MANETs can be characterized by a collection of a large number of nodes that form a network. These nodes are equipped with radio antenna and can directly communicate with others within their broadcast range, nodes outside of their broadcast range are communicated with via intermediate nodes. In this way all nodes can act as both routers and hosts. In both cases all the involved nodes are said to be a part of the network. This is what is seen as a mobile ad-hoc network (Vijayan, Thomas 1880). MANETs, require little to no infrastructure to being communicating. This makes them particularly useful in military operations, disaster relief, and law enforcement scenarios where a quick to deploy network is ideal (Defrawy and Tsudik 1). However if law enforcement or military operations are being conducted in a hostile environment, then steps must be taken to mitigate the amount of information that an adversary could obtain through passive or active attacks. This must be done while maintaining low latency, reliability, recoverability from failure, and security (Nagar 88).

Plenty of research has gone into security systems for MANETs some security systems for them are quite strong already. Less research has gone into anonymity for MANETs. For anonymity factors such as node location and movements, local geography, broadcast range for the nodes, node density etc., plus all the typical anonymity concerns, all are relevant factors that have to be addressed. There are some very robust anonymity routing protocols in existence that do address nearly all of these issues, for this reason this paper isn’t seeking to propose a new anonymous routing protocol. This paper seeks to explore a novel method for improving anonymous routing in MANETs that is unique to MANETs.

The method proposed is adding specialized dummy nodes to a MANET that already employs an anonymous routing protocol. Due to the specialization of the dummy nodes in either software, hardware, or both, they are referred to as arbitrary physical nodes (APN) to differentiate them from their simpler counterparts. This is a topic that has had minimal research focused on it. There are two likely reasons for this: 1. research into MANETs in general is still a new field and 2. the APNs are custom to each anonymity protocol so there has been no formalization for the topic. This paper seeks to begin formalizing APN’s as a research area and show its viability by analyzing its uses and implications for several anonymous routing protocols.

The first routing protocol that is to be analyzed is anonymous on demand routing (ANODR). This is easily the most robust anonymity protocol talked about in this paper. ANODR is a reactive, or on-demand, routing protocol. This means it doesn’t construct routes to the destination until a request for it is made. Typically this means that there is linkability between the persistent identity of the receiver and the data sent to it, by at least the neighboring nodes and the sender. ANODR, however dissociates from this by broadcasting with trapdoor information known only to the receiver(s) (Kong and Hong 293). Before the effects of an APN on a MANET using ANONDR are analyzed, the basics of its functionality will be covered as they relate to how an APN would affect it.

ANONDR can be thought of as using three phases: anonymous route discovery, anonymous route maintenance, and anonymous route forwarding. The route discovery phase can be broken down into the RREQ phase and RREP phase (Nagar and Nadu 90). RREQ starts with the sender locally broadcasting an RREQ packet that has a random nonce as the onion core. Each RREQ forwarder adds a layer of encryption in the RREQ phase, and as its (the RREQ packet) passed along in the RREQ flood the onion is formed. Once the destination receives the RREQ, it initiates the RREP phase. The global trapdoor holds the information secret and the public commitment for the destination. The RREQ onion is used to create the virtual circuit back to the initiator node. Anonymous route maintenance simply recycles routing table entries upon a timeout for each, or when an anomaly is detected such as a link being broken. For anonymous data forwarding a sender wraps their packet using the appropriate outgoing route pseudonym and broadcasts it to its neighbors. Note it is broadcast without specifying a receiver or the sender. Then the local receivers check their route pseudonym table and if there is a match repeat the same procedure, if not, they drop the packet. This system creates a very robust anonymous protocol but one that has a high computational overhead, and one that loads the links in the route discovery phase.

The strengths of ANODR are as follows: Because ANODR dissociates the routing from a member’s identity/pseudonym, an adversary can neither link a member’s identity with their location nor can the adversary follow data flow to its source or destination, and it is highly intrusion tolerant. Even adversaries detecting local wireless broadcasts and transmissions, they can’t infer the number, motion, or identities of the participants. ANODR is intrusion tolerant up to the point where all the forwarding nodes on a route are compromised, until this point unlinkability is maintained.

There are two weaknesses with ANODR that APNs could address. The first is scalability. The RREQ flood in route discovery limits the potential size of the MANET. The other is low network utilization, few people actually in the MANET and fewer actually using it. This paper will address the first weakness when another routing protocol is analyzed and is seen to have a similar issue.

The low utilization issue can be addressed by scattering APNs through the area where the MANET is to be setup. Like onion routing, ANODR does need to have many active participants to ensure that anonymity is strong. If there are few participants traffic analysis becomes significantly easier, and it requires far fewer nodes to be compromised for an adversary to break location privacy and sender, receiver unlinkability. In this case the APNs are functioning solely as dummy nodes. The APNs will generate dummy packets and artificially boost the network utilization. If a scheme can be made to ensure the APNs focus their sending to other dummy nodes, this could reduce some of the overhead on non-dummy nodes. This paper doesn’t explore protocols to make this happen however, and leaves it as an open area of research. An interesting implementation could be allowing it to be known that the MANET is set up with APNs. This would allow the APN to implement a slightly different routing protocol from the rest of the standard nodes. The senders could include slightly more padding and the APN could then include detours in the routing protocol. This would be hugely effective in thwarting an adversary who was seeking to compromise nodes along a certain path. The reason for having the APN do and calculate the detour would be to have push the computational overhead of forwarding to the APNs. One restriction to this is that when setting up the APNs you should set them up in clusters to increase the chances that the detours go through an APN then an arbitrary user node, otherwise its similar to just adding detours to the original protocol.

The costs of adding APNs in this manner are two-fold. These two costs are the simply the costs of using an APN no matter the network. This set up doesn’t incur any anonymity or network weaknesses. The first is a comparatively high implementation cost. The reason I call it comparatively high is that the point of a MANET is being able to quickly set up an infrastructure-less network. The second is maintenance of the APNs. Depending on how long the network is set up and under what conditions, maintenance does have to occur. In the above set up though, no specialized hardware is being used in the APNs and so decreases the likelihood of requiring maintenance disregarding environmental and time factors. ANODR is known to be one of the most robust anonymous routing protocols and given the above analysis unless the owner of the network suspects low network utilization or an attacker that can very quickly compromise nodes there is little need to set up any APNs to aid the network.

The second routing protocol to look at is ALARM. Unlike ANODR, alarm is a proactive routing protocol, this means it doesn’t do route discovery when a node needs to send something. Rather than that, each node actually knows where to send their packets. ALARM, like ANODR isn’t hugely scalable because it also uses network flooding. ALARM, however is far less scalable because ever T seconds all nodes flood the network at the same time with location announcement messages (LAM). These LAMs are from every node to every node and contain the sender’s GPS coordinates and a temporary public key. These are used to create the sending nodes (ones that sent the LAM) temporary pseudonym through which other nodes can send messages to it. For each time period all the nodes, construct a map of the network topology using the info from the LAMs. To send a node first check to see if a receiver is still in the area, then begins sending the data packets using the temporary pseudonym. This systems creates one in which node appearances in the topology can’t be linked to its past and future appearances and it runs without high computational overhead for sending and receiving. This makes fairly resistant to passive attacks but not active attacks and as mentioned above its not highly scalable.

While it is fairly resistant to passive attacks, ALARM nodes do broadcast LAMs and each has a full map of the other nodes locations. It isn’t hugely difficult for an adversary to get access to the location information for each node. Using this along with physical topological information of the area, as well as information from traffic analysis, the adversary can being linking node appearances by predicting where they will move. This is especially true if the physical topology heavily limits movements and there aren’t a large number of nodes in that area. The focus of the following APN implementations if obfuscating or completely hiding node location and/or movement. The implementation after that will discuss the use of an APN to increase the scalability of the network. This won’t discuss implementing APNs to try and mitigate the effect of active attacks as APNs fail to thwart both the Sybil attack and location fraud done by compromised nodes.

One of the more interesting implementation of an APN would be one with a specialized longer range antenna that would act as a router for certain nodes in its broadcast range. This would require implementing a new routing protocol. To summarize it, when a node wants to be hidden within the APNs broadcast range it simply sends a small message with a pseudonym to address it by. When the next time interval passes when nodes broadcast their LAMs, this one won’t and the APN will broadcast its pseudonym if another node wants to address it. The node that wanted to be hidden at this point has cease communication. The communication at this point is completely uni-directional but the node can now move anywhere within the APN’s broadcast range and be completely hidden. If the ALARM protocol is updated to send dummy nodes to the APN when it’s implemented, you end up in a scenario where an adversary can never tell if nodes exist in that area or not. A drawback to this is that the communication is only one way so it’s difficult to affirm whether or not the hidden node(s) have received their message. This makes this set up ideal in an environment with low interference but confirmation of messages is still important but it must occur outside the hidden node directly broadcasting it else it risks losing its complete unobservability. In a military operation setting this could be done through physical signals of soldiers who are being viewed by a surveillance drone or satellite. In a law enforcement setting, physical signals viewed through a scope could work. These are just a few examples, depending on the context other signals could be used and this is only needed if complete unobservability is necessary.

The second implementation is setting up an arbitrary number of single APNs in an area to make it seem more populated. However because location areas are broadcast this isn’t enough, a clever adversary will, after a few round be able to identify APNs from non-APNs. The APNs would then do small amounts of location fraud to make it seem like they are moving. There are two scenarios that can follow from this implementation: its either not enough APNs are set up and the actual user falls within a reduced anonymity set, or unlinkability between appearances at locations remains complete. Extending off this, APNs could go so far as to report phantom nodes by broadcasting spoofed LAMs making it look like there are nodes where no exist. This requires less APNs to be implemented and can be more effective as they can make however many phantom nodes at any location. The downside is that if these phantom nodes form the best route to communicate with another node, the APN has conducted a small DoS on itself. In a real life scenario, however I imagine control messages could be sent to it to prevent it from creating nodes in certain areas. This would effectively mask the movement of any real node and be used as a way to feed false information to an adversary. Note this would only work for temporary ops as under extended traffic analysis an adversary could figure out the phantom nodes from the real ones.

The last APN implementation for obfuscating movement and location information is very similar to the last one. Instead of using single nodes that do location fraud or create phantom nodes, small networks of APNs would be set up where you want to give a slightly larger anonymity set for real users in the area. The APNs in this implementation would have some specialized hardware. Specifically a second smaller antenna to coordinate actions between a group of them. This isn’t totally necessary but it makes it more difficult for an adversary to pick up on their radio transmissions. Essentially a small group spread out APNs would act as a single user, depending on how it wants to show movement a different APN would be sending out the LAM each time. This is less effective than the above implementation but has no chance to not forward messages properly. The two methods can be mixed for increased effectiveness and only a small chance for messages to not be forwarded.

The last APN implementation for ALARM seeks to make the protocol more scalable to large networks. There is actually a fairly straightforward solution already proposed by Defrawy and Tsudik that would fall under the use of an APN. It is essentially assigning a gateway node for each area of the network. LAMs aren’t broadcast outside each area of the network, the gateway node also creates a map of the nodes in its assigned area. Then when a node in one area wants to send to one in a separate area, it first sends a message to the gateway to see if there is a node in the area it wants to send its message. If there is the gateway replies with its pseudonym and the sending node sends as normal, but the request is mapped through the gateway. The only issue with this implementation is that it introduces a single point of failure for inter-area communication.

This method of increasing scalability however, doesn’t apply to the ANODR protocol. The amin reason being is that the gateway needs more information than what ANODR provides to its forwarding nodes and adapting ANODR so it can use a gateway would induce significant anonymity weaknesses that weren’t there before.

In conclusion, using an APN can add significant functionality to a MANET employing an anonymous routing protocol. The main costs come in setting up the APNs and maintaining them if the MANET is to be used for an extended period of time. It seems that APNs work better in pro-active systems where forwarding nodes have more information, else they simply can’t accomplish as much without requiring changes to the network protocol. Further areas of research should be simulating their performance in dynamic settings, further formalizing the syntax used and the boundaries of what does and doesn’t count as an APN, and analyzing more anonymity systems to see what APN solutions could offer them.

Citations

Defrawy, K., & Tsudik, G. (2011). ALARM: Anonymous Location-Aided Routing in Suspicious MANETs.*IEEE Transactions on Mobile Computing IEEE Trans. on Mobile Comput.,* *10*(9), 1345-1358. Retrieved December 6, 2015.

Kong, J., & Hong, X. (n.d.). Anodr. *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing - MobiHoc '03*.

Newman, R., Moskowitz, I., Syverson, P., & Serjantov, A. (n.d.). Metrics for Traffic Analysis Prevention. *Privacy Enhancing Technologies*.

Vargheses, S., & Raja, I. (n.d.). A Survey on Anonymous Routing Protocols in MANET. *RECENT ADVANCES in NETWORKING, VLSI and SIGNAL PROCESSING*.

Vijayan, A., & Thomas, T. (2014). Anonymity, unlinkability and unobservability in mobile ad hoc networks. *2014 International Conference on Communication and Signal Processing*.