International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6956
***Article Received**: 28 March 2023 **Revised**: 16 May 2023 **Accepted**: 30 May 2023*

A Trust-Based Group Key Management Protocol for Non-Networks

Rituraj Jain[1], Dr. Manish Varshney[2]
[1]Department of Computer science
Maharishi University of Information Technology
Lucknow – UP India
jainrituraj@yahoo.com
[2]Department of Computer science
Maharishi University of Information Technology
Lucknow – UP India
itsmanishvarshney@gmail.com

Abstract— In this paper, a secure and trust-based group key management protocol (GKMP) is presented for non-networks such as MANET/VANET. The scheme provides secure communication for group members in a dynamic network environment and does not restrict the users (registered or non-registered), allowing for flexible group communication. The proposed scheme is designed to address the challenges of key distribution, secure grouping, and secure communication. For result evaluation, first of all formal and informal security analysis was done and then compared with existing protocols. The proposed trust-based GKMP protocol satisfies the authentication, confidentiality of messages, forward/backward security concurrently as well as shows robustness in terms of packet delivery ratio and throughput.

Keywords-Mobile ad-hoc networks, non-Network, Security, Privacy, Key Management.

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are formed by combining several wireless nodes responsible for transmission and processing, and data reception [1]. Such networks are used in many areas such as vehicle networking, military defence, and intelligent transportation in order to work effectively in harsh or moving environments [2]-[4]. Its unique architectural features deserve user attention as it raises some security and function issues. Attacks such as forging and tempering, eavesdropping, and impersonation on the wireless channel used for inter-node communication in MANETs are most probably serious security concerns [5]. Thus, secure communication in MANETs has become quite a challenging issue. To provide secure communication channels among wireless nodes the most common solution used by developers is to employ key management which encrypts messages in a proper way, thereby maintaining security [6]. Further, to make sure that all the received messages are unmodified, authentication mechanisms also need to be taken into consideration between wireless nodes. Moreover, the wireless nodes in MANETs are often self-organized in nature and carry out cooperative tasks in groups [7]. It has been seen that it leaves and joins the group dynamically. Group key agreement (GKA) and Group key distribution (GKD) based ones are the existing two categories of group key management for MANETs.

Li et al. [1] presented a blockchain-based mutual-healing group key distribution system. The Ground Control Station creates a private blockchain to store the group keys that GCS disseminated. This protocol also designed to recover lost group keys. Albakri et al.[2] proposed the first multivariate polynomial-based probabilistic kernel based GKPS. Our system's security is probabilistic k-secure, which indicates that after capturing the k+1 sensors, there is a chance that the security of our GKPS will also be compromised. Gomathi et al.[3] proposed an integrated method of hierarchically distributed group key management and fuzzy trust-based clustering. The FTBC uses fuzzy logic rules to separate out misbehaving nodes from genuine data transfer and classify trusted and untrusted nodes. There is no method that is used for all types of applications, so two more clustering schemes-simple clustering and enhanced distributed weighted clustering—are proposed in order to meet various needs. Robinson et al.[4] established the necessary level of security as well as superior output requirements, such as service accessibility and message overhead independent of communication with well-known certificate authorities. Since MTPKM does not support trusted third parties, it seeks for the neighbour node with the highest level of trust that satisfies the trust threshold requirement before certifying the key created. A mutual trust connection between the seeking node and the certificate issuer node is required. The performance of the suggested

DOI: https://doi.org/10.17762/ijritcc.v11i6s.6956
***Article Received**: 28 March 2023 **Revised**: 16 May 2023 **Accepted**: 30 May 2023*

trust-based approach is examined using simulation. Ermis et al. [5] proposed a secure cluster-head selection protocol that provides a dynamic situation. Nathani et al. [6] offer a dynamically authenticated group key agreement technique that is identity (ID) based. Our protocol provides forward and backward confidentiality in addition to meeting all the necessary security requirements. Our protocol's security is predicated on the bilinear Diffie-Hellman (DH) assumption. By utilising bilinear pairing, we expand Lee et alID-based's authenticated key agreement approach from a two-party to a group of users. Zhang et al. [7] proposed a broadcast encryption for providing secure key management algorithm for fog networks. In this algorithm, users encrypt the data using public key encryption technique. Liu et al. [8] presented a protocol integrated with batch authentication algorithm with secure session. The model also contains a trusted authority whose function is to provide authentication to anonymous nodes. Author created a certificate based secret group key to meet the aforementioned communication and security needs. Zhang et al. [9] presented a secure group key protocol using asymmetric algorithm which established a dynamic group key. In this algorithm each member has their own secret key which is based on identity-based cryptosystem. The designed system was more complex and need more resources to manage separate individual key as well as asymmetric group keys. Wu et al.[10] proposed a group key management protocol on broadcast encryption. In this algorithm, a common public key is generated and each member holds their secret keys. Chen et al.[11] presented a novel approach using Proof of Work (PoW) based authentication method to be implemented for fog network. Therefore, according to study presented, it was observed that the security of non-networks such as MANET or VANET are based on cryptographic keys. Therefore, it is needed to design a secure, robust, and scalable key management protocol. For this group key management protocols have achieved researcher’s attention. But the recent group key management protocols (GKMP) have some limitations such as high computational complexity and cost. The overhead increases with group updation. To overcome these limitations, this section introduces a novel group key management protocol for non-networks such as MANET or VANET. The protocol is designed in such a way that it reduces the limitations for key distribution among registered and non-registered nodes/users.

II. METHODOLOGY

Before describing the methodology, it is needed to understand the security requirements of secure communication over any network:

- Secure key management: The management of secure session keys after verification of users over insecure channel is one of the major concerns in any network.
- Confidentiality and data security: A secure model need to be designed for providing privacy to the sensitive data for communication.

A. *System Model*

Trust-based group key management protocol for non-networks (GKMP-NN) is described in this section that is composed of five phases: key generation, authentication, group creation, group key distribution, non-network member updation, and secure communication. The task of key generation and distribution are performed by the key generation server (KGS). Fig 1 presents the proposed system model for non-networks. In GKMP-NN the communications among nodes are conducted through an insecure communication. Some of the major issues for non-networks such as MANET or VANETs are authentication, session management, vulnerability to attacks, etc. To handle these issues, this section presents a secure group key management protocol for non-networks. The steps are described below in sub-sections.

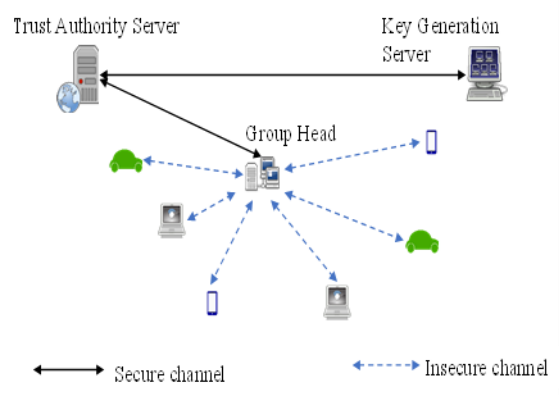


Figure 1. System Architecture

B. *Key Generation*

In this phase public, private, and secret keys are generated. These keys are generated by KGS and used for secure communication among devices in a group through insecure communication channels. In this network, there are two categories of nodes or users. The first categories are the nodes or users who are registered in the network and the second are those who are not registered to the network but are not malicious nodes. Therefore, for authenticated nodes, secret keys are used to communicate and for non-registered nodes, public and private keys are used to communicate. The key generation phase generates public Pub_{key} , Private Pri_{key} and secret key S_{key}. For this, they generate a large

***Article Received**: 28 March 2023 **Revised**: 16 May 2023 **Accepted**: 30 May 2023*

prime number i.e., q over which two random numbers are selected as x, y. These are used to generate public key as "Pub_{key} = (x, y)" and private key as "Pri_{key} = (x, −y)" such that "Pub_{key} + (Pri_{key}) = Θ". For secret key generation, two prime numbers are selected as 'j' and 'k' in which 'j' will be the highest prime number. Then evaluate $m = j \times k$. Generate a Random number "R" and generate $S_{key} = \{j, k, R\}$.

C. User Authentication and Group Creation

The steps for network initialization and user authentication are (as presented in Fig 2):

- User (U_A) registers itself to the server, *TAS*.
- If U_A are registered then, KGS send them S_{key} for further communication and G_{key}.
- If any non-regiatered user *(U_B)* wants to access network, then secure session is established with them using Pub_{key} and Pri_{key}.
- Meanwhile, network administrator (TAS) checks the arriving data from UB and send its authenticity report to KAS and then Pub_{key} and Pri_{key} are provided to them for further secure communication.

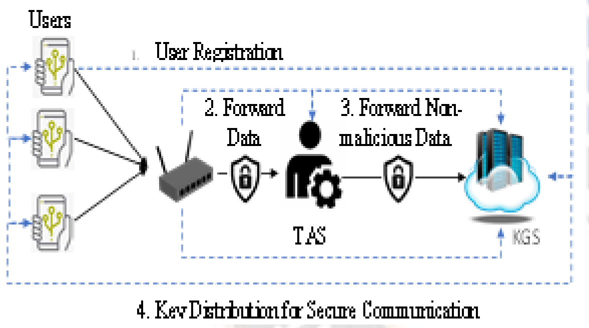

Users
1. User Registration
2. Forward Data
3. Forward Non-malicious Data
TAS
KGS
4. Key Distribution for Secure Communication

Figure 2. Non-Network Initialization and User Authentication

User (U_A) sends a registration request message, then KGS generates a security parameter for U_A by using its credentials such as "*identity*→ UI_{dA} and *identity* → P_A". These parameters are communicated to TA over insecure communication channel. Then TAS then generates a secret number, P_{uid} and perform xor operation with UI_d such that $H_{id} \rightarrow U_{id} \oplus P_{Uid}$. Then P_{uid} *and* H_{id} are transmitted to KGS. KGS then save both identities for further authentication. KGS, then generate a identity, $S_{cd} = \{H_{id}, S_{key}\}$, for U_A. While deploying above mentioned algorithm, there is need to design secure key management and data transmission protocol by using security algorithm with XOR operations that takes less computational resources.

As described in above step, authentication of nodes is done prior group formation. After getting registered user list, these users form a group with n users. Group head send their respective security parameters to TA in form of $G_1,...,G_n$ and $S_1,....S_n$. Then product of the collected parameters is calculated as:

$$G_x = \prod_{n=1}^{N} G_i \tag{1}$$

Then this G_x is used to evaluate the G_{key}, which is mathematically calculated as:

$$G_{key} = \sum_{n=1}^{N} S_n \ mod\ G_x \tag{2}$$

Here, size of the G_{key} is reduced by performing modulus operation over G_x. This will ultimately reduce the execution complexity.

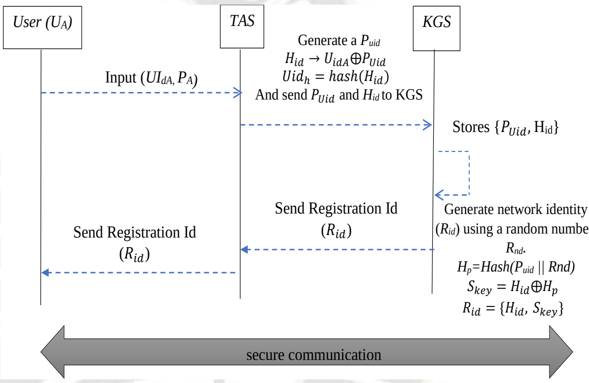

User (U_A)
TAS
KGS
Input (UI_{dA}, P_A)
Generate a P_{uid}
$H_{id} \rightarrow U_{idA} \oplus P_{Uid}$
$Uid_h = hash(H_{id})$
And send P_{Uid} and H_{id} to KGS
Stores {P_{Uid}, H_{id}}
Generate network identity (R_{id}) using a random number, R_{nd}.
H_p=Hash(P_{uid} || Rnd)
$S_{key} = H_{id} \oplus H_p$
$R_{id} = \{H_{id}, S_{key}\}$
Send Registration Id (R_{id})
Send Registration Id (R_{id})
secure communication

Figure 3. Authentication Protocol

D. Group Key Distribution

In this phase, the G_{key} is encrypted using respective group head's S_{key} and computed as:

$$G_{keyenc} = (G_{key} * S_{key})\ mod\ G_x \tag{3}$$

Further, each registered group head GH_A retrieve the respective G_{key} using its secret key S_{key} such as :

$$G_{key} = G_{keyenc}(mod\ m) \tag{4}$$

E. Non-Network Group Member Updation

In this phase, TA need to perform attention for group member updation for nodes joining some nodes/users, U_B which are previously not registered but are not-malicious. Such nodes are provided with Pub_{key} with non-network group key GN_{key}. This GN_{key} is common for all non-network nodes.

F. Secure Communication

Secure transmission consists of following steps:

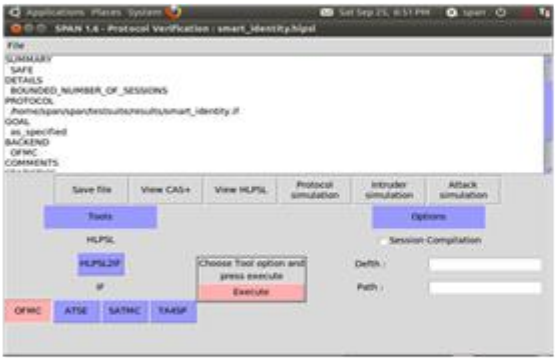
TA got data from U_A or U_B *in form of (U_{id}, Data)*. Then TA encrypt the data (*$Data_{enc}$=Enc(Data)*). The session hash "$R = session_{rnd} \oplus h(Pu_{id}||U_{id})$" is generated by XOR operation of a random number $session_{rnd}$. Then TA generates the *H_s=hash($Data_{enc}$)*. Then TA transmit $Data_{enc}$=M to KGS via insecure communication channel. On receiving message, M, from TA, KGS verifies the message. Then generate $session^*_{rnd} = \mathrm{R} \oplus \mathrm{h}(Pu_{id}||U_{id})$ and verifies $session^*_{rnd}$== evaluate $session_{rnd}$. If the session is verified then decryption process is performed over received encrypted message.

III. REUSLT AND DISCUSSION

In this section, results are discussed in briefly. The security analysis is presented by formal and informal security risk analysis. The further, this section presents the performance analysis in terms of computational complexity, packet delivery ratio, end-to-end delay and throughput. Then finally, the section presents the comparative result analysis for the designed model with state-of-art models for GKMP in non-networks such as MANET and VANETs.

A. Formal Security Analysis

If we have to perform formal security verification on the developed framework a widely-accepted AVISPA tool is used. This tool allows users to test security protocols with the help of just one button. It has been seen that if users have to safeguard against any sort of threats or attacks then this tool is quite helpful in determining a security protocol. For security mechanisms, high-Level Protocol Specification Language (HLPSL) is the language required for participation in AVISPA's evaluation. To translate HLPSL coding in the Intermediate Format HLPSL2IF is used which is a built-in interpreter. It determines whether an authentication process in security is safe or not; this model is commonly best suited for security validation. To verify the proposed protocol for application security, the below fig shows the simulation result of avispa tool. If AVISPA return it as safe that means protocol is resistant to attacks. As presented in fig 4, it is seen that the result summary is "SAFE" therefore, it can be concluded that this protocol can be implemented over non-network simulation models.



```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/smart_identity.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
```

Figure 4. Simulation Result for Authentication in OFMC Backend

B. Informal Security Analysis

The informal security analysis is presented in this sub-section, for designed non-network protocol based on the security features and parameters included. Some of the informal analysis is presented below:

Secret Shared Key Guessing: In proposed system, the security of U_A (registered users) is provided by symmetric algorithm and security of U_B (non-registered users) is provided by session based asymmetric algorithm. Therefore, the designed protocol for both type of users in non-network. For this security parameters such as $Pub_{key}, Pri_{key}, S_{key}$, related with session are used integrated with strength of Hash function. Therefore, this feature creates difficulties for attackers to accessing the database of KGS.

Integrity: Along with confidentiality and secrecy, integrity is also a major concern. Therefore, the protocol integrates the strength of one-way hashing algorithm which provides integrity to the entire system and prevents.

Man-In-The-Middle Attack (MIMA): As it is known that, in MIMA, communicating messages are theft by intermediate intruders whom modifies the sensitive data and send it back to receiver. If in any condition, intruder get succeeded to modify the data then its secure hash cannot be verified.

Collision Attack: Attackers A apply different ways to crack the security protocol. Therefore, the key size makes the security protocol more powerful as the designed algorithm used 256-bit key size which is quite sufficient for resistant to collision attack.

Scalability: The designed system is well organized to add any number of users at any time and are flexible.

Forward/Backward Secrecy: Forward secrecy is termed as potential of attacker to predict the the key pairs for next session whereas the backward secrecy is that attackers is able to fetch previous session keys. Therefore, the current security protocol should to such strong enough to present these secrecy breaches. Therefore, the designed protocols are based on number of parameters such as random number, unique user ID, group key, secure session keys. Therefore, this algorithm is quite enough to achieve Forward/Backward Secrecy.

According to above mentioned parameters, table 1 presents the comparative informal security analysis of proposed secure GKMP protocol with existing state-of-art models. Work done in [7] and [12-15] uses MANET as an NT and it has various disadvantages like lower PDR, non-scalable, has memory constraint as well. From [17-19] uses VANET as an NT it also faces drawbacks like increased computational complexity, prone to attacks, regular group updation. In our proposed work the model is designed for VANET or MANET with GB, SSK, AU, IS_1 IS_2 and IS_3 security features as compared with existing state-of-art models.

TABLE I. COMPARATIVE SECURITY INFORMAL FEATURES ANALYSIS

Ref	**Year**	**NT**	**GB**	**SSK**	**AU**	**IS_1**	**IS_2**	**IS_3**	**NAU**
[7]	2019	Fog	x	x	Sy	x	√	√	x
[12]	2021	MANET	√	x	-	√	x	x	x
[13]	2021	MANET	√	x	-	√	x	x	x
[14]	2019	MANET	X	x	-	√	√	x	x
[15]	2019	MANET	√	x	-	√	√	x	x
[16]	2022	MANET	√	x	Sy	√	√	√	x
[17]	2021	VANET	√	x	As	√	√	√	x
[18]	2020	VANET	√	x	Sy	√	√	x	x
[19]	2022	VANET	√	x	-	√	√	√	x
Ours		MANET/VANET	√	√	Sy/As	√	√	√	√

NT= Network Type, GB= Group Based Protocol, SSK=Secure Session Key, AU=Algorithm Used (Sy=Symmetric and As=Asymmetric), IS_1 = Authentication, IS_2 = Confidentiality, IS_3 = Forward/Backward Secrecy, NAU= Access to non-registered authenticate users.

C. *Performance Analysis*

The protocol presented above is implemented and simulated on MATLAB platform for dynamic and mobile non-networks. In The performance is evaluated in terms of computational complexity, packet delivery ratio, end-to-end delay and throughput. Simulation parameters are presented in table 2.

TABLE II. SIMULATION SCENARIO

Simulation Scenario	**Values**
Area	400m*200m
WSN sensor nodes	Variable
The initial energy of each node in the network	0.5
Transmitting bit energy requirement	0.01J/bits
Receiving bit energy requirement	0.01J/bits/m^2
Energy required for amplification	0.01J/bits/ m^4
Packet size	4000

Below in fig 5, packet delivery ratio of the proposed secure trust aware group key management protocol (STAGKMP) for non-networks are presented with respect to number of varying nodes. The PDR rises more than 0.9 with increased nodes. The graph of end-to-end delay with respect to nodes are presented in fig 6. The delay is evaluated in seconds. With increased number of nodes there is increase in end-to-end delay. Apart from this, another important parameter for result evaluation of the protocol is throughput. The throughput is measured in bits per second delivered. The proposed protocol has achieved approx. 50 bps as throughput.

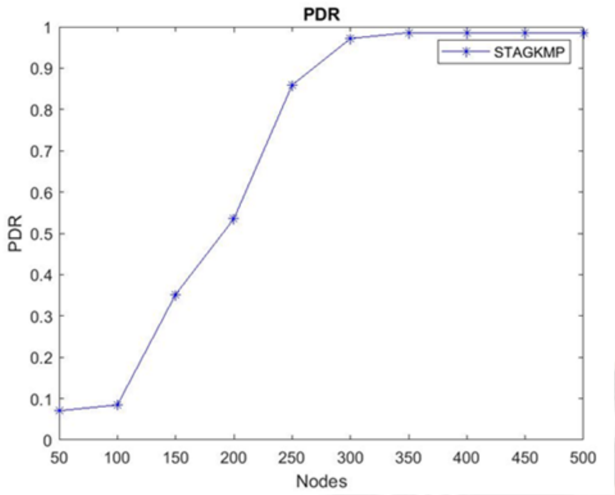


Figure 5. Packet Delivery Ration

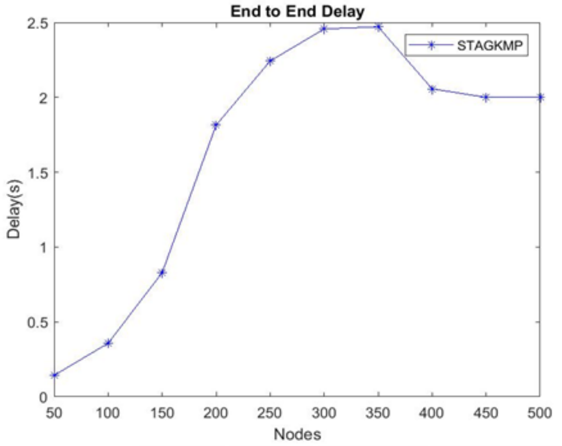


Figure 6. Packet Delivery Ration

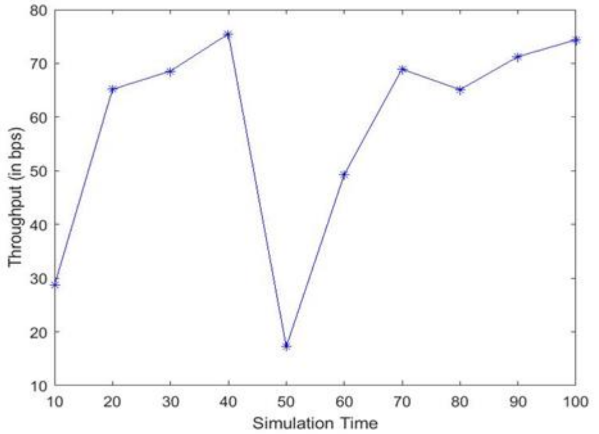


Figure 7. Throughput Assessment

Table 3 shows the comparative state of arts of different protocols discussed in different papers and our proposed work and considering throughput and packet delivery ratio as a performance parameter. For Prasad and Shankar [14] throughput is 0.70 and packet delivery ratio is 74%. For Veeraiah et al. [13] throughput is 0.76 and delivery ratio is 84%. For Srilakahmi et al. [12] throughput is 0.80 packet delivery ratio is 89% and our proposed work has throughput 0.90 and packet delivery ratio is 95% which is almost 20% more than the work proposed in [14].

TABLE III. COMPARATIVE STATE-OF-ART

Protocols	Throughput	Packet Delivery Ratio
Prasad and Shankar [14]	0.70	74%
Veeraiah et al. [13]	0.76	84%
Srilakshmi et al. [12]	0.80	89%
Ours	0.90	95%

IV. CONCLUSION

In this paper, the proposed secure and trust-based group key management protocol is designed for non-networks such as MANET or VANET. The paper presents valuable contribution to the field of secure communication in dynamic network environments with registered and non-registered users. The scheme effectively addresses the challenges of key distribution, group trust, and secure communication, providing enhanced security and flexibility compared to existing state-of-art protocols. The results of simulations and comparisons with previous methods shows the robustness and efficiency of the designed protocol in providing secure communication for group members. In future research the work has potential to improve the energy-efficiency of communication model under non-networks.

REFERENCES

[1] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar and J. Ma, "Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network," in IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 11309-11322, Nov. 2019, doi: 10.1109/TVT.2019.2943118

[2] A. Albakri and L. Harn, “Non-Interactive Group Key Pre-Distribution Scheme (GKPS) for End-to-End Routing in Wireless Sensor Networks,” IEEE Access, vol. 7, pp. 31615–31623, 2019, doi: 10.1109/ACCESS.2019.2900390.

[3] Gomathi, K., Parvathavarthini, B. & Saravanakumar, C. An Efficient Secure Group Communication in MANET Using Fuzzy Trust Based Clustering and Hierarchical Distributed Group Key Management. Wireless Personal Communications 94, 2149–2162 (2017). https://doi.org/10.1007/s11277-016-3366-x

[4] Y. Harold Robinson and E. Golden Julie, “MTPKM: Multipart Trust Based Public Key Management Technique to Reduce Security Vulnerability in Mobile Ad-Hoc Networks,” Wireless Personal Communications, vol. 109,

***Article Received**: 28 March 2023 **Revised**: 16 May 2023 **Accepted**: 30 May 2023*

no. 2, pp. 739–760, 2019, doi: 10.1007/s11277-019-06588-4.

[5] O. Ermiş, Ş. Bahtiyar, E. Anarım, and M. U. Çağlayan, "A secure and efficient group key agreement approach for mobile ad hoc networks," Ad Hoc Networks, vol. 67, pp. 24–39, 2017, doi: https://doi.org/10.1016/j.adhoc.2017.10.003.

[6] S. Nathani, B. P. Tripathi, and S. Khatoon, "A Dynamic ID Based Authenticated Group Key Agreement Protocol from Pairing," International Journal of Network Security, Vol.21, No.4, PP.582-591, July 2019, doi: 10.6633/IJNS.201907.

[7] Widodo, D. A. ., Iksan, N. ., & Sunarko, B. . (2023). Sentiment Analysis of Twitter Media for Public Reaction Identification on COVID-19 Monitoring System using Hybrid Feature Extraction Method. International Journal of Intelligent Systems and Applications in Engineering, 11(1), 92–99. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2447.

[8] L. Zhang, "Key Management Scheme for Secure Channel Establishment in Fog Computing," in IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1117-1128, 1 July-Sept. 2021, doi: 10.1109/TCC.2019.2903254.

[9] L. Liu, Y. Wang, J. Zhang, and Q. Yang, "A secure and efficient group key agreement scheme for VANET," Sensors (Switzerland), vol. 19, no. 3, pp. 1–14, 2019, doi: 10.3390/s19030482.

[10] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin and Z. Dong, "Round-Efficient and Sender-Unrestricted Dynamic Group Key Agreement Protocol for Secure Group Communications," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2352-2364, Nov. 2015, doi: 10.1109/TIFS.2015.2447933.

[11] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs and J. A. Manjón, "Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts," in IEEE Transactions on Computers, vol. 65, no. 2, pp. 466-479, 1 Feb. 2016, doi: 10.1109/TC.2015.2419662.

[12] T. Chen, L. Zhang, K. -K. R. Choo, R. Zhang and X. Meng, "Blockchain-Based Key Management Scheme in Fog-Enabled IoT Systems," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10766-10778, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050562.

[13] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf and B. V. Subbayamma, "An Improved Hybrid Secure Multipath Routing Protocol for MANET," in IEEE Access, vol. 9, pp. 163043-163053, 2021, doi: 10.1109/ACCESS.2021.3133882.

[14] N. Veeraiah, O. I. Khalaf, C. V. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, ''Trust aware secure energy efficient hybrid protocol for MANET,'' IEEE Access, vol. 9, pp. 120996–121005, 2021, doi: 10.1109/ACCESS.2021.3108807.

[15] Prasad P, R, Shankar, S. Efficient Performance Analysis of Energy Aware on Demand Routing Protocol in Mobile Ad-Hoc Network. Engineering Reports. 2020; 2:e12116. https://doi.org/10.1002/eng2.12116

[16] G. Krishnasamy, "An Energy Aware Fuzzy Trust based Clustering with group key Management in MANET Multicasting," 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS), Amman, Jordan, 2019, pp. 1-5, doi: 10.1109/ICTCS.2019.8923088.

[17] W. Han, R. Zhang, L. Zhang and L. Wang, "A Secure and Receiver-Unrestricted Group Key Management Scheme for Mobile Ad-hoc Networks," 2022 IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 2022, pp. 986-991, doi: 10.1109/WCNC51071.2022.9771870.

[18] A. Mansour, K. M. Malik, A. Alkaff and H. Kanaan, "ALMS: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1663-1678, March 2021, doi: 10.1109/TITS.2020.2975226.

[19] G. Xu et al., "BAGKD: A Batch Authentication and Group Key Distribution Protocol for VANETs," in IEEE Communications Magazine, vol. 58, no. 7, pp. 35-41, July 2020, doi: 10.1109/MCOM.001.2000118.

[20] Zhao, C., Guo, N., Gao, T. (2022). Efficient Privacy-Preserving Authentication and Group Key Agreement Scheme in Fog-Enabled VANET. In: Barolli, L. (eds) Innovative Mobile and Internet Services in Ubiquitous Computing. IMIS 2022. Lecture Notes in Networks and Systems, vol 496. Springer, Cham. https://doi.org/10.1007/978-3-031-08819-3_16