JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Design of Multimedia Mobile Ad-Hoc Network for Military Applications: A Review

[1]Rabiu B. Ahmad, [2]S. F. Kolawole, [3]Paschal Uchenna Chinedu
[1]*Department of Aerospace Engineering,*
Air force Institute of Technology, Kaduna, Nigeria
[2]*Department of Electrical/ Electronic Engineering,*
Nigerian Defence Academy, Kaduna State, Nigeria.
[3]*Department of Information Systems and Technology,*
Delta State University of Science and Technology, Ozoro, Nigeria

ABSTRACT
This review explores the design and implementation of Multimedia Mobile Ad-Hoc Networks (MANETs) tailored for military applications. MANETs provide a flexible, dynamic, and infrastructure-less networking solution crucial for military operations that require rapid deployment and reliable communication in diverse and challenging environments. The paper examines key design considerations, including network architecture, routing protocols, quality of service (QoS), and multimedia data handling. Emphasis is placed on the unique requirements of military applications, such as security, robustness, and real-time communication capabilities. Additionally, this review addresses the challenges associated with MANETs, such as dynamic topology management, energy efficiency, and maintaining high QoS. Future directions for enhancing the performance and reliability of MANETs in military contexts are also discussed. This comprehensive overview aims to provide valuable insights for researchers and practitioners working on the development and deployment of MANETs for military use.

ARTICLE INFO
Article History
Received: June, 2023
Received in revised form: August, 2023
Accepted: September, 2023
Published online: December, 2023

KEYWORDS
MANET, QoS, Bandwidth, Security, Topology

INTRODUCTION

Mobile ad-hoc network (MANET) is a collection of autonomous mobile nodes that communicate over relatively bandwidth-constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over a short period of time (Shrivastava, Kumar, & Shrivastava, 2014). The nodes in MANET act as routers, exchanging information with each other in an algorithm, and allowing the nodes to distribute data throughout the network. The participation of these nodes in routing makes MANET dynamic and the topology susceptible to quick changes. The nodes are free to move in any direction and change links to other nodes frequently. MANET is also characterized by some of the unique problems due to its inherent nature, which includes host mobility, bandwidth constraints, less reliable operation, and power-constrained operations (Mane, 2022).

The nature of network requirements for military forces is vastly different from that of traditional business and commercial users. A business user typically wants a large amount of data securely and unaffected by high bit error. For these reasons, current military networks use specialized communication networks designed primarily for text and fault-related communication. New developments in the multimedia field allow for the argument of adding mobile units. Due to strong requirements such as self-organization, rapid setup speed, the capability of ad-hoc nature, and being deployable by air drop, mobile ad-hoc networks represent an advanced and capable solution for fulfilling military network requirements.

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Since the end of the Cold War, military forces have been increasingly tasked with roles such as peacekeeping, humanitarian aid, and disaster relief. Forces deployed in such roles are often operating in environments where no previous infrastructure or logistic support is available(Franz, 2000). To support these roles effectively, forces need to be provided with an information and communication system that facilitates situational awareness at the lowest manpower and cost. Mobile ad-hoc networks (MANET) and multimedia communication can play a significant role in assisting the work of military and civilian personnel in these missions, especially where wireline infrastructure is either not available or available in limited quantities.

FUNDAMENTALS OF MOBILE AD-HOC NETWORKS

Unlike the cellular network that rely on a centralized infrastructure to facilitate communication, in mobile ad-hoc network, there is no centralized authority that keeps track of the mobile nodes connection(Al-Absi, Al-Absi, Sain, & Lee, 2021). In the MANET network, one node is connected to the other only if they at least have the direct wireless link or they have to go through the intermediate through the multi-hops. Additionally, mobile ad-hoc network is designed to change constantly, with nodes joining and leaving the network at random times. Nodes in a mobile ad-hoc network are mobile and the wireless environment is consistently changing, due to the rapid changes in the state of the wireless links (due to fading) of the communication wireless channel (Umoh, Marufat, Basira, Abdulfatai, & Muyideen, 2019; Khan, Olanrewaju, Anwar, Najeeb & Yaacob, 2018). The nodes in the MANET may fail (move out of the transmission ranges of the other nodes) due to channel conditions, mobility or energy depletion. MANET may use nodes that are resource constrained in terms of energy, bandwidth and computational capability. In other words, nodes in the MANET system may be equipped with energy and computational resources. The distinction between cellular networks and MANETs is noteworthy, in that MANETs and cellular networks are both types of wireless communication networks, but they differ significantly in their architecture, functionality, and application areas. Table 1 highlighted the comparison cellular networks and MANETs while Figure 1 depict the architecture.

Table 1: Comparison between cellular networks and MANETs

Features	Cellular Networks	MANETs
Network Architecture	Centralized, fixed infrastructure	Decentralized, self-configuring
Communication	Via base stations	Peer –to- peer
Scalability	Infrastructure-limited	Potentially high, but complex
Mobility Management	Centralized, seamless handover	Node-managed, frequent topology changes
QoS	Easier to guarantee	Challenging, requires advanced algorithms
Energy Efficiency	Infrastructure-optimized	Node-battery dependent
Security	Centralized security measures	Decentralized, more vulnerable

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

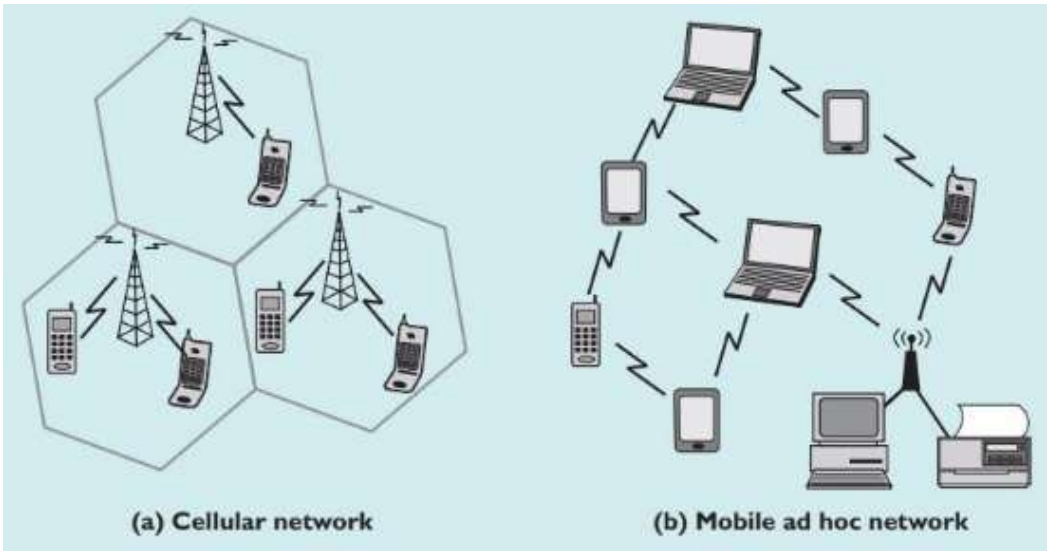

Figure 1: Cellular network versus MANETs

Types of Mobile Ad-Hoc Networks

Mobile ad-hoc networks can be categorized into different types based on various criteria, such as scalability, mobility model used, and the duration of the ad-hoc network. A brief review is as follows:

1. ***Wireless Sensor Network***: This ad-hoc network is composed of a network of tiny sensors called motes for monitoring and data collection. These sensors are low power, low-cost bi-directional relay nodes with the capability to report environmental data such as temperature, humidity, and acceleration (Yahaya, Muazu, Adedokun, & Umoh, 2019).
2. ***Tactical MANET***: This ad-hoc network is used for military applications where information needs to be communicated on demand with maximum efficiency. The network can be programmed to conform to different constraints and to exploit the best of available resources, making it ideal for rapidly deployed tactical networks (Ramphull, Mungur, Armoogum & Pudaruth, 2021).
3. ***Mesh Networks***: This type of ad-hoc network is used to provide wireless access to the internet through long-haul, point-to-point, and point-to-multipoint links. Wireless mesh networks expand the mobility capabilities beyond the WLAN access points and extend the WLAN coverage from indoor to outdoor. The network is scalable and is widely used for urban areas (Manfred, Dmitry, 2021)
4. ***Flying Ad-Hoc Networks***: A flying ad-hoc network is composed of multiple unmanned aerial vehicles acting as network nodes. This type of ad-hoc network is used for surveillance and other applications (Mohammed, Ibrahim, Momoh, Ter, Adetifa & Oluwole, 2022).
5. ***Delay Tolerant Networks***: This type of network has an architecture designed to transport data via coordination between the bearers and the routers in case of irregular connectivity. Among currently deployed delay-tolerant applications is the communication between the Mars Rover and Earth, distributed sensor nodes inside a volcano, and remote communication to Antarctica.
6. ***Vehicular Ad-Hoc Networks***: This network model consists of moving

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

vehicles and mobile devices. It is a fast-growing information technology within the auto, internet, and telecommunications industries communities and has a large potential relevance in the military and public safety application community. Multimedia Communication in Military Operations.

MULTIMEDIA COMMUNICATION IN MILITARY OPERATIONS

In the battlefield, the synchronization and coordination of soldiers against opponents are critical. An efficient synchronization and coordination method is a vital element that can help increase the probability of winning. Successful collaboration and movement from one place to another bring an advantage to the friendly force in accomplishing the mission. Allowing soldiers to exchange information between themselves, with their commander, and with sensors will increase their ability to carry out tasks and accomplish the mission successfully. An example of a soldier's mission is to search a hazardous area with the help of all available sensory elements and later report back to the commander with the results of the area.

The report is in the form of an image taken from a camera, face recognition of a suspect, detection of radiation, chemicals, or mines, position, and time, which are then represented on a map and sent back to the soldiers and commander in a peer-to-peer manner. Would the mission be easier to accomplish if the soldiers who are deploying are equipped with powerful sensory devices that are moving in collaboration? The answer is sure; it is easier for them to plan and make decisions. The soldiers can avoid any contact or conflicts with enemies promptly by sharing information among themselves. This paper will discuss multimedia communication in military operations.

DESIGN CONSIDERATIONS FOR MILITARY MOBILE AD-HOC NETWORKS

Military Mobile Ad-Hoc Networks refer to the mobile ad-hoc networks that are created to support specific military missions and exercises. These networks are used only once and for a limited period of time. Military MANETs pose special challenges on protocol and functional support designing issues as there is the need to guarantee fault tolerant operation, time-critical data communication support (real-time audio/video/convoy position/force tracking), the protection of communication security and quality of service. Notice also that the network traffic is not chaotic as the mobile nodes are on the move due to planned actions. There is also the restricted usage of power supplies. Based on these special characteristics, a proper adaptive architecture must be introduced to design military MANETs.

This paper examines and analyzes some recent research on MANETs including: protocols, security, multicast, quality of service and hierarchical designs. The attitude and charisma suggested by a number of researchers from the MANETs literature do not satisfy the military MANETs characteristics and for this reason they may not serve in the military sector. Reports from experiments of US forces in Iraq with available ad-hoc prototypes on a group of issues that military MANETs should face, including the audio group communication between squad members, convoy tracking and position reporting, achieving reliable communication through the effective use of multiple paths and preserving communication security functionalities. Based on the above literature we propose two system architectures/designs that adapt recent MANET ideas to the military MANETs requirements providing the necessary communication services to selected mobile applications of the battlefield.

Security Requirements

Most of the sensor networks are embedded in some very vulnerable areas, such as uninhabited zones, buildings, under seawater, and under the earth. In certain circumstances, an adversary may place a considerable amount of resources in order to capture as many sensor nodes as possible, hence destroying the sensor networks. Due to this sensitivity, as mentioned in sensor networks, including wireless sensor networks, require new security solutions in the

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

sensing, security, and dynamic paradigm. The major security requirements for sensor networks and mobile ad-hoc networks, in general, include authentication, access control (i.e. authorization), confidentiality, integrity, freshness, robustness against damage, and it should also be highly efficient in terms of computational and communication overhead. Contrary to general mobile ad-hoc networks and wireless sensor networks, multimedia sensors capture, compress, and transmit audio, image, and video data.

For a military WMSNET, the security issues play an important role because sensitive multimedia data is being transmitted. It requires data integrity and source authentication to prevent intrusion and to assure secured video surveillance. In the military, data security is the most important part of the network protocols. Military video and voice applications need to be established over an open data network already secured using various security protocols. These security protocols must be compatible with the first responder's existing communication systems. The special security issues that need to be considered in WMSNET should be in functionality - Securing Real-Time Content, High-Capacity Secure Video Transmission; Network resource application - Use Current Private and Public Wireless Infrastructure; interoperability - Use Commercial, Off-the-Shelf Products; complementary - Use Low-Cost, Commercial, Off-the-Shelf Products(Baldini, Karanasios, Allen, & Vergari, 2013).

Quality of Service (QoS) Considerations

Quality of Service (QoS) is very important for multimedia data. Without QoS, even having data packeted in the shortest queue, will not be able to meet the time requirements of real-time applications. For multimedia devices, delay, jitter, bandwidth, and packet loss are the most important QoS parameters. Delay and packet loss are related to the application's potential to interpret the data flow. The general QoS parameter is defined as the time required to switch traffic from forward to backward. All the service models are classified as Guaranteed Service/IntServ, Multiple Service, Differentiated Service, etc. IntServ is used to classify high discursive traffic and resist these kinds of traffic by providing QoS flows passing through. DiffServ provides more than one service class to the users. It utilizes four classes of services and reserves four of the 8-bit TOS field. A number of developments indicate the roadmap to higher bandwidth and advanced features, including broadband stringent networks that are assumed necessary to provide a global information system serving the deployment of military forces. When advanced capability is brought to the soldier, it might be powered by commercial technology. It should be noted that the time spent within combat, and the tremendous growth of mobile computers provided to the warfighters, form the shape of the interactions and user interface features (Ayo-Bello, Aibinu, Ubadike, Onumanyi & Momoh, 2022).

PROTOCOLS AND ALGORITHMS IN MILITARY MOBILE AD-HOC NETWORKS

In the design and operation of Mobile Ad-Hoc Network (MANET), routing protocol plays a very important role. This is because as the network becomes increasingly complex, routing in network communication should be adaptively adjusted from traditional state-dependent to demand-dependence.

Routing Protocols

This is a great challenge when designing the Multimedia Mobile Ad-Hoc Network (MMANET) for military applications. Due to the mobility nature of the MANET, the routing protocols developed for traditional wired networks might not perform effectively in such an environment. Generally, routing protocols for MANET are classified into two categories: proactive (table-driven) and reactive (on-demand). The proactive approach performs periodical updates of the routing table, no matter whether the route will be used or not. Examples of such algorithms include: Destination-Sequence Distance Vector (DSDV), Wireless Routing Protocol (WRP), and Cluster-head Gateway Switch Routing (CGSR). On the other hand, reactive routing protocols determine the path on an as-required basis. Due to the requirement for timely communication and energy efficiency in

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

responding to frequent network changes, reactive or on-demand routing protocols seem to be more suitable for mobile networks unlike proactive ones. In on-demand routing protocols, only those transmissions required for data forwarding consume energy. When there is no data for transmission, which means there is no activity in the network, no power is used, resulting in energy efficiency(Ayo-Bello, Aibinu, Ubadike, Onumanyi & Momoh, 2022).

Security Protocols

Security is an essential problem in MANETs because mobile radio communications are more susceptible to interception or attack. Unlike conventional static networks which employ security access controls such as walls to keep out trespassers, MANETs have no set defense line. Once an adversary cracks one link in the chain, it can access the entire network and all its resources. To work, they have to react promptly as security in mobile ad-hoc network is much more dynamic than traditional networks. The highlighted security requirement, whether it is authentication, integrity, or confidentiality, must not impose any stringent requirements, as they rely on scarce battery power and memory of mobile nodes. Mobile nodes no longer perform encryption/decryption operations on incoming/outgoing packets. The first proposed secure routing protocol is ARAN, which aims to improve the security level of on-demand routing protocols like AODV. The integrated security protocol uses the necessary identity-based cryptography to bring about the k-anonymous region certifications or the respect of location privacy among members of the same future route.

The effectiveness of ARAN is demonstrated mainly in discovery and maintenance protocol security, thus allowing the use of any AODV-based optimization, in the case of multimedia applications. If multimedia applications use the reservation of resources, the ARAN security concerns are in the interception of resource reservation packets, such as those used by RSVP. The RSVP protocol is a mechanism for reserving resources at the Multimedia Mobile Ad-hoc Network (MMAN) link and also introduces the necessary control placement capability at the level of resource allocation, which offers security for different types of public and/or private information flows. In the case of point-to-point flows that exist between two mobile nodes, resource reservation uses the QoS routing protocol to discover the route and holds the RSVP-SEC by end-to-end etc.stdcall() or conventional IPsec, using cryptographic techniques. As far as the end-to-end transmission of secure multimedia commentators is concerned, the research techniques are applicable (Melliar-Smith, 2005).

CURRENT CHALLENGES AND ISSUES

The development of a MM-MANET design for military applications encounters various challenges and issues. Most MM-MANETs are designed by exploiting the underlying characteristics of MANET technology. These include geocast algorithms, which require the geographic position of each network node; greedy forwarding protocols, which greedily forward a packet to the nearest location of the destination with the help of a next hop; QoS-capable routing protocols, which satisfy a set of QoS service requirements such as minimum bandwidth, delay, and jitter; and data delivery techniques using the available network nodes, path redundancy, and hop-by-hop node cooperation. However, while exploiting the standard networking primitives in designing MM-MANETs, issues including the autonomy operation of mobile nodes, the efficient discovery of the next hop, the high data rate and/or large QoS constraints, the optimal and redundant data delivery of the routing path between source and destination, the limited node relay and transmission power, and the maximum tolerable delay due to frequent network topology changes must be considered.

CONCLUSION

Effective communication and information exchange during combat operations require multimedia mobile ad-hoc networks (MANETs) to be specifically designed for military purposes. MANETs are well-suited for military contexts due to their self-organizing and self-healing properties, which enable adaptation to

Corresponding author: Rabiu B Ahmad
babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

high mobility and irregular connectivity in tactical situations. However, designing MANETs for military use poses significant challenges. Traditional network protocols and techniques may not be suitable for the dynamic nature of MANET networking. To effectively utilize MANET characteristics in military tactical networks, several design issues need to be addressed.

Military mobile ad-hoc networks must consider fundamental features, performance requirements, security considerations, and security threats to be functional and efficient. Research has focused on aspects such as routing protocols, energy-aware backbone formation, cooperative phase-steering techniques, fuzzy logic-based routing, securing Quality of Service (QoS) signaling, and robust and secure routing protocols. These findings can enhance the architecture of multimedia mobile ad-hoc networks for military missions, complemented by the integration of cutting-edge technologies like low-power wide-area networks, IoT, and multimedia communication. These networks facilitate seamless coordination among ground forces, multimedia data transfer, and real-time situational awareness. In conclusion, the success of military missions critically depends on the architecture of multimedia mobile ad-hoc networks. By addressing unique challenges and considering specific military needs, researchers and practitioners can develop efficient and secure network architectures that enable reliable communication, data exchange, and collaboration in dynamic and challenging environments.

REFERENCES

Al-Absi, M.A., Al-Absi, A.A., Sain, M. & Lee, H., (2021). Moving ad hoc networks—A comparative study. *Sustainability*, *13*(11), p.6187.

Ayo-Bello, O., Aibinu, A.M., Ubadike, O., Onumanyi, A.J. & Momoh, M.O., (2022). A QoS Estimation Algorithm from Caller Ringtone Analysis in GSM Network. *International Journal of Software Engineering and Computer Systems*, *8*(1), pp.53-68.

Baldini, G., Karanasios, S., Allen, D. and Vergari, F., 2013. Survey of wireless communication technologies for public safety. *IEEE Communications Surveys & Tutorials*, *16*(2), pp.619-641.

Franz, A. (2000). Ad Hoc Networking-Technology and Trends. *Center for Digital Technology and Management, Trend Report*, *2001*.

Kaur, H., Sahni, V. and Bala, M. (2013). A survey of reactive, proactive and hybrid routing protocols in MANET: a review. *network*, *4*(3), pp.498-500.

Khan, B.U.I., Olanrewaju, R.F., Anwar, F., Najeeb, A.R. & Yaacob, M. (2018). A survey on MANETs: Architecture, evolution, applications, security issues and solutions. *Indonesian Journal of Electrical Engineering and Computer Science*, *12*(2), pp.832-842.

Mane, S. (2022). Conceptual Aspects on Mobile Ad-Hoc Network System. *Int. J. Eng. Technol. Manag. Sci*, *6*(6), pp.555-564.

Manfred, S.S. & Dmitry, N. (2021). On Paradigm Shift in Telecommunication Technologies: a Review of Pentagon's Approach. International Journal of Open Information Technologies, 9(1), pp.58-75.

Melliar-Smith, P.M., 2005. *Protocol, Engineering Research Center, University of California, Santa Barbara* (p. 0067).

Mohammed, A., Ibrahim, B.G., Momoh, M.O., Ter, K.P., Adetifa, A.O. and Oluwole, D.A., (2022). Challenges of Ground Control System in Ensuring Safe Flights for Unmanned Aerial Vehicles. *MEKATRONIKA*, *4*(1), pp.8-19.

Ramphull, D., Mungur, A., Armoogum, S. and Pudaruth, S., 2021, May. A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In 2021 5th international conference on intelligent computing and control systems (ICICCS) (pp. 204-211). IEEE.

Shrivastava, P., Kumar, S. & Shrivastava, M., (2014). Study of mobile ad hoc

Corresponding author: Rabiu B Ahmad
✉ babarabiu@gmail.com
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna

networks. *International Journal of Computer Applications*, *86*(3).

Umoh, I.J., Marufat, G.O., Basira, Y., Abdulfatai, A.D. & Muyideen, M.O., (2019). BANM: A Distributed Network Manager Framework for Software Defined Network-On-Chip (SDNoC). *Covenant Journal of Informatics and Communication Technology*.

Yahaya, B., Muazu, M.B., Adedokun, E.A. & Umoh, I.J. (2019). A Survey of the Ultimate Security Solution in Opportunistic Network: Trust Management. i-Manager's Journal on Information Technology, 8(2), p.40.

Corresponding author: Rabiu B Ahmad
✉ *babarabiu@gmail.com*
Department of Aerospace Engineering, Air force Institute of Techology, Kaduna