MANET Security Issues

Nishu Garg† **R.P.Mahapatra††**

j.i.m.s c.s.Dept C.S.E Dept

Summary
When a routing protocol for manet Networks (mobile and ad hoc networks) does a route discovery, it does not discover the shortest route but the route through which the route request flood traveled faster. In addition, since nodes are moving, a route that was the shortest one at discovery time might stop being so in quite a short period of time. This causes, not only a much bigger end-to-end delay, but also more collisions and faster power consumption. In order to avoid all the performance loss due to these problems, this paper develops a technique to periodically discover shortcuts to the active routes that can be used with any destination vector routing protocol. It also shows
how the same mechanism can be used as a bidirectional route recovery mechanism.[1] We consider the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPSec are not applicable. We look at AODV in detail and develop a security mechanism to protect its routing information. We also briefly discuss whether our techniques would also be applicable to other similar routing protocols and about how a key management scheme could be used in conjunction with the solution that we provide. [2]

Key words:
AODV,I.P,MMN,IETF

1. Introduction

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.

2. Challenges in Ad hoc

The technology of Mobile Ad hoc Networking is somewhat synonymous with Mobile Packet Radio Networking (a term coined via during early military research in the 70's and 80's), Mobile Mesh Networking (a term that appeared in an article in The Economist regarding the structure of future military networks) and Mobile, Multihop, Wireless Networking (perhaps the most accurate term, although a bit cumbersome).
There is current and future need for dynamic ad hoc networking technology. The emerging field of mobile and nomadic computing, with its current emphasis on mobile IP operation, should gradually broaden and require highly-adaptive mobile networking technology to effectively manage multihop, ad hoc network clusters which can operate autonomously or, more than likely, be attached at some point(s) to the fixed Internet. MANET can be established extremely flexibly without any fixed base station in battlefields, military applications, and other emergency and disaster situation. (See Figure 1)[4]

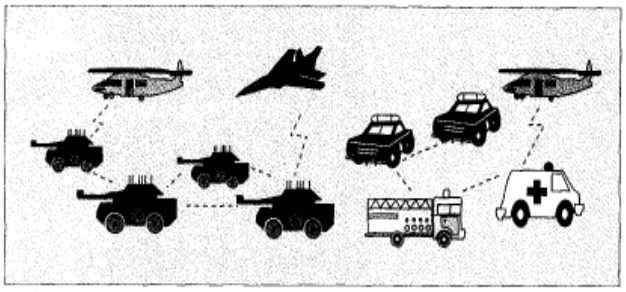

Figure 1. *Example applications of MANETs.*

Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange.
In addition, mesh-based mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures. There are also existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks [1]--many of these networks consist of highly-dynamic autonomous topology segments. Also, the developing technologies of "wearable" computing and communications may provide applications for MANET technology. When properly combined with satellite-based information delivery, MANET technology can provide an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications

Manuscript received August 5, 2009
Manuscript revised August 20, 2009

with survivable, efficient dynamic networking. There are likely other applications for MANET technology which are not presently realized or envisioned by the authors. It is, simply put, improved IP-based networking technology for dynamic, autonomous wireless networks.

3. Characteristics of MANETs

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internet work. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network.
MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omni directional (broadcast), highly- directional (point-to-point), possibly steer able, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

MANETs have several salient characteristics:

1) Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multihop--may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

2) Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions etc.--is often much less than a radio's maximum transmission rate.

One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather than the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently. As the mobile network is often simply an extension of the fixed network infrastructure, mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

3) Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

4) Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches.

4. Goals of IETF Mobile Ad Hoc Network (manet) Working Group

The intent of the newly formed IETF manet working group is to develop a peer-to-peer mobile routing capability in a purely mobile, wireless domain. This capability will exist beyond the fixed network (as supported by traditional IP networking) and beyond the one-hop fringe of the fixed network.
The near-term goal of the manet working group is to standardize one (or more) intra-domain unicast routing protocol(s), and related network-layer support technology which:

* provides for effective operation over a wide range of mobile networking "contexts" (a context is a set of characteristics describing a mobile network and its environment);

* supports traditional, connectionless IP service;

* reacts efficiently to topological changes and traffic demands while maintaining effective routing in a mobile networking context.

5. IP-Layer Mobile Routing

An improved mobile routing capability at the IP layer can provide a benefit similar to the intention of the original

Internet, viz. "an interoperable internetworking capability over a heterogeneous networking infrastructure". In this case, the infrastructure is wireless, rather than hardwired, consisting of multiple wireless technologies, channel access protocols, etc. Improved IP routing and related networking services provide the glue to preserve the integrity of the mobile internetwork segment in this more dynamic environment.
In other words, a real benefit to using IP-level routing in a MANET is to provide network-level consistency for multihop networks composed of nodes using a *mixture* of physical-layer media; i.e. a mixture of what are commonly thought of as subnet technologies. A MANET node principally consists of a router, which may be physically attached to multiple IP hosts (or IP-addressable devices), which has potentially *multiple* wireless interfaces--each interface using a *different* wireless technology. Thus, a MANET node with interfaces using technologies A and B can communicate with any other MANET node possessing an interface with technology A or B. MANET nodes making routing decisions using the IP fabric can intercommunicate using either or both physical-layer topologies simultaneously. As new physical-layer technologies are developed, new device drivers can be written and another physical-layer multihop topology can be seamlessly added to the IP fabric. Likewise, older technologies can easily be dropped. Such is the functionality and architectural flexibility that IP-layer routing can support, which brings with it hardware economies of scale.

5.1. Interaction with Standard IP Routing

In the near term, it is currently envisioned that MANETs will function as *stub* networks, meaning that all traffic carried by MANET nodes will either be sourced or sinked within the MANET because of bandwidth and possibly power constraints, MANETs are not presently envisioned to function as *transit* networks carrying traffic which enters and then leaves the MANET (although this restriction may be removed by subsequent technology advances). This substantially reduces the amount of route advertisement required for interoperation with the existing fixed Internet. For stub operation, routing interoperability in the near term may be achieved using some combination of mechanisms such as MANET-based anycast and mobile IP.
Future interoperability may be achieved using mechanisms other than mobile IP.
Interaction with Standard IP Routing will be greatly facilitated by usage of a common MANET addressing approach by all MANET routing protocols. Development of such an approach is underway which permits routing through a multi-technology fabric, permits multiple hosts per router and ensures long-term interoperability through adherence to the IP addressing architecture. Supporting these features appears only to require identifying host and router interfaces with IP addresses, identifying a router with a separate Router ID, and permitting routers to have multiple wired and wireless interfaces.

5.2. Attacks using modification – False Sequence number

Malicious nodes can cause redirection of network traffic and DoS attacks by altering control message fields.

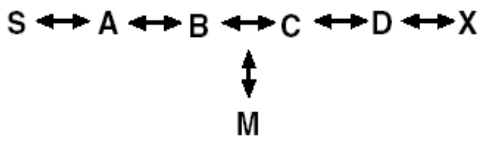

Fig: 2

In AODV, any node may divert traffic through itself by advertising a route to a node with a *destination_sequence_num* greater than the authentic value.

5.3. Attacks using modification – False hop counts, False source routes

AODV uses the hop count field to determine a shortest path Malicious nodes can set hop count to zero. DSR uses source routes in data packets
DoS attack can be launched in DSR by altering the source routes in the packet headers.

Fig: 3

5.4. Attacks using modification – Tunneling

A *tunneling* attack is where two or more nodes may collaborate to encapsulate messages between them.

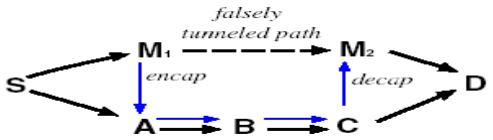

Fig: 4

Similarly, tunneling attacks are also a security threat to *multipath* routing protocol**.**

5.5. Attacks using Impersonation

Spoofing occurs when a node misrepresents its identity in the network.
Forming Loops by Spoofing.

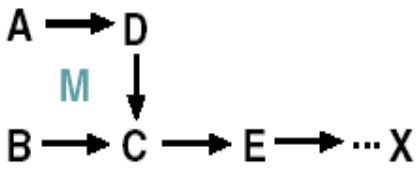

Fig: 5

6. MANET Routing Protocol Performance Issues

To judge the merit of a routing protocol, one needs metrics—both qualitative and quantitative--with which to measure its suitability and performance. These metrics should be *independent* of any given routing protocol.

The following is a list of desirable qualitative properties of MANET routing protocols:

1) Distributed operation: This is an essential property, but it should be stated nonetheless.

2) Loop-freedom: Not required per se in light of certain quantitative measures (i.e. performance criteria), but generally desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL values can bound the problem, but a more structured and well-formed approach is generally desirable as it usually leads to better overall performance.

3) Demand-based operation: Instead of assuming an uniform traffic distribution within the network (and maintaining routing between all nodes at all times), let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done intelligently, it can utilize network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay.

4) Proactive operation: The flip-side of demand-based operation. In certain contexts, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit, proactive operation is desirable in these contexts.

5) Security: Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, eplay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired. This may be somewhat orthogonal to any particular routing protocol approach, e.g. through the application of IP Security techniques.

6) "Sleep" period operation: As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocol through a standardized interface.

7) Unidirectional link support: Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links.
Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, a sufficient number of duplex links exist so that usage of unidirectional links is of limited added value.
However, in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable.

Essential parameters that should be varied include:

1) Network size--measured in the number of nodes

2) Network connectivity--the average degree of a node (i.e. the average number of neighbors of a node)

3) Topological rate of change--the speed with which a network's topology is changing

4) Link capacity--effective link speed measured in bits/second,after accounting for losses due to multiple access, coding, framing etc.

5) Fraction of unidirectional links--how effectively does a protocol perform as a function of the presence of unidirectional links?

6) Traffic patterns--how effective is a protocol in adapting to non-uniform or bursty traffic patterns?

7) Mobility--when, and under what circumstances, is temporal and spatial topological correlation relevant to the performance of a routing protocol? In these cases, what is the most appropriate model for simulating node mobility in a MANET?

8) Fraction and frequency of sleeping nodes--how does a protocol perform in the presence of sleeping and awakening nodes?

A MANET protocol should function effectively over a wide range of networking contexts--from small, collaborative, ad hoc groups to larger mobile, multihop networks. The preceding discussion of characteristics and evaluation metrics somewhat differentiate MANETs from traditional, hardwired, multihop networks. The wireless networking environment is one of scarcity rather than abundance, wherein bandwidth is relatively limited, and energy may be as well.

In summary, the networking opportunities for MANETs are intriguing and the engineering tradeoffs are many and challenging. A diverse set of performance issues requires new protocols for network control.[3]

7. Security Considerations

Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired networks. Existing link-level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level encryption, at the network layer, the most pressing issue is one of inter-router authentication prior to the exchange of network control information. Several levels of authentication ranging from no security (always an option) and simple shared-key approaches, to full public key infrastructure-based authentication mechanisms will be explored by the group. As an adjunct to the working groups efforts, several optional authentication modes may be standardized for use in MANETs.
Security Requirements of Ad-Hoc Network Security Requirements of Ad-Hoc Network are:

- Route signaling can't be spoofed
- Fabricated routing messages can't be injected into the network
- Routing messages can't be altered in transit
- Routing loops can't be formed by through malicious action
- Routes can't be redirected from the shortest path by malicious action
- Unauthorized nodes should be excluded from route computation and discovery.

8. Conclusion

Importance of MANET cannot be denied as the world of computing is getting portable and compact.
Unlike wired networks, MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc.
Security is not a single layer issue but a multilayered issue. It requires a multi fence security solution that provides complete security spanning over the entire protocol stack.The Study of this important issue reveals that security is divided into different directions of the work like secure routing, key exchange, distribution and management, secure architecture, intrusion detection and protection etc.
The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities
As in wired network role definition has been very crucial in security, keeping the same idea in mind we can apply the role based security in MANETs.
Community based solution can be used in role specification. Under this scenario policy distribution techniques, grouping policy, membership management are the major areas to work on.
Agent oriented solutions are very useful in many areas. Similarly MANETs security can also be exploited due to its distributed nature.
Ad Hoc networks pose an interesting problem in networking with dynamic routing and highly insecure working environment Need of Secure, Scalable, Reliable and Efficient algorithms for Key management and Routing.

Passive attacks: Necessary and sufficient condition is cooperation between nodes;
The network performance severely degrade when a large percentage of node do not cooperate in p.f. function;
Then: need to enforce collaboration between nodes.

Active attacks: Routing protocols do not care of security aspect;
Then:
Need of securing routing protocol;
Need of authentication mechanism to prevent spoofing attack;
Need of integrity of routing messages.

References

[1] Manel Guerrero Zapata: "Shortcut Detection and Route Repair in Ad-hoc Networks". In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05), pp. 237-242. March 2005
[2] Manel Guerrero Zapata and N. Asokan: "Securing Ad hoc Routing Protocols". In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pages 1-10. September 2002.
[3] Adamson, B., "Tactical Radio Frequency Communication Requirements for IPng", RFC 1677, August 1994.
[4] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, "A secure routing protocol for Ad-hoc networks," Proc. Of IEEE ICNP, 2002
[5] Zhou L. and Haas Z.J, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, 1999
[6] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", IEEE Networks, Volume 13, Issue 6 1999
[7] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang, "Self-securing Ad Hoc Wireless Networks", IEEE ISCC 2002
[8] Michał Grega, Jakub Jakubiak, Krzysztof Marcisz, Szymon Szott, "Security in Ad Hoc Networks"
[9] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, Security in Mobile Ad hoc Networks: Challenges and Solutions, IEEE Wireless Communications. February 2004. Adam Burg, "Seminar on Ad Hoc Network Specific Attacks"
[10] Tao Lin, "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications", Ph.D. Dissertation, Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 2004.
[11] Yacine Rebahi, Vicente .E Mujica-V, Cyprien Simons and Dorgham Sisalem, SAFE: Securing pAcket Forwarding in ad hoc nEtworks, 5th Workshop on Applications and Services in Wireless Networks, ASWN 2005, June 29th - July 1st, 2005.
[12] M. Ramkumar, N. Memon, KPI: A Security Infrastructure for Trusted Devices, Pre-Conference. Workshop, 12th Annual Network and Distributed System Security Symposium, San Diego, California, 2 February 2005.
[13] L.Buttyan, J.Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM Journal for Mobile Networks, Special Issue on Mobile Ad Hoc Networking, 2002.