Mobile Ad Hoc Networking

ABSTRACT

Mobile Ad Hoc Networks (MANETs) refer to a class of wireless networks that can be formed dynamically and randomly without the need for infrastructural setups. Such networks are able to adapt and reconfigure themselves on the fly according to node mobility and changing network topologies. These characteristics are particularly attractive to the military user due to the inherent unpredictability of the tactical environment. MANET technology has its roots in defence, having been developed from military research efforts. This article presents an overview of MANET technology, its key characteristics and how it can be leveraged for the Third Generation Singapore Armed Forces. Experience gained and lessons learnt from an experiment initiated and funded by the Future Systems Directorate on MANET are also discussed.

Chim Yuen Chong
Raymond Seah Kwang Wee
Sim Soon Lian
Tan Jia Hui

Mobile Ad Hoc Networking

INTRODUCTION

A Mobile Ad Hoc Network (MANET) is an interconnected system of wireless nodes which communicate over bandwidth-constrained wireless links. Each wireless node can function as a sender, a receiver or a router. When the node is a sender, it can send messages to any specified destination node through some route. As a receiver, it can receive messages from other nodes. When the node functions as a router, it can relay the packet to the destination or next router in the route. When necessary, each node can buffer packets awaiting transmission (He, 2003).

The nodes move randomly; hence at a given point in time, an ad hoc network exists between the nodes, giving rise to an arbitrary network topology. MANETs can be dynamically formed among any group of wireless users and require no existing infrastructure or configuration.

MANET CHARACTERISTICS

A MANET has several marked characteristics. First, it does not have a centralised infrastructure. It is unlike the traditional mobile wireless networks in which base stations, access points and servers have to be deployed before the networks can be used. Figure 1(a) illustrates how an infrastructure-based wireless network would operate[1]. Instead, as shown in Figure 1(b), the ad hoc network is decentralised, with all mobile nodes functioning as routers and all wireless devices being interconnected to one another. Intuitively, this means that the MANET is also a self-configuring network in which network activities, including the discovery of the topology and delivery of messages, are executed by the nodes themselves.

The second characteristic of a MANET is that it has a dynamic topology. Nodes are free to move arbitrarily, causing the network topology to change rapidly and unpredictably over time. Alternative paths are automatically found, after which data packets are forwarded across the multi-hop paths of the network. MANETs use various routing mechanisms to accomplish this. This is further elaborated in Annex A.

Thirdly, a MANET operates on bandwidth-constrained variable-capacity links. Wireless links have significantly lower capacity than hard-wired links. As such, a MANET has relatively low bandwidth links, high bit error rates, and unstable and asymmetric links. This is in contrast to wired networks which are characterised by high bandwidth links, low bit error rates and stable and symmetric links. One effect of having a low link capacity is that congestion is typically the norm rather than the exception (Corson and Macker, 1999).

Fourthly, a MANET is often bound by energy-constrained operations (Corson and Macker, 1999). This is because its nodes are often hand-held battery-powered devices. Since

(a) Infrastructure-based wireless network *(b) Ad hoc wireless network*

Figure 1.

the mobile nodes rely on these exhaustible means for energy, power conservation is important in a MANET system design.

Lastly, there is limited physical security. Mobile wireless networks are more prone to the physical security threats of eavesdropping, interception, denial-of-service and routing attacks as compared to fixed-cable networks (Corson and Macker, 1999). Hence, security techniques have to be applied to reduce these threats. Nodes prefer to radiate as little power as necessary and transmit as infrequently as possible. This will decrease the probability of detection and interception. In addition, the decentralised nature of network control will add robustness against failure as opposed to the centralised networks.

LIMITATIONS OF MANETs

There is a current and future need for dynamic ad hoc networking technology. This highly adaptive networking technology, however, still faces various limitations.

Throughput Drops with More Hops

Nodes that are in the transmission range of each other are able to send the data packets directly. However, when the node needs to send data to a non-neighbouring node, the data packets will have to be sent through a sequence of multiple hops, with the intermediate nodes acting as routers. This indicates an increase in the number of hops taken. Throughput will decrease rapidly when the number of hops is increased. This can be explained using the four-hop network illustrated in Figure 2.

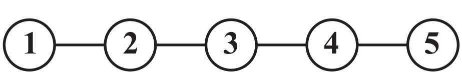

Figure 2. Multi-hop network

When link 1-2 is active, link 2-3 cannot be active because a node cannot be transmitting and receiving at the same time. Link 3-4 is also inactive because communication by node 3 may interfere with node 2 (Holland and Vaidya, 2002). Thus, with more hops, there are in turn more idle nodes, which reduces the throughput.

Throughput Drops with Increasing Mobility

Highly mobile nodes will result in more overheads due to frequent topology changes. This is because of the increase in the number of routing packet transmissions due to the need to determine new routes after route failures. When the routing table is used, each node keeps a list of all available destinations as well as the number of hops required to reach each destination. Changes in the topology will be reflected in the routing table. Any routing table changes are relayed to all the other nodes. This imposes a larger overhead on the overall network. When the overhead is large, a lower percentage of the packet goes towards the transmission of data, resulting in a lower throughput.

Delay

Delay represents the average time duration which a packet takes from the time it leaves a source to the time it arrives at its destination. As seen above, there is a need to keep the nodes busy with the transmission and receiving of packets in order to increase the throughput of the network. This, in turn will mean that the queue of each node is always not empty, leading to a longer delay.

MILITARY APPLICATIONS OF MANETs

The operating concept of the Third Generation Singapore Armed Forces (3G SAF) is characterised by fast operational tempos and is hence subjected to dynamic topology changes. The environment is dense and there is usually no direct line of sight between military users who need to communicate. Thus, a range extension is required for this operating environment. Hence, in military applications, rapid network formation, extended operating range and survivability are key requirements. Wired networking requires base stations to be set up in the correct locations. This is a task that is not easily done or not applicable in hostile or foreign environments. The network is also vulnerable to failures, as the system will not be usable if one or several base stations are destroyed.

A MANET, on the other hand, can meet military requirements in such environments. In the distributed network architecture, all the nodes are equipped with routing capability. They are hence able to forward information on behalf of other nodes, resulting in multi-hop routes. The limitation of having short radio transmission ranges is hence overcome. Nodes are also easily added, removed or relocated. The dynamics of a MANET hold great promise for improving the communication network and in turn enhance the Integrated Knowledge-based Command and Control capability of the SAF.

MANETs for the SAF

The SAF's operating environment is characterised by heavy vegetation and increasing concentrations of built-up areas. These present challenging obstacles for communications as radio signals experience blockages and fading as they are transmitted through such terrain. While a MANET could potentially mitigate some of these undesirable effects through its inherent dynamic routing and self-healing and self-forming characteristics, a direct adoption of the MANET concept for the SAF's ground troops is unlikely to yield very high returns. This is because the MANET data path will probably go through several hops in the heavily shielded terrain, resulting in poor overall network throughput and latency performance. To overcome this, the vertical (i.e. non-terrestrial) dimension, through the use of an Airborne Communication Node (ACN), needs to be exploited.

The ACN is essentially an airborne platform that carries a communications payload to perform communications and networking relay functions[2]. The advantage of such a platform is that it enjoys a high vantage point. This increases the likelihood of having direct LOS with ground nodes, grounding connectivity across physical barriers that might occur in wireless networks. Several ACNs may be deployed in a network to provide a more robust architecture. ACNs therefore form an important complementary concept to MANETs. This is shown in Figure 3.

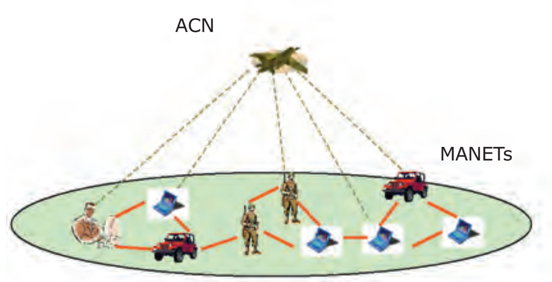

Figure 3. A MANET with ACN backbone

EXPERIMENT ON MANET-ACN CONCEPT

This section describes an experiment initiated by the Future Systems Directorate on the MANET-ACN concept.

Two-tier Communications Network Architecture

The network architecture focuses on two types of wireless networks: intra-cluster networking and inter-cluster networking. Intra-cluster networking concentrates on the connectivity for ground client terminals that are within the air-to-ground communications coverage of an air platform. Inter-cluster networking concentrates on the connectivity of ground client terminals that are from different clusters. It relies on

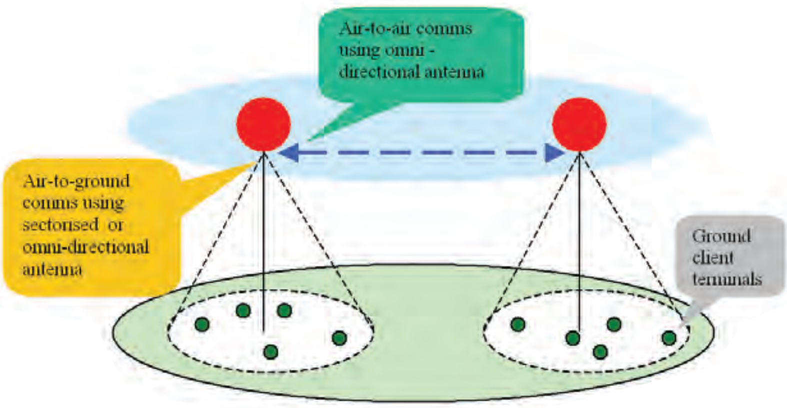

Figure 4. Two-tier communications architecture network configuration

the air-to-air communications backbone radios to form a point-to-point, point-to-multipoint or mesh networks.

Figure 4 shows the two-tier communications architecture with two separate radios to provide the backbone connectivity and end user connections. The two separate radios for air-to-air and air-to-ground communications operate on different frequency bands/channels and thus a higher data throughput performance can be achieved.

An omni-directional antenna is used for the air-to-air communications to provide an all-round coverage. This is necessary since the air platforms can be deployed at any location. For air-to-ground coverage, either sectorised or omni-directional antennas can be used.

MANET Radios

Different commercial off-the-shelf (COTS) MANET radios were tested and assessed by the team for deployment. These radios incorporate various MANET protocols and are based on the IEEE 802.11b/g or 802.11a Wi-Fi standards for physical transmission. A final radio configuration was selected and integrated on the air platform.

Air Platform

The air platform is required to hoist the communications payload to an elevated height. Possible air platforms include unmanned aerial vehicles, remote-controlled airships, blimps or helicopters, and tethered balloons and blimps. For the purpose of the experiment, tethered balloons were used due to their low cost and ease of deployment.

Results and Challenges

Initial trials showed that a data rate of several megabits per second (Mbps) can be delivered on the move with the MANET-ACN concept. Some of the key challenges encountered during the experiment are described below:

• The balloon platform, though relatively easy to deploy, is susceptible to wind conditions. Strong winds can sway the balloon (and the antennas on board) in unpredictable directions, creating havoc for the stability of the wireless links. To overcome this, a bigger balloon was used to provide a larger effective uplift, improving stability. The use of multiple anchor points to hold down the balloon was explored. The team also came up with an innovative method of securing the payload and antenna to minimise movement in strong wind conditions. Lastly, an antenna with a wider beamwidth was used to provide a larger tolerance for movement.

- The antenna radiation patterns will critically affect system performance. For instance, the use of sectorised antennas for the air-to-ground link would provide good coverage for a limited range directly below the balloon platform. On the other hand, the use of omni-directional antennas for the same purpose would provide good performance at further distances, but this comes with a null zone (i.e. no/poor coverage) at certain locations near the balloon. A careful balance needs to be struck in order to deliver optimal performance for the required operational scenario and requirements.

- For local trials, there are limitations on the permissible transmission power as well as the altitude of the tethered balloon. The Infocomm Development Authority of Singapore limits the permissible transmission power of these radios while the Civil Aviation Authority of Singapore limits the permissible altitude of the tethered balloon. There are also policy constraints from the Republic of Singapore Air Force on when airborne platforms can be deployed. The team therefore had to conduct the trials within these limitations. More extensive trials and experiments, both local and overseas, are being planned to further evaluate and improve system performance.

- Because of the long hours of operation under direct sunlight, there is the problem of heat dissipation. Temperatures within the payload increase significantly as heat builds up. This leads to the overheating and consequently the under-performance of some of the COTS components. The payload design had to take these factors into account, through the use of appropriate housing and fans for better air circulation and heat dissipation. The team is currently considering additional means of improving the ventilation of the payload.

CONCLUSION

A MANET, with its inherent dynamic and flexible architecture, demonstrates attractive potential for military applications. It is able to overcome traditional communications limitations through its automatic relaying and self-healing/forming features. Coupled with the ACN concept incorporating one or more airborne platforms, MANETs could be exploited to provide the 3G SAF with unprecedented communications reach and operational flexibility, especially in the low-echelon tactical environment. Other than supporting traditional SAF military roles, MANETs, being "infrastructureless", can also be leveraged for increasingly important functions such as Operations Other Than War, or OOTWA, in which quick deployability is of prime concern.

In the commercial sector, developments in MANETs are still ongoing. Emerging technologies such as Multiple-Input Multiple-Output, or MIMO, and smart antennas can be integrated within a MANET framework for an even more powerful networking experience. Experimentation will be the key to identifying, introducing and assimilating such technologies for transforming SAF into a 3G fighting force.

ANNEX A: MANET ROUTING PROTOCOLS

MANET nodes perform the routing functions themselves. Due to the limited wireless transmission range, the routing generally consists of multiple hops. Therefore, the nodes depend on one another to forward packets to the destinations. The nature of the networks places two fundamental requirements on the routing protocols. First, it has to be distributed. Secondly, since the topology changes are frequent, it should compute multiple, loop-free routes while keeping the communication overheads to a minimum.

Based on route discovery time, MANET routing protocols fall into two general categories:

- Proactive routing protocols
- Reactive routing protocols

There is also a new class of routing protocols known as the hybrid routing protocols, which tries to encompass the advantages of both the proactive and reactive routing protocols.

Proactive Routing Protocols

Proactive MANET protocols are table-driven and will actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, a complete picture of the network is maintained at every single node. There is hence minimal delay in determining the route to be taken. This is especially important for time-critical traffic (Scientific Research Corporation, 2004).

However, a drawback to a proactive MANET of protocol is that the life span of a link is significantly short. This phenomenon is brought about by the increased mobility of the nodes, which will render the routing information in the table invalid quickly. When the routing information becomes invalid quickly, there are many short-lived routes that are being determined and not used before they turn void. Hence, another drawback resulting from the increased mobility is the amount of traffic overhead generated when evaluating these unnecessary routes. This is especially aggravated when the network size increases. The fraction of the total control traffic that consists of actual practical data is further decreased.

Lastly, if the nodes transmit infrequently, most of the routing information is deemed redundant. The nodes, however, continue to expend energy by continually updating these unused entries in their routing tables (Scientific Research Corporation, 2004). As mentioned, energy conservation is very important in a MANET system design. Hence, this excessive expenditure of energy is not desired.

Thus, proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently.

Examples of proactive MANET protocols include:

- Optimised Link State Routing, or OLSR
- Topology Broadcast based on Reverse Path Forwarding, or TBRPF
- Fish-eye State Routing, or FSR
- Destination-Sequenced Distance Vector, or DSDV
- Landmark Routing Protocol, or LANMAR
- Clusterhead Gateway Switch Routing Protocol, or CGSR

Reactive Routing Protocols

Reactive MANET protocols only find a route to the destination node when there is a need to send data. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and destination. This is known as the global flood search, which in turn brings about a significant delay before the packet can be transmitted. It also requires the transmission of a significant amount of control traffic (Scientific Research Corporation, 2004).

Thus, reactive MANET protocols are most suited for networks with high node mobility or where the nodes transmit data infrequently.

Examples of reactive MANET protocols include:

- Ad Hoc On-Demand Distance Vector, or AODV
- Dynamic Source Routing, or DSR
- Temporally Ordered Routing Algorithm, or TORA

Hybrid Routing Protocols

Since proactive and reactive routing protocols each work best in oppositely different scenarios, there is good reason to develop hybrid routing protocols, which use a mix of both proactive and reactive routing protocols. These hybrid protocols can be used to find a balance between the proactive and reactive protocols.

The basic idea behind hybrid routing protocols is to use proactive routing mechanisms in some areas of the network at certain times and reactive routing for the rest of the network. The proactive operations are restricted to a small domain in order to reduce the control overheads and delays. The reactive routing protocols are used for locating nodes outside this domain, as this is more bandwidth-efficient in a constantly changing network.

Examples of hybrid routing protocols include:

- Cornell's Zone Routing Protocol (ZRP)
- Scientific Research Corporation's Wireless Ad hoc Routing Protocol (WARP) - based on ZRP with additional enhancements for Quality of Service, or QoS support (MobileRouteTM)

The most recognised protocol among these is the ZRP. In this protocol, the radius of each node's local routing zone plays an important part in determining the proactive zone. The proactive routing protocol is used to determine the topology within the radius of the node. The reactive routing protocol is then used to locate nodes outside the radius of the node on demand.

The adjustment of the zone radius will allow the protocol to adapt to different MANET environments. A larger radius will favour the proactive routing protocol, optimal for slow-moving nodes or large amounts of traffic (Scientific Research Corporation, 2004). Consequently, a smaller zone radius will favour the reactive protocol, which is optimal for fast-moving nodes or small amounts of traffic.

The WARP, on the other hand, constantly updates all the active routes between the nodes in the network. This is done using routing tables and link-update propagations (De Renesse and Aghvami, 2004). When there are link breakages, the destination may become unreachable. In this scenario, WARP will use reactive protocols to find alternative routes to break the deadlock.

ENDNOTES

1. ARC Communications Research Network. Ad Hoc Networks (http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.cfm).

2. DARPA. Airborne Communications Node (ACN/AJCN). Advanced Technology Office (http://www.darpa.mil/ato/programs/ACN/).

REFERENCES

Corson, S. and Macker, J. (1999). Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. Network Working Group.

De Renesse, R. and Aghvami, A.H. (2004). Formal Verification of Ad-hoc Routing Protocols using SPIN Model Checker. Centre for Telecommunication Research, King's College London, UK.

He, C. (2003) Throughput and delay in Wireless Ad hoc Networks. Final report of EE359 Class Project, Stanford University.

Holland, G & Vaidya, N. (2002). Analysis of TCP Performance over Mobile Ad Hoc Networks. Texas A&M University.

Scientific Research Corporation. (2004). Mobile RouteTM. White Paper.

BIOGRAPHY

Chim Yuen Chong is Programme Manager (C3I). He manages, designs and conducts communications experimentation and exploration for the Singapore Armed Forces (SAF). His role also requires him to identify and assess emerging areas in wireless communications and networking technologies, and support the SAF in integrating these technologies with evolving warfighting concepts. A Public Service Commission Scholar, he graduated with a Master of Engineering from the National University of Singapore in 1997.

Raymond Seah Kwang Wee is Senior Communications Engineer (C3I). He is actively involved in communications experimentation, conducting technical evaluation and engineering assessment of new wireless communications and networking technologies and systems for the 3G SAF. He graduated with a Bachelor of Engineering (Electrical and Electronics Engineering) from the Nanyang Technological University in 2000.

Sim Soon Lian is Project Lead (C3I). He is responsible for the exploration and assessment of emerging wireless communications and networking technologies for the SAF. His work entails the design, conduct and analysis of experiments to evaluate the performance of these technologies and their potential application in the 3G SAF. He graduated from the National University of Singapore in 1999 with a Bachelor of Engineering (Electrical Engineering).

Tan Jia Hui is Communications Engineer (C3I). She is currently involved in the experimentation and exploration of wireless communications and networking technologies for the SAF. She graduated with a Bachelor of Engineering (Electrical and Electronic Engineering) from the Nanyang Technological University in 2005.