International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Hierarchical Group Authentication and Key agreement for Machine Type Communication in LTE Networks

Srinivas Kalime[1], Dr. K. Sagar[2]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: The 3GPP LTE-A standard for Machine Type Communication (MTC) was created to facilitate communication between entities without human involvement, in response to the rapid increase in wireless data communication volume. The conventional Mutual Authentication and Key Agreement (AKA) mechanism in LTE networks is struggling due to the rising signaling load caused by the expanding device count. Group-based architecture has been proposed as a solution in the literature to solve authentication traffic, but it has its own problems.

In this paper, we propose a hierarchical group based mutual authentication and key agreement (HGMAKA) protocol to address these challenges. This protocol ensures privacy, prevents unauthorized access to information, and helps prevent many types of assaults such as replay attacks, distributed denial of service, and man-in-the-middle attacks. The proposed protocol enables MTC services to be supported by small cells with heterogeneous architecture that aligns with 5G networks. The Aggregate Message Authentication Code based approach is more lightweight, resource-efficient, robust against authentication message failures, and scalable to heterogeneous network topologies compared to earlier protocols. We experimented our proposed system and the results demonstrated increased efficiency, resolved existing difficulties, and will enhance the reliability and security of the M2M system.

Keywords: *Authentication, Key management, Lightweight Cryptography, IoT, WSN, Machine-type communications.*

I. Introduction

Machine Type Communication (MTC) is a significant mobile communication method in the Internet of Things (IoT), serving as one of the communication methods in future mobile communications. When multiple MTC devices attempt to access the network simultaneously, each MTC device must undergo individual identity validation, resulting in network congestion. A dynamic group-based identity authentication and key agreement system was developed in Long Term Evolution-Advanced (LTE-A) networks to address the problem and enhance the security of key agreement for MTC devices. The introduction of new high speed cellular systems, the wireless communication field has been coined M2M (machine to-machine) or MTC (machine-to-computer) communication [1,2] is termed as communication without any human involvement. These devices are Machine Type Communication Devices (MTCD'S). In Health care services, fleet management, smart grid, and other scenarios will all benefit from the MTC. These are hardware-based machines deployed in a closed system. These use point-to-point one way communication usually embedded in hardware [3,4]. The main purpose of these devices is to monitor and control. These machines deal only with structured data and it always operates via triggered responses based on an action. Example of these machines is that vending machine whenever a refill is required and it will communicate to distributor's machines. Any Networked Devices capable of performing actions without any interventions can be termed as Machine-to-Machine communication. This has laid the foundation for the IoT (Internet of Things). The M2M systems captures sensor data and transmit it to the network. Public Networks are used by M2M Systems for cost effectiveness like cellular or Ethernet. The M2M [5,6] system has sensors Wi-Fi or cellular communications link etc to perform triggered actions on some conditions.

A. Motivation and Contribution of the paper

Machine Type Communication are associated with big numbers of sensors tracking a few devices nation or events or actuation for an environment. These devices are mostly easy to manage but must always take highest level of safeguarding these devices to protect the surveillance and monitoring and controlling of homes or offices or buildings or traffic etc. Securing these devices is very crucial the efficient and secure protocol was being proposed to be used in M2M system. The scope of this paper is to layout and put in force a stable and light-weight key management protocol that enables the low resource nature of IoT devices, i.e. this device use much less quantity hardware and power required to system.

[1] *Research Scholar, Department of Computer Science and Engineering University College of Engineering, Osmania University, Hyderabad, Telangana, India,*
E-mail: srinivaskits966@gmail.com
[2] *Professor, Department of Computer Science and Engineering,*
Sreyas Institute of Engineering and Technology, Hyderabad, Telangana, India

i. Our Contribution

- A proposed solution to tackle the aforementioned problems involves the implementation of a streamlined key management protocol that utilizes a symmetric key method.
- The implementation utilizes a modified version of the Diffie-Hellman key exchange algorithm to ensure group authentication.
- Given the presence of a pre-existing, reliable pathway connecting the Femtocells to the HSS, the solution is deemed secure and can effectively address the challenges of the current system.
- Our system is resistant to attacks due to its utilization of lightweight encryption, such as the TEA algorithm.
- Our method aims to address the shortcomings of the existing system and enhance the reliability and security of the M2M system.

B. Organization of paper

The rest of the paper is organized as follows: In section 2, we present M2M communication security and section 3 explains the related work and the drawbacks in existing methods. Section 4 discusses the proposed method procedure and its overview and experiment results presented in section 5. Security analysis of the proposed method is presented in, and the outputs are kept for analysis in section 6, section 7 concludes the paper.

II. M2M Communication Security

There are many key features of M2M Communications [11,12]. The major advantage is always low power usage by the devices so efficiency increased and M2M service is done effectively. Packet-switched service monitoring abilities are given by network operator which provides with capacity of event detection. Time control and tolerance is an amazing feature where, delayed transfers are accepted by system and also data can be sent or received at predetermined intervals[44]. When a device enters area triggers are automatically set to alert the devices. Since the data sent by the devices is very less it's continually sent.

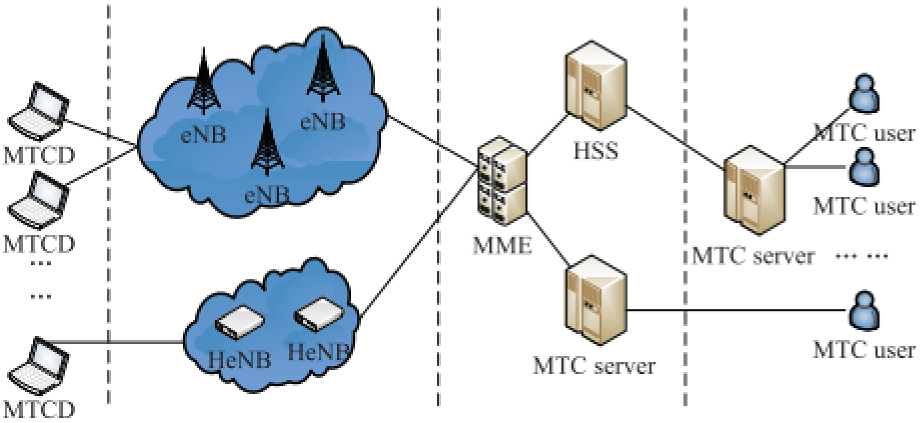


Fig1: Network architecture of M2M Communications

A. Requirements for M2M Communication

There are some standards that are required for this Machine-to-Machine communication [6,7,8]. Scalability. The efficient functioning of the system should be very robust such that more addition of machines is done on the go. Anonymity is whenever there is requirement the system of M2M must hide the identity of the devices. It's done such as to secure devices while re-connecting to the network [23,24]. Logging is a major requirement cause important events such as failures, faulty operations and service down time can be traced to investigate what went wrong in the M2M system. Communication principles in M2M systems enable communication in M2M applications [18,19,20] in the network so that all objects in the system can communicate with each other in a peer-to-peer manner. The M2M system sometimes minimizes the load on the network such that all the objects must support uni or multi or any-cast communication methods. Message transmission scheduling is done for just to maintain delay tolerances in the network[25]. To make a Machine-to-Machine system secure the physical device must be made tamper-resistant. The network being used must also be secure. In the backend server security must also be implemented to make Machine-to-Machine communication more secure. Since there is no human intervention, all these elements must be strongly encrypted when the devices are either offline or online.

B. M2M Authentication

Authentication plays a major part in Machine-to-Machine communications [4,9]. For efficiency and due to increase in the number of devices the scheme that is being used must be faster and also should give less overhead. There are different authentication schemes for M2M, however the main motive here is group authentication in an efficient way.

C. M2M Key management

Key Management is an important security characteristic for M2M communications. For efficient communication light weight key distribution is used in M2M communications [8,9]. There are different key distribution mechanisms used in M2M communications such as group key distribution, individual key distribution etc. The main motive of key management is to use light weight cryptography and increase the efficiency of the system.

III. Related Work

Previous research works in [2,3,13,15,16] has addressed security in group-based communication that takes sensor networks into account, with recommendations that increase performance. The result after these phases is to share a unique secret session key with network. A group key GK_i is assigned to a group which has some number of MTCD's by the operator. Through a secure channel the group key GK_i is shared between all the elements. All MTCD devices have a manufacturer given number known as IMSI (Unique International Mobile Subscriber Identity Number) signaling messages The protocol reduces signaling messages because of hierarchical authentication which uses aggregate messages. Re-authentication increases with larger group size, but in case of failure entire group need not be re-authenticated. Communication cost for a full round the costs are calculated. This protocol when compared to others in multiple smaller group size there are other protocols which perform little better such as SE-AKA[7], Choi-AKA[27] etc. Computational cost of the cryptographic operations like hashing, pairing, ex-oring and were considered. The cost by this protocol is very low, and the same with three protocols: MTC-AKA[28], Choi-AKA[27], and G-AKA.

During the authentication stage of the proposal, asymmetric cryptography [27] is used, which demands more computer power than symmetric cryptography. A protocol known as GLARM (group-based lightweight authentication scheme for resource-constrained machine-to-machine communications) was described in [28,29]. It offers quick and mutual group authentication as well as key agreement and is entirely based on symmetric keys and hash functions. Its differentiation is the use of location area identification (LAI) of the base station involved in the authentication method to prevent assaults originated from intruder base stations. It comprises of two phases: Initialization and group authentication and key agreement. Base stations are uniquely identified by LAI.

Based on symmetric cryptography, the protocol created by [32, 33] controls a collection of devices using a binary tree in which each node is given a secret value that is inherited from its parents. In addition to allowing each device to be authenticated concurrently with the group leader and establishing distinct session keys between the MME and each device, the tree offers an effective and secure framework for managing groups of devices. The secret values of the common tree nodes connecting every device to the MME and a random number produced by the HSS during the authentication process serve as the foundation for the session key [34].

A. Drawbacks in Existing Method

In the existing methods [21,22] group key can be known by any user who newly joins the group and since each parameter is sent in plain text to the next tiers so it will be easy to perform a man in the middle attack on the network. In replay attack, an attacker captures the messages and may use it for the current session in the authentication and for further rounds fresh random numbers are generated for a new round of authentication. Since there is no encryption used in the communication process there's a chance of getting some device IMSI numbers and acting as a legitimate device by the intruder. This method puts the whole system at risk of being attacked by an intruder. Also, there is a performance issue when a new device joins the whole group must be dynamically updated with a new group key and the authors did not discuss anything further about this group authentication scenario which makes the existing method not only vulnerable but also less efficient in terms of group authentication.

IV. Proposed Method

This section presents in detailed steps our proposed hierarchical authentication and key agreement for machine type communication devices.

A. Overview of the scheme

The proposed system reduces the signaling cost and increases the efficiency of the group authentication procedure using light weight cryptography. There is hierarchical authentication between the devices and the home subscriber server.

This proposed scheme, each device has a unique number called IMSI (International Mobile Subscriber Identity). Each device sends a Message which includes it's IMSI and a random number a_{imsi-i} to the Tier-2. For each group the generated random numbers of every MTCD devices are added by the Femtocell to set a value known as

$$\mathrm{RG}_i = \sum_{i=1}^{n} a_{imsi-i}$$

This is used as a value to set a key for the whole group by the HSS (Home Subscriber Server) and even the HSS will set a random number and uses Diffie Hellman to authenticate the whole group by coming to the same key

K at the both ends. Thus, this modified use of Diffie Hellman for the group authentication procedure makes the Tier-2 and the HSS derives the same key at both the ends.

B. Details of the Proposed Method

The communication link between the Mobility Management Entity (MME) and the Home Subscriber Server (HSS), as well as between Tier-3 and Tier-2 components, is pre-established and secured using the Diameter protocol. Diameter is a protocol used for Authentication, Authorization, and Accounting (AAA) purposes in telecommunications networks. It ensures secure communication between network elements. Additionally, this communication link can provide security services for the transmitted data, ensuring confidentiality, integrity, and authenticity.

The Group Key (GK) is a cryptographic key established by the Network Operator. It is used for securing group communications within the network. The HSS (Home Subscriber Server) plays a significant role in network authentication and authorization processes. It publishes a prime number P and a generator g of prime P to the network. These parameters are essential for cryptographic operations, particularly in establishing secure communication channels and generating cryptographic keys.

Each device within the network is assigned a unique secret key, denoted as Kij. This key is shared between the device and the HSS (Home Subscriber Server). The unique secret key Kij is used for various security purposes, such as authentication, encryption, and integrity verification. It ensures that communication between the device and the network remains secure and private. Having a unique secret key for each device enhances security by limiting the impact of potential key compromises and unauthorized access attempts.

i. The communication link between MME and HSS and Tier-3 to Tier-2 is pre-established and secure (based on Diameter protocol [37]), it can also supply security service for the transmitted data. The Group Key is GK which is setup by the Network Operator. HSS also publishes a Prime P and a generator g of Prime P to the network.

ii. A Unique secret key K_{ij} is with each, and every device will also be with the HSS.

he proposed system has two phases:

a. message aggregation phase

b. authentication and key agreement phase.

a. Message Aggregation Phase

i. Each device has a unique number called as IMSI (International Mobile Subscriber Identity)

ii. Each device sends a Message which include it's IMSI and a random number a_{imsi-i} to the Tier-2 $MSG_{-MTCDi} = IMSI_i + a_{imsi-i}$

iii. Group formation is done by the Operator based on different criteria's such as location, availability to the nearest femtocells etc.

iv. Based on location the femtocell which is Tier-2 device aggregates all the Messages and forms a single Message which is Agg.MSG – G_i.

v. For each group the generated random numbers of every MTCD devices are added by the Femtocell to set a value known as

$$\mathrm{RG}_i = \sum_{i=1}^{n} a_{imsi-i}$$

b. Authentication and Key Agreement Phase

i. HSS publishes a prime P and a generator g. For each group HSS selects a secret $RHSS_i$ and calculates $HSS_i=g^{RHSSi}$ mod P.

ii. Femtocell for each and every group it generates a random number b_i and adds it with RG_i, $c = RG_i + b_i$ and calculates $TS_i = g^c$ mod P.

iii. For each and every group the TS_i is sent to HSS and HSS sends HSS_i.

iv. At both the ends HSS and Femtocell, key agreement is done by multiplication under modulus P. i.e., K = (TS_i). (HSS_i) mod P.

i.e. K = g^c mod P. g^{RHSSi} mod P

= g $(^{C*RHSSi}$)mod P

v. Now both the ends have the same key K, femtocell encrypts the aggregated messages of each group using the group key and sends it to MME. MME just adds the serving network identity SN − ID to the aggregated messages.

vi. HSS receives these aggregated messages Agg.MSG $_{-Gi}$ from every group, it decrypts the messages using group key GK and it forms a table known as the group table.

vii. Session keys SK_{MTCDi} for each MTCD is generated by the HSS using the IMSI number $IMSI_i$ and group-ID and random number a_{imsi-i} .

Identifier	IMSI	Rand.mtcd	Session Key
GID_{Gi}	$IMSI_{gi}$	R_{IMSI-i}	SK_{IMSI-i}
GID_{Gj}	$IMSI_{gj}$	R_{IMSI-j}	SK_{IMSI-j}
GID_{Gk}	$IMSI_{gk}$	R_{IMSI-k}	SK_{IMSI-k}

Table 1: At HSS

viii. Each group table has group-ID and IMSI number and random number column and session key column. The session key column is filled with the generated session keys SK_{MTCDi}. group table is formed for each group.

ix. This group table is now encrypted with the key K and sent to the Femtocell. Femtocell receives this encrypted message and decrypts it with key K.

x. The session keys SK_{MTCDi} of each MTCD device are first encrypted with the random number a_{imsi-i} and then sent to the respective MTCD devices.

xi. The MTCD Devices decrypts the session key and uses that key for a respective time interval. Thus, secrecy is maintained throughout the communication process.

Overall, the process of decrypting and using session keys for communication sessions enables MTCD devices to maintain secrecy and confidentiality throughout the communication process. By leveraging encryption techniques and secure key management practices, the integrity and privacy of data exchanged within the network environment are preserved, mitigating potential security threats and vulnerabilities.

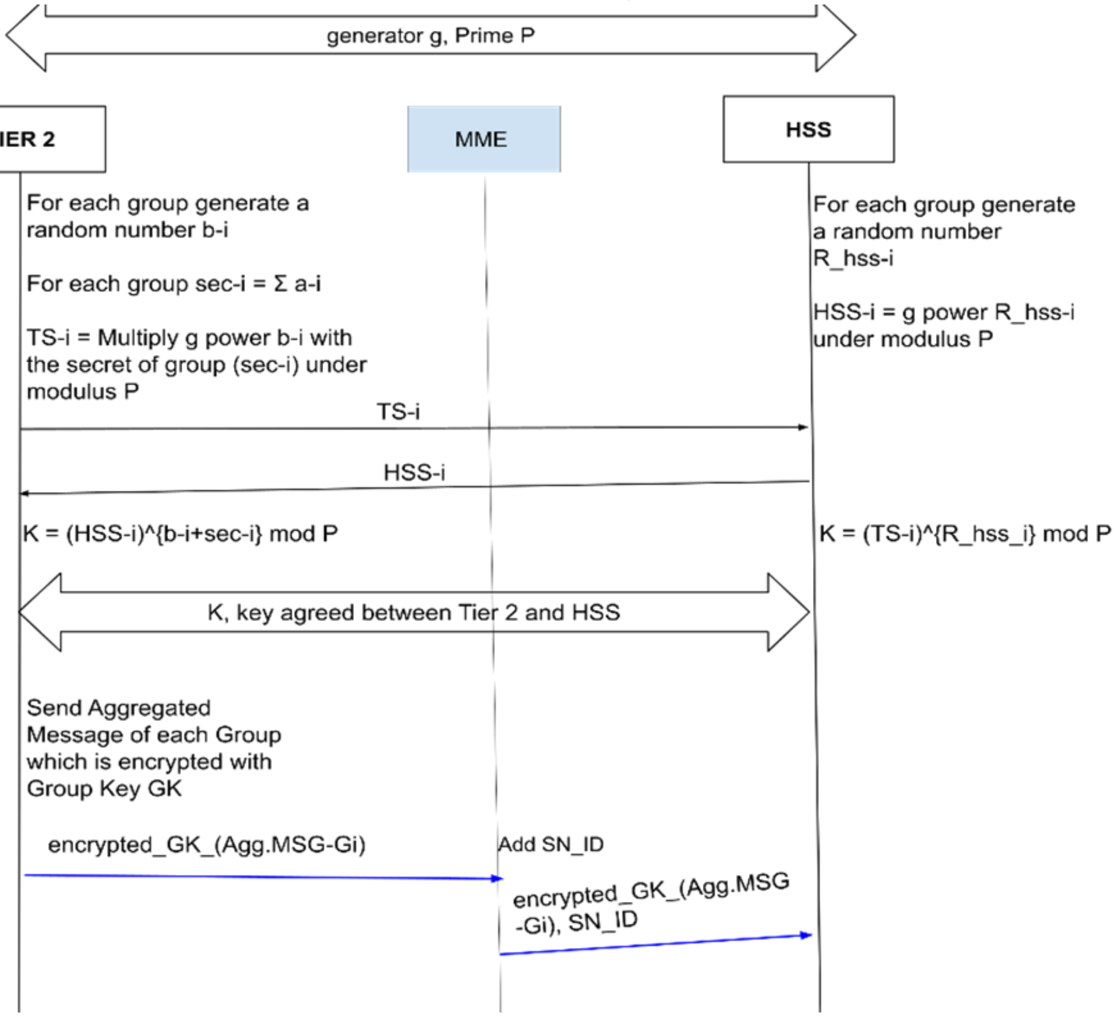

generator g, Prime P
TIER 2
MME
HSS
For each group generate a random number b-i
For each group sec-i = Σ a-i
TS-i = Multiply g power b-i with the secret of group (sec-i) under modulus P
For each group generate a random number R_hss-i
HSS-i = g power R_hss-i under modulus P
TS-i
HSS-i
K = (HSS-i)^{b-i+sec-i} mod P
K = (TS-i)^{R_hss_i} mod P
K, key agreed between Tier 2 and HSS
Send Aggregated Message of each Group which is encrypted with Group Key GK
encrypted_GK_(Agg.MSG-Gi)
Add SN_ID
encrypted_GK_(Agg.MSG -Gi), SN_ID

Fig.2. Interactive process of our Authentication and Key Agreement Phase.

The figure 2, describes a process wherein Machine-Type Communication Devices (MTCDs) decrypt session keys received during communication establishment and utilize them for specific time intervals to maintain secrecy throughout the communication process. This approach ensures confidentiality by securely transmitting and decrypting session keys, which are then used exclusively for encrypting and decrypting data during active communication sessions. Regular key rotation further enhances security. Overall, this method safeguards the integrity and privacy of data exchanged within the network, mitigating potential security risks.

V. Experiment Results

The proposed scheme is implemented in and also was written in SPDL (Security Policy Definition Language). In Java the 5 tiers which are the end devices and Tier-2 which is Femtocells and MME and HSS and two end devices were coded in Java and was tested for the performance and also security analysis done. The output was taken and was analyzed for the performance. The experiment's goal was to see performance of the protocol when implemented on devices. The number of computations performed, and the amount of storage required to store data required by the protocol are important parameters that protocol designers must optimize in devices. As a result, we assessed the protocol's performance in terms of these two parameters. This section presents the performance and security analysis results that were obtained from implementations of Gateway, Node1, and Node2 on a Java socket programming for time and space consumption.

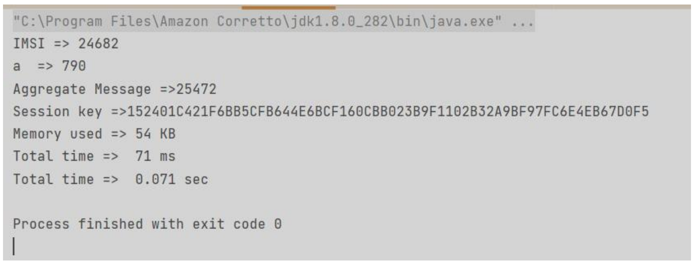
Memory used table-2 and table-3 show the total amount of resources (memory, and time) that the protocol requires. In terms of memory, HSS uses 143Kb of memory, MME uses 100Kb of memory, Femtocell uses 89Kb of memory, Node1 and Node2 requires 54Kb of memory to store the program code. The time taken by each component for operation is as follows: HSS has taken 4371ms, MME has taken 2371ms, Femtocell has taken 1548ms, node1 and node2 have taken 71 and 47ms respectively.

Parameter	Components	Memory Used (Kb)
Memory Usage	HSS	143
	MME	100
	Femtocell	89
	Node1	54
	Node2	54

Table-2: Memory Used

Table-3: Execution Time

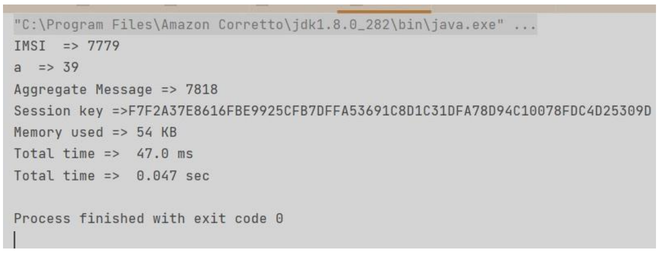
Parameter	Components	Time(ms)
Execution times	HSS	4371
	MME	2371
	Femtocell	1548
	Node1	71
	Node2	47



```
"C:\Program Files\Amazon Corretto\jdk1.8.0_282\bin\java.exe" ...
IMSI => 24682
a  => 790
Aggregate Message =>25472
Session key =>152401C421F6BB5CFB644E6BCF160CBB023B9F1102B32A9BF97FC6E4EB67D0F5
Memory used => 54 KB
Total time =>  71 ms
Total time =>  0.071 sec

Process finished with exit code 0
```

Fig. 6. Output at Node1



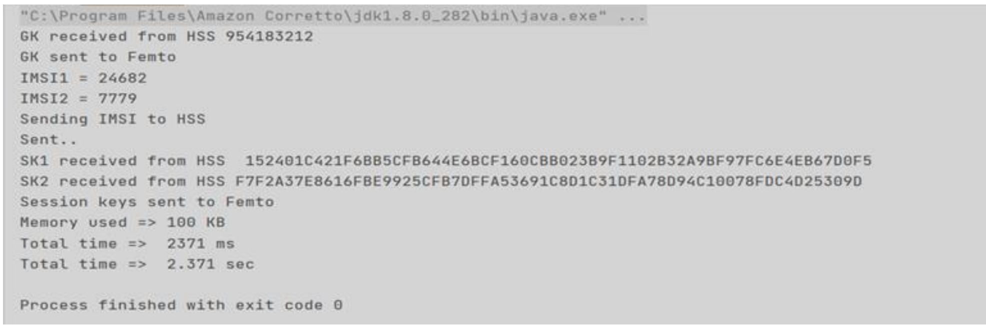
```
"C:\Program Files\Amazon Corretto\jdk1.8.0_282\bin\java.exe" ...
IMSI  => 7779
a  => 39
Aggregate Message => 7818
Session key =>F7F2A37E8616FBE9925CFB7DFFA53691C8D1C31DFA78D94C10078FDC4D25309D
Memory used => 54 KB
Total time =>  47.0 ms
Total time =>  0.047 sec

Process finished with exit code 0
```

Fig. 7. Output at Node2

In Node1, Output shows generating IMSI and Random Number and sent forward to get the session key.

In Node2, Output shows generation of IMSI and Random Number and sent forward to get the session key.

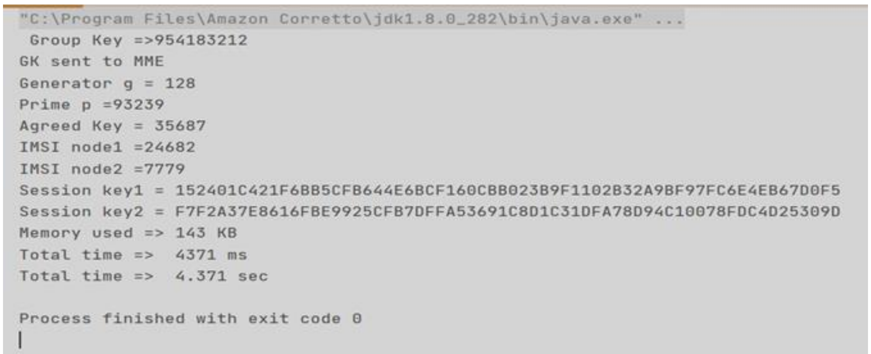


```
"C:\Program Files\Amazon Corretto\jdk1.8.0_282\bin\java.exe" ...
GK received from HSS 954183212
GK sent to Femto
IMSI1 = 24682
IMSI2 = 7779
Sending IMSI to HSS
Sent..
SK1 received from HSS  152401C421F6BB5CFB644E6BCF160CBB023B9F1102B32A9BF97FC6E4EB67D0F5
SK2 received from HSS F7F2A37E8616FBE9925CFB7DFFA53691C8D1C31DFA78D94C10078FDC4D25309D
Session keys sent to Femto
Memory used => 100 KB
Total time =>  2371 ms
Total time =>  2.371 sec

Process finished with exit code 0
```

Fig. 8. Output at MME

In MME, Output shows session keys of Node1 and Node2 received and are then sent to Femtocell.

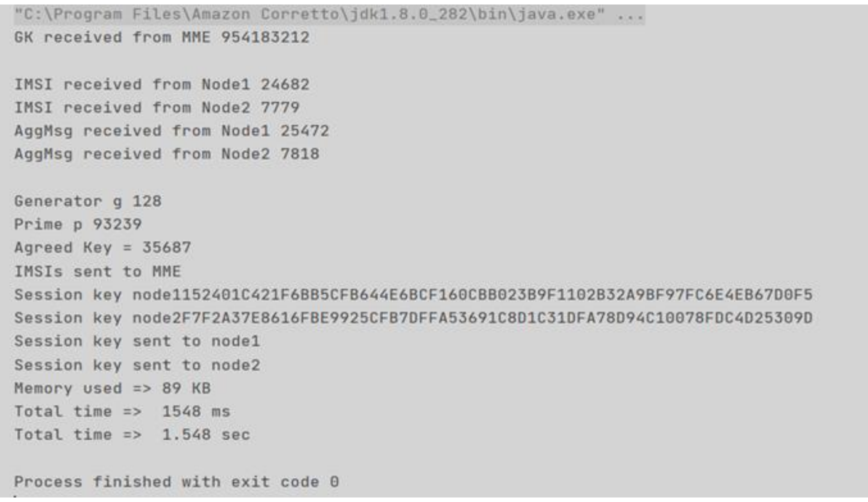


```
"C:\Program Files\Amazon Corretto\jdk1.8.0_282\bin\java.exe" ...
 Group Key =>954183212
GK sent to MME
Generator g = 128
Prime p =93239
Agreed Key = 35687
IMSI node1 =24682
IMSI node2 =7779
Session key1 = 152401C421F6BB5CFB644E6BCF160CBB023B9F1102B32A9BF97FC6E4EB67D0F5
Session key2 = F7F2A37E8616FBE9925CFB7DFFA53691C8D1C31DFA78D94C10078FDC4D25309D
Memory used => 143 KB
Total time =>  4371 ms
Total time =>  4.371 sec

Process finished with exit code 0
|
```

Fig. 9. Output at HSS

In HSS, Output shows publishing public parameters such as a generator g and prime P and shows generation of session keys for Node1 and Node2. Overall, the process of publishing public parameters and generating session keys within the HSS enables the establishment of secure communication channels between nodes within the network, ensuring the protection of sensitive information and the integrity of data exchanges.



```
"C:\Program Files\Amazon Corretto\jdk1.8.0_282\bin\java.exe" ...
GK received from MME 954183212

IMSI received from Node1 24682
IMSI received from Node2 7779
AggMsg received from Node1 25472
AggMsg received from Node2 7818

Generator g 128
Prime p 93239
Agreed Key = 35687
IMSIs sent to MME
Session key node1152401C421F6BB5CFB644E6BCF160CBB023B9F1102B32A9BF97FC6E4EB67D0F5
Session key node2F7F2A37E8616FBE9925CFB7DFFA53691C8D1C31DFA78D94C10078FDC4D25309D
Session key sent to node1
Session key sent to node2
Memory used => 89 KB
Total time =>  1548 ms
Total time =>  1.548 sec

Process finished with exit code 0
```

Fig. 10. Output of Femtocell

In Femtocell, output shows agreed key between HSS is shown and using the group table session keys are sent to individual devices. In a Femtocell network, the output typically displays the agreed-upon key between the Home Subscriber Server (HSS) and the Femtocell. This key is crucial for establishing a secure communication channel between the Femtocell and the core network. Once this key is established, the Femtocell utilizes a group table to distribute session keys to individual devices within its coverage area.

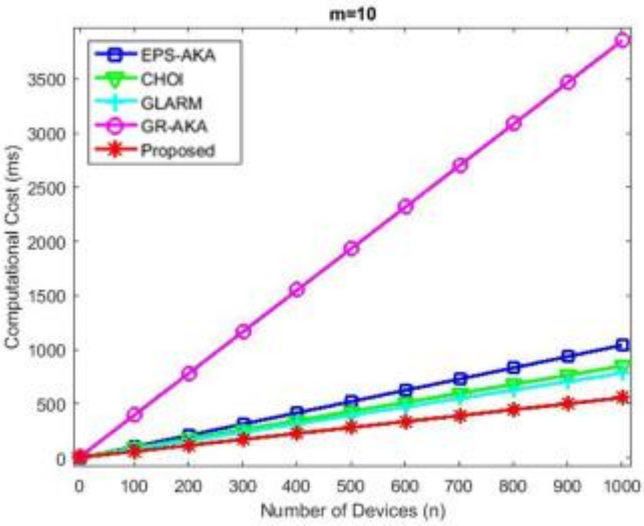


Fig. 11. Comparison of computational costs, for m = 10.

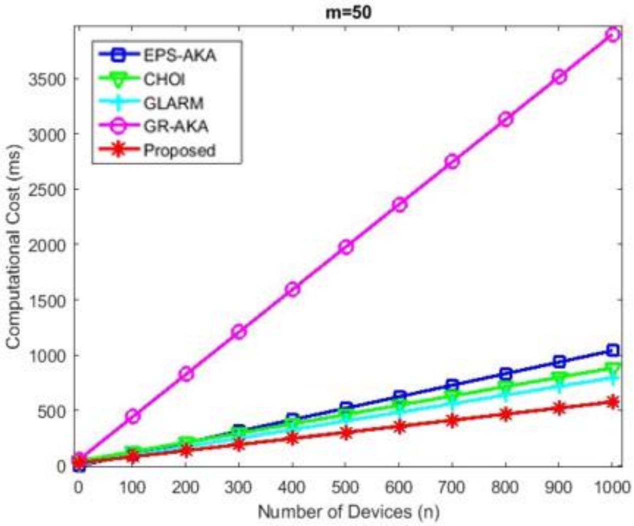


Fig.12. Comparison of computational costs, for m = 50.

For specific values of m (where m represents the number of groups), Figures 11 and 12 illustrate the computational costs of the five examined protocols in relation to the number of devices. Both the formulas and graphs demonstrate that the communication cost escalates linearly with the number of devices (n). Generally, the proposed protocol outperforms existing protocols as the number of devices increases, particularly when the number of groups is expanded to 50. This observation indicates the efficiency and scalability of the suggested protocol in managing communication costs across a growing network of devices, offering a promising solution for large-scale deployments.

VI. Security And Complexity Analysis

The proposed scheme does not require many complex operations. It just uses aggregation and Diffie Hellman key exchange and through a secure channel. The proposed scheme is very efficient in terms of speed. It distributes the symmetric key. When there is a key agreement going on Femtocell end by the HSS the only processing power is taken by Femtocell and the HSS only and when the session keys are sent to each individual MTCD's then they decrypt using the random number which they generated. This scheme uses as much less storage as possible and since HSS is a high-end machine which can set up a safe prime P and a generator g and publicly broadcast to any Tier devices which want communication with the HSS. In the outputs we can see that the devices are taking around only 40-70 milliseconds which is a good start, similarly when there are many devices then the time needed to authenticate also becomes very less.

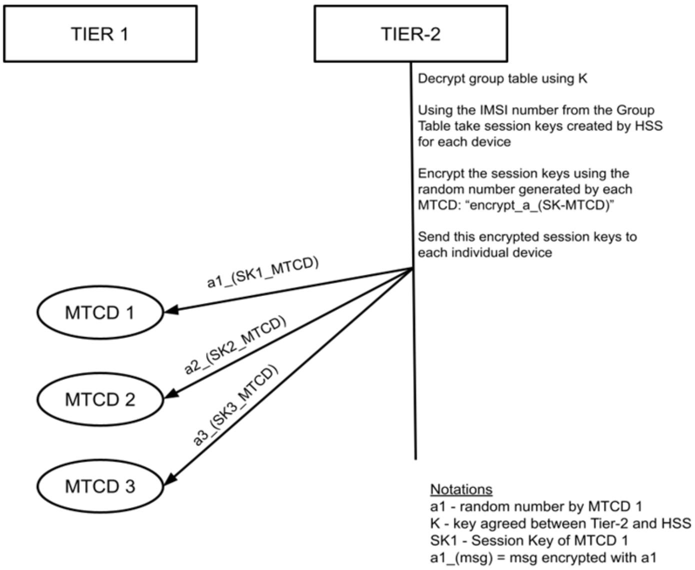
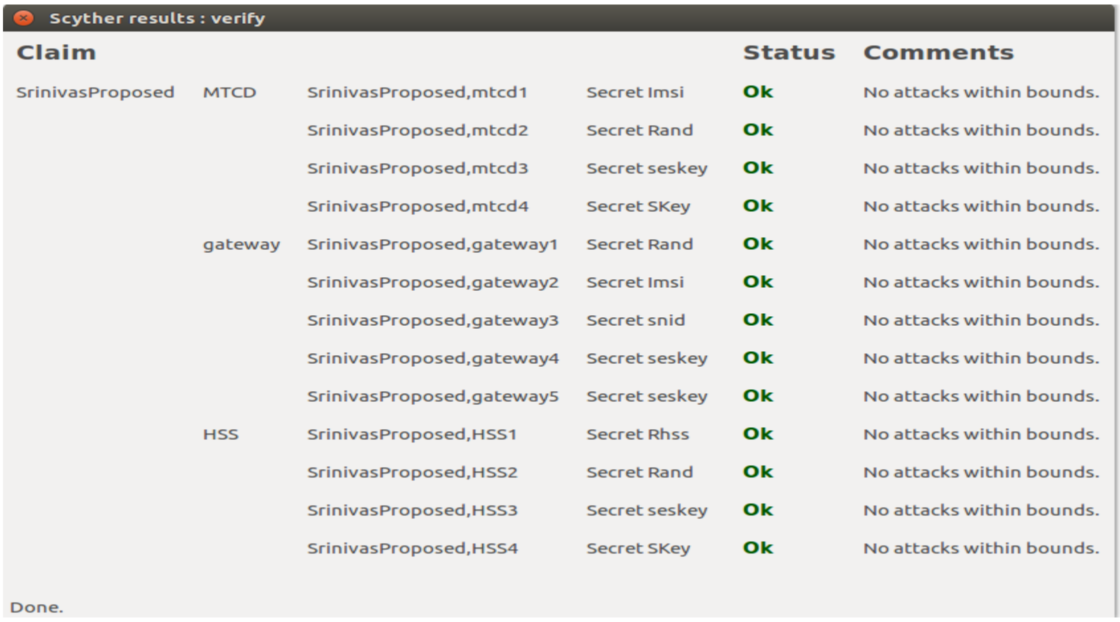

TIER 1
TIER-2
Decrypt group table using K
Using the IMSI number from the Group Table take session keys created by HSS for each device
Encrypt the session keys using the random number generated by each MTCD: "encrypt_a_(SK-MTCD)"
Send this encrypted session keys to each individual device
a1_(SK1_MTCD)
a2_(SK2_MTCD)
a3_(SK3_MTCD)
MTCD 1
MTCD 2
MTCD 3
Notations
a1 - random number by MTCD 1
K - key agreed between Tier-2 and HSS
SK1 - Session Key of MTCD 1
a1_(msg) = msg encrypted with a1

Fig. 3. Session Key Distribution by Tier-2: Femtocell

A. Scyther Results

The experiment's goal was to see performance of the protocol when implemented on devices. The number of computations performed, and the amount of storage required to store data required by the protocol are important parameters that protocol designers must optimize in devices. As a result, we assessed the protocol's performance in terms of these two parameters. This section presents the performance and security analysis results that were obtained from implementations of Gateway, Node1, and Node2 on a Java socket programming for time and space consumption. In Figure 4 presents security analysis of our scheme using Scyther and it shows no attacks found within bounds.



Scyther results : verify

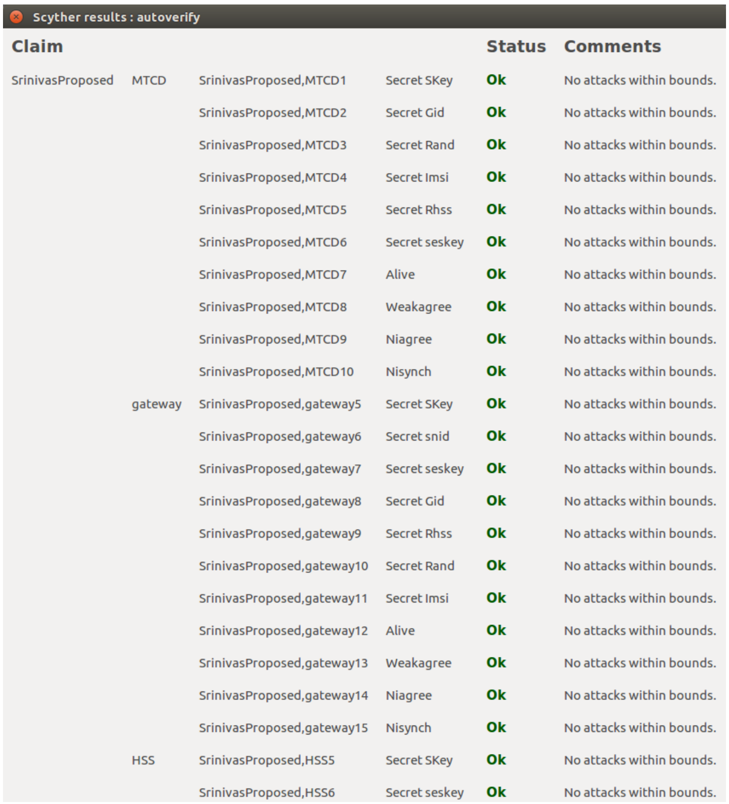
Claim				Status	Comments
SrinivasProposed	MTCD	SrinivasProposed,mtcd1	Secret Imsi	Ok	No attacks within bounds.
		SrinivasProposed,mtcd2	Secret Rand	Ok	No attacks within bounds.
		SrinivasProposed,mtcd3	Secret seskey	Ok	No attacks within bounds.
		SrinivasProposed,mtcd4	Secret SKey	Ok	No attacks within bounds.
	gateway	SrinivasProposed,gateway1	Secret Rand	Ok	No attacks within bounds.
		SrinivasProposed,gateway2	Secret Imsi	Ok	No attacks within bounds.
		SrinivasProposed,gateway3	Secret snid	Ok	No attacks within bounds.
		SrinivasProposed,gateway4	Secret seskey	Ok	No attacks within bounds.
		SrinivasProposed,gateway5	Secret seskey	Ok	No attacks within bounds.
	HSS	SrinivasProposed,HSS1	Secret Rhss	Ok	No attacks within bounds.
		SrinivasProposed,HSS2	Secret Rand	Ok	No attacks within bounds.
		SrinivasProposed,HSS3	Secret seskey	Ok	No attacks within bounds.
		SrinivasProposed,HSS4	Secret SKey	Ok	No attacks within bounds.

Done.

Fig. 4. Scyther Results on Proposed System

In Figure 4 protocol Claim Aliveness(Alive), weak-agreement(weakagree), Non-injective

Agreement (Niagree), Non-injective synchronization (Nisynch)



Scyther results : autoverify

Claim				Status	Comments
SrinivasProposed	MTCD	SrinivasProposed,MTCD1	Secret SKey	Ok	No attacks within bounds.
		SrinivasProposed,MTCD2	Secret Gid	Ok	No attacks within bounds.
		SrinivasProposed,MTCD3	Secret Rand	Ok	No attacks within bounds.
		SrinivasProposed,MTCD4	Secret Imsi	Ok	No attacks within bounds.
		SrinivasProposed,MTCD5	Secret Rhss	Ok	No attacks within bounds.
		SrinivasProposed,MTCD6	Secret seskey	Ok	No attacks within bounds.
		SrinivasProposed,MTCD7	Alive	Ok	No attacks within bounds.
		SrinivasProposed,MTCD8	Weakagree	Ok	No attacks within bounds.
		SrinivasProposed,MTCD9	Niagree	Ok	No attacks within bounds.
		SrinivasProposed,MTCD10	Nisynch	Ok	No attacks within bounds.
	gateway	SrinivasProposed,gateway5	Secret SKey	Ok	No attacks within bounds.
		SrinivasProposed,gateway6	Secret snid	Ok	No attacks within bounds.
		SrinivasProposed,gateway7	Secret seskey	Ok	No attacks within bounds.
		SrinivasProposed,gateway8	Secret Gid	Ok	No attacks within bounds.
		SrinivasProposed,gateway9	Secret Rhss	Ok	No attacks within bounds.
		SrinivasProposed,gateway10	Secret Rand	Ok	No attacks within bounds.
		SrinivasProposed,gateway11	Secret Imsi	Ok	No attacks within bounds.
		SrinivasProposed,gateway12	Alive	Ok	No attacks within bounds.
		SrinivasProposed,gateway13	Weakagree	Ok	No attacks within bounds.
		SrinivasProposed,gateway14	Niagree	Ok	No attacks within bounds.
		SrinivasProposed,gateway15	Nisynch	Ok	No attacks within bounds.
	HSS	SrinivasProposed,HSS5	Secret SKey	Ok	No attacks within bounds.
		SrinivasProposed,HSS6	Secret seskey	Ok	No attacks within bounds.

Fig. 5. Verification of Proposed System

Our proposed method is resistant to standard attacks and performance of the method is an efficient compared other existing methods.

VII. Conclusion

The primary goal of this paper is to identify and resolve design flaws in the current system while introducing a lightweight and secure solution for M2M communication. The existing system relies solely on hashes without employing encryption for security. In this design modified Diffie Hellman key exchange is used to provide group authentication. Since there is already a safe and secure channel from the Femtocells to the HSS the design is safe to use and it overcomes the issues of an existing system. This proposed system is resistance to attacks because it uses lightweight encryption such as TEA encryption algorithm. This proposed system removes the issues of existing system and will increase the reliability and security of M2M system. Furthermore, we intricate and optimized hierarchical authentication method can be developed and some efficient key management schemes can be explored.

References

[1] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks," in Proceedings of the IEEE Global Communications Conference (GLOBECOM '13), pp. 832–837, December 2013.

[2] D. Choi, S. Hong, and H.-K. Choi, "A group-based security protocol for machine type communications in LTE-advanced," in Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS '14), pp. 161–162, IEEE, Ontario, Canada, May 2014.

[3] C. Lai, R. Lu, D. Zheng, H. Li, and X. Sherman, "GLARM: group-based lightweight authentication scheme for resource constrained machine to machine communications," Computer Networks, vol. 99, pp. 66–81, 2016.

[4] Balu L. Parne; Shubham Gupta; Narendra S. Chaudhari, SEGB: Security enhanced group-based AKA Protocol for M2M communication in an LTE Network, IEEE 2019.

[5] F. Haider, C.-X. Wang, H. Haas et al., "Spectral efficiency analysis of mobile Femtocell based cellular systems," in Proceedings of the IEEE 13th International Conference on Communication Technology (ICCT'11), pp. 347–351, IEEE, Jinan, China, September 2011.

[6] A Scheme of Group-based AKA for Machine Type Communication over LTE Networks, GR-AKA. Mariya Ouaissa, A. Rhattoy, July 2016.

[7] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks," Computer Networks, vol. 57, no. 17, pp. 3492–3510, 2013.

[8] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," Transactions on Emerging Telecommunications Technologies, vol. 26, no. 3, pp. 414–431, 2015.

[9] Junfeng Miao, Zhaoshun Wang, Mei Wang, Xiao Feng, Nan Xiao, Xiaoxue Sun, Security Authentication Protocol for Massive Machine Type Communication in 5G Networks, 2023.

[10] A.N.Tentu, PVS Kumar, P Guddeti, Code based Secret Sharing Schemes for MANET, Indian Journal of Science and Technology, 2018/4/16 – 2018.

[11] A.N.Tentu, Kamakshi Prasad V, V.Ch Venkaiah, Multi-Stage Secret Sharing Schemes Based on Asmuth's bloom sequence, CiiT Int. J. of Networking and Communication Engineering, Vol. 8, No.3, 2016.

[12] A.N. Tentu,, Kamakshi Prasad V, V.Ch Venkaiah, Secret sharing schemes for multipartite access structures, Int. J. of Applied Engineering Research, ISSN 0973-4562 Vol. 11, No. 7, pp 5244-5249, 2016.

[13] Y.-L. Huang, C. Y. Shen, S. Shieh, H.-J. Wang, and C.-C. Lin, "Provable secure AKA scheme with reliable key delegation in UMTS," in Proceedings of the 3rd IEEE International Conference on Secure Software Integration Reliability Improvement (SSIRI '09), pp. 243–252, Shanghai, China, July 2009.

[14] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, Springer, Berlin, Germany, 2003.

[15] D. Naccache, M. Just, B. Preneel et al., "Nyberg–rueppel signature scheme," in Encyclopedia of Cryptography and Security, p. 879, Springer, Boston, Mass, USA, 2011.

[16] J.-L. Huang, L.-Y. Yeh, and H.-Y. Chien, "ABAKA: an anonymous batch authenticated and key agreement scheme for value added services in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248–262, 2011.

[17] E. Klaoudatou, E. Konstantinou, G. Kambourakis, and S. Gritzalis, "A survey on cluster-based group key agreement protocols for WSNs," IEEE Communications Surveys and Tutorials, vol. 13, no. 3, pp. 429–442, 2011.

[18] T. Rams and P. Pacyna, "A survey of group key distribution schemes with self-healing property," IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 820–842, 2013.

[19] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the

context of the Internet of Things," Computers and Electrical Engineering, vol. 37, no. 2, pp. 147–159, 2011.

[20] Steri G, Baldini G, Fovino IN, Neisse R, Goratti L (2016) A novel multi-hop secure LTED2D communication protocol for IoT scenarios. In: 2016 23rd international conference on telecommunications (ICT).

[21] Taleb T, Kunz A (2012) Machine type communications in 3GPP networks: potential, challenges, and solutions. IEEE Commun Mag 50(3):178–184.

[22] Ghavimi Fayezeh, Chen Hsiao-Hwa (2015) M2M communications in 3GPP LTE/LTE-A networks: architectures, service requirements, challenges, and applications. IEEE Communications Surv Tutor 17(2):1–26.

[23] Chengzhe Lai,Hui Lix, Rongxing Lu, Xuemin "A Unified End-to-End Security Scheme for Machine-Type Communication in LTE Networks"ICCC,pp. 698–703, K. K. Jyothi and S. Chaudhari.

[24] A. Singh, Vikas Tiwari, A.N.Tentu. " Authenticated Key Agreement Scheme for IoT Networks Exploiting Lightweight Linear Algebraic Computations", International Journal of Information Technology, Springer, 15(4), (2023), pp. 1-9

[25] A.N.Tentu, Kallepu Raju, V. Ch. Venkaiah, Cryptanalysis of a Group Key Transfer Protocol: Generalization and Countermeasures, Journal of Combinatorics, Information & System Sciences (JCISS): A Quarterly International Scientific Journal, Vol.44, 2019.

[26] Cao Jin, Ma Maode, Li Hui (2014) A survey on security aspects for LTE and LTE-A networks. IEEE Commun Surv Tutor 16(1):283–301.

[27] Swamy Naidu A., A.N.Tentu., Ajeet Singh," Reduced Complexity of LDPC Codes using Hard Decision Decoder". In: Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies, vol 117, pp. 367–382. Springer, Singapore (2022).

[28] Ajeet Singh, Vikas Tiwari, A.N.Tentu, Ashutosh Saxena. " Securing Communication in IoT Environment using Lightweight Key Generation Assisted Homomorphic Authenticated Encryption", In: Computer Communication, Networking and IoT, Lecture Notes in Networks and Systems (LNNS), vol 459, pp. 195-204. Springer, Singapore 2023.

[29] Choi D, Hong S, Choi H-K (2014) A group-based security protocol for machine type communications in LTE-advanced. In: INFOCOM, pp.161–167.

[30] Li J, Wen M, Tao (2016) Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-a networks group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. IEEE IoT J 3 (3):408–417.

[31] Qi P, Xiangming W, Zhaoming L, Huan W (2016) Group controller-based authentication for machine type communication under LTE network. Conference on MEITE, pp. 223–226.

[32] An Efficient Multi-Group Key Management Protocol for Internet of Things by Mohamed Ali Kandi, Hicham Lakhlef, Abdelmadjid Bouabdallah, yacine Challal, UMR CNRS 7253, 2019.

[33] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, "CPAL: A conditional privacy-preserving authentication with access link ability for roaming service," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 46–57, 2014.

[34] A.Singh, A.N.Tentu, V.Ch. Venkaiah. A Dynamic Key Management Paradigm for Secure Wireless Ad Hoc Network Communications", International Journal of Information and Computer Security, Vol. 14, No. 3-4, pp 380-402, 2021.

[35] A.N.Tentu, Venkaiah V.Ch., Kamakshi Prasad, CRT based Multi-Secret Sharing Schemes: Revisited, Journal of Security and Networks, Vol.13(1): pp.1-9 (2018).

[36] J. Cao, M. Ma and H. Li," A group-based authentication and key agreement for MTC in LTE networks", Proc. Global Commun. Conf. (GLOBECOM'12), pp. 1017-1022, 2012.

[37] V. Fajardo, J. Arkko, J. Loughney, "Diameter base protocol," IETF (The Internet Engineering Task Force) Request for Comments, 2012.

[38] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu and H. Li," LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5329-5344, June 2020.

[39] Liu, J., Tong, X., Wang, Z. et al. A centralized key management scheme for space networks with resistance of nonlinear channel noise. Wireless Netw 26, 4061–4078 (2020).

[40] Rodhe, I., Rohner, C. (2010). Secure Overlays: Making Static Key Distribution Schemes Work with Mobile Base Stations in WSNs. In: Osipov,E., Kassler, A., Bohnert, T.M., Masip-Bruin, X. (eds) Wired/Wireless Internet Communications. WWIC 2010. Lecture Notes in Computer Science, vol 6074. Springer, Berlin, Heidelberg.

[41] Maity, S., Hansdah, R.C. (2012). Certificate-Less On-Demand Public Key Management (CLPKM) for Self-organized MANETs. In: Venkatakrishnan, V., Goswami, D. (eds) Information Systems Security. CISS 2012. Lecture Notes in Computer Science, vol 7671.

[42] A.N.Tentu; Renuka Cheeturi, An ECC based Anonymous Authentication Protocol for Internet of Things, 2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). 2023.

[43] A. Aijaz and A. H. Aghvami, “Cognitive machine-to-machine communications for internet-of-things: a protocol stack perspective,” IEEE Internet of Things Journal, vol. 2, no. 2, pp. 103–112, 2015.

[44] M.M. Modiri, J. Mohajeri 2 M. Salmasizadeh, A novel group-based secure lightweight authentication and key agreement protocol for machine-type communication, Volume 29, Issue 6 - Serial Number 6, Transactions on Computer Science & Engineering and Electrical Engineering (D), pp3273-3287, 2023.