Applying Mobile Ad-Hoc Networks (MANETs) to Civilian Evacuation Convoys

Cassandra Young

CIS553 2022S

**Introduction**

Mobile Ad-hoc Networks (MANETs) are self-governing systems of connected devices which form an autonomous peer-to-peer mesh network. Devices, acting as nodes, connect to each other over wireless communications methods such as Wi-Fi, Bluetooth, and cell or radio signal boosters if available. While these networks are commonly applied to situations where other infrastructure is limited or unavailable, such as disaster relief, search and rescue, and military operations, they can also be applied to civilian evacuation situations in warzones, where coordination and resource sharing are of particular importance. They may also be used to collectively report group status to support services and other individuals when there is internet connectivity. In this scenario, MANETs and the applications atop them must be designed to mitigate complicating factors such as lack of robust infrastructure, intermittent internet and cellular connectivity, finite device energy, and high mobility as nodes change relative location.

**Overview of MANETs and Example Scenarios**

Characteristics of MANETs include a dynamic network topology which changes rapidly, limited bandwidth and range due to the use of local device wireless links, autonomous and distributed behavior where each node acts as both host and router, energy constraints due to nodes with finite power sources such as batteries, and minimal wireless security due to their decentralized nature (Corson & Macker, 1999). MANETs can be modeled using a graph G = (V, E) with V representing the nodes within the network, and E representing the overlap of nodes’ communication range, where overlapping signal is the basis for linking nodes to form the network (Rodríguez-Covili et al., 2012).

Applying MANETs to civilian evacuations from a warzone may cover multiple use cases, including but not limited to:

1. Local area evacuation, where individuals on the ground must coordinate with each other to meet at set pickup points for departure, possibly in areas obstructed by collapsed structures.
2. Intra-group communication within an evacuation convoy, whether walking or driving. This could take the form of requests to the group for supplies or other aid, warnings about road damage or weapons fire, or personal communication between individuals or groups in different vehicles.
3. Reporting one’s status, ie. that a user is alive and progressing toward an exit point such as moving across a country toward a border crossing. This would take the form of registering with a web-based application and sending updates during times where internet connectivity is available.

In cases of civilian evacuation, users are more likely to only bring smaller, lightweight devices such as mobile phones or tablets. It is therefore a requirement that for all use cases, the application and underlying services must be able to run on those devices, each mobile device acting as a node.

**Ad-hoc Routing Protocols**

The primary challenge of a MANET is determining traffic routes such that the network is adaptive to topographical change yet energy efficient. Routing protocols, typically operating on the network layer, present options for a variety of use cases. In a situation involving multiple moving vehicles, nodes may frequently change location relative to each other, drop outside the range of the network, or otherwise become intermittently unavailable. Due to the reliance on small, handheld devices to create the network, energy drain on these devices must also be accounted for and minimized when considering which routing protocol to use.

In one study(Quispe & Galan, 2014), the authors analyze ad hoc routing protocols in emergency and rescue situations, studying top performers in each of three types of routing protocol categories.

In proactive routing protocols, each node maintains a route table for the entire network whether data is flowing or not, periodically sending route updates to other nodes. While proactive routing protocols prove more adaptable to route changes and the introduction of new nodes, they consume more bandwidth and energy (Quispe & Galan). The protocol chosen in this category was Destination-Sequence Distance-Vector (DSDV).

Reactive routing protocols, on the other hand, allow nodes to update their route tables on demand, by using *route discovery* and *route maintenance*. When receiving a message to be forwarded, *route discovery* is performed to determine the best path to the destination. When path failure occurs after a node is removed or relocated, *route maintenance* is performed. While the on-demand element of route discovery adds to initial latency when sending messages, reactive protocols are more energy efficient and use less bandwidth, such that they are preferable in emergency situations. The reactive routing protocol compared in this study is Ad Hoc Demand Distance Vector (AODV).

Other studies show support for variations on AODV for fast data transmission across MANETs, including one (Jalade & Patil, 2021) where the authors propose an optimization technique targeted at fault recovery and fast data transmission which uses an adapted AODV protocol for route discovery. In this technique, paths are prioritized based on each node’s energy levels and mobility.

Lastly, hierarchical routing protocols subdivide the network into clusters, designating a “cluster head” node to centralize and distribute data. Cluster heads can be selected based on mobility, ie. the stability of its presence in the cluster, or any other combination of factors such as degree of connectivity, or residual energy. For this study, the authors selected Cluster Based Routing Protocol (CBRP), which is a reactive protocol overall, but with a hierarchical component.

The study’s analysis of the selected routing protocols is conducted through a simulation which emphasizes location awareness. Given that the context is emergency and rescue, an evacuation point is designated in the simulation, with the goal being to find the quickest route to the evacuation point. The study finds that the least effective protocol is DSDV, followed by AODV, which has better performance. However, CBRP ranks the highest when used to navigate to an evacuation point while accounting for physical obstructions. While the cluster head is directing the group toward an exit point, another node transmits to nearby groups informing them of the best point of evacuation. (Quispe & Galan)

The advantages of Cluster Based Routing Protocol (CBRP) map directly to the first use case specified, where an evacuation is being coordinated with a clearly designated exit point, however it applies less directly to the second use case surrounding intra-group communication. The protocol’s natural grouping by geospatial location given the proximity of nodes could be used to limit the range, in number of hops, to which messages are broadcast, but this would limit the ability of individuals to broadcast needs to the group. Additionally, it may be difficult to maintain geospatial cluster accuracy in MANETs where nodes change relative location frequently.

Given that a vehicular convoy may result in higher node mobility than in a localized evacuation, comparing AODV and CBRP with similar route prioritization would be worth further investigation to determine if CBRP is the best protocol in a scenario with higher node mobility, but most papers read for this discussion point to hierarchical routing protocols as the more efficient choice in comparative studies. As such, this paper will focus on them.

**Node Hierarchy**

A subset of research in the MANET space focuses on cluster head selection for cluster routing protocols, taking into consideration factors such as node mobility and residual energy, or highest number of neighboring nodes. In a study (Szucs & Wassouf, 2018) proposing improvements to CBRP, the authors incorporate elements of another enhancement of CBRP called Backup Cluster Head Protocol (BCHP), which introduces a Backup Head Cluster to assume the cluster head position if the original is unavailable. Their improvements to the existing protocols include power-aware clustering through a weighted clustering algorithm, which uses the following parameters for cluster head selection:

1. Degree difference: the number of direct connections that node has to other nodes compared to a specified threshold
2. Distance summation: the sum of distances to neighboring nodes
3. Mobility: average speed of the node
4. Remaining battery power: consumed battery power

The node with the lowest total is then selected as the cluster head. The first node to start the cluster broadcasts out and begins to create a routing table, later selecting the backup cluster head based on which node has the next-lowest weight. Once all joined nodes have been assessed, the cluster head and backup cluster head synchronize data, proactively reassigning themselves if the backup cluster head’s weight falls below that of the cluster head’s and beginning the backup head selection anew. (Szucs & Wassouf, 2018)

Given high node mobility within vehicle-based evacuations, cluster head selection and membership updates may be subject to frequent change, and this strategy would likely result in improved performance.

**Cluster Management and Connectivity to the Internet**

An *isolated* MANET is designed to act as an autonomous local network, while a *hybrid* MANET can also be used to extend internet connectivity. During travel through rural areas, or areas under attack, cellular and internet connectivity may be intermittent and unpredictable due to destruction of infrastructure. Additionally, movement through a geographical area combined with intermittent connectivity to cellular or internet service may also cause faster device power drain, complicating the device’s functionality as a node within the MANET. At the device level, limiting or throttling cellular or internet service may mitigate traffic spikes, congestion and energy drain on devices during passage through areas with connectivity.

One of the challenges faced by both hybrid and isolated MANETs is the merging of clusters, whether internet gateway to clusters within the network. Managing potentially overlapping IP addresses during cluster merges and augmentation is explored using different approaches to duplication address detection (DAD). While prior research proposed using duplicate-IP address detection servers, these were found to be too resource-intensive to adapt to the level of mobility in MANETs, and other proposed solutions create excessive network load, as they apply a flooding technique for address duplication detection. The authors of this study (Priya et al., 2020) discuss nature-based algorithmic approaches to solving this problem, as applied to different types of nodes in the cluster. The node types proposed in this model are a gateway node, which supplies the connectivity to the greater internet, coordinator nodes that perform DAD operations, leader nodes or cluster heads, and member nodes which are the cluster members situated at the lower part of the hierarchy. The authors found that moving the DAD operation to a pre-selected coordinator node improved performance by reducing broadcast traffic and, consequently, conserving node energy.

**Security and Privacy Preservation**

Security and privacy at are often at odds with speed and usability, and security of MANETs inherits the vulnerabilities of wireless networks in that signal can be physically intercepted. Potential attacks on MANETs can be categorized as internal and external. Internal attacks involve an attacker gaining access to the network with intent to compromise the contents of intercepted messages. In external attacks, the intent is to disrupt the flow of traffic to the point of rendering the network unusable, for example in the case of a denial of service attack. Attacks can be active, with a malicious node consuming its own resources to perform the attack, or passive, conserving its resources. (Keerthana & Anandan, 2018)

Denial of service attacks can take many forms, including using the *route discovery* features of routing protocols to flood a network with traffic, clogging it past the point of usability. If multiple nodes are compromised, this can scale up to a distributed denial of service attack. Compromised nodes may also be drained of their residual energy, or others drained due to the volume of requests. Disruption of the routing protocol itself can take the form of route table poisoning, when a malicious node transmits false route information, or packet reproduction, where the node re-transmits received data excessively to flood the network. At the network layer, attacks may attempt to advertise fake routes in order to redirect traffic, create routing loops, or simply drop intercepted packets. When attempting to read traffic, a malicious node may advertise itself as the best route, redirecting target traffic to itself. These internal attacks may target the contents of the message itself, or exposed metadata including location data. (Keerthana & Anandan, 2018)

In the case of wartime, the objective of these attacks may be to target a specific person or group of persons, disrupt coordinated rescue operations, or to negatively impact morale of civilians. Nation-state level attacks are a considerable challenge in the information security space, and given the adaptive and flexible nature of MANETs, difficult to mitigate at both the network and applications layers.

Multiple papers reference architectures where routing information messages are sent over UDP, and therefore are unencrypted, but the resulting data traffic is sent over TCP using keys established by the nodes in communication. In the case of a group chat or ‘broadcast’ type of message, the only way to mitigate impersonation would be to enforce node authentication during the cluster joining process, which may conflict with the goal of a lightweight, quick to use implementation. Further research is needed in this area.

**Extending MANET Design to Application**

In this discussion, one example use case is an evacuation convoy of vehicles and/or groups of people walking who need to coordinate when other communications infrastructure is damaged or intermittently unavailable. A MANET could be used to support a multi-purpose application design for several use cases within that scenario: broadcasting messages to all users across the local network, user-to-user direct communication, and user check-ins with a web-based service when external connectivity is established.

To accomplish user check-ins with a web-based service during times of internet connectivity, gateway or cluster head nodes would be designated to transmit this information, with other nodes prioritized lower for internet connectivity. Each device holds a unique identifier which can be registered in a web application beforehand, and as devices communicate, these identifiers would be stored alongside the timestamp of their last message. When a subset of nodes are granted connection to a now-available cellular network through a specified gateway node, they would transmit this information for the web-based service to extract and use to update the ‘last checked in’ time for each participant.

**Conclusion**

Given the constraints discussed previously, applying MANETs to civilian evacuation convoys would require that the implementation be lightweight and functional on mobile devices, with a minimum volume of network traffic. This suggests the use of an energy-efficient, adaptive routing protocol to maintain connectivity throughout the network with minimal overhead and network traffic. Hierarchical routing protocols such as Cluster Based Routing Protocol (CBRP) and its adaptations have been proven to be more efficient and fit this purpose. The management of clusters must also be robust and secure, and efficient schemes put in place to manage intermittent connectivity through gateways for the purposes of communicating status.

**References:**

Corson, M. & Macker, J. (1999) Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, IETF, RFC 2501.   
https://www.rfc-editor.org/rfc/pdfrfc/rfc2501.txt.pdf

Jalade, S. C., & Patil, N. B. (2021). Optimization technique for fault recovery and fast data transmission in Manet. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.03.699

Keerthana, G., & Anandan, P. (2018). A survey on security issues and challenges in mobile ad-hoc network. EAI Endorsed Transactions on Energy Web, 5(20), 155743. <https://doi.org/10.4108/eai.12-9-2018.155743>

Perkins, C., Belding-Royer, E. & Das, S. (2003) Ad hoc On-Demand Distance Vector (AODV) Routing, IETF, RFC 3561.  
<https://doi.org/10.17487/RFC3561>

Priya, J. S., Femina, M. A., & Samuel, R. A. (2020). APSO-MVS: An adaptive particle swarm optimization incorporating multiple velocity strategies for optimal leader selection in Hybrid Manets. Soft Computing, 24(24), 18349–18365. <https://doi.org/10.1007/s00500-020-05034-z>

Quispe, L. E., & Galan, L. M. (2014). Behavior of ad hoc routing protocols, analyzed for emergency and rescue scenarios, on a real urban area. Expert Systems with Applications, 41(5), 2565–2573. <https://doi.org/10.1016/j.eswa.2013.10.004>

Rodríguez-Covili, J., Ochoa, S. F., & Pino, J. A. (2012). High level manet protocol: Enhancing the communication support for mobile collaborative work. Journal of Network and Computer Applications, 35(1), 145–155. https://doi.org/10.1016/j.jnca.2011.02.006

Sandeep, J., & Kumar, J. S. (2015). Efficient packet transmission and energy optimization in military operation scenarios of Manet. Procedia Computer Science, 47, 400–407. <https://doi.org/10.1016/j.procs.2015.03.223>

Szucs, V., & Wassouf, M. (2018). Modified manet protocol to extend the emergency network. 2018 9th IEEE International Conference on Cognitive Infocommunications (CogInfoCom). https://doi.org/10.1109/coginfocom.2018.8639908