ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse01922020.pdf
https://doi.org/10.30534/ijatcse/2020/01922020

Group-based Authentication Methodologies

Pathan Mohd Shafi[1], Vijaykumar S Bidve[2], Vinod V Kimbahune[3], Yogesh B Gurav

[1]Professor, Computer Engineering Department, Smt. Kashibai Navale College of Engineering, Pune, India. shafipathan@gmail.com
[2]Professor, Information Technology Department, Marathwada Mitra Mandal's College of Engineering, Pune, India. vijay.bidve@gmail.com
[3]Professor, Computer Engineering Department, Smt. Kashibai Navale College of Engineering, Pune, India. vinodvkimbahune01@gmail.com
[4]Professor, Department of Information Technology, Zeal of College of Engineering, Pune, India. ybgurav@gmail.com

ABSTRACT

Internet of Things (IoT) is expected to grow exponentially and billions of devices will take part in communication globally by 2020 according to International Data Corporation (IDC). With this huge number of devices, it is very difficult to authenticate or identify each user or device in IoT. The Internet of Things (IoT) by which any items could be connected via Internet. The access to the Internet has emerged from static access like desktop machines to the mobile access. Hybrid authentication is the combine of device authentication and access authentication. Device authentication ensures device identification that is the only authorized IoT equipment has the access to network. It will secure the legitimate interests of the user, and avoid conflicts of interest because of the access of illegal device along with the network security issues. Group signature mechanism TCGA (Threshold Cryptography-based Group Authentication) addresses security issue or parameter by considering shamir's secret key generation, public key infrastructure and group authority. It is lightweight by using very low level hardware as well as software. GAS (Group Authentication System) is another scheme which we have considered to compare or to evaluate; It also uses shamir's secret key generation method and public key infrastructure for security or to provide seamless communication. Group signature try to address problem faced in TCGA and GAS i.e. to generate new key every time whenever any new member adds in group by creating static key at first time or at the time of starting of communication between groups here it reduces cost to generate key. This approach is scalable in nature and also it improves the time complexity.

Key words : Group signature, Hash Message Authentication Code, Group-based authentication mechanism, Threshold Cryptography-based Group Authentication, Internet of Things formatting

1. INTRODUCTION

1.1 Background

The Internet of Things (IoT) by which any items could be connected via Internet. The access to the Internet has emerged from static access like desktop machines to the mobile access. Many types of devices like mobiles, cameras, printers, tablets, televisions may connect to the internet which is called as ubiquitous computing. In that way it introduces many challenges.

The aim is to connect physical world to digital world. IoT focuses on the way by which the devices can be monitored and controlled Figure 1 shows the basic idea behind IoT. The IoT is mainly divided into three parts, application layer, the perception layer, and network layer.

IoT experience the procedures of information perception, integration, access, transmission, aggregation, decision-making and control, storage and mining. Data processing in IoT related to questions about privacy protection and location-based services in information processing.

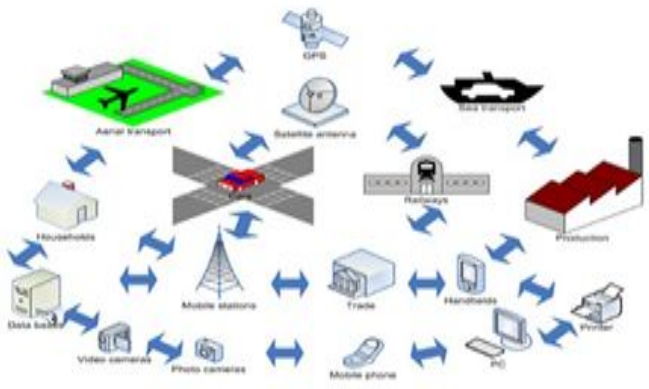

Figure 1: Basic idea of IoT

IoT applications do not face with the security of information collect, additionally consider the privacy of information transition. In wireless sensor network (WSN), the lightweight public key-based authentication technology is used. Caused by open nature of the network deployment region besides radio network's broadcasting features, the security risks of the IoT is very severe.

Hybrid authentication is the combine of device authentication and access authentication. Device authentication ensures device identification that is the only authorized IoT equipment has the access to network. It can shield the legitimate interests of the user and avoid disagreement of illegal equipment as well as the network security issues.

Radio-Frequency Identification (RFID) labels, cell phones, sensors, and so on, in which computing, and communication systems are seamlessly embedded. The IoT complete deployment will increase the novel opportunities for the Information and Communication Technologies (ICT) area. From the perspective of a private user, IoT introduction is playing a leading role in several services and industries in both working and domestic fields -such as surveillance, domotics, e-learning, e-healthv, and security etc.

To making complete interoperability of heterogeneous interconnected devices which require adaptive and autonomous behaviour of device while guaranteed trust, security and privacy; networking aspect is not in rest, low computation and energy volumes. It not just proposes IoT would interface both virtual and physical conventional articles as a worldwide framework, yet additionally stresses the significance of consolidating the customary Internet related advancements and foundations in the improvement of IoT.

1.1 Basic Concepts

Group Authentication system is a new authentication system which is used to authenticate to each other in groups. It is beyond one to one authentication system[2]. A group manager(GM) is key elements here. It issues token to every user. Tokes are reusable and may be used for authentication without compromising security. Every user nedd to regiser with group manager and in registration process, the group manager uses Shamir's secret sharing(SS) scheme to generate the token and then it is issued each group member. Each user then can authenticate to each other without involving GM[3]. There are two types cryptographic techniques used in authentication. One is secrete key cryptography where key is shared among users participating in authentication and other is public key cryptography where key is not shared among the users participating in authentication. The big difference between these two techniques is of computational time. Public key cryptography takes huge computational time in comparison to secrete key cryptography. Figure 2 shows the working and idea of group communication, there two groups which want to communicate with each other securely so in this type of communication group authentication plays very vital role to authenticate group members as well as to made communication secure and seamless between the groups.

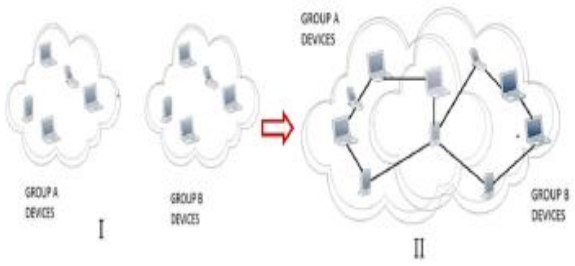

Figure 2: Group Communication

Group authentication uses lightweight public key cryptography to make group communication secure. Group authentication used in Mobile Ad-hoc networks [4], RFID systems [5], in Wireless sensor network [6], vehicular ad-hoc netwoks [7] and also in machine type communication [1].

One of the component of public key crypto system is a public-key infrastructure (PKI). It stores digital certificate issued by certificate authority (CA). Along with this PKI takes care of management of certificates. In each CA domain user identity must be unique. The binding between user and CA is established through the registration process and extended till issue of certificate. The assurance level of the binding is bringing off by at CA by software or under human supervision. The binding is assured by registration authority (RA). Non-repudiation is avoided in this way. By using Public-key cryptographic technique, users are ensured that they communicate securely in public network which is inherently insecure. Via digital signatures user's identity is verified. A public-key infrastructure (PKI) is used to for creation of digital certificates and subsequently used for storage as well as distribution.

Components of PKI are as given below:

- A certificate authority (CA) – It issue and verifies the digital certificates
- A registration authority - It checks the identity of users listed in CA
- A central directory - It is a location where keys are stored and indexed
- A certificate management system. – It takes care of distribution and keeps track of certificates
- A certificate policy – These are rules by which users and PKI is abide

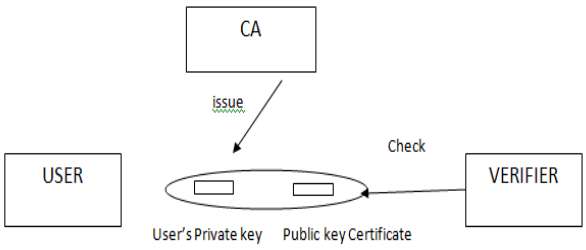

Figure 3: Public Key Infrastructure and components

Figure 3 shows that public and private key's are created at user end using the public key cryptographic algorithm such as RSA(Rivest-Shamir-Adleman) by (CA).

Table 1: Use of key's in public key infrastructure

To do this	Use whose	Kind of key's
Sending the encrypted message	Use the receiver	Public key
Sending the encrypted signature	Use the sender	Private key
Decrypts the encrypted messsage	Use the receiver	Private key
Decrypts the encrypted signature	Use the sender	Public key

The generated private key is given to respective user and is not shared with anyone other than concern user and the public key is made public so that all the users can have access to it. The private key is not never shared with any entity. The message is encrypted by public key of respective user and due to property possessed by key pair it can now be decryptible by the private key of respective user only ensuing the authenticity by digital certificate. Table 1 shows the use of keys and operation may be performed by keys.

1.3 Relevance

Internet of Things (IoT) is expect to grow to $8.9 trillion and 212 billion devices/peripherals globally by 2020 according to International Data corporation (IDC). With this huge number of device it is very difficult to authenticate or identify each user or device in IoT. A new mechanism like group authentication is very efficient to manage authentications and in that way it will save time as well energy. According to IDC the devices which connected to internet i.e. IoT increasing very rapidly where must be consider issue of scalability. Similarly in group communication also new members are adds dynamically so need scalable group authentication protocol or strategy or methodology.

In IoT for most of the time to authenticate group it uses public key infrastructure. In this case public key cryptography will used to authenticate group members for group authentication mainly for group communication in IoT with scalable property for groups.

2. LITERATURE SURVEY

2.1 Motivation

In group authentication there can be any numbers of group members and also allowed to dynamically add the new members i.e. group must be scalable over number of group members. If we want to provide scalability for groups in group authentication need to consider three main issues which are present now in current scenarios. In some of the current methodologies, there is scope to improve following properties

1. Key generation time

As soon as a member joins the group, keys is generated and distributed again [8][11][12][13]. Addition of new member needs to create new key and distribute again by dividing so it will take time and each and every time required to do this. In dynamic group authentication if number of members are added frequently in that case it is very inefficient as we are considering IoT and scalability, new members join the group very frequently, key generation is one of most important parameter which required to consider and improve.

2. Time complexity

Every time to begin group activity, group confirmation should be executed as a pre- requisite to check if every one of the individuals are a part of the group which is did by group authority in certain situations same called as group manager. In case of verification fails, extra user authentication needed to identify members which are not in group. This is called as group authentication time, so need to improve group authentication time.

3. Scalability

Due to above two properties or parameter it is very time consuming and costly to add new member dynamically in group. Key generation time and group authentication time directly affects on scalability of group so it is required to improve scalability property by adding new members without considerably changing or increasing key generation time and group authentication time.

2.2 Related Work

In a group authentication [3], participants are authenticated if they belongs to same group. It is many-to-many type of authentication. It is m-user, t-secure, n-group Group Authentication Scheme (GAS): ((t, m, n) GAS). Efficiency of the framework is determined as though the result of the proposed scheme is negative then user isn't confirmed. The proposed (t; m; n) GAS is utilized as a pre-process for regular user authentication scheme to recognize non-members. In this way, the proposed (t; m; n) GAS must be effective. Also, in the proposed scheme, similar tokens produced by the GAS is might be reused for numerous authentications. This course of action can improve the efficiency of token distribution. The scheme must probably oppose up to t-1 connived inside adversaries. Also, since values are released asynchronously, any outside enemy can't imitate to be a member by altering a legal value after knowing at most n-1values from different member. For group authentication with numerous validate, there are several secrets to be recovered successively. The scheme must almost certainly secure revealed privileged secrets when a few secrets have recoup. Adaptability, the scheme should work appropriately for different size m (i.e., t - m - n) of users involved in the authentication. The (t; m; n) GAS is described by the go along with scheme:

Initialization: All system parameters are generated and published by the group manager in initialization.

Distribution: The GM generates the token si and distributes it to each group member Ui, secretly where i= 1, 2, . . . , n.

Authentication: Each user computes the value ci using his token.

After receiving all ci where i= 1, 2, . . .,n and $t \leq n \leq m$), users verify these values. If the verification is not successful then

additional user authentication is to be carried out for identify nonmembers. Model uses token generation and group authentication phases.

Likewise, the author proposes [3] the work appropriately for discharging values synchronously and non-concurrently. Also in the proposed worked, an interactive basic essential (t; m; n) GAS utilizing Shamir's (t; n) SS scheme. In any case, this essential scheme works adequately if all values are released at the same time. They will modify the essential scheme to an interactive asynchronous (t; m; n) GAS. At long last, [3] propose a noninteractive asynchronous (t; m; n) GAS for different authentications/validations with the Correctness, adaptability, and Security. In [1] they have proposed diverse scheme to be specific,

1. BASIC (t; m; n)
2. ASYNCHRONOUS (t; m; n)
3. ASYNCHRONOUS (t; m; n)

This scheme decide if all users took an interest in a group communication have a place with a similar group. Group authentication can confirm various users without a moment's delay. Proposed (t; m; n) group authentication schemes, schemes 1 and 2, are progressively efficient since the schemes are pursues Shamir's (t; n) SS scheme and the calculations include just polynomial operations. Scheme 3 enables tokens to be reused acquired from the GM at first for numerous authentications. Group authentication opens another exploration heading for the SS. It utilizes (t,m,n) threshold scheme. Resources constrained devices being poor computational and memory limit are not considered. Group authentication [1] have predominantly considered parameters like security, correctness, scalability and adaptability to demonstrate execution and convenience of proposed scheme.

In [8], Proposes A Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT). Paper focuses on cryptography scheme for the IoT. This scheme is dependent upon paillier threshold scheme. The Paillier Threshold Cryptography is a public key variant of the (t, n) threshold scheme. Here n is number of group members and t is threshold for group. It is probabilistic asymmetric public key encryption system. Encryption of same plain texts leads to different cipher text for every new instance thus ensuring the randomness. The main properties of Paillier Cryptosystem are homomorphic addition, indistinguishability, and self-binding. The Paillier Cryptosystem consists of three algorithms for operations like key generation, encryption and decryption. Authentication of each members is ensured. The scheme also helps for establishment of a shared secret key. This secret key can be used further for any group-oriented applications. These groups can even overlap intersection point with many devices capable of being a part of more than one group. Let us say that there are two groups A and B. if a member of group A wish to communicate with member from group B then member of group A is first authenticated to group B and now it should be communicating with all the members of the group B. On another way, all the devices of the group A except the authenticated one cannot communicate with the group B devices. Whenever a new member enters in the group, the head of the group generates key pairs to keep up group key leakage and is referred as Group Authority (GA) in [8] paper. TCGA Scheme for the Internet of Things (IoT) consists of following five modules:

1. Key Distribution – to distribute the key.
2. Key Updation – to update the key.
3. Group Credits Generation – to generate the group credentials for authentication.
4. Authentication Listener – the device to whom user want to authenticate.
5. Message Descriptor – Algorithm for decryption.

At the point when a specific member wants to begin a set of elements(group) activity, it sends a request to the present GA. On gathering of the request, the GA creates a session secret which can be shared by every one of the individuals from that group. Public key of the group is used to encrypt this session secret. This gives the necessary security as it must be decrypted by the whole private key. A Hash map function is applied to the session secret which can be utilized in next steps to demonstrate the integrity of this message. Then it will be sent all with the encrypted session secret in a solitary message. This message is sent to every one of the individuals from the set of points(group). All the devices at that point utilize their own private key to decrypt this message which gives them a PDM which isn't the final session secret. Currently it sends this PDM to each member in the group. Until n-1 PDMs are received every one of the devices waits. Each device at that point attempt to combine the majority of the offers which will eventually give them the final session secret. If the event is successful, implies that all around the PDMs received are by the genuine group members only, and, consequently the group authentication succeeds. The group activity would then be able to be begun utilizing the session secret for further communication. If the event is failing implies that there is in any one device which is utilizing a fake private key and thus the incomplete decryption created by him isn't genuine. In this manner, after attempting to consolidate all the shares it was result in failure. This implies group authentication barriers, and there is a need to restart the procedure.

At last in paper [8] they have compared group authentication scheme proposed in paper [3] and TCGA with respect to group authentication time and number of devices and depending upon some parameter they have proved TCGA is efficient than GAS.

For group-based authentication, Group Signature is one more scheme or methodology. The idea of group signatures is group-based authentication to accomplish security and privacy of signers against potential verifiers. At a high level, group signatures implement the following idea: All potential signer are considered as individuals from some group. Every

signer issues a signature in the interest of the entire group. Utilizing public key of whole group such group signature is confirmable publicly. Along these ways it gives secrecy to the genuine signer. Notwithstanding this there exists a committed trusted third party. It connects the group signature to the identity of the signer. The design of a group signature scheme consists of the group manager (GM) and different group members. The GM is either a solitary authority or an alliance of a few elements is presented here. The group manager deals with initialization of the group for the admission. Denial of group members is likewise taken care of by group manager. During the initialization procedure the GM chooses own secret key and defines public group members parameters containing the group public key. At first group parameters are set up. GM initializes own secret key and uses this secret key to issue membership certificate to individual group members. Assignment and cancelling of group members are also the task carried out group manager. Each group member uses this certificate for authentication.

This certificate appears for to the secret signing key of the individual GM. That is, each group member can utilize it to create group signatures on arbitrary messages. Authentic user can publicly check the authenticity of some group signature by taking advantage of the group public key. The group signature authenticates the group member to the group. The crucial property of group signatures utilizing this signature group members and be confirmed by group manager using information collected during the admission procedure.

In contrast with standard digital signatures, group signatures were increased security objectives. Specifically, only group members can issue substantial group signatures that the indelible requirement guaranties. Furthermore, group signatures provide privacy by requiring that no other party, aside from the manager of the group, should be able to identify the actual signer. Moreover, group signatures should remain unlikeable, can link multiple signatures produced by the same signer implying that no party, without for the group manager. Additionally, the opening methodology performed by the group manager infers security prerequisites of its own to protect a group member from malicious actions of having produced some group signature if this was not the situation. Group signature schemes would be classified dependent on their functionality. As such schemes is the ability of the signer, while being a member of the group, to produce group signatures that can be publicly confirmed utilizing the group public key and that don't leak any information about the signer's identity. Group manager is the main party that can revoke signer's anonymity. This fundamental idea offers flavours to various types of group signature schemes, contingent upon the optional support for the following set of actions:

1. The ability of the group manager to dynamically admit new group members and/or revoke previously decided membership.
2. The ability of the group manager to provide publicly supportable proofs that some group signature opens to a concrete signer, and
3. Support for the distribution of the group manager's duties amongst several entities: (i) an issuer being responsible for the exclusive management of the group membership, and (ii) an opener being equipped with exclusive rights to open signatures and identify the signer

.

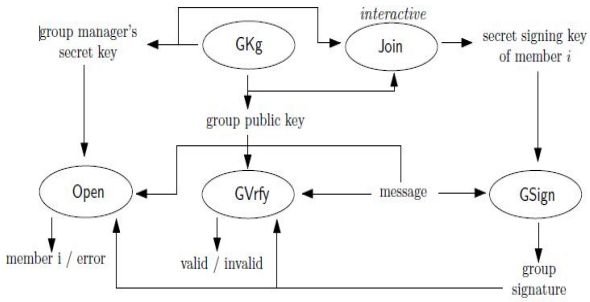

Figure 4: Dynamic group signature

In static group signature, number of group members are fixed at start of activity so it will limit the scalability but in case of dynamic group signature scheme new members can be joined at any time of communication so it is consider special algorithms for this

Many group signature schemes is constructing using the RSA setting. This scheme considers following phases.

1. Initiation
2. Signing and verification
3. Identification

Group signature supports to dynamic behaviour of schemes, to open group signatures in a publicly verifiable way (VO property), partition of responsibilities through distribution of management roles between the issuer and the opener (DA property), and to invalidate issued membership certificates. Anonymity of signers is one of the key security properties of group signatures. The traceability property guarantees that the group manager (or opener in DA- schemes) can generally open (legitimate) group signatures and distinguish the signer. The non-frame ability property avoids else attribution of group signatures to group members that were not associated with their generation. In the analysis of computational complexity of group signature scheme, we estimate the amount of most expensive activities for various algorithms, which serves in as a decent heuristic for the evaluation of its efficiency.

In [5], paper proposes a grouping-proofs-based authentication protocol (GUPA). The author tried to resolve the security issue of multiple readers. RFID tags are used for simultaneous identification in distributed. In GUPA, distributed authentication mode is used along with independent subgrouping. It enhances hierarchical protection. An illegal reader or tag is discarded based upon an asymmetric denial scheme is applied to grant fault-tolerance. A sequence-based odd-even alternation group subscript is proposed so as to

define a function for secret enhancement. Meanwhile, GUPA is tested and analyzed to resist major attacks such as replay, tracking, forgery and denial of proof. It is then compared with Furthermore; performance analysis shows that compared with the known grouping-proof or yoking-proof based protocols and found that GUPA has lower communication overhead as well as computation load. It is presented that that GUPA is secure as well as simultaneous identification can be performed effectively for resource-constrained device such as RFID systems. Further paper gives analysis of attacks like replay attack, tracking attack, DOP, forgery attack. The protocol applies grouping proofs to realize multiple readers and tags secure and simultaneous identification. It is concluded that GUPA has more advantages for lightweight RFID applications compared with other schemes. But paper have some disadvantages like GUPA needs little larger units tag storage, due to the additional reader group identifiers and need to compromise communication overhead.

Group authentication system is proposed in vehicular ad-hoc networks (VANET) [9][10][14], Group signature scheme is proposed for VANET. The existing group signature-based schemes is based on group signatures but it suffers due computational delay in the certificate revocation list (CRL) checking. In the same consequences signature verification process is also carries time loss leading to high message loss. Due to heavy delay verification of messages per second in is less in VANETs making it heavy on the system. In proposed scheme the precinct is divided into several domains. Roadside units (RSUs) takes care of distribution of private keys of group in a localized manner. It then, uses a hash message authentication code (HMAC) for integrity of message to reduce the time of CRL checking. At the end cooperative message is adopted for authentication among entities. Each vehicle only verifies a small number of messages, It reduces the burden of authentication greatly. The security and performance analysis is done at the end which reflects that proposed scheme is more efficient on the parameters such as authentication speed not compromising the privacy in VANETs. [9] Paper proposes an efficient privacy-preserving group signature-based authentication scheme for VANETs. Paper proposes to use both the techniques of distributed management using HMAC batch group signature verification and cooperative authentication. Initially whole network is divided into multiple domains which subsequently allows localized management. IN proposed scheme HMAC is replaces the CRL time consuming checking before batch verification. Due to this number of invalid messages is discarded in the batch. Cooperative authentication is used to further improve the efficiency of proposed scheme. By employing the given methods, our scheme can meet the requirement of verifying 600 messages per second. The security and performance analysis at the end done reflects that the proposed scheme achieves higher efficiency keeping intact conditional privacy for VANETs. System suffers with high message loss ratio since verifying a group signature consumes more time to authenticating a pseudonym.

In [2] author proposes another group authentication which is intended for group communications, for example, an ad hoc wireless network. The proposed group authentication protocol is a many-to-many kind of authentication that authenticates different users. Here author discussed on group authentication protocol without revealing tokens. Author also focused on importance of group authentication, is very efficient since the computation is based on the computation of linear polynomial. The polynomial interpolation turns into the principle computational task in our proposed protocol. Be that as it may, the modulus p polynomial interpolation is very small than the modulus value in most public-key cryptosystems. Furthermore, proposed authentication protocol authenticates all users. It is efficient in comparing and all current existing authentication protocols. Paper primarily focuses around authentication protocol without revealing tokens. Additionally talked about one time group authentication protocol, it utilizes Shamir,s key generation for generating secrete key, it uses entities like group users, group manager and attackers.

In [10], group-based communication for machine type communication is proposed in cellular networks, Machine-Type Communication (MTC) has advantages in terms of good coverage and lower network deployment cost. The current cellular network is designed for human-to-human communication (H2H). naturally it is not very much suitable for machine-to-machine, human-to-machine(H2M) and machine -to human (M2H) applications. One of the most urgent issues, which network operators are currently facing, is MTC related signalling congestion and overload. Especially, when a large co-located MTC group concurrently wishes to accesses the message or periodically transmits the message, the authentication data causes a congestion in VLR/SGSN node. In the way it overloads the link between home environment (HE) and serving network (SN). Author proposes group-based authentication scheme along with key agreement mechanism for MTC scenario in roaming. Each MTC device in group shares a secret key in the home environment along with group secret key. It is shared to other MTC devices of the same group. Then initial message exchange data is kept less possible when messages are exchanged between serving network and home environment. It is achieved by the MTC by making group key as an authentication key locally. Addition to this dynamic group key update is incorporated for dynamic MTC group. At the end analysis of the proposed system is done which shows it lower the effort of handling remarkably for large MTC group. It also minimizes the change of operator's core network(CN). Machine-to machine type Communication is a data communication involving one or more entities. It does not essentially involves human interaction. It is different than the current mobile network communication services. It has some characteristic features viz different market scenarios, data communications, lower costs and effort, little traffic per terminal and a very large number of communicating terminals. Traditional wireless terminals communicating in the networks are largely "manned" by humans while

communications within MTC devices are this constrain free. MTC communication is proposed as future in wireless communications technology. Paper addresses many attacks like Denial of service attack, Access priority indicators attack, External interface attack, Device triggering attack. Finally they have compared proposed protocol with all existing protocols.

The author [1] focuses on security protection in IoT as well as group authentication mechanism along with certification issues. Paper evaluates key technology in the security and show the Internet integration model. It likewise put focus on key technologies required in the safety certification. The user devices indicated a geometric growth in IoT, the subscribers of IoT business is probably going to have various IoT devices, these devices are made one or more groups, the number of devices might be inconsistent inside each group, yet they have the same behavioral characteristics. In the IoT, all devices in a same sensor network basically have the same behavioral characteristics. Therefore, whole sensor network can be realized as a group. Group authentication mechanism can provide a function which the sensor network devices can be access to the mobile communication network, it enables operators to better billing, control and manage the sensor network devices.

Firstly, Group authentication technology of IoT uses the idea of mutual authentication between IoT and sensor gateway of the group. It also uses mutual authentication in the existing communications network. At that point they have a certification between sensor gateway and sensor devices within the group. Session key generated between the sensor gateway and the IoT is transmitted to the sensor device after the certification, or authentication node of IoT and the sensor devices use this shared session key as the root key, or Deduction generates new shared secret between the sensor devices and the IoT. So that the sensor devices can be encrypted transmission of user information of the IoT. The recently included sensor device in the group can get the group session key after authentication with the sensor gateway. Accordingly it can get the key which can be required to communicate with the system. Lastly, paper concludes as security authentication and control technology of the IoT is the key of requirement to apply the services at large-scale. Presently, the IoT surfaces from many of security issues. To achieve M2M communication which is based on the safety of objects communication.

In [6] paper, the author proposes a novel symmetric-key-based authentication schemes. As it is based upon symmetric-key system it exhibits low computation overhead. The proposed system based upon the Bloom filter. Key binary tree is used for distribution and updating of the authentication keys. Analysis and evaluation of the proposed authentication schemes at the end demonstrates that the estimated average number of concatenated message authentication code in a packet from time 0 till time t is 4pt where p is the probability that a key is corrupted and t is time. Proposed mechanism is lightweight inters of computation and efficient in terms of communication overhead and energy efficiency.

1) It is proposed a key management mechanism for the efficient, and rapid adoption of a new authentication key, by a group of one-hop communicating sensor nodes. Nodes are organized in accordance with binary tree overlay topology. The root is the communication source as shown in Figure 4 The efficiency is high as it provides low communication overhead in comparison with system communicating with individual keys..

2) The group key is poised against malicious attacks. It first focuses on proposing a reputation generator in each node to reduce the impact. Reputation generator evaluates the reputation value for each node. Once a malicious node on the basis of low reputation is detected, it is discarded.

3) End to End authentication is ensured via a series of a hop by hop authentication on the path from the source to group members. At each hop, communication between a node and its immediate neighbors is authenticated.

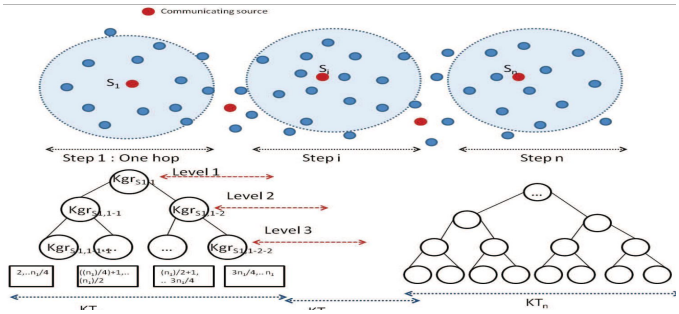

Figure 4. Architecture model for WSN

Source authentication is in its infancy in wireless sensor networks which are featured with resource constraints and deployed in strategic areas. To address this problem, they have proposed a family of source authentication schemes which rely on a key tree to update the authentication group key in order to prevent the compromised nodes from understanding the communications between non compromised ones. The performances of the schemes have been analyzed mathematically, confirming its effectiveness.

[4] paper proposes a trust based authentication system In ad hoc networks where trust calculation is done to seprate the nodes in category as trustworthy and untrustworthy nodes. Trust metric is drawn via the authenticity of the participants in the network and proposes self-organized group-based authentication mechanism (SGAM). Social relationship between each individual along with social relationship between groups is also considered to authenticate to each other. Proposed model defines the notion of trust between groups which is calculated based on different relationships. Low reputed groups are identified containing malicious members.

Consider a network containing of different clusters. All nodes in each cluster uses a short range radio and set up the low-level network; after starting association, they usually select one of the node as a cluster head (CH). Similarly the nodes of the low-level network, the cluster heads of all

clusters high-level network via a long-range radio. CHs set up trust association with other CH-peers by communicating with one another, in multi hop form, in the high-level network. In high-level network, a cluster head acts as representative of its cluster and has the duty of informing the status of their members to other clusters. Then again, in low level network, each cluster also contains boundary nodes (BNs). These nodes, which are in direct contact with the individual from neighboring region(s), are additionally responsible to give information about the trust level of the adjoining areas. Figure 5 demonstrates the 2-level wireless ad-hoc network.

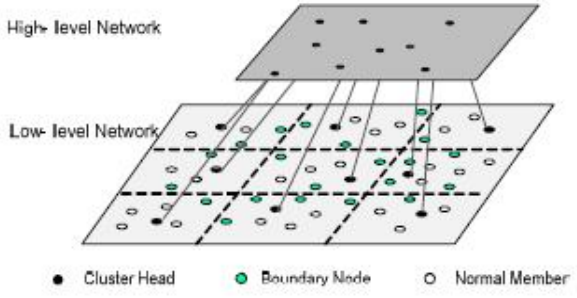

Figure 5: Two level group-based network

In this the clusters are based on a grid formed network, divided into equal sized regions. In this paper author discussed about the use of region, cluster, region and group interchangeably in their work. The design of the SGAM supports distributed management of intra and inter region trust computation, discussed in the following parts: In this model every region acts as an entity that, in view of its complete trust value, different entities make decision while authenticating its member. The trust between regions shows the confidence level of authenticity of the members of the regions. Every region is made out of three unique kinds of node: CH, BNs and normal node (NN). CH is a node in the region with highest trust value; in this way, based on the trust level every node could be a CH. Figure 6 shows, every node locally has a trust the management service which stores and processes the intra- region (trust relationship in an region) and inter-region trust (trust relationship between regions)

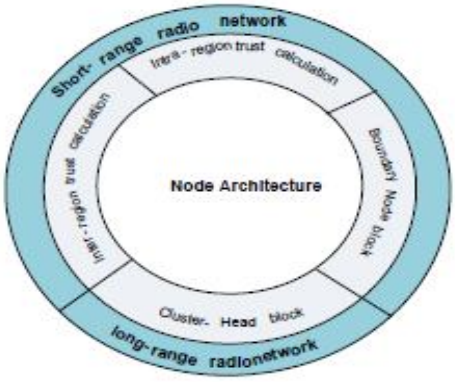

Figure 6: Node architecture of group-based network

In this work author suggested a self- self-organized group-based authentication mechanism for mobile ad-hoc networks. The model aims encouraging the authentication procedure for mobile nodes by making the idea of trust between regions. Author proposes a model to calculate the intra- and inter-group trust values in a collaborative and distributed form. As future work we intend to evaluate our model by simulations and to explore the effectiveness of the proposed autonomous group-based authentication mechanism by comparing it with a flat form model.

Addressing security and privacy issues is a prime concern Ad Hoc Networks. In [7] paper author proposes a system called as anonymous batch authentication scheme. It is used for authenticating multiple requests sent simultaneously from different vehicles. The pseudonyms are used to privacy and backward privacy revoked by hash chain of vehicle. Batch authentication system is implemented by using an identity-based signature (IBS). Broadcasting communication overhead is reduced. Revocation of the vehicle is done on the basis of calculation of Hash Message Authentication Code (HMAC) by using the group key. Furthermore, integrity of the batch messages is confirmed and efficient batch authentication is accomplished. Latterly analysis is done. Proposed scheme shows better performance than the current batch authentication schemes on the parameter like communication overhead, authentication delay and revocation. The realization of HMAC doesn't require additional overhead.

The VANETs model in this paper consists of the entities shown in Figure 7 is the Trust authority, the fixed RSUs at the road side and the mobile onboard units (OBUs) equipped on the running vehicles. For RSUs and OBUs TA is a registration and certification centre, which also offers numerous value added services. The connection between RSUs and TA is wired links and with OBUs by wireless links. For authenticating the identity and message of the OBUs, RSUs are responsible and issue the group key materials to the legal OBUs when the OBUs join the domain.

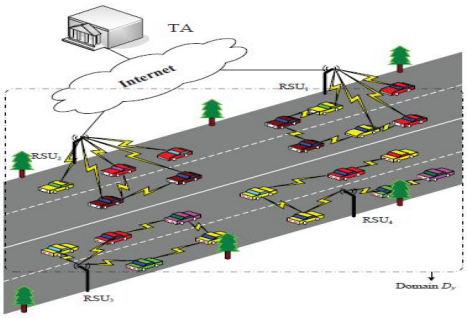

Figure 7: VANET system model

Author describes the scheme as the following phases: system start, RSU's certificate issue, vehicle's aliases and private keys generation, mutual authentication of RSU and vehicle, periodic update of group key.

3. EVALUATION OF RELATED WORK

Table 2: Evaluation of related work

Parameter	TCGA	GAS	Group Signature
Integrity	×	×	✓
Privacy	×	×	✓
Security	✓	✓	✓
Flexibility	✓	✓	✓
Scalability	✓	×	✓
Lightweight	✓	×	×
Reusability	×	✓	×
Traceability	×	×	✓
Authentication Delay	×	×	✓
Resist the attack	✓	×	✓
Unforgeability	×	×	✓
Computation Time at GA	✓	✓	✓
Anonymity	✓	✓	✓
Unlinkability	✓		✓
Exculpability	✓	✓	✓
Confidentiality	✓	✓	✓
Non-repudiation	×	✓	✓
Efficiency	✓	✓	✓
Fault tolerance	✓	✓	✓
Communication overhead	✓	✓	✓
Revocation Overhead	✓	✓	✓
Authenticity	✓	✓	✓

3.1 Parameters

1. Integrity: Receiver can check the messages to confirm whether it is sent by the sender.
2. Privacy: Communication must be seen by anyone and communication maintained between valid two parties.
3. Security: Senders message correctly received by receiver without any attack and secretly.
4. Flexibility: Scheme works properly for some users within allowed numbers
5. Scalability: Ability to add any number of new members in group dynamically.
6. Lightweight: Hardware, software are memory properties are simple and light which must not be consume more energy as well cost.
7. Reusability: Some characteristics can de possible to use again in system e.g. characteristic like any authentication token or key.
8. Traceability: The group manager is always able to open a valid signature and indentify the actual signer.
9. Authentication delay: Time required in authentication.
10. Resist the attack: Safe from attacks e.g. Man-in middle, battery exhaustion, Replay etc.
11. Unforgeability: Only group member are able to sign message on behalf of the group.
12. Computation time at GA: Computation time or calculation time at group authority like group manager or it can be key management time.
13. Anonymity: It is computationally hard for the group manager to identify the legimated signer.
14. Exculpability: Neither a group member nor the group manager can sign on behalf of other group member.
15. Confidentiality: The message cannot be eavesdropped by an intruder in the transmitted process.
16. Non- repudiation: To avoid sender/receiver contradicting have already transmitted/ received messages each other.
17. Efficiency: Can be defined on many other parameters like communication overhead, energy overhead, performance etc.
18. Fault tolerance: Must not allow illegal access.
19. Communication overhead: Number of handshakes between group manager and group member as well as within group members.
20. Revocation overhead: If new member add in group again revoke certificate.
21. Authenticity: When receiver receive the message, can verify the validity and sender identity.

3.2 Discussion

Group signature addressed almost all performance parameters than the remaining two schemes i.e. TCGA and GAS.

TCGA addressed security issue or parameter by considering shamir's seceret key generation, public key infrastructure and group authority. IT is very lightweight by using very low level hardware as well as software. Flexibility and scalability addressed by allowing adding any number of devices any time. Whenever new member adds it will generate secret key as well as new public key to authenticate group members and for communication. Group manager can identify all group members but at the time of communication it hides identity of individual group member. Computational time at GA need to be consider because it will add time complexity so TCGA consider computation time at GA for evaluation of scheme. As soon as new member add in group TCGA revoke new certificate for group to complete communication securely. This considers many attacks like man-in-middle attack, battery exhaustion attack etc to improve scheme efficiency.

GAS is another scheme which I have considered to compare or to evaluate, GAS also used shamir's secret key generation method and public key infrastructure for security or to provide seamless communication. This scheme is also allowed to add any number of devices dynamically in group and in this way addressed flexibility and scalability. This scheme not effectively consider the attacks which can be effected on efficiency of scheme. It consider synchronous and asynchronous group authentication and its correctness. It consider group manager or group authority which generate

token every time for group members and then authenticate group members.

Group signature is the third scheme which can be used for group authentication over any network. Group signature can be implemented in both public as well as private key infrastructure but due to advantages of public key infrastructure it uses PKI. Group signature try to address problem faced in TCGA and GAS i.e. to generate new key everytime whenever any new member adds in group by creating static key at first time or at the time of starting of communication between groups here it reduces cost to generate key. This leads to reduce security due to staticness of key it is easy to identify.

3.2 Conclusion and Future Work

- In TCGA, GAS and group signature schemes if number of devices increases time to authenticate that devices are also increases.
- Handshaking between group manager or group authority are different for different schemes.
- Scalability is one of the most important parameter in era of IoT and also for dynamic group communication.
- All existing methodologies are consider scalability as performance parameter still there is problem of time complexity in case of key generation and authentication time.
- RFID systems, Mobile ad-hoc networks, Vehicular ad-hoc netwoks, Machine type systems, Wireless sensor networks, Wimax, Wi-Fi widely used group authentication protocols.
- In future scalability, time complexity can be improved.

REFERENCES

1. Xu Xiaohui, "**Research on Safety Certification and Control Technology in Internet of Things**", In Fourth International Conference on Computational and Information Sciences, Vol.7, No. 3, pp. 669- 677, September 2012. https://doi.org/10.1109/ICCIS.2012.253
2. Lein Harn and Changlu Lin, "**An Efficient Group Authentication For Group Communications**", In International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, pp. 2014-2020, May 2013.
3. Lein Harn, **"Group Authentication",** In IEEE Transactions on computers, Vol. 62, No. 9, pp. 1893 –1898, September 2013.Parisa https://doi.org/10.1109/TC.2012.251
4. Memarmoshrefi, Omar Alfandi, Ansgar Kellner, Dieter Hogrefe,"**Autonomous Group-based Authentication Mechanism in Mobile Ad Hoc Networks**", In the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications , Vol. 30, No. 10, pp. 594-600, July 2012.
5. Hong Liu, Huansheng Ning, Yan Zhang, Daojing He, Qingxu Xiong and Laurence T. Yang, "**Grouping-Proofs-Based Authentication Protocol for Distributed RFID Systems"**, In IEEE Transactions on parallel and distributed systems, Vol. 24, No. 7, pp. 333-343, July 2013.
6. Wafa Ben Jaballah, Mohamed Mosbah, Habib Youssef and Akka Zemmari**,"Lightweight Source Authentication Mechanisms for Group Communications in Wireless Sensor Networks"** In IEEE 27th International Conference on Advanced Information Networking and Applications, Vol. 69, No. 9, pp. 1435-1441, June 2013. https://doi.org/10.1109/AINA.2013.56
7. Shunrong Jiang, Xiaoyan Zhu and Liangmin Wang, **"A Conditional Privacy Scheme based on Anonymized Batch Authentication in Vehicular Ad-Hoc Networks",** in IEEE wireless communication and networking conference, Vol. 45, No.5, pp. 923- 929, September 2013.
8. Parikshit N. Mahalle, Neeli R. Prasad and Ramjee Prasad, **"Novel Threshold Cryptography-Based Group Authentication (TCGA) Scheme for the IoT"** in seventh IEEE conference on Advanced Networks and Telecommunication Systems, 2013
9. Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li, **"Efficient Privacy- preserving Authentication for Vehicular Ad Hoc Networks"** In IEEE Transactions on vehicular technology , Vol. 63, No. 2, pp. 293-305, February 2014.
10. Yueyu Zhang, Jie Chen, Hui Li, Wujun Zhang, Jin Cao and Chenzhe Lai**,"Dynamic Group base Authentication Protocol for Machine Type Communications",**In Fourth International Conference on Intelligent Networking and Collaborative Systems, Vol.78, No.9, pp. 756-764, March 2012.
11. Mr. S. K. Pathan, Mr. S. N. Deshmukh, Dr. R. R. Deshmukh**, Kerberos Authentication System – A Public Key Extension,** International Journal of Recent Trends in Engineering, May 2009, Vol. 1, No. 2, 15-19
12. Gao T., Qi J. (2019) **An Anonymous Access Authentication Scheme for VANETs Based on ID-Based Group Signature.** In: Barolli L., Leu FY., Enokido T., Chen HC. (eds) Advances on Broadband and Wireless Computing, Communication and Applications. BWCCA 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 25.
13. Liu, Y., Sun, Q., Wang, Y. et al. **Cluster Computing** (2018). https://doi.org/10.1007/s10586-018-1929-1.
14. Mrs. Reshma Sonavane, Mr. V. S. Bidve, **Data gathering In Multiple Mobile Sink Environment for WSN**, International Journal of Scientific and Engineering Research (IJSER), ISSN: 2229-5518, Volume 5, Issue 7 Edition, 2014.