth generation networks, the necessity to protect these Internet of Things devices against different types of cyber-attacks is also increased. For this reason, many researchers proposed different protocols and schemes to achieve the security of the Internet of Things devices. In this article, we introduce a survey of some protocols proposed by researchers in different domains and make a comparative study between them in terms of their category, authentication process, evaluation methodology, advantages, target, development year and applications within Internet of Things environment. The objective of this survey is to provide researchers with rich information about these protocols and their uses within Internet of Things systems, whether they can be used for cloud radio access networks, Internet of Things general purposes, telecommunications systems, e-healthcare systems or drone delivery service systems. It can also assist them in choosing the proper protocol to be used according to the type of their Internet of Things system.

Keywords

Fifth generation, Internet of Things, mutual authentication, protocol, scheme

Date received: 3 September 2021; accepted: 24 June 2022

Handling Editor: Peio Lopez Iturri

Introduction

5G is the fifth-generation mobile broadband (MBB) network which has begun spreading among cellular phone companies worldwide since 2019. It is predicted that 4G Long Term Evolution (LTE) connection will be replaced by the 5G network, and by the year 2025, it will have more than 1.7 billion users worldwide according to the Global System for Mobile communications Association (GSMA). GSMA's main vision is to

[1]Computer Science Department, Jordan University of Science and Technology, Irbid, Jordan
[2]Computer Science Department, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA
[3]Information Security Applied Computing, Eastern Michigan University, Ypsilanti, MI, USA
[4]Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II For Information Technology, The Hashemite University, P.O. Box 330127, Zarqa 13133, Jordan.
[5]Computer Science Department, Taibah University, Medina, Saudi Arabia

Corresponding author:
Yahya Tashtoush, Computer Science Department, Jordan University of Science and Technology, P.O.Box 3030, Irbid 22110, Jordan.
Email: yahya-t@just.edu.jo

accommodate billions of Internet of Things (IoT) devices and applications as it provides faster speed, very low latency, higher data rate and connection reliability.

Despite several advantages of using the 5G networks, it still has a big disadvantage in the context of security and privacy. The reason behind this is a huge number of devices connected to the network within a small area which increases the chance of the attack surface on these devices. This challenge motivated the researchers to look for a mechanism to protect the IoT devices and users from these attacks.

One of the researchers' main concerns is the mutual authentication. Using 4G network and earlier, mutual authentication was considered as one of their weaknesses.[1] Mutual authentication is usually achieved when a device connects to a home network. However, if the user is roaming, the authentication can be achieved by connecting via the serving network. This allows the involvement of the serving network in the process, and consequently having an access of the device International Mobile Subscriber Identity (IMSI)/ Subscription Permanent Identifier (SUPI) (https://www.etsi.org/). In this case, IMSI/SUPI is sent in plain text (unencrypted) over radio interface, making it subject to interception and reuse.

These weaknesses in the authentication process motivated 5G network to make the authentication decision only by home network. The protocol works as follows: when a device requests authentication, the home network sends an authentication vector (a large random number) as a challenge to the device, then this device must encrypt it again as a response using a shared key, then the home network can decrypt the response and check if it corresponds to the value that was originally has been sent. This means that the device's data in 5G network are always encrypted.

Another way of mutual authentication is called AUTH (authentication token) which is used by both 4G and 5G. AUTH allows the devices to authenticate the network using a token returned by the network and a shared key. In earlier generations, this authentication token was only encrypted over radio link. However, once a device is authenticated in 5G, the protocol decides how the traffic will be encrypted and the subsequent messages using a Subscriber Concealed Identity (SUCI) (https://www.etsi.org/) to identify the device. This traffic is encrypted throughout the whole infrastructure. The mutual authentication process is illustrated in Figure 1. In recent years, researchers have developed protocols and schemes to achieve strong mutual authentication between 5G networks and devices (User Equipment (UE)) in IoT environment, such as Authentication and Key Agreement (AKA) and Elliptic Curve Cryptography (ECC) protocols. In this article, a survey on some of these mutual authentication protocols with a comparison between them is introduced.

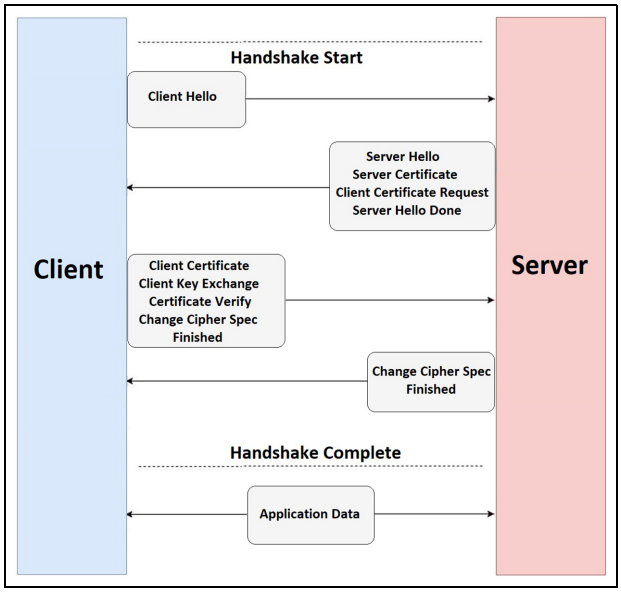

Figure 1. Simple mutual authentication process.

These days, a huge number of cyber-attacks in IoT environment due to the increasing number of new connected devices to 5G networks come up with a real security challenge, which needs to be solved.[2] That motivated us in our research project to present a survey of some protocols suggested by researchers in different fields and make a comparative study between them in terms of their category, authentication process, evaluation methodology, advantages, target, development year and applications within IoT domain. The aim of this survey is to enrich researchers with precious information about these protocols and their applications within IoT fields, whether they used for cloud radio access networks (RANs), IoT general purposes, telecommunications systems, e-healthcare systems or drone delivery service systems. This survey will provide researchers with the chance to choose the convenient protocol according to the kind of their IoT system.

In this survey, we divided mutual authentication protocols into four categories, namely AKA-based, Public Key Infrastructure (PKI)-based, ECC-based and others. Each category has a separate section, that is, sections 'AKA-based protocols', 'PKI-based protocols', 'ECC-based protocols' and 'Other protocols' are dedicated to survey AKA-based protocols, PKI-based protocols, ECC-based protocols and others protocols in which we survey the protocols that do not fall into any of the previous categories. In section 'Protocols comparison', we made a comparison between these protocols in terms of their category, authentication process, evaluation methodology, advantages, target, development year and applications within IoT domain.

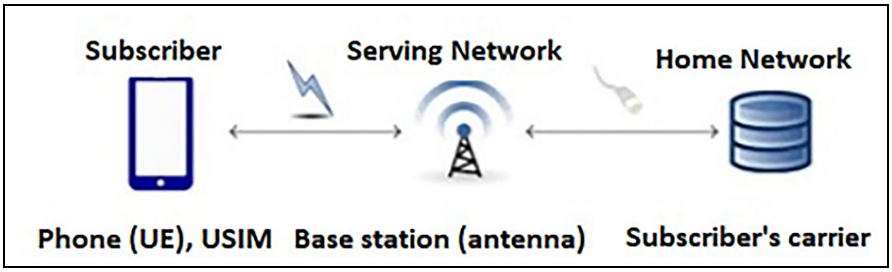

Figure 2. Mutual authentication with AKA.

Protocols in section 'Other protocols' have not been included in the comparison, as there is no available information specified about them in the table fields. Finally, section 'Conclusion' concludes the article.

AKA-based protocols

With the emergence of 5G networks, many IoT applications have appeared. These applications and the devices that rely on must be protected from cyber-attacks. Therefore, many protocols and schemes were developed to achieve the security and privacy of these devices by mutual authentication. Mutual authentication with AKA is illustrated in Figure 2.

The history of AKA protocols started with the proposal of Li et al.[3] using neural networks. After that, during the last two decades, a lot of AKA protocols incorporating both symmetric cryptography as in Kumar and Om[4] and asymmetric cryptography as in Xu et al.[5] have been proposed. Recently, many researches developed authentication protocols to resolve a specific problem, whereas some of them introduced critical deficiencies in the existing literature, developing a break-fix-break chain.

In 2020, Zhang et al.[6] proposed a Flexible and Anonymous Network Slicing (FANS) method for cloud RAN to enable authentication of emerging 5G service. FANS is basically based on AKA protocol to achieve mutual authentication between the user's equipment and the chosen network slice. It provides users' identity confidentiality preservation by hiding the public key associated with the actual user's identity in the transmitted messages. Fine-grained network slice selection is realized based on the one-to-many matching technique which is used in anonymous attribute-based encryption. This method has been evaluated using security and performance tests.

Haq et al.[7] provided a comparison of Ying-Nayak's protocol,[8] which is ECC-based, and their proposed protocol and improved a multi-server authentication protocol, which is called secure two-factor lightweight authentication protocol. It is AKA-based protocol. It prevents riskiness such as identity estimation, password estimation and user exemplification attacks. They got rid of the shortcoming in Ying-Nayak's protocol in context of computation and communication and provided mutual authentication between the user and service-providing server. This protocol has several advantages such that it prevents all known attacks and secure across active attacks. This protocol was tested using Burrows–Abadi–Needham (BAN) Logic and Automated Verification of Internet Security Protocols and Applications (AVISPA) tool. The results of testing show that it is effective regarding computational complexity and communication costs.

In 2020, Braeken[9] presented a new AKA protocol that is based on symmetric key and used cryptographic primitives in the Universal Subscriber Identity Module (USIM) devices. The target of this protocol is to prevent all familiar attacks, provide important privacy features, such as pseudonym, unlinkability, mutual authentication and exclusiveness. The proposed protocol did not need to use the public key encryption to hide the real identity. To ensure the mutual authentication, it needed just two communication rounds to derive a session key successfully. This protocol has been proved using RUBIN Logic.

Lee et al.[10] proposed an improved three-factor user authentication scheme that relies on mobile node, sensor node and the gateway. Their proposal aimed to resolve the security issues, which are linked with the three-factor user authentication scheme, such as not protecting from robbed mobile device attack, not inhibiting a user exemplification attack, not supplying a session key agreement and not having an emergency plan. They proved that their scheme was able to achieve mutual authentication because all three participants check the validity of one another throughout the login and authentication process. It presents attractive features for IoT environments. Also, its communication and computation costs are proper for excessively low-cost IoT devices.

Another deployment of AKA-based protocols took place in e-healthcare. In which a surgeon has the benefits of Tactile Internet to perform a surgery for patient using some control actions via a robotic system and receiving a haptic feedback. However, if unauthorized access to the robotic system happened, that would lead

to some fault in the procedures of surgeries, and eventually, causing havoc or even death. So, Kamil and Ogundoyin[11] developed a mutual AKA protocol for Tactile Internet-assisted remote surgery application. The remote surgeon asks to access the robotic arms through the gateway, after the gateway authenticates the remote surgeon, it sends a message to the robotic arm, then the robotic arm validates the message and returns a verification response to ensure the authentication process. Their protocol is considered very lightweight; for this reason, it is suitable for ultra-low latency-sensitive Tactile Internet-based applications. It was proved using Real-Or-Random (ROR) model, AVISPA tools and BAN Logic. Practical simulations show that it is very effective and appropriate for actual deployment.

In cellular network, handling the connectivity of the UE and devices with the networks is one of the main concerns in networks domain since the rapid growth of the number of IoT devices which needs authenticating and controlling access to the network. To manage the authentication and access control (AAC) of these devices, Behrad et al.[12] proposed Slice-Specific Authentication and Access Control (SSAAC) mechanism which delegate the AAC to third party by implementing fully virtualized mobile network. These mechanisms achieved by defining new RAN would be able to Host AAC functions specific to the third parties and Route the AAC requests to the corresponding third party network. When a third party device requires connectivity, it mentions its corresponding slice in its attachment request as the first step. The RAN processes the device's request and routes it to the right network slice (or to the core network (CN) in case of an MBB user). In the second step, the RAN establishes a direct connection between the device and the corresponding network slice. Finally, the device is able to use the network. If the device is a UE, the RAN routes the attachment request to the 5G CN and the AAC is done with the 5G AKA-based AAC protocols. This mechanism reduces the connectivity load of the core network, achieves strong mutual authentication and allows the third parties to choose suitable AAC mechanisms for their constrained devices. It also supply cellular networks the chance to beat the security weakness in their AAC methods. This mechanism has been evaluated using the Open Air Interface (OAI) open-source platform. It is also tested by calculating the expected number of AAC signalling messages against the current AAC methods in cellular networks.

PKI-based protocols

PKI is a set of software and hardware tools that can perform a full range of digital certificate operations. Also, it is a specialized technology solutions and the cornerstones of digital certificate management.

One of the advanced and modern systems which is using the 5G networks is the unmanned delivery aircraft (UAV) system that works to transport goods and other things without a pilot. This system provides great assistance for faster delivery. Therefore, there are security functions that has to be enforced, which protect the aircraft and the transported goods from being lost and ensure the arrival at the right time and place. To complete the delivery process successfully, the drone must identify some information previously, such as landing spot and customer's information, so when the customer receives the package, they will not be able to repudiate it. The other thing must be protected is the customer's private information and any communicated data between the drone and the customer, impersonation and seizure of the aircraft. To encounter these challenges, Seo et al.,[13] presented a security system using the white-box cryptography (WBC) as a software protection tool in the aircraft and the PKI as the authentication and non-repudiation method; PKI used to verify the identity of the user (home and application servers of a delivery company) and a seller by sharing the authentication token of each delivered item. They compared the white-box encryption (WBE) algorithm with Rivest–Shamir–Adleman (RSA)[14] algorithm and the results showed that WBE outperformed RSA encryption 6.7 times and thus can consumes less energy than RSA. Experimental results show that this security framework is efficient regarding cost according to resource utilization and appropriate even for resource-restricted UAV. Another security issue in using 5G networks is Insecure Connection Bootstrapping in Cellular Networks. Base station is the intermediary between the mobiles and the core network; when bootstrapping the connection, the mobile will be connected to the base station without any authentication mechanism and that will allow the fake base stations to make a connection with device and launch its attacks. This motivated the Hussain et al.[15] to propose an efficient authentication mechanism based on PKI which allows the cellular device to mutual authenticate the base station when bootstrapping by computing the signature of the core network and mobility management entity (MME) offline and share this signature with the base station when boot it up. Evaluations by a real testbed show that this mechanism executes superior than a symmetric key-based scheme (i.e. TESLA) regarding security warranty, overhead and deployment restrictions.

ECC-based protocols

The history of the ECC started in 1985 by Neal Koplitz and Victor Miller.[14] It is a way to crypt the public key

using algebraic structure of elliptic curves. The main advantage of ECC is that it allows to create smaller key size with the same security level of the RSA system, which reduces the storage and transmission requirements.

In 2017, Kumar and Om[16] proposed an ECC scheme based on USIM to manage the handover between the heterogeneous networks and achieve the integration among them, such as 5G and wireless local-area network (WLAN). Thus, it can provide the users with seamless connection during handover and reduce the latency to reach the required network. During the handover process, the devices must be re-authenticated to the network that finally will be connected with. The proposed ECC scheme achieved the mutual authentication for heterogeneous networks; when the device converts to new network, it gets the public key of the accessed point from the current base station or the target accessed point. This scheme has been examined using the BAN Logic, and the results indicated that it can provide strong security and superior implementation regarding computation, power and storage costs.

In 2021, Ayub et al.[17] proposed an ECC protocol to protect the medical data of patients from hacking and tampering. The target of this protocol also is to block some huge attacks, such as user pseudonym, offline password assessment, representation and robbed smart card attacks. Their protocol was based on three factors of authentication (the smart card, password and biometrics). Using this protocol, only the legitimate user and service provider can calculate the authentication key, then they make sure that both keys are equal. Therefore, the protocol provides mutual authentication. This protocol has been proved using the Random Oracle Model (ROM). Evaluations indicated that it is superior to many available protocols regarding computation and communication costs. It is also active, powerful and secure.

Other protocols

As we mentioned before, many IoT applications have appeared. Samaila et al.[18] discussed some of these applications (Smart Environmental Monitoring, Smart Healthcare, Smart Firefighting, Smart Manufacturing, Smart Wearables and Smart Toy) and the security threats for each domain. Then, they introduced some security countermeasures for it in general. Their study was not intended to serve or propose any security protocol. They introduced the IoT Hardware Platform Security Advisor (IoT-HarPSecA) framework. This framework is used from the manufacturer companies in the design of the IoT devices regardless of the used application. When the user of the IoT device inserts the query, which consists of three components (system resources, system model and security requirements), the security manager of the framework will look into the system resources and system model and design the suitable security services for the security requirements. The framework is still under development.

Shaik et al.[19] proposed a comprehensive study about the vulnerabilities in 4G and 5G cellular access network protocols by discussing the devices' capabilities which can be exposed by the attackers, unless it is securely protected. They used actual devices (more than 30), networks and operators (20 operators over LTE network).

Long-Range Wide-Area Networks (LoRaWANs) are operated by private organizations and companies. It is designed to optimize low-power wide-area networks (LPWANs) in term of battery lifetime, capacity, range and cost. It provides secure solutions to protect the companies and their customers from cyber-attack. However, it does not guarantee the trust of the network operators, as the customer needs to be sure that their information is not tampered. Therefore, Lin et al.[20] built a blockchain in the layers of LoRaWANs. Whereas blockchain is a distributed database which record and save every transaction that will be executed and shared between all participants. In addition, the information for each transaction will be verified from all participants in the system. This integration between LoRaWAN and blockchain builds an open, trusted, decentralized and tamper-proof system.

Many applications are developed in the context of saving human life, especially, healthcare as we mentioned earlier, but we have another domain that needs to be focussed on, in order to help saving lives, which is accidents risk. To avoid that, researchers developed Vehicular ad hoc networks (VANETs), which are composed of vehicles equipped with communication and computing equipment and roadside infrastructures. This system informs the drivers about the traffic status to avoid traffic jam, and if the distances between vehicles were less than needed or the vehicle takes the off road to take the suitable action. Messages between vehicles and the system and the vehicles themselves are easily hacked; so, to avoid fake messages, Cui et al.[21] proposed a mutual authentication scheme to ensure that the messages are sent from actual vehicles and not a fake one. The process of authentication is achieved when the driver gets the verification of his fingerprint, then the vehicle gets the authentication code from the system, after that the vehicle will be allowed to send messages to other vehicle or any other roadside unit connected with the system. In their scheme, they did not use the bilinear pairs to reduce the overhead of the system. They proved that their scheme is tamper-proof, free from side-channel attack, confidentiality of message, unlinkable and not traceable.

Identity management of IoT devices is one of the main concerns in IoT environment. In 2018, Santos

Table 1. AKA-, PKI- and ECC-based protocols comparison over 5G networks.

Ref.	Proposed protocol	Authentication process	Evaluation methodology	Advantages	Target	IoT applications
Category: AKA-based protocol						
Xu et al.[5]	FANS method	Mutual authentication between the user's equipment and the chosen network slice	Evaluated using security and performance tests	It provides users' identity confidentiality preservation by hiding the public key linked with the real identity in transmitted messages	It is used for cloud RAN to help in authentication of novel 5G services	Implemented by cloud RANs
Haq et al.[7]	Secure two-factor lightweight authentication protocol	Mutual authentication between user and service-providing server	Tested using BAN Logic and AVISPA tool	(1) It prevents all known attacks. (2) It is secure across active attacks. (3) It is effective regarding computational complexity and communication costs	Preventing riskiness, such as identity estimation, password estimation and user exemplification attacks	Used for IoT general purposes
Braeken[9]	Symmetric key-based 5G AKA authentication protocol	Mutual authentication and privacy	Evaluated using RUBIN Logic	(1) It does not need the utilization of public key encryption, to hide the real identity. (2) The number of communication stages for the protocol is improved and restricted to two	(1) Preventing all familiar attacks. (2) Providing important privacy features, such as pseudonym, unlinkability, mutual authentication and exclusiveness	Applied on telecommunications systems

(continued)

Table 1. Continued

Ref.	Proposed protocol	Authentication process	Evaluation methodology	Advantages	Target	IoT applications
Lee et al.[10]	An improved three-factor user authentication scheme	Mutual authentication because all three participants check the validity of one another throughout the login and authentication process	N/A	(1) It presents attractive features for IoT environments. (2) Its communication and computation costs are proper for excessively low-cost IoT devices	Solving security issues linked with a three-factor user authentication scheme, such as not protecting from robbed mobile device attack, not inhibiting a user exemplification attack, not supplying a session key agreement and not having an emergency plan	Implemented on telecommunications systems
Kamil and Ogundoyin[11]	A lightweight mutual AKA protocol for remote surgery application in Tactile Internet environment	Mutual authentication and particularity	Proved using ROR model, AVISPA tools and BAN Logic	It is very effective and appropriate for actual deployment	Implementation of remote surgery using Tactile Internet	Utilized by e-healthcare systems
Behrad et al.[12]	SSAAC mechanism	Authentication and access management of IoT devices are delegated to the third parties	(1) Evaluated using the OAI open-source platform. (2) Tested also by calculating the expected number of AAC signalling messages against the current AAC methods in cellular networks	(1) It is very effective and appropriate for actual deployment. (2) It supplies cellular networks the chance to beat the security weakness in their AAC methods. (3) It also decreases the AAC signalling capacity towards the connectivity provider's CN	Controlling the AAC of huge number of devices connected to 5G networks	Applied on telecommunications systems

(continued)

Table 1. Continued

Ref.	Proposed protocol	Authentication process	Evaluation methodology	Advantages	Target	IoT applications
Category: PKI-based protocol						
Seo et al.[13]	Security framework for a drone delivery service	PKI is used to prove the identity of the user (home and application servers of a delivery company) and a vendor by sharing the authentication token for every delivered item	Tested using experimental results	(1) It is efficient regarding cost according to resource utilization. (2) It is appropriate even for resource-restricted UAV	Providing a security framework that uses WBC for preserving sensitive information and encryption keys in delivery drones against white-box attacks	Used by drone delivery service systems
Hussain et al.[15]	Authentication mechanism based on PKI	Mutual authentication between cellular device and base station by computing and sharing signature of CN with the base station when bootstrapping	Evaluated by a real testbed	It executes superior than a symmetric key-based scheme (i.e. TESLA) regarding security warranty, overhead and deployment restrictions	Presenting an efficient authentication mechanism based on PKI, which allows the cellular device to mutual authenticate the base station when bootstrapping	Implemented on telecommunications systems
Category: ECC-based protocol						
Kumar and Om[16]	An ECC scheme based on USIM	Mutual authentication for heterogeneous networks. When the device converts to new network, it gets the public key of the accessed point from the current base station or the target accessed point	Examined using the BAN Logic	(1) It can provide the users with seamless connection during handover. (2) It can reduce the latency to reach the required network. (3) It provides strong security and superior implementation regarding computation, power and storage costs	Managing the handover between the heterogeneous networks and achieving the integration among them, such as 5G and WLAN	Used by telecommunications systems

(continued)

Table 1. Continued

Ref.	Proposed protocol	Authentication process	Evaluation methodology	Advantages	Target	IoT applications
Ayub et al.[17]	Lightweight authentication protocol for e-health clouds	(1) Mutual authentication between user and service provider. (2) Only the legitimate user and service provider can calculate the authentication key, then they make sure that both keys are equal.	Proved using the ROM	(1) It is superior to many available protocols regarding computation and communication costs. (2) It is active, powerful and secure	(1) Protecting the medical data of patients from hacking and tampering. (2) Blocking some huge attacks, such as user pseudonym, offline password assessment, representation and robbed smart card attacks	Applied on e-healthcare systems

AKA: Authentication and Key Agreement; PKI: Public Key Infrastructure; ECC: Elliptic Curve Cryptography; BAN: Burrows–Abadi–Needham; AVISPA: Automated Verification of Internet Security Protocols and Applications; OAI: Open Air Interface; UAV: unmanned delivery aircraft; USIM: Universal Subscriber Identity Module; ROM: Random Oracle Model.

et al.[22] introduced a solution for identity federation by reusing the SIM card of the cellular IoT devices to enable an authenticated single sign on. To achieve this goal, the networks must be provided with identity provider (IDP) which acts like a bridge between the IoT applications and the network server. When the device asks to access the network, the IDP checks if the device is registered in any serving node, if yes, then the device is successfully authenticated. Otherwise, it could be an attack.

Protocols comparison

In this section, a comparison between the proposed protocols (AKA, PKI and ECC) was presented, which are introduced in the literature review, in context of category, authentication process, evaluation methodology, advantages, target, development year and applications within IoT environment. Table 1 illustrates this comparison

In general, AKA protocols have been searched for long time, and a lot of efforts have been done to make them lightweight in terms of costs, computation and communication. This leads to be used widely within IoT environment for general purposes. So, as we notice in Table 1, AKA protocols are the most used protocols among the other protocols, while PKI protocols are considered very strong in terms of security with relatively high computation and communication. As a result, this leads these protocols to be used within high-risk IoT systems, such as drone delivery service systems. ECC protocols are relatively small and fast in comparing with the other protocols according to its computation and communication. Therefore, they are suitable for IoT systems, which require speed in its performance, such as the telecommunications and e-healthcare systems.

Conclusion

Due to the growing number of new connected devices to 5G networks in IoT environment, large number of distinct cyber-attacks against these IoT devices appeared as a real security problem, which require to be solved. For this reason, we motivated in our research to introduce a survey of some protocols provided by researchers in distinct fields to solve this security challenge. We made a comparative study between them in terms of their category, authentication process, evaluation methodology, advantages, target, development year and applications within IoT field. The goal of this survey is to supply researchers with worthy information about these mutual authentication protocols and their uses within IoT domain, whether they can be used for cloud RANs, IoT general purposes, telecommunications systems, e-healthcare systems or drone delivery service systems. We recommend researchers to benefit from the valuable information, which introduced in this research because it will provide them with the opportunity to find the adequate protocol to protect their IoT system. In fact, AKA protocol was the most widely used one compared to other protocols for its low costs of computation and communication. In future works, we may shed the light on AKA-based protocols in real IoT environments for intensive evaluation, with more comparative features between them.

Acknowledgement

This class file was developed by Sunrise Setting Ltd, Brixham, Devon, UK. Website: http://www.sunrise-setting.co.uk

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

Omar Darwish https://orcid.org/0000-0001-8346-7148
Majdi Maabreh https://orcid.org/0000-0003-4822-417X

References

1. Liu F, Peng J and Zuo M. Toward a secure access to 5G network. In: *2018 17th IEEE international conference on trust, security and privacy in computing and communications/ 12th IEEE international conference on big data science and engineering (TrustCom/ BigDataSE)*, New York, 1–3 August 2018. New York: IEEE.
2. Gravrock E. Challenges to 5G networks from IoT devices, 2021, https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/15/challenges-to-5g-networks-from-iot-devices/?sh = 2dd878877f5c
3. Li LH, Lin LC and Hwang MS. A remote password authentication scheme for multiserver architecture using neural networks. *IEEE Trans Neural Netw* 2001; 12: 1498–1504.
4. Kumar A and Om H. An improved and secure multiserver authentication scheme based on biometrics and smartcard. *Digit Commun Netw* 2018; 4: 27–38.
5. Xu D, Chen J and Liu Q. Provably secure anonymous three-factor authentication scheme for multi-server environments. *J Amb Intel Hum Comp* 2019; 10: 611–627.
6. Zhang Y, Wu A, Chen Z, et al. Flexible and anonymous network slicing selection for C-RAN enabled 5G service authentication. *Comput Commun* 2020; 166: 165–173.

7. Haq I, Wang J and Zhu Y. Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. *J Netw Comput Appl* 2020; 161: 102660.
8. Ying B and Nayak A. Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. *J Netw Comput Appl* 2019; 131: 66–74.
9. Braeken A. Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability. *Comput Netw* 2020; 181: 107424.
10. Lee H, Kang D, Ryu J, et al. A three-factor anonymous user authentication scheme for Internet of Things environments. *J Inf Secur Appl* 2020; 52: 102494.
11. Kamil IA and Ogundoyin SO. A lightweight mutual authentication and key agreement protocol for remote surgery application in tactile internet environment. *Comput Commun* 2021; 170: 1–18.
12. Behrad S, Bertin E, Tuffin S, et al. A new scalable authentication and access control mechanism for 5G-based IoT. *Future Gener Comp Syst* 2020; 108: 46–61.
13. Seo SH, Won J, Bertino E, et al. A security framework for a drone delivery service. In: *14th Annual international conference on mobile systems, applications, and services*, Singapore, 26 June 2016. New York: Association for Computing Machinery.
14. Menezes AJ and Vanstone SA. Elliptic curve cryptosystems and their implementation. *J Cryptol* 1993; 6: 209–224.
15. Hussain SR, Echeverria M, Singla A, et al. Insecure connection bootstrapping in cellular networks: the root of all evil. In: *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*, Miami, FL, 15 May 2019. New York: Association for Computing Machinery.
16. Kumar A and Om H. Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. *Digit Commun Netw* 2020; 6: 341–353.
17. Ayub MF, Mahmood K, Kumari S, et al. Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. *Digit Commun Netw* 2021; 7: 235–244.
18. Samaila MG, Sequeiros JB, Freire MM, et al. Security threats and possible countermeasures in IoT applications covering different industry domains. In: *International conference on availability, reliability and security*, Hamburg, Germany, 27–30 August 2018. New York: Association for Computing Machinery.
19. Shaik A, Borgaonkar R, Park S, et al. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In: *12th ACM conference on security and privacy in wireless and mobile networks*, Miami, FL, 15–17 May 2019. New York: Association for Computing Machinery.
20. Lin J, Shen Z and Miao C. Using blockchain technology to build trust in sharing LoRaWAN IoT. In: *2nd International conference on crowd science and engineering*, Beijing, China, 6–9 July 2017. New York: Association for Computing Machinery.
21. Cui J, Xu W, Han Y, et al. Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Veh Commun* 2020; 21: 100200.
22. Santos B, Do VT, Feng B, et al. Identity federation for cellular internet of things. In: *2018 7th International conference on software and computer applications*, Kuantan, Malaysia, 8–10 February 2018. New York: Association for Computing Machinery.