Software Defined Network aided cluster key management system for secure fusion multicast communication in Internet of Vehicles

Antony Taurshia*, Jaspher Willsie Kathrine, Venkatesan

Karunya Institute of Technology and Sciences, India
Emails: antony18@karunya.edu.in; kathrine@karunya.edu, rlvenkei_2000@karunya.edu

Abstract

Smart applications came into existence with technological advancements like Software Defined Networks (SDN), Cloud computing, Network Function Virtualization (NFV), and the Internet of Things (IoT). Internet of Vehicles (IoV) is a highly dynamic application with limited tolerance to latency since a small delay can lead to drastic disasters. For efficient network and vehicle management clusters are formed in IoV. Secure key management is unavoidable to secure communication between the vehicles in the cluster. In this article, a sustainable cluster key management approach is proposed to handle the dynamic and latency-sensitive nature of IoV. Security analysis proves that the proposed approach holds secrecy in group key management. The proposed approach reduces the communication complexity to a single broadcast for re-keying. The analysis proves that the computation and storage complexity is also minimal, hence proving that the scheme is sustainable with limited resource usage and efficient for usage in latency-sensitive IoV environments.

Keywords: secure fusion communication; internet of things; internet of vehicles; group key management; security

1. Introduction

The era of the Internet of Computers shifted to the Internet of Things (IoT) with the advent of technologies like Radio Frequency Identification (RFID) tags, Wireless Sensor Networks (WSNs), and Lightweight Communication protocols [1]. These technologies enable even mundane objects to connect to the internet to do some smart functions. The IoT system is the collaborative working of this internet or intranet-connected objects and efficient service platforms to form applications like smart homes, smart grids, intelligent transportation, healthcare, and Industry 4.0. Though the use of these applications is incomparable, they come with their vast vulnerabilities and security threats. Securing this system is crucial, as the devices getting connected are resource constrained with limited storage and computational capabilities. The burden of securing the system increases if it is highly dynamic and latency-sensitive too. One such heterogeneous, dynamic, and latency-sensitive application is the Internet of Vehicles (IoV). The IoV is an extended form of Vehicular Adhoc network (VANET), capable of obtaining and providing services using internet-connected service platforms

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

like the cloud [2]. In the process of Vehicle-to-Vehicle communication, dynamic clusters are generated in VANET for efficient network management using IEEE 802.11p [3].

Software Defined Networks (SDN) is a technology that virtualizes networking by segregating the control plane from the data plane[4]. The control layer contains the SDN controller that contains applications for programming the network. The data plane contains network devices that only forward the traffic based on the information generated by the controller. As SDN is capable of locating the vehicle and partitioning the network, it is used for efficient cluster management to aggregate the vehicles and handle their heterogeneity[3]. The communication between these vehicles needs to be secured through efficient key management. Using symmetric keys in this system will be inefficient as the clusters generated and the vehicles that fall within the range are dynamic. Computationally expensive public key cryptography-based schemes and distributed key management systems are widely proposed for the security management of VANETs and IoV [5]–[7].

In this paper, a sustainable key management approach proposed to secure fusion communication between vehicles that come and go within the clusters generated using SDN is proposed. The proposed cluster key management approach uses LFSRs used for pseudorandom key generation, which is used in the encryption of data stream using stream ciphers like ZUC, SNOW-3G, trivium, WG-8 [8], [9]. The sequences generated by LFSRs are flexible and can be tailored according to the needs of the algorithm. It also uses less chip area and time [10], which makes it more suitable for IoT devices. The keys generated are used only for a limited timeline making the scheme more secure. This enhances the security of the system against man-in-the-middle attacks and replay attacks. Even with captured data, the adversary won't be able to perform an attack and disrupt the working of vehicles in transit.

The following section unfolds as follows. Section 1 gives a literature review on key management specific to WSN and IoT and also key management specific to VANETS and IoV. Section 2 gives the insight into communication and threat model of our proposed system. Section 3 depicts the LFSR-based functions used in our proposed system. Section 4 gives a detailed explanation of our proposed security management system Section 5 gives the security analysis and Section 6 depicts the performance analysis of our system.

2. Related Work

Key Management Specific to WSN And IoT

The key management schemes can be classified into a centralized scheme, where a centralized server is responsible for generating, distributing, and updating the keys, a distributed scheme where all the nodes of the group participate to perform efficient key management and a decentralized scheme where both the nodes and server coordinate in key management. Several key management schemes are proposed so far for securing WSN and IoT. Among them, the probabilistic-based key management scheme is the widely proposed scheme for cluster-based WSN [11]. But a probabilistic scheme does not guarantee the availability of a common key between two nodes of different clusters to establish secure fusion communication. Moreover, the compromise of a node may reveal more keys to the adversary and lead to the capture of the entire network. Other probabilistic schemes loop-based key management schemes [12] and random key management schemes [13] are proposed to increase the probability of finding a common key and reduce the impact of node capture attacks on the network.

A time-based key management scheme [14] is proposed which uses a one-way function to generate and update keys with time to reduce the impact of node capture attacks. A cluster-based cognitive key management scheme was proposed in [11] for a mobile IoT environment. The proposed scheme reduces the computation overhead and delays when a node leaves from one location area to another. A scalable group key management scheme is proposed in [15] to generate the key for communication in two steps using ECC. In [16] a horizontal model for group management was proposed using SDN. The group key is obtained through Deffie-Hellman and members of the same group will be able to form a session key and exchange a vector of values that are used as packet keys. Packet keys are relatively small size keys but security strength is obtained as different keys are used for encrypting the packets. Another lightweight group key management for the Internet of Things is proposed in [17]. LKH is used for key distribution and keys are generated using a hash of group id and node id. This technique reduces the computation cost and storage overhead. But this scheme is vulnerable to forgery of messages as members subscribing to the same group can get access to all members' ids. A

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

centralized lightweight key management approach for groups in IoT is proposed in [18]. The approach similarly uses a pseudorandom sequence generator and GCD method with minimal computation, storage, and communication overhead. Still, the approach needs a key tree to identify adjacent nodes to obtain the group key using the KEK.

Key Management Specific To VANET And IoV

A combination of elliptic curve cryptography (ECC) and a dynamic secret sharing scheme based on the El Gamal threshold mechanism for key management in VANETS is proposed in [19]. Though the scheme has less processing time compared to its previous RSA-based schemes, it uses complex operations like Lagrange interpolation for secret sharing. Moreover, the scheme doesn't provide a non-repudiation feature. Another ECC-based dynamic secret sharing scheme for VANETS is proposed in [20]. The proposed scheme has less computation overhead than the previous scheme but still uses a signature for verification. A dynamic key distribution using PKI is proposed in [7] where a Certificate Authority issues a certificate to authenticated vehicles based on a vehicle authentication code containing license plate details and chassis number. As long as the certificate is valid the vehicles can participate in the network. A Diffie-Hellman-based key distribution for VANETS is proposed in [5]. To avoid man-in-the-middle attack a pre-shared secret is used along with the group key. Another Chinese Remainder Theorem (CRT) based key management system is proposed in [21]. Yet CRT has scalability issues. An authenticated key management scheme for IOV is proposed in [6]. A simple hash function is used and authentication of the vehicle is done based on arrival time. Still, the scheme is prone to impersonation attacks.

3. Communication And Threat Model

The difference between VANET and IoV is depicted in [2]. IoV is an extended form of VANET where the latter supports only three types of communication as Vehicle-to-Vehicle, Vehicle-to-Infrastructure, and Vehicle-to-Road Side Unit. IoV is extended to support Vehicle-to-Everything kind of communication and this Everything includes the user's devices and sensors. IoV is a complex and heterogeneous network compared to VANET and hence needs a dedicated software platform like cloud and fog for efficient management. To conclude through IoV the applications of VANET can be enhanced.

In our scheme, we are considering only two types of communication, Vehicle-to-Vehicle, and Vehicle-to-Road Side Unit (RSU). The Trusted Authority (TA) is placed in the fog server and is responsible for authenticating the vehicle. The RSU acts as a gateway between TA and the vehicle for authentication. The RSU is also equipped with lots of resources and an SDN-based security controller is integrated with each RSU. One of the applications of IoV is vehicle platooning where vehicles move in a group to avoid collision. The SDN controller embedded in the RSU is responsible for the formation of vehicle clusters that come within the range of the RSU. As the clusters change dynamically, the security controller in RSU is responsible for updating the new session key and notifying the vehicles of cluster change. All the messages flow through SDN and will be stored in the fog server and thereby to the cloud for future reference. Fig 1. shows the communication model of our system.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

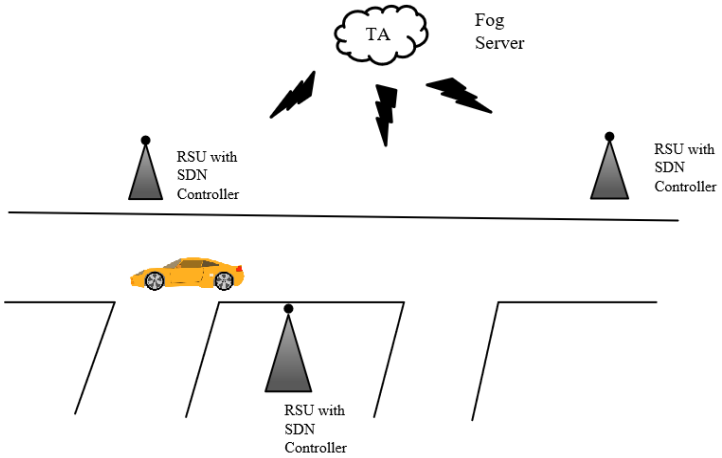

Figure 1: Communication network of our system

SDN for dynamic cluster formation

The concept of clustering using SDN is discussed in several literature. In [22] the IoT network is divided into clusters using SDN with a cluster head embedded with SDN. A similar proposal is made in [23] where the network is divided into domains with a root controller and a border controller in it. The security rules and routing functions are deployed in the border controller and whenever a new flow is encountered it is checked for authenticity. In [3][24] the formation of dynamic clusters in VANETS using SDN is proposed for efficient network management. A horizontal model for end-to-end security management and group management using SDN is proposed in [16]. Two different groups can communicate with the SDN controller as intermediate and provide a horizontal model of group management compared to vertical models. The use of SDN and blockchain for efficient network management is proposed in [25]. SDN segregates the IoT network into clusters and is responsible for device registration and reducing network delay. The architecture also eliminates the expensive Proof of Work in blockchain with a distributed trust-based authentication method. A blockchain-based group management is proposed in [26] for efficient service delivery to IoT networks using Unmanned Aerial Vehicles (UAV)s. The density of devices in groups is monitored and UAVs are used to deliver service to highly dense groups. This work also uses SDN to form vehicle clusters for efficient network and SDN-based security controller for security management in case of vehicle platooning. There is no cluster head-based communication in our system. An update will be unicasted by RSU to the vehicles of its cluster.

Threat model

As the consequences of error in IoV will be fatal, executing strict security measures is undeniable. Moreover, the nature of IoV is very dynamic, which makes it liable to lots of insider attacks. A malicious insider may want to send false data to disrupt the system. There is a possibility for a replay attack or a man-in-the-middle attack [27]. Threats from outsiders include impersonation attack, where a malicious person may act as an authorized user, and denial of service attack to prevent the servers from providing normal service. Moreover, while securing the system, the privacy of the user should also be maintained. The vehicles that form a group, do not necessarily disclose the private information of the user or the vehicles' identity. Hence the anonymity of the system needs to be maintained along with security [27].

4. LFSR Based Functions in the Proposed System

LFSR for authentication

With LFSR a cryptographically secure hash function can be generated which can be used for message authentication [28]. For a message M of length L and a non-zero term polynomial $q(x)$ of degree n over Galois Field $GF(2)$, a hash function H_q is defined as

$$H_q = M(x).x^n.\bmod q(x) \quad (1)$$

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

$$K_{tav} = H_q \text{ xor } s \quad (2)$$

The hash function uses LFSR for polynomial division over GF(2) with q(x) as the primitive polynomial. In our proposed system, this hash function is used for mutual authentication between TA and vehicle as both share a pre-shared secret which is used as message M(x) of the H_q. The xor function makes the hash function furthermore secure.

LFSR for Key Generation

Linear Feedback Shift Registers are used for pseudorandom key stream generation whose current state s_i is an output of its previous stage s_{i-1}. To generate a long sequence of key sstreamsalong with the input seed value, feedback is provided to LFSR based on the feedback function over Galois Field GF(2). The feedback function is a primitive polynomial of form $p(x) = x^l + c_{l-1}x^{l-1} + c_{l-2}x^{l-2} + \ldots\ldots x^0$ where l is the length of the LFSR [8], [29]. The key stream generated is split into n keys of b bits each to generate distinct keys.

In LFSR a duplicate i.e., the repetition of the same bit pattern is attained at the key period, $2^n - 1$ where n is the length of the input bits. For a 16-bit non-zero input seed value, the period is $2^{16} - 1 = 65536$. If the seed value size is 128 bits, then approximately 512 distinct keys can be obtained.

5. Our Contribution

The dynamic nature of IoV, makes the deployment of a complete security solution, as hard to achieve. The IEEE 1609.2 standard is lacking in addressing key management and identity management [30]. Ipv6 has issues regarding group management[31]. Our proposed scheme is lightweight with enhanced security and suitable for highly dynamic environments. In the proposed approach SDN is used for efficient network management as the vehicles adopt different communication networks. RSU distributes the cluster keys to the vehicle clusters formed in IoV. The notations used in the proposed scheme are depicted in table 1.

Table 1: Notations used in our scheme.

$K_{TA(pub)}$	The public key of trusted authority
$K_{TA(pri)}$	The private key of trusted authority
pp	Primitive Polynomial
Vv_{id}	Vehicle validation ID
V_{id}	Vehicle ID
pp_e	Primitive Polynomial for encryption
ts	Timestamp
Ck	Cluster Key
K_{tav}	Key of trusted authority and vehicle
Tv_{id}	Temporary vehicle ID
K_{TRSU}	Key of trusted authority and RSU
N	Number of vehicles in cluster
I_v	Index value
M_x	Secret message shared between trusted authority and vehicle
H(.)	Hash

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

E(m, k)	Encrypt message m using key k
Dk(i)	Distinct keys
TEK	Temporary Encryption Key

Proposed Scheme

Our proposed model considers, the trusted authority (TA) placed in the fog server as safe and cannot be compromised. The vehicle's keys and its essential credentials are stored in the Hardware Security Module (HSM) of the vehicle's On-Board Unit and hence cannot be tampered with. The Road Side Units are equipped with an SDN controller, which is responsible for cluster formation and communication. A vehicle that enters the network is broadcasted with the public key of TA and primitive polynomial encrypted using Key Policy- Attribute Based Encryption, hence an eligible vehicle can decrypt it. The vehicle then sends its' validation ID Vv_{id} , which it obtained during vehicle registration, encrypted using TA's public key to TA with a timestamp. TA upon receiving the message decrypts it using its private key $K_{TA(pri)}$and obtains the validation id Vv_{id}, and then looks for its matching Vehicle ID V_{id}. A registered and valid vehicle's ID will be in the list. Hence the TA knows it as unauthenticated vehicle values calculates the key $K_{tav} = \text{hash}(M_x||pp||s)$, where M_x and s is the secret shared between TA and vehicle during registration. It then encrypts the primitive polynomial for key generation pp_e, timestamp ts, temporary secret s_t with the generated key K_{tav} and sends to the vehicle. The hash function used in this step is the LFSR generated hash. If the vehicle is able to generate the same hash function using shared secrets, then the vehicle is an authenticated vehicle as well as the TA. Now the vehicle is able to obtain the temporary key to obtain the cluster key for group communication. TA then sends the temporary ID Tv_{id}, and temporary secret s_t individual for the vehicle and sends it to RSU using the key shared between them. The vehicles use the temporary secret s_t as seed to the pseudorandom sequence generator and pp_e as feedback function. For a vehicle, the first 128-bit generated is the first TEK. When a vehicle changes to second timeline then the next 128-bit is taken as TEK. It is mandatory for RSU to keep track of a vehicle's timeline

An authenticated vehicle will enter the cluster formed using SDN when it comes within the range and of RSU. The RSU calculates the cluster key Ck as follows

$$\gamma = \text{GCD}[(H(TEK_{v1})H(TEK_{v2}).....H(TEK_{vn})] + Ck \quad (3)$$

where $Ck<H(TEK_{v1},H(TEK_{v2}).....H(TEK_{vn})$ (4)

TEK_{vi} is the TEK of vehicle i in the cluster. $H(TEK_{v1})$denotes hash of TEK_{vi}. The vehicles obtain the CK by performing a mod function on γ as follows

$$\gamma = MOH(TEK_{vi}) \quad (5)$$

After a certain time period the vehicle cluster formation change hence the timeline changes, a new Ck is calculated by RSU and broadcasted. Fig. 2 depicts the mutual authentication between Vehicle and RSU, plus cluster key distribution. The proposed authentication and cluster key management are sustainable as it uses KP-ABE-based decryption, and a hash function for mutual authentication, a mod function for obtaining the cluster key. If the pseudorandom key generation reaches the period of $2^n - 1$, a new seed can be generated by hashing the previous cluster key Ck and temporary secret s_t.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

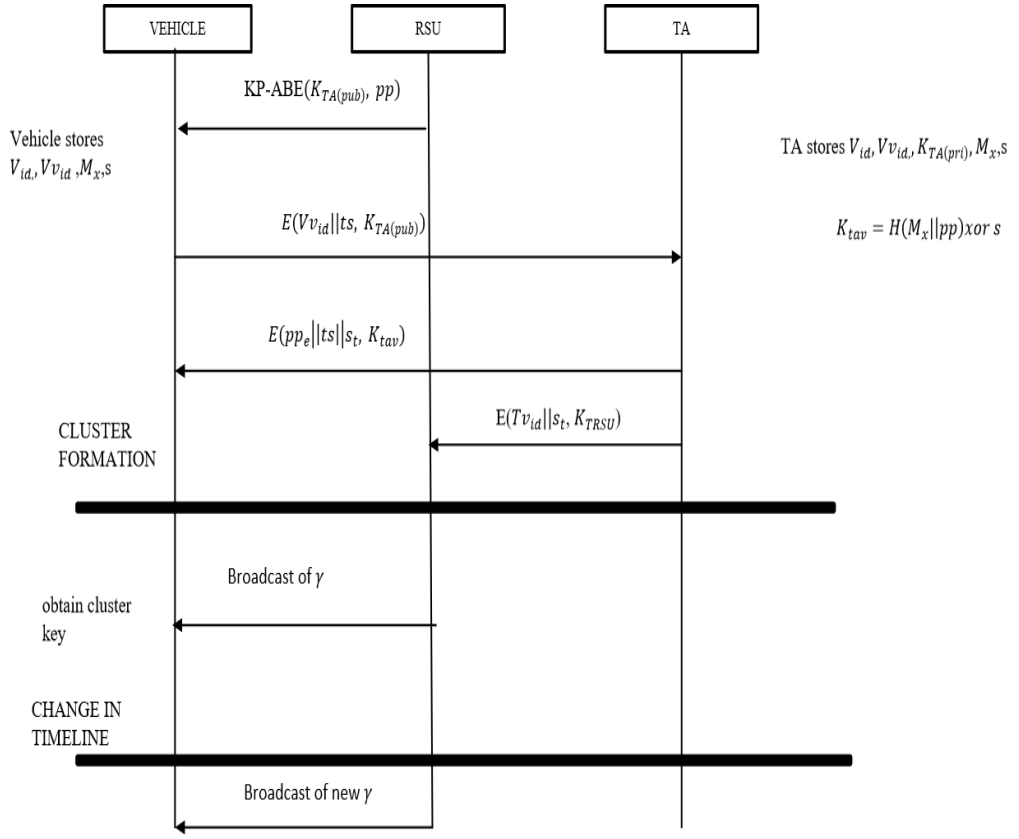

Figure 2: Mutual authentication and distribution of cluster key

Algorithm

Early Registration

An authenticated vehicle will be assigned a vehicle validation ID Vv_{id}, and obtains trusted authority id TA_{id} and shared secret M_x and s.

Vehicle Entry

Step 1. A vehicle V(i) entering the network gets the message KP-ABE($K_{TA(pub)}$, pp) broadcasted by RSU. An authorized vehicle can decrypt the message and obtain the public key and primitive polynomial pp.

Step 2. The vehicle then sends the message $E(Vv_{id}||ts,\ K_{TA(pub)})$ to TA with its vehicle validation ID Vv_{id} received during the vehicle registration. The message is decrypted using the private key $K_{TA(pri)}$ of TA. The TA then checks for the vehicle's ID V_{id} in its authenticated list using the vehicle validation ID Vv_{id} . If the vehicle's ID is in the list it will be able to generate the key K_{tav} using the pre-shared secret shared between the vehicle and TA during registration.

Step 3. TA then calculates $K_{tav} = \text{hash}(M_x||pp||)$xor s, and replies to the vehicle with a message $E(ts|s_t|pp_e,\ K_{tav})$. The vehicle then calculates K_{tav} using the shared secret M_x and s to decrypt the message and obtains temporary secret key s_t and primitive polynomial pp_e for key generation.

TA To RSU

Step 4. TA updates the RSU with the temporary vehicle ID and temporary secret key s_t for obtaining the cluster key.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

RSU To VEHICLE

Step 5. The cluster of vehicles is formed by SDN that comes within the range of RSU. The RSU then calculates the cluster key Ck as in equation 1 for the vehicles forming the cluster and broadcasts the value δ. The vehicles obtain the Ck by performing a mod function as in equation 2.

Key Update

Step 6. When there is a change in the timeline, RSU broadcasts the new δ value to the vehicles in cluster to update the cluster key.

Step 7. The process repeats from step 6 with the new cluster key.

Step 8. When the next RSU is reached, the process repeats from Step 2. Hence a misbehaving vehicle can be removed from the network during this authentication process.

6. Security Analysis

The security of the proposed system comes with short-lived keys. The lifetime of $K_{TA(pub)}$, $K_{TA(pri)}$, and pp is for a day or week. The cluster key's Ck lifetime is only till the change in timeline or change in cluster. The security analysis of the proposed authentication and cluster key management goes as follows.

AUTHENTICATION

Man-in-the-Middle attack

In the proposed approach for a malicious outsider, even if he manages to obtain the pp value, the only way to obtain the session key is through brute force attack, which is not feasible, and the session key keeps changing with the change in phase.

Replay attack

A replay attack is not feasible in the proposed scheme as the packets are appended with the timestamp and is verified with the IP address and temporary ID Tv_{id} of the vehicle by the RSU server. Moreover, when the vehicle reaches a new RSU, the clusters are reassigned. Even during the authentication phase, the messages are appended with the timestamp.

Impersonation attack

An adversary can pose as TA only if he knows the secret message M_x and s shared between the vehicle and TA. An adversary can pose as an RSU only if it knows the temporary secret of the vehicle, which will be stored in a trusted fog server.

CLUSTER KEY MANAGEMENT

Theorem 1: A leaving or joining user cannot obtain the future cluster key.

Proof: The cluster key can be obtained only when a vehicle's TEK is added for computing γ value. A vehicle can leave or join only with the change in timeline. When the timeline changes, the exiting vehicle's TEK is removed and the new vehicle's newly generated TEK will be included based on the timeline of the vehicles. Unless a vehicle knows the temporary secret s_t of another vehicle participating in the cluster, the cluster key Ck cannot be compromised.

Theorem 2: Even after collision with the malicious vehicle in the cluster, the future or past cluster key Ck cannot be compromised.

Proof: When the number of vehicles in the cluster is less than 3, the vehicle can obtain the adjacent vehicle's H(TEK) value. Still when the timeline changes the TEK value as well as the number of vehicles in the cluster changes. Hence even after a collision with a malicious vehicle in the cluster, the previous or future cluster keys cannot be compromised.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

7. Performance Analysis

Computation Overhead for authentication.

The previous schemes of VANET and IoV rely on asymmetric cryptography like Diffie-Hellman, ECC and complex bi-linear pairing operations, certificates, and signature-based schemes for authenticated key agreement, and group key management. The proposed scheme uses a KP-ABE decryption which uses only l pairing operations, where l is the number of attributes that matches the access policy, and two hash functions for authentication and key agreement. If only a vehicle's validity-based access token is used as an attribute for KP-ABE-based decryption, then there is only one pairing operation. Table 2 shows the comparison of our scheme with the existing schemes [32]–[34], where T_p, T_h, T_m, T_{ep-1} and T_{ep-2} are the computation time for pairing operation, hash, multiplication, and exponentiation operation in multiplicative additive cyclic groups G1 and G2 respectively. The comparison shows the proposed scheme is optimal.

Table 2: Comparison of computation cost of various schemes.

Method	Computation cost
Shim's scheme	$5T_p + 2T_h + 8T_m$
Bayat et al. scheme	$5T_P + 1T_{ep-1} + 1T_h$
Pandi et al. scheme	$2T_p + 2T_{ep-1} + 1T_{ep-2} + 1T_h$
Proposed scheme	$1T_p + 1T_h$

Computation overhead on device for group key management

The proposed technique possesses minimal overhead yet is secure. The proposed group key management approach is compared with existing key management approaches for groups [31] [32] [33] [17] [18]. Table 3 gives the comparison on the overhead for computation in devices. C_d, keygen, C_h represents the time taken for performing AES decryption, key generation using LFSR, and SHA hash. The time taken for proposed cluster key management approach is computed in an Intel i5 system with 8GB RAM and a 64-bit processor. It took almost 780 microseconds to compute SHA-256 and 300 microseconds to compute AES-128 decryption. The LFSR key generation took 20 microseconds and mod operation took 88 microseconds. Fig. 3 shows the proposed work has the least computation cost compared to all other existing approaches as it uses a single hash and mod function to compute the cluster key. The approaches OFT and ROFT share the same overall computation cost.

Table 3: Comparison of computation cost.

Approach	device join event	User or device leaves event	Total computation cost
LKH	$(3\log_2 n + 1) * C_d$	$2\log_2 n * C_d$	$(5\log_2 n + 1) * C_d$
OFT	$(2\log_2 n + 1) * C_d + (\log_2 n + 1) * C_h$	$(\log_2 n + 1) * C_d + (\log_2 n) * C_h$	$(3\log_2 n + 1) * C_d + (2\log_2 n + 1) * C_h$
ROFT	$(2\log_2 n + 1) * C_d + (2\log_2 n) * C_h$	$(\log_2 n + 1) * C_d + (\log_2 n) * C_h$	$(3\log_2 n + 1) * C_d + (2\log_2 n + 1) * C_h$

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

Group-It	$(\log_2 n) * C_d + C_h$	C_d	$(\log_2 n + 1) * C_d + C_h$
GKM-LRD	1keygen+2mod+1C_h	1keygen+2mod+1C_h	2keygen+4mod+2C_h
proposed	C_h+mod	C_h+mod	2(C_h+mod)

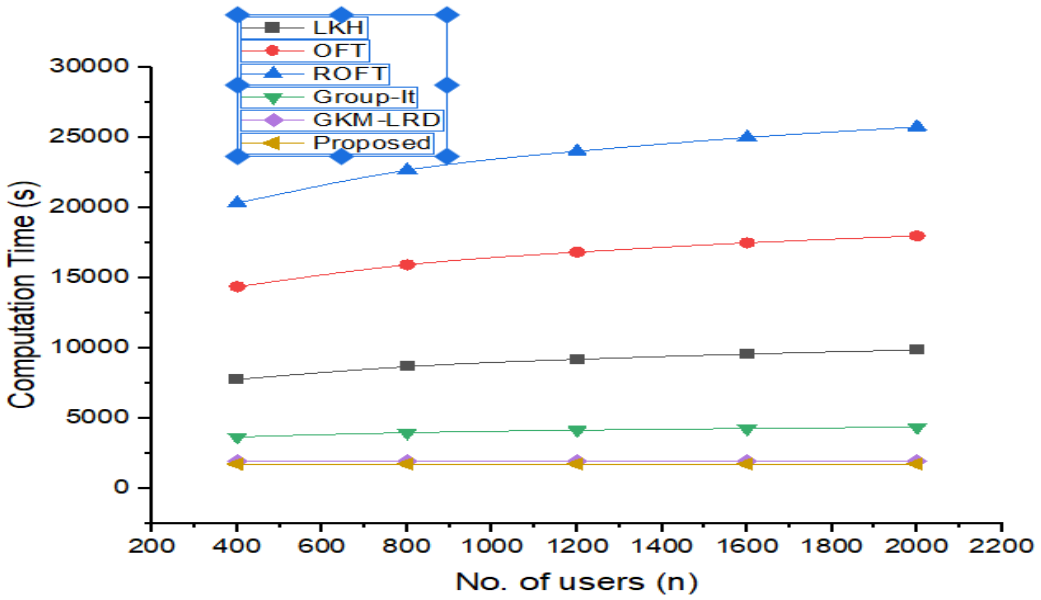

Figure 3: Comparison of computation cost.

Communication overhead on the device for group key management

The communication overhead of the cluster key management approach depends on the number of keys to be transmitted. Table 4 gives a comparison on the overhead for communication between the key management approaches for groups. From Fig. 4 it is derived that the proposed work has the least communication overhead with a single broadcast.

Table 4: Comparison of communication cost.

Approach	User or device join event	User or device leave event	Total communication cost
LKH	$3\log_2 n+1$	$2\log_2 n$	$5\log_2 n + 1$
OFT	$(2\log_2 n + 1) * L$	$(\log_2 n + 1) * L$	$3(\log_2 n + 1) * L$
ROFT	$(2\log_2 n + 1) * L$	$(\log_2 n + 1) * L$	$3(\log_2 n + 1) * L$
Group-It	$\log_2 n + 1$	1	$\log_2 n$ +2
GKM-LRD	4	3	7
proposed	1	1	2

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

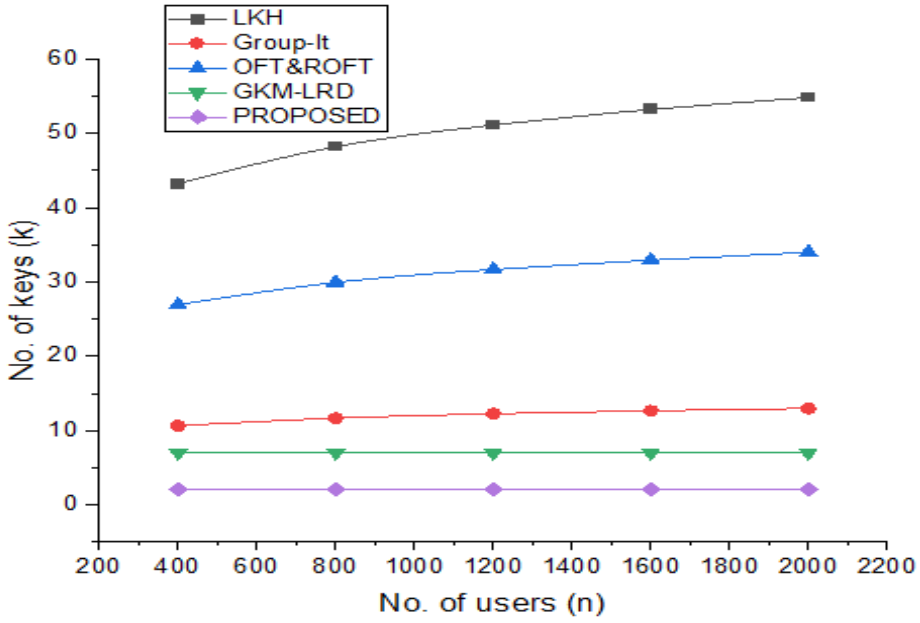

Figure 4: Comparison of communication cost.

Storage overhead on the device for group key management

The storage overhead of the proposed approach depends on the number of keys to be stored on the device. Table 5 gives the comparison of storage load on the device for the key management approaches in groups. In the proposed system the vehicle can store only three values s_t, pp_e and Ck. Fig. 5 exhibits the minimal overhead imposed on the device by the proposed key management approach for groups compared with the existing centralized approaches.

Table 5: Comparison of storage cost.

Approach	Total storage cost
LKH	$2\log_2 n+1$
OFT	$2\log_2 n+1$
ROFT	$3\log_2 n$
Group-It	$\log_2 n +4$
GKM-LRD	4
proposed	3

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

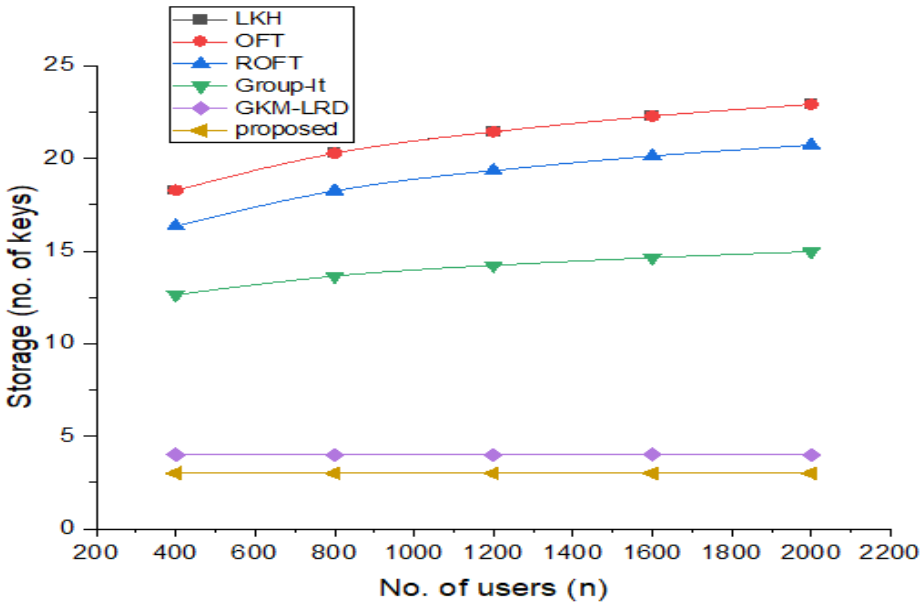

Figure 5: Comparison of storage cost.

Latency in Key Generation using modified LFSR

In order to improve the non-linearity of the key stream generated using LFSR, a modified LFSR which uses minimum time for key stream generation is proposed in [8]. The time taken for key stream generation using the modified LFSR along with the ZUC stream cipher is mentioned in table 2. Hence even with the modified LFSR, the latency due to dynamic key generation and encryption is negligible.

Table 6: Time taken for key generation and encryption using modified LFSR.

Length of Key Stream	Time Taken(seconds)
$4*10^7$	1
$6*10^7$	2
$1*10^8$	4

8. Conclusion

Providing information fusion security in vehicular networks is undeniable. The proposed work uses SDN for cluster formation and a sustainable approach for cluster key management. Since the network of IoV is dynamic and heterogeneous with limited tolerance to latency providing a computationally less expensive cluster key management solution is inevitable. The proposed work uses a centralized cluster key management approach without the need to maintain a tree data structure. The performance comparison of the proposed approach shows that the work is lightweight with minimal overhead for authentication as well as for key updating in cluster key management. Minimal computation overhead inflicts lesser energy usage in the vehicles making the proposed approach sustainable. The security analysis ensures secrecy in cluster key management. The work can be extended with computationally less expensive decentralized and distributed cluster key management approaches instead of a centralized approach.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

References

[1] Smarandache, F., Neutrosophic set a generalization of the intuitionistic fuzzy sets. Inter. J. Pure Appl. Math., 24, 287 – 297, 2005.

[2] S. Li, "Security Requirements in IoT Architecture," in Securing the Internet of Things, Elsevier Inc., 2017, pp. 97–108.

[3] R. Gasmi and M. Aliouat, "Vehicular Ad Hoc NETworks versus Internet of Vehicles-A Comparative View," in Proceedings - ICNAS 2019: 4th International Conference on Networking and Advanced Systems, 2019, pp. 1–6, doi: 10.1109/ICNAS.2019.8807870.

[4] X. Duan, X. Wang, Y. Liu, and K. Zheng, "SDN enabled dual cluster head selection and adaptive clustering in 5G-VANET," in IEEE Vehicular Technology Conference, 2016, no. December 2018, doi: 10.1109/VTCFall.2016.7881214.

[5] S. Sezer et al., "Are we ready for SDN? Implementation challenges for software-defined networks," IEEE Commun. Mag., vol. 51, no. 7, pp. 36–43, 2013, doi: 10.1109/MCOM.2013.6553676.

[6] M. N. Mejri, N. Achir, and M. Hamdi, "A new group Diffie-Hellman key generation proposal for secure VANET communications," in 2016 13th IEEE Annual Consumer Communications and Networking Conference, CCNC 2016, 2016, no. January, pp. 992–995, doi: 10.1109/CCNC.2016.7444925.

[7] [M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment," IEEE Internet Things J., vol. 6, no. 5, pp. 8804–8817, 2019, doi: 10.1109/JIOT.2019.2923611.

[8] A. Hesham, A. Abdel-Hamid, and M. A. El-Nasr, "A dynamic key distribution protocol for PKI-based VANETs," in IFIP Wireless Days, 2011, vol. 1, no. 1, doi: 10.1109/WD.2011.6098221.

[9] R. Muthalagu and S. Jain, "Modifying LFSR of ZUC to reduce time for key-stream generation," J. Cyber Secur. Mobil., vol. 5, no. 4, pp. 257–268, 2016, doi: 10.13052/jcsm2245-1439.541.

[10] [M. A. Philip and V. Vaithiyanathan, "A survey on lightweight ciphers for IoT devices," in Proceedings of 2017 IEEE International Conference on Technological Advancements in Power and Energy: Exploring Energy Solutions for an Intelligent Power Grid, TAP Energy 2017, 2018, no. December, pp. 1–4, doi: 10.1109/TAPENERGY.2017.8397271.

[11] S. Mukhopadhyay and P. Sarkar, "Application of LFSRs for parallel sequence generation in cryptologic algorithms," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2006, vol. 3982 LNCS, pp. 436–445, doi: 10.1007/11751595_47.

[12] A. B. F. Khan and G. Anandharaj, "A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment :," SN Appl. Sci., vol. 1, no. 12, pp. 1–7, 2019, doi: 10.1007/s42452-019-1628-4.

[13] Y. Z. Zeng, B. K. Zhao, J. S. Su, X. Yan, and Z. Shao, "A loop-based key management scheme for wireless sensor networks," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2007, vol. 4809 LNCS, pp. 103–114.

[14] L. Zhu and Z. Zhan, "A random key management scheme for heterogeneous wireless sensor network," 2015, doi: 10.1109/SSIC.2015.7245677.

[15] J. Jang, T. Kwon, and J. Song, "A Time-Based Key Management Protocol for," pp. 314–328, 2007.

[16] S. Ali et al., "SGKMP: A scalable group key management protocol," Sustain. Cities Soc., vol. 39, no. November 2017, pp. 37–42, 2018, doi: 10.1016/j.scs.2018.01.003.

[17] E. Festijo, Y. Jung, and M. Peradilla, "Software-defined security controller-based group management and end-to-end security management," J. Ambient Intell. Humaniz. Comput., vol. 10, no. 9, pp. 3365–3382, 2019, doi: 10.1007/s12652-018-0678-6.

[18] Y. H. Kung and H. C. Hsiao, "GroupIt: Lightweight Group Key Management for Dynamic IoT Environments," IEEE Internet Things J., vol. 5, no. 6, pp. 5155–5165, 2018, doi: 10.1109/JIOT.2018.2840321.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

[19] A. Taurshia et al., "Software-defined network aided lightweight group key management for resource-constrained Internet of Things devices," Sustain. Comput. Informatics Syst., vol. 36, no. June, p. 100807, 2022, doi: 10.1016/j.suscom.2022.100807.
[20] N. Ruan, T. Nishide, and Y. Hori, "Elliptic curve ELGamal threshold-based key management scheme against compromise of distributed RSUs for VANETs," J. Inf. Process., vol. 20, no. 4, pp. 846–853, 2012, doi: 10.2197/ipsjjip.20.846.
[21] G. Duan, Y. Xiao, R. Ju, and H. Song, "A novel key management scheme in VANETs," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014, vol. 8630 LNCS, no. PART 1, pp. 587–595, doi: 10.1007/978-3-319-11197-1_45.
[22] K. K. Chauhan, S. Kumar, and S. Kumar, "The design of a secure key management system in vehicular ad hoc networks," in 2017 Conference on Information and Communication Technology, CICT 2017, 2018, vol. 2018-April, pp. 1–6, doi: 10.1109/INFOCOMTECH.2017.8340636.
[23] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, "SDN-based security framework for the IoT in distributed grid," 2016 Int. Multidiscip. Conf. Comput. Energy Sci. Split. 2016, 2016, doi: 10.1109/SpliTech.2016.7555946.
[24] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN Based Architecture for IoT and Improvement of the Security," Proc. - IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2015, no. February 2018, pp. 688–693, 2015, doi: 10.1109/WAINA.2015.110.
[25] M. A. Saleem et al., "Expansion of Cluster Head Stability Using Fuzzy in Cognitive Radio CR-VANET," IEEE Access, vol. 7, pp. 173185–173195, 2019, doi: 10.1109/ACCESS.2019.2956478.
[26] S. A. Latif et al., "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," Comput. Commun., vol. 181, no. August 2021, pp. 274–283, 2022, doi: 10.1016/j.comcom.2021.09.029.
[27] G. Heo, K. Chae, and I. Doh, "Hierarchical Blockchain-Based Group and Group Key Management Scheme Exploiting Unmanned Aerial Vehicles for Urban Computing," IEEE Access, vol. 10, pp. 27990–28003, 2022, doi: 10.1109/ACCESS.2022.3157753.
[28] X. Shen, C. Huang, W. Pu, and D. Wang, "A Lightweight Authentication with Dynamic Batch-Based Group Key Management Using LSTM in VANET," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/9779670.
[29] E. Dubrova, M. Näslund, G. Selander, and F. Lindqvist, "Message Authentication Based on Cryptographically Secure CRC without Polynomial Irreducibility Test," Cryptogr. Commun., vol. 10, no. 2, pp. 383–399, 2018, doi: 10.1007/s12095-017-0227-8.
[30] H. Krawczyk, "LFSR-based hashing and authentication," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1994, vol. 839 LNCS, pp. 129–139, doi: 10.1007/3-540-48658-5_15.
[31] [L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "Ad Hoc Networks A novel batch-based group key management protocol applied to the Internet of Things," AD HOC NETWORKS, 2013, doi: 10.1016/j.adhoc.2013.05.009.
[32] A. Mehdizadeh, F. Hashim, and M. Othman, "Lightweight decentralized multicast-unicast key management method in wireless IPv6 networks," J. Netw. Comput. Appl., vol. 42, pp. 59–69, 2014, doi: 10.1016/j.jnca.2014.03.013.
[33] Fabiana Meijon Fadul, "済無No Title No Title No Title," 2019.
[34] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," Wirel. Networks, vol. 21, no. 5, pp. 1733–1743, 2015, doi: 10.1007/s11276-014-0881-0.
[35] [P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy-preserving authentication and key distribution techniques for vehicular ad hoc networks," Cluster Comput., vol. 20, no. 3, pp. 2439–2450, 2017, doi: 10.1007/s10586-017-0848-x.
[36] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444–458, 2003, doi: 10.1109/TSE.2003.1199073.
[37] Y. Sun, M. Chen, A. Bacchus, and X. Lin, "Towards collusion-attack-resilient group key management using one-way function tree," Comput. Networks, vol. 104, pp. 16–26, 2016, doi: 10.1016/j.comnet.2016.04.014.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023

[38] C. S. Manigandaa,V. D. Ambeth Kumar,G. Ragunath,R. Venkatesan,N. Senthil Kumar. "De-Noising and Segmentation of Medical Images using Neutrophilic Sets." Fusion: Practice and Applications, Vol. 11, No. 2, 2023 ,PP. 111-123.

[39] S. Hemamalini ,V. D. Ambeth Kumar ,R. Venkatesan,S. Malathi. "Relevance Mapping based CNN model with OSR-FCA Technique for Multi-label DR Classification." Fusion: Practice and Applications, Vol. 11, No. 2, 2023 ,PP. 90-110.

Doi: https://doi.org/10.54216/FPA.120103
Received: May 06, 2023 Revised: June 10, 2023 Accepted: July 05, 2023