International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Review Paper on Enhanced Security Using Multiple Paths Routine Scheme in Cloud

Prof. Rajendra Arakh[1], Prof. Apoorv Khare[2], Mr. Sandeep Rao[3]

Shri Ram Institute of Technology , Jabalpur (M.P.)

Abstract: Cloud Mobile Ad-hoc Networks (Cloud-MANETs) is a framework that provides access to cloud services for MANET users through their mobile devices. MANETs are self-organized networks of mobile devices that communicate with each other without any central infrastructure. Clustering is a commonly used technique in MANETs to manage the mobility of nodes. In clustering, the network is divided into sub-networks or clusters, each with a Cluster Head (CH) responsible for routing tasks. The CH is an enhanced node that manages the cluster and ensures efficient data communication.

In a clustered MANET, having a Cluster Head (CH) to oversee routing tasks can reduce overhead on member nodes and improve the overall performance of the system. The relationship between nodes and the CH may change randomly, leading to re-associations and re-clustering. Therefore, an efficient and effective routing protocol is necessary to enable networking and find the most suitable paths between nodes. Routing in MANETs must be spontaneous, infrastructure-less, and provide end-to-end interactions while ensuring maximum network load distribution and robustness. The primary goal of routing is to create the most optimal route between a pair of nodes to ensure accurate packet delivery. To achieve this goal, the proposed solution must ensure routing can be carried out with the lowest bandwidth consumption.

Compared to existing protocols, the proposed solution has a control overhead of 24, packet delivery ratio of 81, the lowest average end-to-end delay of 6, and an improved throughput of 80,000. Multipath routing enables the network to identify alternate paths connecting the source and destination, which conserves energy and optimizes bandwidth utilization. Overall, the proposed solution enhances the output of the network.

Keywords: Mobile Ad-Hoc Network (MANET), Weighted clustering, Offloading, Energy efficiency, Multipath routing

Introduction: With the advancement of wireless networking technologies and the internet, there has been a significant increase in the number of applications available on the web. Among these technologies, Mobile Ad-hoc Networks (MANETs) have significant potential for research and application development in wireless networks.Ad-hoc networks are a dynamic area of research that can operate as a standalone network or in conjunction with other networks or the Internet at multiple points. This makes them suitable for a wide range of applications, including road safety management, household monitoring, healthcare systems, disaster and rescue operations, defense areas, handling weapons, robotics, and many more.

The field of wireless communication has been blooming in recent times, and MANETs are one area that holds great promise for the development of novel and exciting applications. As the technology continues to evolve, we can expect to see more innovative applications of MANETs in various fields.

MANETs are commonly deployed in various applications that require dynamic communication, such as emergency and rescue operations, military and battlefield environments, intelligent transportation systems, conferences, patient monitoring, smart homes, and security-sensitive applications. In recent times, MANETs have also gained popularity in the application of drones for environmental control purposes. For example, drones can be used for forest fire detection and monitoring, pollution monitoring, and surveillance. The use of drones in conjunction with MANETs can provide real-time data and enable faster response times to environmental threats and disasters.

Overall, the versatility and flexibility of MANETs make them suitable for a wide range of applications, and their popularity is expected to continue to grow as technology evolves and new use cases are identified.

The objective of this study is to develop an energy-efficient routing protocol that enables secure and reliable information exchange in modern MANETs. To achieve energy efficiency, increase network lifetime, and scalability in dense areas, the clustering approach can be applied. Moreover, using multiple node-disjoint paths can enhance reliability, stability, and network robustness. To ensure the security of MANETs and minimal delay, mitigating malicious attacks is essential. Fig. 1 is likely a diagram or illustration that represents the proposed approach, which may include the clustering approach, multiple node-disjoint paths, and security measures. Such diagrams can be useful in understanding the proposed methodology and visualizing the different components involved in the system.

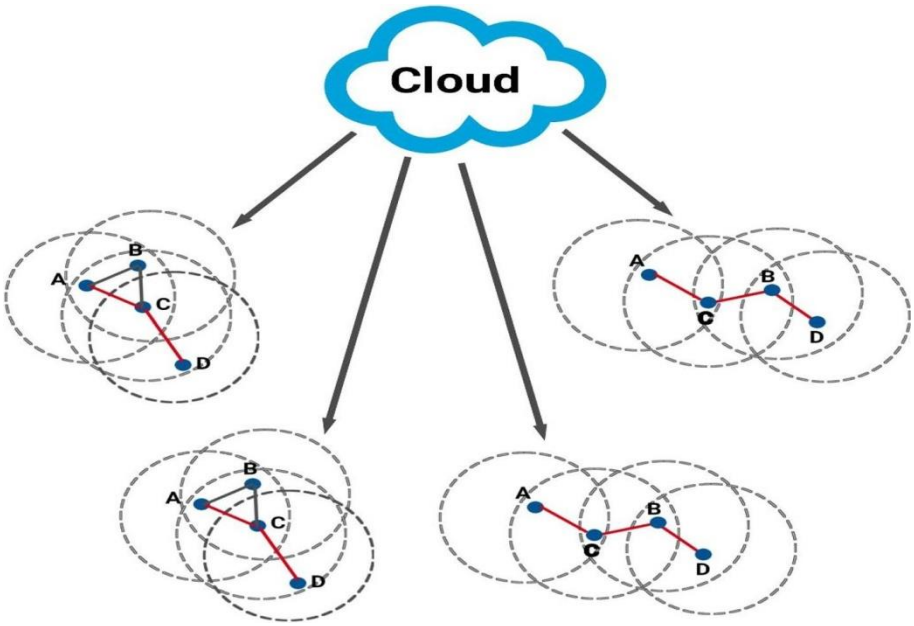

Fig. 1 Cloud mobile ad-hoc networks

The major features of a MANET can be characterized as:

- Dynamic topology: MANETs have a random and fast-changing topology due to the mobility of nodes.
- Bandwidth-constrained, variable capacity links: The wireless channel has limited bandwidth and variable capacity due to free space and open media.
- Autonomous behavior: All nodes in the network are independent and act as both host and router while forwarding data.
- Limited power/energy: Nodes are wireless and depend on battery power for their operation. These device batteries have limited operation duration.
- Limited security: Due to the absence of any central authority and open media, MANETs are highly vulnerable to security threats.

MANETs are dynamic and have mobile nodes with limited power, which can result in delays and packet loss. As a result, energy-efficient approaches are essential to improve the network lifetime. Moreover, since there is no central monitoring, all the network nodes are responsible for managing the network and routing, making MANETs more susceptible to routing and security issues compared to conventional networks. Hence, it is crucial to design effective mechanisms to handle mobility-induced issues while making routing decisions in MANETs.

Clustering is a popular approach in MANETs to manage the mobile nodes efficiently. It reduces the overhead on individual nodes and improves the performance of the system by dividing the network into clusters. Each cluster has a Cluster Head (CH) node that is responsible for performing various tasks related to routing, such as route discovery and maintenance. The CH node is an enhanced node that has more resources, such as energy and processing power, than the other nodes in the cluster. The clustering approach can be used with both overlapping and disjoint clusters, and the relationship between the nodes and CH may vary randomly, leading to re-clustering and re-associations in the network.

MANETs have dynamic and unpredictable topologies, which makes it difficult to use traditional wired networks' routing protocols. Therefore, efficient and effective routing protocols specifically designed for MANETs are required to find the most suitable paths between nodes. These routing protocols must be able to handle the challenges of low power, limited bandwidth, and high packet loss in MANETs. They should also be infrastructure-less, spontaneous, and provide end-to-end interactions to ensure the accurate delivery of packets. The main objective of MANET routing protocols is to create a maximal route between a pair of nodes while minimizing bandwidth consumption, packet loss, and control overhead to enhance the overall performance of the network.

Security is a major concern in MANETs due to their unique characteristics. Since there is no centralized monitoring or control, it becomes difficult to detect and prevent security attacks. The open medium of MANETs makes it easy for an attacker to eavesdrop on the communication between nodes, which can lead to

data leakage and confidentiality breaches. In addition, the dynamic topology of the network makes it vulnerable to attacks such as routing attacks, where attackers can disrupt or modify the routing process to redirect traffic or cause network failures.

Modification attacks involve modifying the contents of data packets, while fabrication attacks involve creating fake packets that appear to come from a legitimate source. Impersonation attacks involve an attacker pretending to be a legitimate node in the network. Black-hole and worm-hole attacks are two common types of impersonation attacks. In a black-hole attack, an attacker falsely claims to have a shorter route to a destination node and attracts traffic towards itself, while in a worm-hole attack, attackers create a tunnel between two points in the network and reroute traffic through this tunnel to eavesdrop on or modify the data.

To secure MANETs, various security mechanisms can be used, including cryptographic techniques such as encryption and digital signatures, intrusion detection systems, and secure routing protocols. These mechanisms can help to detect and prevent security attacks and ensure the confidentiality, integrity, and availability of the data transmitted in the network.

Problem definition

To address these issues, several approaches have been proposed to improve clustering in MANETs. One such approach is the Low-Energy Adaptive Clustering Hierarchy (LEACH) algorithm. LEACH is a self-organizing, adaptive clustering algorithm that aims to reduce energy consumption by using distributed clustering, data aggregation, and data compression techniques. It uses probabilistic techniques to distribute the energy consumption evenly among the nodes in the network.

Another approach is the Threshold Sensitive Energy Efficient sensor Network (TEEN) protocol. TEEN is a hierarchical clustering protocol that dynamically adjusts the cluster formation threshold based on the energy level of the nodes in the network. This approach minimizes energy consumption by ensuring that only nodes with sufficient energy are selected as cluster heads.

A third approach is the Stable Election Protocol (SEP), which uses the remaining energy of the nodes to elect cluster heads. In this protocol, nodes with the highest remaining energy are chosen as cluster heads, and nodes with lower energy levels are selected as members of the cluster.

Overall, these approaches aim to reduce the energy consumption of the nodes in the network while maintaining high network performance and reliability.

It is important to develop efficient and effective algorithms to address the challenges faced in clustered MANETs, such as delay and packet loss caused by the difference in reception and transmission capacity of the Cluster Head. Moreover, the frequent reorganization of nodes and changes in the network topology due to node movement and clustering may lead to link failures. To ensure secure communication in inter and intra cluster routing, lightweight key management algorithms are required, as the cluster head acts as a Trusted Third Party (TTP) in the clustering-based framework. However, traditional approaches often suffer from problems such as increased computational complexity, network overhead, inefficient security, unreliability, and reduced network

throughput. Therefore, it is necessary to explore new solutions that can overcome these challenges and improve the overall performance and security of clustered MANETs.

Related work

Cluster-based routing protocols, as mentioned earlier, group the network into clusters, with a Cluster Head (CH) managing routing tasks within each cluster. Examples of cluster-based routing protocols include LEACH (Low Energy Adaptive Clustering Hierarchy) and HEED (Hybrid Energy-Efficient Distributed clustering).

Multipath routing protocols, on the other hand, use multiple paths to transmit data, increasing the network's reliability and fault tolerance. Examples of multipath routing protocols include AOMDV (Ad Hoc On-Demand Multipath Distance Vector) and OLSR (Optimized Link State Routing).

Secure routing protocols aim to provide secure and reliable communication in MANETs by detecting and mitigating various security attacks, such as node misbehavior, packet dropping, and network partitioning. Examples of secure routing protocols include SEAD (Secure Efficient Ad hoc Distance vector routing) and Ariadne.

It is important to note that the choice of routing protocol depends on the specific requirements and constraints of the MANET application. For example, a high mobility scenario may require a more robust multipath routing protocol, while a low-power sensor network may require a more energy-efficient clustering-based protocol.

Literature review

Sulyun Sung et al. proposed a distributed cluster formation scheme that includes algorithms for creating and maintaining clusters in high mobility networks. The scheme employs a novel approach to identify the cluster head and member nodes based on the node's residual energy and connectivity to other nodes. The algorithm considers the node's distance from the cluster head, the energy required to communicate with the cluster head, and the residual energy of the node to select a suitable node as the cluster head. The proposed scheme also provides a mechanism to handle cluster member failures and reformation of clusters. The simulation results showed that the proposed scheme has better performance in terms of energy consumption, network lifetime, and packet delivery ratio compared to other clustering schemes.

Waqar Asif et al. proposed control overhead and delay are significant challenges in designing routing protocols for ad-hoc networks. While PSO(Parti-

cle Swarm Optimization)-based protocols can be effective in optimizing clusters and conserving energy, minimizing control overhead and delay remains an important research area.

N. Shukla et al. proposed a clustering protocol named SYN, which aimed to improve the energy efficiency of MANETs by reducing energy consumption during cluster formation, cluster maintenance, and data transmission. The protocol used a Max-heap tree to model varying levels of energy of the nodes and employed a distributed algorithm for cluster formation.

Sudha, K.Ranjith et al. prposed Zone-based protocol is a routing protocol for MANETs that divides the network into multiple non-overlapping zones. Each node in the network is assigned to a specific zone based on its geographic location. The protocol uses one-hop clustering, where each node forms a cluster consisting of itself and its immediate neighbors.

Swarna Priya R. M. et al. proposed an energy-efficient cloud-based Internet of Everything (IoE) framework that leverages cloud computing to provide valuable services to consumers. The framework is designed to minimize energy consumption in the IoE network while ensuring that the quality of service (QoS) requirements of consumers are met. The proposed framework uses a cloud-based approach to store and process data generated by the IoE devices, thereby reducing the energy consumption of individual devices. The framework also includes a scheduling algorithm that efficiently allocates resources to different tasks based on their QoS requirements and energy consumption. The proposed framework has the potential to improve the energy efficiency of the IoE network and enable the development of sustainable and scalable IoE applications.

Zou Fengfu et al. proposed an extension to detect black hole attacks using this protocol. The extension added a new mechanism to monitor the route established by the AODV protocol and detect abnormal behavior that might indicate a black hole attack. However, as you mentioned, their proposed solution had some shortcomings, including increased latency due to additional overhead and a lack of robustness in detecting black hole attacks in networks with unstable links.

Chakeres et al. proposed reactive routing protocol that aims to discover loop-free routes in MANETs through the use of on-demand route discovery. When a node needs to send data to a destination, it initiates a route discovery process by broadcasting a Route Request (RREQ) packet. The neighboring nodes that receive the RREQ packet can either forward it or reply with a Route Reply (RREP) packet if they have a route to the destination. This way, AODV avoids the need for maintaining a complete routing table at each node, reducing the control overhead and improving scalability.

Perkins et al. proposed DSDV (Destination-Sequenced Distance Vector) routing protocol for long before the concern of black hole attacks in MANETs became prominent. DSDV is a proactive routing protocol that maintains a routing table at each node and periodically exchanges routing updates with its neighbors to ensure loop-free and shortest-path routing.

Mainak Chatterjee et al. proposed a new multipath routing protocol called Node-Disjoint Multipath Routing Protocol (NDMRP) for Mobile Ad hoc Networks (MANETs). The protocol is built on top of the well-known AODV protocol and aims to provide guaranteed packet delivery with high reliability and low latency.

ALGhafran et al. introduced a Group Mobility-based Multipath Routing protocol (GMR). GMR utilizes a clustering technique that organizes nodes into groups and selects multiple disjoint paths between the source and destination nodes. The protocol uses a group mobility-based algorithm that can detect and adjust to node movements, ensuring that the selected paths remain stable. However, the protocol does not consider energy consumption, and scalability could also be an issue in large networks.

Proposed Methodology

The proposed work aims to improve the stability and energy efficiency of MANETs through a weight-based clustering scheme for electing a Cluster Head (CH) based on energy and node mobility. It also introduces a data offloading mechanism for efficient data traffic management in heterogeneous networks. The network lifetime and robustness to failure are increased through a node-disjoint weighted multipath routing protocol. Finally, the network's security is improved using a cryptography-based mechanism employing an Elliptic Curve Cryptography (ECC) encryption mechanism to protect against malicious attacks and increase throughput. The proposed methodology is broken up into four phases:

Phase1 –Weight based energy aware clustering scheme

Phase 2—Data offloading in clustered MANET for data synchronization

Phase 3 - weighted multipath energy aware routing

Phase 4- Secure routing through cryptography

Conclusion

It is important to secure MANETs against malicious attacks, and the proposed SCCM mechanism provides a solution for message confidentiality and authentication. The use of the WMECS routing protocol helps to ensure that data is transmitted via multiple paths, reducing packet loss and delay time. The proposed approach can lead to increased throughput in MANETs, providing a more efficient and secure network for communication. Future research can explore the scalability and energy consumption of the SCCM mechanism and how it can be improved to address these issues.

References

- Sakhaee E, Jamalipour A (2008) Stable clustering and communications in pseudolinear highly mobile ad hoc networks. IEEE Trans Veh Technol 56(8):3769–3777
- Silva L et al (2021) Computing paradigms in emerging vehicular environ- ments: a review. IEEE/CAA J Autom Sin 8(3):491–511. https://doi.org/10. 1109/JAS.2021.1003862
- Huiyao A, Xicheng L, Wei P (2004) A cluster-based multipath routing for MANET. Computer School, National University of Defense Technology, Changsha, China, pp 405–413
- Huang H, Huang C, Ma D (2020) A method for deploying the minimal number of UAV base stations in cellular networks. IEEE/CAA J Autom Sin 7(2):559–567. https://doi.org/10.1109/JAS.2019.1911813
- Chatterjee M, Das SK, Turgut D (2009) A weight based distributed cluster- ing algorithm for mobile ad hoc networks. HiPC, LNCS 1970:511–521
- Asif W, Qaisar S (2011) “Energy and path aware clustering algorithm for mobile ad hoc networks. ICCSA, Part IV, LNCS 6785:133–147

- Basu P, Naidu W (2012) A mobility based metric for clustering in mobile ad hoc networks," in International conference on Distributed computing systems workshop. pp 413–418
- Zhong J, Huang Z, Feng L, Du W, Li Y (2020) A hyper-heuristic framework for lifetime maximization in wireless sensor networks with a mobile sink. IEEE/CAA J Autom Sin 7(1):223–236. https://doi.org/10.1109/JAS.2019. 1911846
- Shukla N (2013) Mobile Ad-Hoc Network (MANET): Security Issues Regarding Attacks. in International Journal of Computer Applications (0975–8887), National Conference on Recent Trends in Engineering and Management "NCRTEM-2013
- Sudha K, Ranjith JP, Ganapathy S, Sasidharan MSR (2015) Secure trans- mission over remote group: a new key management prototype. Int J Comput Sci Netw Secur (IJCSNS) 15(1):101
- Morris R, Jannotti J, Kaashoek F, Li J, Decouto D (2010) CarNet: A Scalable Ad Hoc Wireless Network System. Proc. of 9th ACM SIGOPS European Workshop, Kolding, Denmark
- Grossglauser M, Tse D (2001) Mobility increases the capacity of ad-hoc wireless networks. Proc. of INFOCOM'01. pp 1360–1369
- Steenstrup M (2001) Cluster-Based Networks. Chapter 4, Ad Hoc Net- working, edited by C. E. Perkins, Addison-Wesley
- Neethu V, Singh AK (2015) Mobility aware loose clustering for mobile ad hoc network. Procedia Comput Sci 54:57–64
- Sung S, Seo Y, Shin Y (2010) Hierarchical clustering algorithm based in mobile ad hoc networks. ICCSA, LNCS 3982:954–963
- Loutfi A (2014) An energy aware algorithm for OLSR clustering. Ann Telecommun 69:201–207
- Basurra SS, De Vos M, Padget J, Ji Y, Lewis T, Armour S (2015) Energy efficient zonebased routing protocol for MANETs. Ad Hoc Netw 25:16–37
- RM SP, Bhattacharya S, Maddikunta PKR, Somayaji SRK, Lakshmanna K, Kaluri R, Hussien A, Gadekallu TR (2020) Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. J Paral- lel Distrib Comput 142:16–26. https://doi.org/10.1016/j.jpdc.2020.0.2.010
- Kulkarni SB, Yuvaraju B (2016) Challenges and issues of cluster based security in MANET. IOSR J Comput Eng (IOSR-JCE) 18:01–05
- Kaur I, Rao A (2017) A framework to improve the network security with less mobility in MANET. Int J Comput Appl 167:21–4

- Jhaveri RH, Patel NM (2015) A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. Wireless Netw 21(8):2781–2798
- Kavitha P, Mukesh R (2018) Detection of impersonation attack in MANET using polynomial reduction algorithm. IJ Network Security 20(2):381–389