Journal of Applied Engineering and Technological Science
Vol 4(2) 2023: 783-794

A CRITICAL STUDY ON GROUP KEY MANAGEMENT PROTOCOLS AND SECURITY ASPECTS FOR NON-NETWORKS

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

Received : 09 April 2023, Revised: 10 May 2023, Accepted : 11 May 2023
Corresponding Author

ABSTRACT
The rise in internet usage and advanced communication systems has led to an increase in security issues. The need for more robust and flexible secure communication has led to the introduction of mobile non-network multicast communication systems like MANET or VANET. Multicasting is increasingly being used for group-oriented applications such as video conferencing, interactive games, TV over Internet, e-learning, etc. To address the security concerns, this paper highlighted the confidentiality, authentication, and access control for non-network multicast communication systems like MANET or VANET. For this, paper explores the group key management protocols. The paper concluded that centralized and asymmetric group key management protocol (GKMP) is most effective for designing secure, and efficient communication models for non-networks. The key findings of the paper are that in group key management protocols (GKMPs) for multicast communication systems adoption of asymmetric GKMPs provides better security, and reduces computational overhead. Therefore, this paper help to improve the robustness and security of multicast communication systems and meet the growing demands of group-oriented applications over the internet.
Keywords: *Non-Network, Security Issues, Privacy, Cryptography, Group-Key Management*

1. Introduction

Multicast technology has the important capability that allows for the effective execution of group interaction, in which a particular transmitter sends a text to multiple recipients at the same moment (Hinden and Deering, 2006). One of the most important cryptographical service is “group key management protocol (GKMP)” (Hillebrand, 2002). Furthermore, it is vital that mechanisms for managing cryptographic keys be safe and satisfy the security needs of specific apps. It is also necessary to defend multicast group apps from security issues like observing critical conversations, introducing misleading informational traffic, altering key characteristics, or impersonating multicast members of the groups. As per the "Internet Engineering Task Force," (IETF), the fundamental challenge in the communication process is managing cryptographic key groups. Mobile Ad hoc Networks (MANETs) are self-contained networks built with wireless mobile nodes that do not require any infrastructure. Nodes in a MANET may easily and continuously interact with one another using frequency spectrum (Othman and Mokdad, 2010; Kumar et al., 2020; El-Hadidi and Azer, 2021). When persistent infrastructures are not available, Mobile Ad Hoc Networks (MANETs) enable portable consumers to interact with each other. However, noise exposure, transmitting intervention, and movement commonly prevent MANET connections from functioning properly(Wu and Liaw, 2015). Despite these challenges, the increased use of the internet has significantly increased the use of MANETs in various vital operations (Devi and Hegde, 2018; Gomathy et al., 2020). Communication is performed through numerous hops due to the restricted communication range, making effective navigation crucial to determine the best route between the origin and destination(Kousar et al. 2020).

The aim of this paper is to explore the importance of Group Key Management Protocol (GKMP) for managing cryptographic keys, the need to protect multicast group applications from security issues, the challenge of managing cryptographic key groups in multicast technology, the challenges faced by Mobile Ad Hoc Networks (MANETs), and the crucial need for effective navigation to determine the best route in MANET communication.

To fulfill these objectives, the paper presented a critical analysis on GKMP for non-network. The paper first of all explored usage of non-networks and then security issues in such network. Then paper presented a bibliometric analysis for GKMP protocols used in existing non-networks such as MANET and VANET and also highlighted the key features of each protocol. Then paper summarize with some future research directions for researchers.

2. Literature Review

Because researchers presume that group key management should function over several connectivity, especially in multicast networking, they should presume that group key management should include substantially a few of the attributes of Internet key management. These features are summed up in the following points:

- Defense for man-in-the-middle threats, network attempting to hijack, replay/reflection, and denial-of-service attacks.
- Important formation with a chosen degree of security preservation, including such alternate transformations, additional PFS, and identification safeguard, to accommodate heterogeneous web apps and PCs.
- Additional verification methods, such as sharing keys, PKI, and public keys, accommodate various security frameworks.
- A route for additional security methods, including additional cryptographic transformations and perhaps a novel exchange of information, to migrate ahead.
- A unified key management architecture to facilitate the formation of secure connections by the regional regulations of internet hosts and intermediary services.

Non-Networks are the networks in which devices are not part of that network. In recent communication models, wireless networks are a collection of non-registered nodes or devices (Zheng X. et al., 2007; Lim, K. et al., 2017). Such networks are termed non-networks. For multicast communication over non-networks such are MANET or VANET is unreliable (Bhoi et al., 2018). Therefore, these non-reliable must meet security aspects such as confidentiality, integrity, privacy, etc. Therefore, it is quite a challenging task for such communication over non-networks. Before discussing the security concerns and respective solutions, first of all, it is needed to discuss non-network architecture and its characteristics (Vijayakumar, P. et al., 2016; Zhou, J. and Ou, Y. H., 2009; Vijayakumar, P. et al., 2013; Islam S. H. et al.,2018). Some of the characteristics of non-networks such are MANET or VANET are presented in Fig 1.

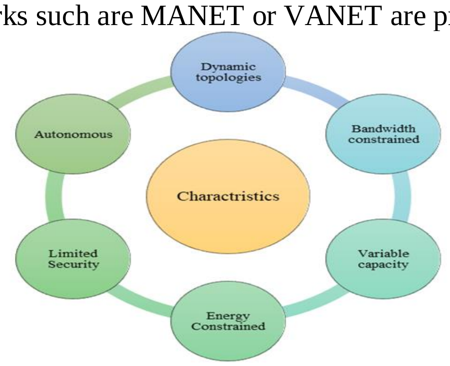

Fig. 1. Characteristics of non-Networks

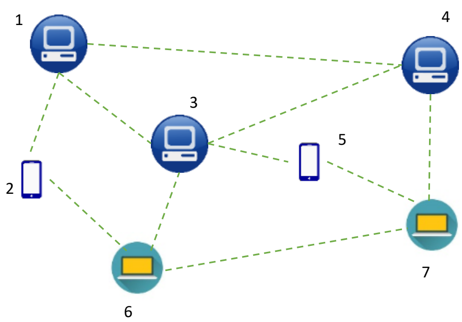

Fig. 2. Data Communication among Non-Networks

Non-Network means any node or device that is not part of the network “MANET”, as presented in fig 2. In above fig 2, node 6 and node 7 are non-registered nodes of the given network whereas node 1, node 2, node 3, node 4, and node 5 are registered or authorized users. In such networks, there is a requirement for security protocols that establishes a connection between these authorized and non-authorized nodes. In most, non-Network security, architecture is centralized. As central server maintains and updates the list of non-network nodes and network nodes time-to-time.

Security Risks in Non-Networks

There are major security concerns in the communication process, like unicast. Reliability, authenticity, availability, and privacy were all major considerations for group communication security services suppliers (Bilal, M. and Kang, S. G., 2017; Azees M. and Vijayakumar P, 2017; Saravanan, K. and Purusothaman, T., 2012; Kumar Vinod et al., 2016). The unicast opponent will bear both active and passive threats when attacking a multicast broadcast.

- Monitoring of private conversations
- Transmission of the information is being impeded
- the group communication is disturbing
- Adding fictional congestion
- Pretending to attend a group

In non-network like VANET and MANET, there are a collection of different properties that gives the foundation to exist independently in the domain of its category. However, occasionally these qualities make it difficult to implement non-network (Kumar V et al., 2020; Mejri M. N. et al., 2016; Lv Xixiang et al., 2012; Mansour A. et al., 2021; Oubbati, O. S. et al., 2019). Those difficulties are divided into two categories: technical difficulties (including managing network dynamicity, administration of delay, assessment of congestion and collisions, atmospheric effect, and security difficulties) and societal and economical difficulties (Ding, Y. et al., 2007; Hartenstein, H. and Laberteaux, L. P, 2008). Non-network offers security and traffic assessment methods, therefore the data exchanged should be secured and the network requires to be strong. To create a safe and effective VANET system, they have taken into account the security concerns. Significant security obstacles that non-networks like MANET and VANET must overcome are listed in (Sepulcre et al., 2019; Zhang Y, 2009):

Uniformity of information: Every harmful modification of data that is essential to human survival can result in catastrophes. As a result, some system is required to prevent harmful behavior by authorized and unauthenticated nodes that would otherwise result in inconsistent information. Cross-verification of acquired data from several nodes is carried out to prevent such behaviors.

Great Mobility: Even while VANET networks have a high computational and storage capacity, their high-speed means that they require less complicated security algorithms.

Error Tolerance: Because VANET reception and response actions happen so quickly, any error in the algorithms or procedures might severely damage the system. Therefore, this problem needs to be taken into account when designing procedures.

Delay Regulation: In the communication systems, data are time-dependent and to accomplish these constraints, security protocols or algorithms should satisfy these.

Key Administration: All security algorithms in non-network are key-dependent which need proper management or updations.

No predefined boundary: In mobile as ad hoc networks, one cannot identify and define the network's physical demarcation line. The nodes operate in nomadic surroundings, allowing them to enter and leave the wireless connection. When an opponent enters a node's radio frequency band, it will be capable of communicating with that node. Eavesdropping and a Denial of Service (DoS) invasion are among the threats (Wei et al., 2014).

Network Adversary: Mobile nodes within the MANET can readily access and depart the network. Harmful behavior might also occur among nodes in the network. It is difficult to determine whether the node's activity is harmful or not (Wei et al., 2014).

No centralized control facility: MANETs lack a centralized management infrastructure, which can result in numerous security issues. Any attack gets extremely challenging to identify. The command is spread at every node and cannot be inspected from a centrally controlled place. When

the advice modifies the attacking style and the objective of the invasion, identification becomes much more challenging. A disruption to the node could be triggered by an attacker or a network fault. Researchers cannot categorize the nodes as trusted or untrustworthy because of the absence of a security connection (Wei et al., 2014).
Energy Constraints: In any WSNs, all devices or nodes are with limited battery or power to participate in communication. The intruder can send massive amounts of traffic to the targeting node which results in wastage of energy. This will result in a "denial of service". Sometime, these intruders instruct the nodes to perform useless time-consuming processing that results in energy depletion (Wei et al., 2014).
Scalability: As in non-network such as MANET or VANET, there is no pre-determined scalability. It is quite un-predictable.

Noteworthy Contributions

Several trust-based networking techniques were proposed and examined when creating a MANET. The majority of reliable management strategy was designed for cooperative navigation to identify self-destructive nodes generated by faulty nodes. Several anticipated route algorithms were also created and utilized to objectively detect different forms of security attacks. Several academics explored topics about major challenges linked with IoT-based MANETs. Several security and susceptibility threats were addressed throughout protocol architecture (Maheswari M. et al. 2021; Funderburg, L. E. and Lee, I. Y., 2021).

Routing tables must be updated regularly in preemptive routing protocols like the Destination Sequence Distance Vector (DSDV) (Perkins, C. E., & Bhagwat, P., 1994). As a result, a large amount of control signals is created. As a result, several procedures were discovered to be inappropriate for MANETs. Ad hoc on-demand distance vector routing (AODV) (Royer et al., 2003) and dynamic source routing (DSR) (Abdollahi et al., 2021) were developed as a result. Several cryptography-based procedures have been developed to safeguard connectivity amongst MANET nodes. "Effective Node Admittance and Certificateless Safe Information exchange (Saxena N. et al., 2008), Unverified Location-Aided Routing (Eldefrawy, Karim and Tsudik, Gene, 2011), Energy-Efficient Partial Permutation Encryption (Khan A. et al., 2017), Friend-Based Ad hoc Routing to Establish Security (Dhurandher S.K. et al., 2018), Unverified Multipath Routing Protocol (Chen, S., & Wu, M., 2011), Statistical Traffic Pattern-Discovery System (Qin Y. et al., 2014), and Non-Interactive Self-Certification (Saxena N. and Yi J.H., 2009)" are several well-known procedures. Such procedures, nevertheless, are vulnerable to a variety of security concerns and necessitate additional power from the nodes (Hammamouche et al., 2018; Subramaniyan et al., 2014).

Several safe and energy-aware transmitter networking strategies, like "Trust Aware Secure Energy Efficient Hybrid Procedure (Veeraiah N. et al., 2021), Hybrid Secure Multipath Navigation Procedure (Srilakshmi U. et al., 2021), Sign Encryption Technology (ST) (Veeraiah N. et al., 2021), and Recurring Reward-Based Training (Srilakshmi U. et al., 2021)", have lately been developed for MANETs. These methods have demonstrated outstanding functionality against a variety of security challenges. Even though these procedures use lesser power than traditional procedures, there remains an opportunity for improvement.
Therefore, the research gaps are:

- Security concerns in unicast communication, where the opponent can bear both active and passive threats when attacking a multicast broadcast.
- Technical difficulties in implementing non-networks like VANET and MANET, including managing network dynamicity, administration of delay, assessment of congestion and collisions, and security difficulties.
- Societal and economic difficulties in implementing non-networks, such as the uniformity of information, great mobility, error tolerance, delay regulation, key administration, no predefined boundary, network adversary, no centralized control facility, energy constraints, and scalability

3. Research Methods

To ensure security in multicast situations, it is important to have entity authenticity, information security, and confidentiality. Specific requirements for secure group connectivity include having a server with security policies, verifying the credentials of group participants and admins, and updating group keys in dynamic strategies when there are changes in the network. The paper is dedicated to present the systematic review on GKMP protocols for non-networks. For this bibliometric analysis is performed using steps presented in fig 3. But before designing the architecture of paper it is required to highlight some research questions that are intended.

RQ. 1 What are the security concerns associated with mobile non-network multicast communication systems such as MANET or VANET?

RQ. 2 What is the confidentiality, authentication, and access control requirements for securing non-network multicast communication systems?

RQ. 3 What are the existing group key management protocols for non-network multicast communication systems, and how do they address security concerns?

RQ. 4 How can the adoption of asymmetric GKMPs improve the security and computational efficiency of non-network multicast communication systems?

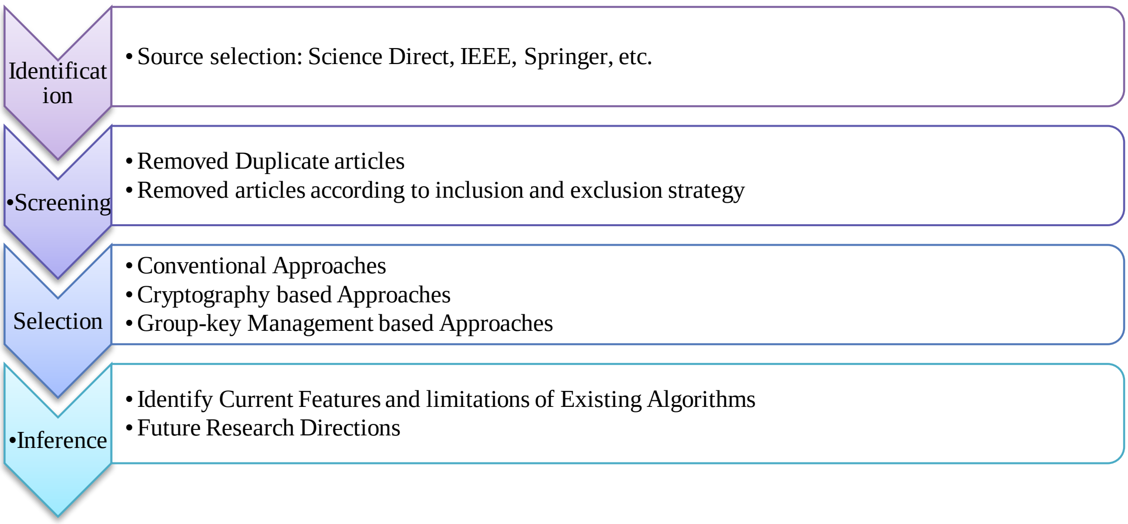

Fig. 3. Flowchart of Working

To address these research questions, the paper describes the steps taken to conduct a systematic review of research articles related to security of non-networks. The eligibility criteria for articles were based on study methodology, timeline, and language. A search string was developed using Boolean operators, and multiple articles were identified from multiple databases. After screening for inclusion and exclusion criteria, some articles were removed, resulting in a final selection of relevant articles. The selected articles were categorized based on the type as: Conventional approach, cryptography-based approach and group key management based approaches, which are further presented in sub-sections.

This section discusses security techniques to combat the attacks mentioned in earlier sections. The first technique is a decentralized and collaborative system proposed by Zhang and Lee (2000) for intrusion detection in MANETs. Each node in the network identifies signs of intrusion autonomously and shares the information with other nodes. Another technique discussed is the use of packet leashes to defend against wormhole attacks, as described by Luo et al. (2019). These leashes restrict the maximum range and time a packet can travel, allowing the recipient to check if it has moved beyond the allowed range. Therefore according to type of protocol used further sub-sections are divided as:

Conventional Approaches for Protection in Non-Network

ARAN: This navigation protocol, Authenticated Routing for Ad-hoc Network (ARAN), is built on AODV (Fatemidokht et al., 2021). A third-party CA is used in this strategy to give verified certificates to nodes. Every node that joins the network must send certification requests to the CA. All authorized nodes have access to the CA's public key. For verified safe path identification, an asymmetric cryptographic approach is utilized, and timestamps are employed to determine path authenticity.

SEAD: Safe and effective Ad hoc Distance (SEAD) vector technique operates on top of DSDV. For verification, it employs a one-way hash function. This approach guards against erroneous navigation. It employs a destination-sequence code to assure the path's authenticity and to prevent long-lived routes. To validate the legitimacy of paths, scrambling is used at every intermediary node.

Ariadne protocol operates on the DSR on-demand networking method (Choi and Lee, 2019). In this approach, symmetric cryptographic procedures are exceedingly effective. This approach is built on the TESLA broadcasting authenticating technologies. TESLA time intervals are employed in the path-finding and authenticating processes.

SAODV: This approach was introduced to incorporate security features into the AODV protocols (Abusalah et al., 2008). To ensure legitimacy and to safeguard hop count hash operations, all routing instructions are securely verified. Regardless of whether the intermediary node knows the new path, it cannot send a route response in this method. This issue could be overcome with Double Signature, however, it raises the system's sophistication.

One-Time Cookie: Cookies are typically allocated each session for session administration. However, to protect the system against session intrusion and SID theft, this approach introduces the idea of "one-time cookie (OTC)" (Dacosta, I. et al., 2012).

ECDSA: Elliptical Curve Digital Signature Algorithm (Cui et al., 2018), which uses digital signatures as the name implies. This system provides authentication and protection through the use of a hash function and asymmetrical cryptographic procedures. The elliptical curve domain characteristics must be agreed upon by both the transmitter and the recipient.

RobSAD: Robust approach for Sybil Threat Identification, the key idea underlying this technique is that two separate automobiles cannot share similar motion patterns when influenced by various drivers, because every individual drive as per their convenience and requirement.

Holistic Protocol: This protocol outlines the authenticating process used by RSU for the registration of vehicles. During the registration stage, the car sends a Hello message to the RSU, and the RSU responds by generating a Registration id (containing the license number and the vehicle registration number) and sending it to the automobile. Furthermore, RSU's certificate is used for verification. Only information is exchanged with the node if it is authorized; else, the node is blocked.

Cryptography for Protection in Non-Network

Cryptography is one of the mathematical model to secure the communication in which readable data are converted into unreadable format. As a result, it is impossible to construct a novel layout depending on composite cryptographic approaches without a strong security assessment, which is based primarily on cryptographic reasoning. One approach to achieving this objective is to study and comprehend from other people by assessing existing MANET/WSN security strategies, as well as to fully comprehend the network to better comprehend how cryptographic technologies merge with MANETs/WSNs to focus on providing a security provider with satisfactory network connectivity, expandability, retrieval, and synchronization.

Multiple methodologies can be used to assess the security architecture. The purpose is to present insight into the use of cryptographic methods and to investigate basic cryptographic approaches as they apply to authenticity, integrity, and key management in MANETs/WSNs. Similarly, in the security and functionality of MANETs/WSNs, cryptography algorithms could be efficiently applied in various phases of network bootstrapping, packet transmission, and variables to be assessed (Zhao et al., 2011). After the examination, these strategies can undoubtedly be repurposed as known cryptographic approaches. One strategy they use here is to disintegrate the layout utilizing cryptographic methods and reprogram it, then examine how the new layout is constructed using alternative cryptographic methods.

Group-Key Management for Non-Network

There are three types of group key management policies and procedures: centralized, decentralized, and distributed (El-Bashary, M. et al., 2015). A group key server (KS) is accountable for group key dispersion and upgrading in centralized group key administration procedures. The organization is separated into subgroups in decentralized group key management approaches. There is a group key that is used by all members of the group, and each subgroup has a shared key. There is a group key (GK) server for the group and a subgroup key (SGK) server for every subgroup in this situation. In distributed group key administration methods, also known as the key agreement, all group members work together to develop and share the transportation encryption key for safe interactions (He et al., 2009). Although the centrally controlled group key administration techniques are simpler to set up for non-networks. A bottleneck and a single point of breakdown are thought to exist in the KS. The procedure of upgrading keys requires lesser bandwidth when using decentralized group key administration methods. Although decentralized group key administration methods are convoluted and less flexible, they might be the best course of action for MANET because they do away with bottleneck and single point of failure issues in addition to the "1 impacts n" phenomenon. An energy-efficient routing protocol using group key management and asymmetric key cryptography was proposed by Bondada et al. (2022). Performance analyses showed that the proposed protocol outperforms competitive protocols in terms of EED, PDR, throughput, and energy consumption by up to 3.6872%. Yadava et al. (2021) presented a new group key management protocol called ALMS, which has been implemented and tested against existing protocols.

The results show that ALMS is more scalable than other protocols, with low computational overhead for both the TA and receiving vehicles, and does not suffer from key distribution limitations. ALMS outperforms CGKD and CGKMS with 99% and 98% lower average computational cost and is 24 and 51 times faster than VGKM with 128-bit key size for group key computation when group size is 20, and the number of registered vehicles equals 200 and 500, respectively. ALMS with double key size performs 496K and 132K times faster than CGKD and CGKMS, respectively. Mansour et al. (2021) proposed an efficient centralized group key distribution (CGKD) protocol that minimizes the computation cost of the key server (KS) during key updating. The proposed scheme is implemented in JAVA and tested on a computer with an Intel Core i5 processor, 4 GB RAM, and 1000 GB HDD running Windows-8 OS. The proposed protocol outperforms existing similar protocols by significantly reducing the computation and storage complexity of the KS while maintaining less and balanced communication overhead of the KS and storage load of each group member. The protocol is also extended based on a clustered tree that is very scalable and efficient to handle enormous membership changes

4. Results and Discussions

Group key management protocols (GKMP) are based on multicast cryptography to establish secure channels among nodes in highly dynamic networks, such as MANET or VANETs. In this paper, GKMP is categorized and reviewed into two types: one is symmetric GKMP and asymmetric GKMP. Symmetric GKMP is the protocol that use the secret key for both transmission and retrieval. Whereas in Asymmetric GKMPs, a pair of keys are used i.e., public and private keys. There are significant research contributions for designing symmetric as well as asymmetric GKMPs. Some of them are contributed in below table 1. The table summarizes various key management protocols and their characteristics such as GKMP type, network type, pre-key distribution, communication overhead, forward secrecy, backward secrecy, and collusion attack. The protocols are divided into symmetric and asymmetric types, and centralized and distributed network types. The table also indicates if the protocols provide forward and backward secrecy and protection against collusion attacks. Pre-key distribution is used in all protocols listed, and some protocols have low overhead, while others have high overhead. According to study presented in the table some current research gaps are presented in fig 3.

Table 1 - Research Contributions with their key features for GKMP

Ref	T	NT	PKD	CO	FS	BS	CA
Zheng X. et al. (2007)	S	C	√	Low	√	√	√
Zhou, J. and Ou, Y. H. (2009)	S	C	√	High	√	√	√
Saravanan, K. and Purusothaman, T. (2012)	A	C	√	High	√	√	√
Lv, X. et al. (2012)	A	D	×	Low	√	√	√
Vijayakumar, P et al. (2013)	S	C	√	Low	√	√	√
Vijayakumar, P. et al (2016)	S	C	√	High	√	√	√
Azees, M. and Vijayakumar, P. (2016)	A	C	√	High	×	×	×
Kumar, Vinod et al (2016)	A	C	×	High	√	√	√
Mejri M. N. et al. (2016)	A	D	√	High	×	×	×
Lim, K.et al. (2017)	S	C	√	High	×	×	×
Bilal, M. and Kang, S. G. (2017)	S	D	√	Low	√	√	√
Islam, S. H. et al. (2018)	S	C	√	Low	√	√	√
Kumar, V. et al (2020)	A	C	√	High	√	√	√
Mansour A. et al. (2021)	A	C	×	Low	√	√	√
Yadava et al. (2021)	A	D	×	Low	×	×	×
Bondada et al. (2022)	A	D	√	Low	×	×	×
Zhang et al. (2023)	A	D	√	High	√	√	×

T= GKMP Type (S= Symmetric, A=Asymmetric), NT = Network Type (C= Centralized, D=Distributed), PKD= Pre-key distribution, CO=Communication Overhead, FS=Forward Secrecy, BS=Backward Secrecy, CA= Collusion Attack.

From table 1, the following points are concluded:

- Most of the algorithms are centralized and require pre-key distribution.
- Asymmetric GKMPs are better to adopt as they are more secure.
- Computational overhead needs to be reduced.
- More attack needs to be explored.

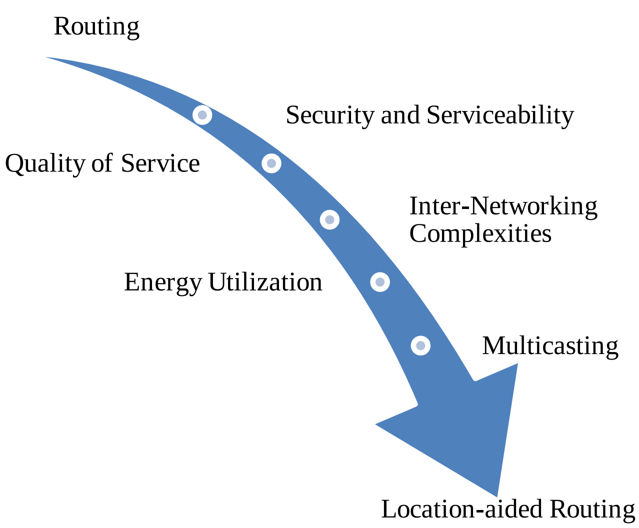

Fig. 4. Current Challenges and Future Scope

5. Conclusion

In this article, we propose a group key management strategy for protected group connectivity in non-networks, like as MANETs and VANET, that guarantees verification, text integrity, known-key security, forward and backward secretiveness, as well as the fully functioning properties of no trustable vendor, receiver non-restriction, and certificate modifiability and dynamic nature. To demonstrate the effectiveness of security algorithms in non-networks, the paper has presented a meta-analysis on group key management protocols for non-networks such as MANET or VANETs. The paper also presented the recent contributions and research works with their key features that will direct future researchers to design safe, secure, and efficient communication models for non-networks. Based on result analysis presented, it was concluded that existing GKMPs rely heavily on pre-key distribution, which can be exploited by attackers. Asymmetric GKMPs have been found to be more secure than symmetric ones. However, this may increase computational overhead, which requires further investigation. Therefore, researchers should aim to develop GKMPs that balance security with computational efficiency. Future research should aim to address the limitations of centralized, symmetric algorithms and instead focus on developing decentralized, asymmetric approaches that balance security and computational efficiency.

References

Abdollahi, M., Ashtari, S., Abolhasan, M., Shariati, N., Lipman, J., Jamalipour, A., & Ni, W. (2022). Dynamic Routing Protocol Selection in Multi-Hop Device-to-Device Wireless Networks. IEEE Transactions on Vehicular Technology, 71(8), 8796-8809.

Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. IEEE communications surveys & tutorials, 10(4), 78-93.

Azees, M., & Vijayakumar, P. (2016). CEKD: Computationally efficient key distribution scheme for vehicular ad-hoc networks. Australian Journal of Basic and Applied Sciences, 10(2), 171-175., Available at SSRN: https://ssrn.com/abstract=2791871

Belding-Royer, E. M., & Perkins, C. E. (2003). Evolution and future directions of the ad hoc on-demand distance-vector routing protocol. Ad Hoc Networks, 1(1), 125-150.

Bhoi, S. K., Puthal, D., Khilar, P. M., Rodrigues, J. J., Panda, S. K., & Yang, L. T. (2018). Adaptive routing protocol for urban vehicular networks to support sellers and buyers on wheels. Computer Networks, 142, 168-178.

Bilal, M., & Kang, S. G. (2017). A secure key agreement protocol for dynamic group. Cluster Computing, 20, 2779-2792. https://doi.org/10.1007/s10586-017-0853-0

Bondada, P., Samanta, D., Kaur, M., & Lee, H. N. (2022). Data security-based routing in MANETs using key management mechanism. Applied Sciences, 12(3), 1041.

Chen, S., & Wu, M. (2011). Anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks. Journal of Systems Engineering and Electronics, 22(3), 519-527. https://doi.org/10.3969/j.issn.1004-4132.2011.03.023.

Choi, H. H., & Lee, J. R. (2019). Local flooding-based on-demand routing protocol for mobile ad hoc networks. IEEE Access, 7, 85937-85948.

Cui, J., Wei, L., Zhang, J., Xu, Y., & Zhong, H. (2018). An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 20(5), 1621-1632.

Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. (2012). One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. ACM Transactions on Internet Technology (TOIT), 12(1), 1-24.. https://doi.org/10.1145/2220352.2220353

Devi, V. S., & Hegde, N. P. (2018). Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer. Wireless Personal Communications, 100, 923-940. https://doi.org/10.1007/s11277-018-5358-5

Dhurandher, S. K., Obaidat, M. S., Verma, K., Gupta, P., & Dhurandher, P. (2010). Faces: friend-based ad hoc routing using challenges to establish security in MANETs systems. IEEE Systems Journal, 5(2), 176-188. https://doi.org/10.1109/JSYST.2010.2095910

El-Bashary, M., Abdelhafez, A., & Anis, W. (2015). A comparative study of group key management in MANET. Int J Eng Res Appl, 5(8), 85-94.

El Defrawy, K., & Tsudik, G. (2011). ALARM: Anonymous location-aided routing in suspicious MANETs. IEEE Transactions on Mobile Computing, 10(9), 1345-1358. https://doi.org/10.1109/TMC.2010.256.

El-Hadidi, M. G., & Azer, M. A. (2021, May). Traffic Analysis for Real Time Applications and its Effect on QoS in MANETs. In 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 155-160). IEEE. https://doi.org/10.1109/MIUCC52538.2021.9447611

Fatemidokht, H., Rafsanjani, M. K., Gupta, B. B., & Hsu, C. H. (2021). Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4757-4769.

Funderburg, L. E., & Lee, I. Y. (2021). A privacy-preserving key management scheme with support for sybil attack detection in VANETs. Sensors, 21(4), 1063. https://doi.org/10.3390/s21041063

Gomathy, V., Padhy, N., Samanta, D., Sivaram, M., Jain, V., & Amiri, I. S. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. Journal of Ambient Intelligence and Humanized Computing, 11, 4995-5001. https://doi.org/10.1007/s12652-020-01797-3.

Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. Journal of information security and applications, 43, 12-20. https://doi.org/10.1016/j.jisa.2018.10.004.

Hartenstein, H., & Laberteaux, L. P. (2008). A tutorial survey on vehicular ad hoc networks. IEEE Communications magazine, 46(6), 164-171., https://doi.org/10.1109/MCOM.2008.4539481.

He, W., Huang, Y., Sathyam, R., Nahrstedt, K., & Lee, W. C. (2009). SMOCK: a scalable method of cryptographic key management for mission-critical wireless ad-hoc networks. IEEE Transactions on Information Forensics and Security, 4(1), 140-150.

Hillebrand, F. (2002). GSM and UMTS: *The Creation o Global Mobile Communication*. 3rd ed., John Wiley & Sons, Ltd.

Hinden, R., & Deering, S. (2006). RFC 4291: IP version 6 addressing architecture, Available online: https://www.rfc-editor.org/rfc/rfc4291.html (accessed on 16 January 2021)

Islam, S. H., Obaidat, M. S., Vijayakumar, P., Abdulhay, E., Li, F., & Reddy, M. K. C. (2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems, 84, 216-227. https://doi.org/10.1016/j.future.2017.07.002.

Khan, A., Sun, Q. T., Mahmood, Z., & Ghafoor, A. U. (2017). Energy efficient partial permutation encryption on network coded MANETs. Journal of Electrical and Computer Engineering, 2017. https://doi.org/10.1155/2017/4657831

Kousar, R., Alhaisoni, M., Akhtar, S. A., Shah, N., Qamar, A., & Karim, A. (2020). A secure data dissemination in a DHT-based routing paradigm for wireless ad hoc network. Wireless Communications and Mobile Computing, 2020, 1-32. https://doi.org/10.1155/2020/2740654

Kumar, K. V., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks. International Journal of Intelligent Networks, 1, 36-42. https://doi.org/10.1016/j.ijin.2020.05.005.

Kumar, V., Kumar, R., & Pandey, S. K. (2020). A computationally efficient centralized group key distribution protocol for secure multicast communications based upon RSA public key cryptosystem. Journal of King Saud University - Computer and Information Sciences, 32(9), 1081–1094. https://doi.org/10.1016/j.jksuci.2017.12.014

Kumar, V., Pandey, S. K., & Kumar, R. (2016). Centralized group key management scheme for secure multicast communication without re-keying. arXiv preprint arXiv:1603.01542.

Lim, K., Tuladhar, K. M., Wang, X., & Liu, W. (2017, October). A scalable and secure key distribution scheme for group signature based authentication in VANET. In 2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference (UEMCON) (pp. 478-483). IEEE., https://doi.org/10.1109/UEMCON.2017.8249091.

Luo, X., Chen, Y., Li, M., Luo, Q., Xue, K., Liu, S., & Chen, L. (2019). CREDND: A novel secure neighbor discovery algorithm for wormhole attack. IEEE Access, 7, 18194-18205.

Lv, X., Li, H., & Wang, B. (2012). Group key agreement for secure group communication in dynamic peer systems. Journal of Parallel and Distributed Computing, 72(10), 1195-1200. https://doi.org/10.1016/j.jpdc.2012.06.004.

Maheswari, M., Geetha, S., Kumar, S. S., Karuppiah, M., Samanta, D., & Park, Y. (2021). PEVRM: probabilistic evolution based version recommendation model for mobile applications. IEEE Access, 9, 20819-20827. https://doi.org/10.1109/ACCESS.2021.3053583.

Mansour, A., Malik, K. M., Alkaff, A., & Kanaan, H. (2021). ALMS: Asymmetric lightweight centralized group key management protocol for VANETs. IEEE Transactions on Intelligent Transportation Systems, 22(3), 1663-1678. https://doi.org/10.1109/TITS.2020.3029936

Mejri, M. N., Achir, N., & Hamdi, M. (2016, January). A new group Diffie-Hellman key generation proposal for secure VANET communications. In 2016 13th IEEE annual consumer communications & networking conference (CCNC) (pp. 992-995). IEEE. https://doi.org/10.1109/CCNC.2016.7444925.

Othman, J. B., & Mokdad, L. (2010). Enhancing data security in ad hoc networks based on multipath routing. Journal of parallel and Distributed Computing, 70(3), 309-316.. https://doi.org/10.1016/j.jpdc.2009.02.010

Oubbati, O. S., Chaib, N., Lakas, A., Lorenz, P., & Rachedi, A. (2019). UAV-assisted supporting services connectivity in urban VANETs. IEEE Transactions on Vehicular Technology, 68(4), 3944-3951. https://doi.org/10.1109/TVT.2019.2898477.

Perkins, C. E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM computer communication review, 24(4), 234-244.. https://doi.org/10.1145/190809.190336

Qin, Y., Huang, D., & Li, B. (2013). STARS: A statistical traffic pattern discovery system for MANETs. IEEE Transactions on Dependable and Secure Computing, 11(2), 181-192 https://doi.org/10.1109/TDSC.2013.33

Saravanan, K., & Purusothaman, T. (2012). Efficient star topology based multicast key management algorithm. Journal of Computer Science, 8(6), 951-956 https://doi.org/10.3844/jcssp.2012.951.956

Saxena, N., & Yi, J. H. (2009). Noninteractive self-certification for long-lived mobile ad hoc networks. IEEE transactions on information forensics and security, 4(4), 946-955. https://doi.org/10.1109/TIFS.2009.2031946.

Saxena, N., Tsudik, G., & Yi, J. H. (2008). Efficient node admission and certificateless secure communication in short-lived MANETs. IEEE Transactions on Parallel and Distributed Systems, 20(2), 158-170. https://doi.org/10.1109/TPDS.2008.77.

Sepulcre, M., Gozalvez, J., & Lucas-Estañ, M. C. (2019). Power and packet rate control for vehicular networks in multi-application scenarios. IEEE Transactions on Vehicular Technology, 68(9), 9029-9037.

Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9, 163043-163053 https://doi.org/10.1109/ACCESS.2021.3133882.

Subramaniyan, S., Johnson, W., & Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. EURASIP Journal on Wireless Communications and Networking, 2014(1), 1-10 https://doi.org/10.1186/1687-1499-2014-205.

Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEE Access, 9, 120996-121005. https://doi.org/10.1109/ACCESS.2021.3108807.

Vijayakumar, P., Azees, M., Kannan, A., & Deborah, L. J. (2016). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 1015-1028 https://doi.org/10.1109/TITS.2015.2492981.

Vijayakumar, P., Bose, S., Kannan, A., & Jegatha Deborah, L. (2013). Computation and communication efficient key distribution protocol for secure multicast communication. KSII Transactions on Internet and Information Systems (TIIS), 7(4), 878-894 https://doi.org/10.3837/tiis.2013.04.016.

Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. IEEE Transactions on Vehicular Technology, 63(9), 4647-4658.

Wu, W. C., & Liaw, H. T. (2015). A study on high secure and efficient MANET routing scheme. Journal of Sensors, 2015. https://doi.org/10.1155/2015/365863.

Yadava, M., Pandey, A. S., & Singh, K. (2021). Secure and efficient wireless multicast communication using trust-based key management. Journal of Discrete Mathematical Sciences and Cryptography, 24(3), 711-727.

Zhang, R., Han, W., Zhang, L., Wang, L., & Meng, X. (2023). Provably Secure Receiver-Unrestricted Group Key Management Scheme for Mobile Ad Hoc Networks. Sensors, 23(9), 4198.

Zhang, Y., & Lee, W. (2000, August). Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 275-283). https://doi.org/10.1145/345910.345958

Zhou, J., & Ou, Y. H. (2009). Key tree and Chinese remainder theorem based group key distribution scheme. In Algorithms and Architectures for Parallel Processing: 9th International Conference, ICA3PP 2009, Taipei, Taiwan, June 8-11, 2009. Proceedings 9 (pp. 254-265). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03095-6_26

Zhao, S., Aggarwal, A., Frost, R., & Bai, X. (2011). A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Communications surveys & tutorials, 14(2), 380-400.

Zheng, X., Huang, C. T., & Matthews, M. (2007, March). Chinese remainder theorem based group key management. In Proceedings of the 45th annual southeast regional conference (pp. 266-271) https://doi.org/10.1145/1233341.1233389