A Systematic Dynamic Key Agreement Mechanism for LTE Advanced Networks in the Internet of Things

Saraswathi Pedada, Muralidhara Rao Patruni, Reddyprasad A, RK Chandana Mani

Abstract*: Of late, Session Initiation Protocol (SIP) has become one of the popular signaling protocols especially for the multimedia communication system. Various protocols have been proposed by researchers to ensure access independence, authentication, and Key Agreement security characteristic. With the extensive growth of cellular networks, mobile traffic connected with the advancements of the wireless communication channel. In this scenario, Machine Type Communication (MTC) plays a crucial role in line with Long Term Evaluation-Advanced Networks as their communication happened between Machine to machine without human intervention. In order to reach Mobile Type Transmission (MTT) security condition, the access verification process required to pursue the verification and Key Agreement protocol. Moreover, the development of Group premised communication and individual authentication mechanisms to every Machine Type Communication device (MTTD) would lead to signal-congestion in real-time networking scenarios. Jinguo et al. proposed a Group-Based Verification and Key-Agreement protocol with dynamically updating policy for mutual authentication. Especially, they chose an asynchronous secret shared key merged to work with Diffie-Hellman protocol for establishing disjoint verification and session-key establishment across LTE Advanced Networks. However, the DH algorithm could not provide message integrity to upgrade the security feature namely integrity. In this paper, the algorithms Advanced Encryption Standard (AES) in addition to Elliptic Curve Diffie-Hellman (ECDH) can be integrated called an Elliptic Curve Digital Signature Algorithm (ECDSA)" which addresses verification and integrity.

Keywords: verification and Key Agreement, GR-AKA, Diffie-Hellman, AES, ECDH, ECDSA.

I. INTRODUCTION

Today, the growth of Internet applications plays a critical role in every human life. This can be an enormously difficult job to optimize Internet usage according to the level of application usage. Basically, physical things may associate with an Internet known as the Internet of Things (IoT). Of late, various definitions have been suggested by various organizations based on the use of its applications. Particularly, various security mechanisms have been proposed for the improvement of security, privacy, access control.

In the physical environment, the IoT has limited storage capacity and computing power to process a huge number of real-time data. To devise a secured and robust authentication scheme, a lightweight mechanism can be highly recommended. A recent report says that around more than 40 billion devices will be remotely connected to IoT by 2020. The growth of IoT rapidly increased in the past few years. So as to modernize in various fields, IoT has become a premier part of several real-time application domains such as healthcare, agriculture, remote weather forecasting, smart vehicles, smart grid, smart city and many more. However, many devices communicate remotely to another device via the wireless communication channels. Wireless Sensor Networks (WSN) can be the best suitable networking model to work efficiently with the IoT communication platform. In order to ensure privacy, security a light-weight authentication and key agreement protocols to validate other users a reliable architecture is highly demanded. Various challenges have been considered. For example, a huge amount of IoT physical devices requested access from the specified network, during a little span all the clients will be faced heavy network-access latency and authentication. Because of each and every IoT device has to execute authentication schemes that will elastically increase the burden to the server environment.

MTT can be institutionalized by the Third Generation Partnership Project (3GPP) and widely connected in the organization. To help MTC, the 3GPP versatile administrator needs to oblige its system to help a substantial count of MTC gadgets that can over-burden its system assets and present blockage in both system information and control planes. On the off chance that an expansive number of gadgets solicitation to get to the system amid a brief period, clients will get to know the ill effects of the high system get to dormancy and validation flagging clog. This is on the grounds that each gadget needs to play out the entire AKA confirmation strategy, which would quickly expand verification vectors produced by native validations, disjoin [1]. The reason is that each gadget must play out a full AKA validation system with a native confirmation server, separately [3].

Along these lines, a validation conspires for blockage shirking is required. Indeed, the clog may happen because of concurrent verification flagging messages from MTC gadgets [3]. MTC is viewed as an imperative correspondence method in LTE-A systems.

Revised Manuscript Received on December 13, 2019.

Saraswathi Pedada[1]*, Department of Computer Science and Engineering, GITAM, Visakhapatnam, India. Email: saraswathi.pedada@gitam.edu

Muralidhar Patruni[2], Research Scholar, School of Computer Science and Engineering, VIT, Vellore. Email: patrunimuralidhar@gmail.com

Reddy Prasad A[3], Department of CSE, Mother Theresa Institute of Engineering and Technology, Palamner, India. Email: prasad2p@gmail.com

RK Chandana Mani[4], Research Scholar, School of Computer Science and Engineering, VIT, Vellore. Email: rkchandana510@gmail.com

MTC does not contain any human collaboration and is ease. For the Mobile Type Transmission Devices, the entrance verification processes still pursue the current institutionalized strategies, for example, the Evolved Packet System Verification and Key Agreement (EPSAKA). At the point when various MTCDs at the same time solicitation to access the system, every gadget needs to play out a full access validation methodology with then work to guarantee MTC security [6]. This may help to associate with one device to another in IoT physical system. The IoT expands its application usage in various application areas such as education, smart transport, medical fields, and energy management. It is stated by Gartner that there exist 30 billion connected communication devices of machine type and they will reach 1.9 trillion of economic value till 2020.

Notwithstanding Gartner, arrange association CISCO additionally revealed MTC development will achieve 50 billion in the year 2020 and esteem will achieve 14.4 trillion. From this study it is normal information conveyed from MTC gadget to IoT will be at a high rate in the future [7]. In spite of the fact that Machine Type correspondences are advantageous and productive however security and protection are most testing things in MTC. Gigantic confirmation demand from an extensive number of MTC gadgets will prompt system clog and disavowal of administration. To maintain a strategic distance from this issue bunch based verification convention is actualized in MTC gadgets which additionally increment execution in verifying the huge number of MTC gadgets. With the aim to obtain challenges for higher data rates, adaptable growth and quality coverage; a novel wireless communication platform can be essential to create a standard communication between the devices [6]. What's more, the gadgets should be defined in the current remote stages to satisfy the needs of higher information rates, better inclusion, and adaptable extension. This can be assessed based on the quantity of MTCDs' that can be multiple times bigger compared to the quantity over regular client equipment [6]. The 3GPP measures the improved standards of LTE services in today's communicating networks utilizing the LTE Advanced network. So as to meet the requirements of these advanced technologies, effective resource allocation mechanisms are required to minimize the communication delay of sensitive real-time data. Basically, the core objective of this method is to provide improved service connectivity between IoT physical devices and LTE Advanced networks.

Table 1: Important Notations Used

Notation	Description
LTE-A	Long Term Evaluation Advanced
IoT	Internet of Things
DH	Diffie-Hellman
M2M	Machine to Machine
SIP	Session Initiation Protocol
MTT/D	Mobile Type Transmission/Devices
ECDH	Elliptic Curve Diffie-Hellman
AES	Advanced Encryption Standard
GTK	Group Temporary Key
AKA	Authentication and Key Agreement
IIoT	Industrial Internet of Things
ECC	Elliptic Curve Cryptography
GRAKA	Group-Based AKA protocol
HSS	Home Subscriber Server
3GPP	Third Generation Partnership Project
ECDSA	Elliptic Curve Digital Signature Algorithm

A. Motivation

To maintain a strategic distance from this blockage issue bunch based confirmation convention is executed in MTC gadgets which additionally increment execution invalidating of a vast number of MTC gadgets. Aside from security and protection issues, there exists an integrity issue in MTC gadgets where the client can't decide the message from an approved client or from an ill-conceived client. These security issues can be overcome by using a group-based verification protocol with the Elliptic curve Digital Signature Algorithm (ECDSA). Diffie Hellman calculation could give verification yet it couldn't give message verification and integrity to maintain these highlights to be specific confirmation and trustworthiness. In this paper, we utilize the Elliptic bend Digital Signature Algorithm (ECDSA). Confirmation can assess the client and uprightness approves the message. Respectability is a component of a group of three which is the most critical segment of security and confirmation that the data is dependable and precise [8]. An ECC-based prominent secure user authentication scheme along with privacy protection to the Industrial Internet of Things (IIoT) ensured that this could also be robust to various security attacks.

B. Literature Survey

In order to strengthen the system from these issues, various group-based authentication mechanisms have been proposed especially for MTT [5]. Subsequently, Cao et al. [5] proposed a mass gadget to get a confirmation plot for Mobile Type Transmission in LTE to organize. It took a total mark innovation in which a gathering head of MTC gadgets totals every mark that is created by each Mobile Type Transmission gadget and sends the total mark to MME, at that point MME could viably and rapidly verify a lot of MTT gadgets. Be that as it may, its computational overhead is moderately vast in light of the fact which takes bilinear matching and Elliptic Bend Calculation innovation. Lai et al. [2] devised another standard protocol namely SE-AKA of protective and productive AKA convention, that can be fitted to make major validation possibilities in the LTE systems. This can resolve the group verification method over the calculation of GTK.

However, that can receive Elliptic bend Diffie– Hellman to acknowledge key forwarding reverse mystery and utilizations keys in the cryptosystem to ensure client protection. In any case, it can't check a gathering of MTC gadgets at the same time, and it just generally decreases correspondence overload. , Zhang et al. [2] suggested a GB dynamic verification mechanism that can be similar to SE-AKA. Initially, MTCD plays a complete verification with native condition, the rest Mobile Type Transmission Devices of this gathering simply verify with the serving system. Later, a group key update method can be planned to suits the dynamic grouping MTC. Subsequently, in ref [3] advised a light-weight authentication protocol for MTC using group key especially for the LTE systems, named as LGTH. At this, it embraces a total mark dependent on information verification codes, and it could validate a gathering of Mobile Type Transmission gadgets rapidly and at the same time.

LGTH has a next to no calculation and correspondence costs, yet it can't give security insurance.

Choi et al. [5] proposed another gathering confirmation convention for Mobile Type Transmission in LTE-A systems. For proficiency and in reverse similarity, symmetric cryptography is just utilized in the suggested a plan. Be that as it may, it likewise does not consider the DoS assault and security assurance. The Authentication and Key Agreement (AKA) protocols used a GRAKA in which it simplifies whole verification procedure by computing a GTK; secure and efficient group AKA (SE AKA), Extensive Authentication Protocol-AKA (EAP-AKA) [2] In which access point requests identification data that are transmitted to verification server, cocktail AKA in which mutual verification will be principle design concept, Secure AKA (S-AKA) and so on. But GR AKA avoids the signal congestion at the network layer during the transmission especially for wireless communication and also updates the access policy frequently. Signal congestion happens when verification processed to each MTC device. Specifically, In GR AKA they can choose an asynchronous secret-key shared to combine in conjunction with the Diffie-Hellman (DH) key redemption protocol to appliance distribute verification and session-key establishment in LTE Advanced Networks. As it may, it likewise does not consider the DoS assault and security assurance. The AKA protocol used a GRAKA that simplifies whole verification process by computing a GTK, secure and efficient group AKA (SE AKA), Extensive Authentication Protocol-AKA (EAP-AKA) [2] In which access point requests identification data that are transmitted to verification server, cocktail AKA in which mutual verification will be the principle Design concept, Secure AKA (S-AKA) and so on. But GR AKA avoids signal congestion in the networks and also updates the access policy frequently. Signal congestion happens when verification processed to each MTC device. Specifically, In GR AKA they selected based on asynchronous shared secret key joining with Diffie-Hellman (DH) key interchange protocol to appliance distribute verification and session key establishment in LTE Advanced Networks.

Table 2: Summarizes the key challenges of existing authentication schemes

Existing Schemes	Techniques used	Benefits	Challenges
Li et al.[1]	Group-based AKA protocol, Diffie-Hellman	Avoids signal congestion, verification,	Integrity
Lai et al.[3]	Lightweight group verification protocol(LGTH)	Minimize the verification overhead, Robust security	Integrity, Security attacks may possible
Lai et al.[2]	SE-AKA, ECDH	Effectively authenticate group devices, secure over various malicious attacks	verification, Integrity
Cao et al.[4]	Group based anonymity handover verification protocol (GAHAP)	reduce the signaling costs	verification, Integrity, Security attacks may possible
Fuet al.[5]	Advanced Group verification protocol with privacy-preserving	minimize the signaling overhead, robust privacy-preserving, avoid denial of service attack, secure against various malicious vulnerabilities	Integrity and security issues
Wang et al. [11]	The dynamic identity-based authentication protocol	Better results to mitigate delay transmission	Integrity

Li et al. [23] focused on proving that various existing schemes based on symmetric-key cryptographic and secure hash-based user authentication schemes cannot assure anonymity and smart-card stolen/lost attacks. In order to control the weaknesses, they proposed a robust ECC-based secure authentication and biometric-based authentication scheme for preserving privacy for IIoT.

Ref. [11] proposed an advanced group verification protocol with privacy-preserving to strengthen the security system against various security vulnerabilities. It also proved that their scheme can be secure when compared with other authentication protocols such as Young An, Das, et al., Chang et al., Khurram et al. Alongside they described that their protocol can be offered better specifications including privacy preservation service scalability reliability to the client system.

Recently, Roychoudhury et al. [24] proposed a group authentication protocol utilizing “extended Chebyshev’s Chaotic Map” to provide efficiency during the authentication process. Also, they proposed a provably secure method to authenticate a group of MTCD by LTE-A Network.

II. RELATED WORKS

The verification and key Agreement protocols (AKA) used are Group-based AKA protocol (GR AKA) in which group temporary key (GTK) simplifies the whole verification procedure. The SEAKA and EAP-AKA in which access point requests identification data that are, transmitted to verification server, cocktail AKA in which mutual verification is principle design concept, Secure AKA (S-AKA) and so on. But GR AKA avoids signal clogging in the networks and also updates the policy access frequently. Signal congestion happens when verification processed to each MTC device.

Specifically, while using Group-based AKA it selects an asynchronous secret-share mechanism that can merge with Diffie-Hellman (DH) key exchange scheme to implement distributed verification and session key establishment in LTE-A networks.

III. SECURITY REQUIREMENTS AND PROPERTIES

It is well defined that IoT device computing and storage capabilities are very limited. The computation cost, communication cost, and storage requirements are essential for IoT applications. Alongside several security requirements have been identified for various authentication schemes. According to various research studies, there are many security requirements that can assure authentication schemes in different ways.

a) Physical attacks caused us to destroy the sensor nodes physically or to slink from the location. The adversary may even do more damage such that they can examine internal code and modify, extract secret keys, and inject vulnerable information. Hence this challenge may lead to going future communications in the attacker's hands.

b) Logical attacks are known to be communication attacks. These may cause to damage the nodes remotely without physical intervention of the attacker.

c) Sink-node accumulates the data from other surrounding nodes and reports to the system via wireless network access. If this is compromised the entire system will lead to a failed state because the entire deployment cost completely depends on the sink-node.

d) Indisposed programming behavior leads to susceptible software that may cause to be a code level security challenge that a malicious user can easily attack.

e) The OS should be appropriately designed, implemented and tested to defend software bugs. Ref [27] says the majority of vulnerabilities can be related to the application level.

The communication of the IoT physical system provides the successive security behaviors for secured authentication including; mutual authentication, online and offline guessing reply, session-key creation, and privileged insider attacks and so on assure security and privacy.

a. Session-key creation: A security mechanism that can establish the communication between server and client.

b. Forward Secrecy: in case one or more private keys may be compromised in any aspect by the attackers, the secrecy of the last session should not affect on next session.

c. Mutual Authentication: Every communication node that enables its mutual authentication to transmit their individual integrity and this should be done both the side vice-versa.

d. Efficiency: this can be observed by several indicators such as computation cost, storage space, interaction times and energy management.

e. Anonymity: can ensure that the sensor node must be untracked underneath of attacks performed by the adversary. It comprises of two well-known methods such as symmetric or asymmetric key cryptographic algorithm and a pseudonym.

IV. STUDY FRAMEWORK

The verification and key Agreement conventions utilized a gathering based AKA convention (GR AKA) [1] in which it rearranges the entire confirmation method by figuring a gathering transitory key (GTK). It additionally dodges flag clog in the systems and furthermore refreshes the entrance approach much of the time Diffie Hellman calculation utilized in GR AKA couldn't give message trustworthiness to redesign this component. In this paper, the algorithms Elliptic Curve Diffie-Hellman (ECDH) and Advanced Encryption Standard (AES) can be integrated called an ECDSA which addresses verification and integrity. In this algorithm there exist two distinct keys (private key and public key) and a signature. The number which is known only to the person who generated it is termed as the secret number or private key. A public key is a number that corresponds to a private key but is not secret. A signature is a notation that affirms a signing activity took place. A Mobile Type Transmission Device can be constrained by Mobile Type Transmission clients by means of Mobile Type Transmission servers when it interfaces with the LTE-A Mobile Type Transmission client can be an individual or a control focus outside the system administrator area.

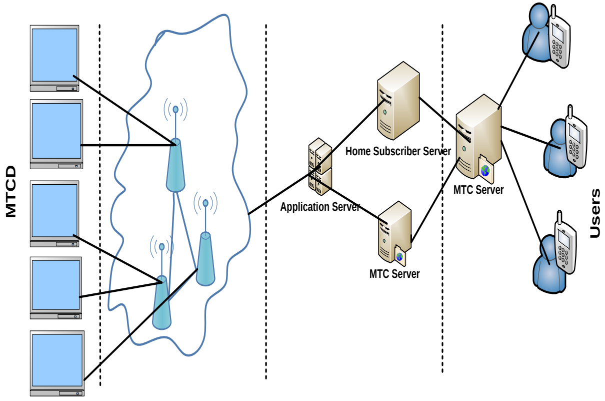

Figure 1: System Model in LTEA Networks

Approved Mobile Type Transmission clients can utilize the administrations given by at least one MTC server to work a mass of MTTD. Figure 1 depicts the proposed generic system model LTEA networks [1]. For security necessities of the framework, MTTD can confirm the use of the HSS via MME, and for set up session keys with MME. At the point that exists at least one Mobile Type Transmission Devices joining or leaving the framework. In this framework, the responsibility of the HHS, MME, and gathering pioneers can be trustworthy, while the MTTD and BS may cause to mimic over aggressors upon dispatch replay assaults, redirection invades DOS and mimics assaults.

Retrieval Number: B10311292S319/2019©BEIESP
DOI: 10.35940/ijitee.B1031.1292S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Figure 2 depicts the steps to initial verification and privacy checking.

Step 1: Access demands will be sent from some Mobile Type Transmission Devices of a similar gathering through relating MME from bunch pioneer.

Step 2: A personality demand is sent to the gathering chief from MME.

Step 3: Group leader generates the identity response. Each Mobile Type Transmission Device calculates a public key, signature and will send it to the group leader as well. In order to protect from various security vulnerabilities, a timestamp can be added into the self-identity response, subsequently, the MAC code also is computed. Then the identity response can be generated and sent over MME.

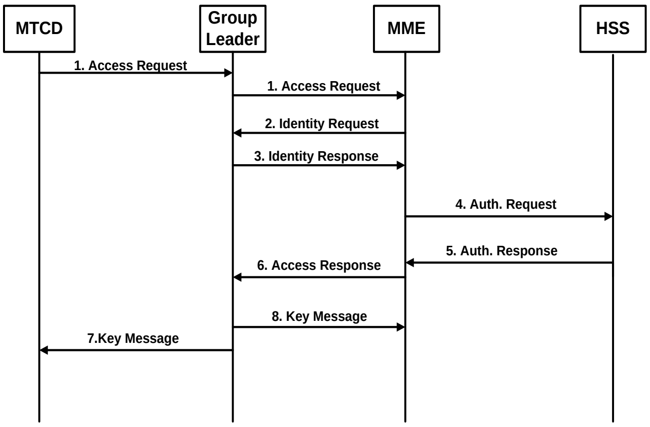

Figure 2: Initial verification and Privacy checking

Step 4: A verification information demand and the area data of the base station can be sent through MME to HSS. Because of the HSS, which checks to distinguish the false base station?

Step 5: The HSS produces the verification information reaction

Step 6: After getting a successful validation motion from HSS, MME registers an open key and creates an entrance reaction. The reaction is sent to the gathering head.

Step 7: Initially, a group leader checks to the given timestamp has exceeded the threshold or not. If it can successfully verify, the Group leader can distribute the MTTD session-key-generating message to MTCDs.

Step 8: Each Mobile Type Transmission Device in gathering requiring getting to the LTE-A system checks Mobile Type Transmission Device, and figures the session key utilizing MME checks and processes a mystery session key with each Mobile Type Transmission Device. Hence, after an effective common confirmation, each Mobile Type Transmission Device and their SN share a mystery session key for correspondence safely.

V. RESULTS AND DISCUSSIONS

The results of this proposed model basically carries based on two measurements such as amount signaling message traffic and cost computation. The expected scheme may reduce the signaling cost in terms sending the messages through MTTD device. Fig 3 depicts the comparison between other proposed methods. This was the sample performance evaluation considered based on various networks such as edge network, access network and main network. The evaluated performance metrics can be based on the signaling message exchanges. We have considered this networking scenario based on n number of MTTD devices cells. We assumed that all other schemes require n number of times of total signaling message exchanging per unit time. Moreover, we have different number of groups for generating and distributing keys for cryptographic function and verification of the user as well. In order to increase the performance of various groups in terms of various networks namely edge, aces and main network signaling.

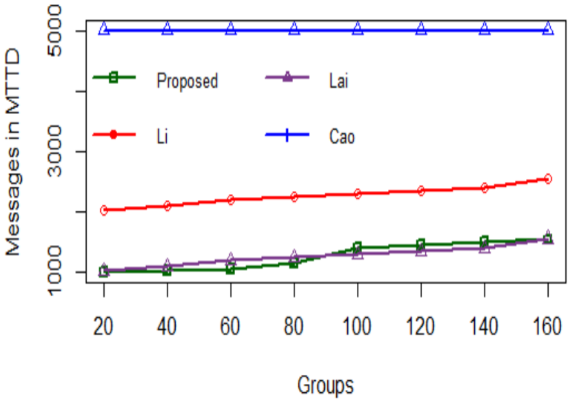

Figure 3: Message traffic in MTTD

In this paper the table 2 depicts the performances of various methods comparing with our proposed method to evaluate the total number of messages exchanged.

Table 2: No of Messages exchanging

Scheme	Edge N/W	Access N/W	Main N/W	Total
Lao	$N+1$	$N+3$	2	$2N+6$
Li	$2N$	4	2	$2N+6$
Lai	$2N$	3	2	$2N+5$
our	$2N$	2	2	$2N+4$

According the details included in fig 3 the performance of the proposed model is expensive when compared with some other models. However, this perform better when compared with traditional models but not with light weight models because light weight protocols uses hash functions for reducing the over heads and increasing the performances. Therefore the future work will carry based on the comparison

VI. DISCUSSIONS AND CONCLUSIONS

Secure and efficient AKA provides powerful security insurance and protection conservation. The lightweight group verification protocol utilizes a pre-shared gathering key. Dynamic Verification and Key Agreement based on group additionally utilize the pre-shared gathering key. In addition to that, the creation of group key and group key update schemes are suggested to achieve dynamic nature. Group based Handover verification reduces the signaling costs in both the access network and the core network; also achieves the preservation of privacy.

Group-Based AKA protocol with dynamic updating policy. Particularly, they selected asynchronous based shared secret key joined with Diffie-Hellman (DH) key interchange procedure onto establish the distributed verification and session-key in LTE Advanced networks. However, the DH algorithm could not provide message integrity to upgrade the security feature namely integrity. In this paper, propose the algorithms Advanced Encryption Standard (AES) and Elliptic Curve Diffie-Hellman (ECDH) can be integrated called an Elliptic Curve Digital Signature Algorithm (ECDSA) which addresses integrity and verification. ECDSA is a cryptographic algorithm used to ensure rightful owners.

The results comparison of this work can be further extended and produced in another variant. And further will discuss efficiency.

REFERENCES

1. Li, J., Wen, M. and Zhang, T., 2016. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. IEEE Internet of Things Journal, 3(3), pp.408-417.
2. Khumalo, P., Nleya, B., Gomba, A., & Mutsvangwa, A. (2018, December). Services and Applications Security in IoT Enabled Networks. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)* (pp. 1-7). IEEE.
3. Lai, C., Li, H., Lu, R., Jiang, R. and Shen, X., 2013, December. LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks. In 2013 IEEE Global Communications Conference (GLOBECOM) (pp. 832-837). IEEE.
4. Cao, J., Li, H. and Ma, M., 2015, June. GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks. In 2015 IEEE International Conference on Communications (ICC) (pp. 3020-3025). IEEE.
5. Fu, A., Song, J., Li, S., Zhang, G. and Zhang, Y., 2016. A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks. Security and Communication Networks, 9(13), pp.2002-2014.
6. Modiri, M. M., Mohajeri, J., & Salmasizadeh, M. (2018, December). GSL-AKA: Group-based Secure Lightweight Authentication and Key Agreement Protocol for M2M Communication. In 2018 9th International Symposium on Telecommunications (IST) (pp. 275-280). IEEE.
7. Gazis, V., 2017. A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Communications Surveys & Tutorials, 19(1), pp.482-511.
8. Kong, Q., Ma, M., & Lu, R. (2017, September). Achieving Secure CoMP Joint Transmission Handover in LTE-A Vehicular Networks. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)* (pp. 1-5). IEEE.
9. Sharma, S., & Bilandi, N. (2017). Augmenting Security for Identity-based Batch Verification Scheme using TDMA based MAC Protocol in VANET. International Journal of Computer Applications, 162(9).
10. Koti, N., Keni, E., & Purushothama, B. R. (2015, August). Non-tree Based Group Key Management Scheme With Constant Rekeying and Storage Cost. In Proceedings of the Third International Symposium on Women in Computing and Informatics (pp. 564-572). ACM.
11. Wang, Z., Huo, Z., & Shi, W. (2015). A dynamic identity-based authentication scheme using chaotic maps for telecare medicine information systems. Journal of medical systems, 39(1), 158.
12. Au, M. H., Liang, K., Liu, J. K., Lu, R., & Ning, J. (2018). Privacy-preserving personal data operation on the mobile cloud—Chances and challenges over the advanced persistent threat. Future Generation Computer Systems, 79, 337-349.
13. CheonJH, KimY, YoonHJ.A new ID-based signature with batch verification. Trends in Mathematics Information Center for Mathematical Sciences 2005; 8(1): 119–131.
14. Cheng X, Liu J, Wang X. Identity-based aggregate and verifiably encrypted signatures from bilinear pairing, Proceeding of ICCSA’05, LNCS 3483, Singapore, 2005; 1046–1054.
15. Lamport L. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers. Addison-Wesley Publishing Company: Boston, USA, 2002.
16. Al-Turjman, F., & Mostarda, L. (2019). A hash-based RFID authentication mechanism for context-aware management in IoT-based multimedia systems. Sensors, 19(18), 3821.
17. Narayana P, Chen R, Zhao Y, Chen Y, Fu Z, Zhou H. Automatic vulnerability checking of IEEE 802.16 WiMAX protocols through TLA+, Proceedings of 2nd IEEE Workshop on Secure Network Protocols, CA, USA, 2006; 44–49.
18. Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 101, 55-82.
19. Deebak, B. D., Ever, E., & Al-Turjman, F. (2018). Analyzing enhanced real-time uplink scheduling algorithm in 3GPP LTE-advanced networks using multimedia systems. Transactions on Emerging Telecommunications Technologies, 29(10), e3443.
20. Roychoudhury, P., Roychoudhury, B., & Saikia, D. K. (2018). Provably secure group authentication and key agreement for machine type communication using Chebyshev’s polynomial. Computer Communications, 127, 146-157.

AUTHORS PROFILE

Pedada Saraswathi* obtained the degree of M.Tech from JNTUK Kakinada, India, 2016. She had around 2 years of academic experience. She is currently working as Assistant Professor, GITAM, Visakhapatnam, India. Her research includes Computer Networks, Wireless Networks, and Network Security and Machine Learning**.**

Patruni Muralidhara Rao obtained the degree of M.Tech (Software Engineering), JNTUH, Hyderabad, India, 2014. He worked as Assistant Professor GITAM, Visakhapatnam, India. His research includes Computer Networks, Wireless Networks, and Network Security.

REDDY PRASAD A Obtained the degree of MCA and M.Tech at JNTUA, Ananthapur, India. He had 4 years of Industry experience and 1 year of academic experience. Assistant Professor, Mother Theresa Institute of Engineering and Technology, Palamner, India. His research interests include Computer Networks, Cyber Security

RK Chandana Mani Obtained the degree of M.Tech at JNTUA Ananthapur, India, 2016. She had 1 year of academic experience. She worked as Assistant Professor, Dept. Of CSE, Mother Theresa Institute of Engineering and Technology, Palamner, India. Her research interests include Image Security, Biomedical Images, Wireless Networks, and Internet of Things.