Overcoming the Challenge of Security in a Mobile Environment

Ioannis Broustis and Michalis Faloutsos
Department of Computer Science and Engineering
University of California, Riverside
Riverside, CA, 92521
{*broustis, michalis*}*@cs.ucr.edu*

Abstract

The secure operation of ad hoc networks faces the novel challenge of location verification on top of the security challenges that wireline networks face. The novelty lies in the fact that a node can correctly validate who it is, but lie about its location and exploit this to create problems to the network. There are three main factors that make ad hoc networks more vulnerable: (a) nodes can overhear other nodes announcements, (b) nodes can lie about their location, and (c) nodes can avoid detection and isolation by moving. As a result, malicious nodes can fake their position and this way obstruct the routing. In this work, we explain how location and topology related malice can affect the security of wireless ad hoc networks. First, we present the most important attacks that can stem from misuse of location information. Second, we provide an overview of location verification techniques, and security routing approaches. Although several of the current techniques are promising, we conclude that there does not exist a bulletproof approach as of yet.

Keywords: Wireless Ad Hoc Communications, Location Verification, Network Topology, Security.

1 Introduction

Wireless ad hoc networks are more vulnerable to malicious attacks than wireline networks, due to several reasons: (a) the broadcast nature of the medium, which exposes information to a passive listener, (b) the lack of an authoritative certification source, (c) the limited battery supply, which precludes overhead and computational intensive solutions, and finally, (d) the mobility, which makes tracing malicious nodes more difficult. Even though many intrusion detection techniques have been developed for wireline networks, the above major differences of wireless ad hoc networks demand new security approaches.

The dynamically changing topology introduces a new set of security challenges [4]. The main idea here is that a node may verify its true identity, but it can lie about its location. Consequently, it can harm the network by modifying routes, monitoring all information etc. In more detail, the use of the common wireless medium makes ad hoc networks susceptible to both active and passive attacks. In passive attacks, the attacker does not actively harm the network, other than possible not forwarding packets, but it mainly acts as a spy, and determines the weaknesses of the network (e.g. bottleneck points). A passive attacker can enable an active attack, by sending this information to active attackers. In active attacks, the attacker can advertise erroneous topology information, drop or modify packets, fabricate messages or flood the network. Typically, most attacks in either of the above cases. As a consequence, any intrusion detection mechanism requires extensive evidence gathering. A fundamental component of any such solution is a mechanism to verify the location of a node.

As our main contribution, we present an overview of attacks and solutions for network threats that stem from the abuse of location information. First, we explain how the location information and topological aspects of the network can be used by malicious and compromised nodes. In addition, we present the major current mechanisms that atttempt to detect and deter such attacks. We describe the four main node location estimation techniques based on: GPS, Infrared, Ultrasound and RF. We explain why location is difficult to verify and why these methods are vulnerable to attacks. Furthermore, we present the main studies on node positioning and verification of location claims. We describe the metrics that each method uses, their assumptions, and discuss their efficiency. We conclude that there is no mechanism guaranteeing security, and hence more work needs to be done.

The remainder of this paper is organized as follows. In section 2, we provide a categorized overview of the known attacks in wireless ad hoc networks. We present schematically some of them that are related to the network topology and routing. In section 3, we present a comparison of the position verification techniques according to their security vulnerabilities. In section

4, we describe algorithmic solutions, which employ these techniques, so as to secure the claimed location of a node. We also discuss designing issues for secure position-aided ad hoc routing protocols. Finally, section 5 concludes the paper.

2 Ad Hoc Network Attacks

2.1 Background

Our definition of *attack* includes any behavior that causes anomalies to the network functionality. Here we present background knowledge on the various methods that attackers can use to harm the network. Our focus is to relate the nature of the attacks with the topology of the network. These attacks are possible as soon as malicious nodes penetrate the network, by misleading others about their location. Some of those common attacking techniques are [4]:

1. *Fake location:* A node provides misleading information about its location. Hence, other nodes may not think of it as a neighbor, while in fact it is. Also, the node may not lie in the same region, however it can make other nodes believe that it is their neighbor.
2. *Wormhole:* Two attackers create a tunnel that can be secretly used to transmit packets. They both may deceive other nodes about their locations at the same time. As a result, the atackers may be mutually reachable and exchange packets without other nodes being aware about it.

These topology-related attacks can be manifested or enable the following attacks:

1. *Hit and Run*: A node arrives in the neighborhood, transmits malicious content and further dissapears.
2. *Spoofing:* Data or control packets are injected, which have their source addresses modified.
3. *Malicious flooding:* Unusually large amounts of data/control packets are delivered to some target nodes or the whole network.
4. *Packet dropping:* A node deliberately drops data packets that was supposed to forward.
5. *Cache poisoning:* According to the routing protocol nodes may store routing information. With cache poisoning, this information is modified or deleted.

6. *Message fabrication:* Routing information with malicious contents are injected into the network.
7. *Rushing:* An attacker disseminates a malicious control message quickly, to block legitimate messages that arrive later.
8. *Modified paths:* The paths traversed by packets are different than those that the routing protocol would like to establish. The new alternative path may include additional malicious/compromised nodes, which take advantage of the transmitted information.
9. *Blackhole:* All the traffic is redirected erroneously to a specific node that may not forward it. This node advertises itself as having the shortest path to the nodes whose packets it wants to intercept.
10. *Routing loops:* Loops are introduced in the routes. The routing information is modified, so as for packets being sent only to nodes that have forwarded them already, without reaching their final destinations.
11. *Partitioning:* The network is partitioned into sub-nets, each of which cannot communicate with the rest of them. This could be achieved through the use of excess traffic, or erroneous routing information.

All these attacks lead to some sort of Denial of Service (DoS): a node cannot send or receive packets as it would be supposed to.

The core of a secure wireless protocol must achieve several goals, when trying to detect and eliminate misbehaving nodes. The first goal is *authentication*. That is, the identity of each device of the network must be verified. In addition, *confidentiality* is required, to ensure that secret information is never disclosed to unauthorized nodes. Another goal is the *integrity* of the received messages, meaning that they must be delivered unaltered. Finally, *non-repudiation* ensures that a node will accept to perform a particular action. The latter can help in detecting compromised devices.

At this point we should distinguish between malicious and compromised nodes. The former are unauthorized nodes that attempt to bring the network down [5]. Such nodes are deployed to perform a malicious activity, such as the ones described above. On the other hand, a compromised node is initially a legitimate node, which at some point falls under the influence of an attacker. Such attackers may produce legitimate IDs, valid signatures and certificates; thus, detecting such nodes is more difficult.

After mentioning the above goals, we may now classify network nodes into the following three categories:

1. **Trusted:** Nodes that a verifier node can trust. We call *verifier* a node that is used to verify the location of other nodes, which we call *claimants* or *provers*. Trusted nodes are usually pre-specified nodes, for which the verifier assumes that they cannot be malicious.

2. **Certificate-trusted:** Nodes which show a certificate issued by a trusted certification authority of the verifier node.
3. **Non-trusted:** Nodes that do not belong into either of the above categories.

It is possible to have different levels of trust for devices, as well as different levels of security for the services. The former determines the level of access to services, while the latter specifies the required trust level of the nodes.

2.2 Relation to Network Topology

Mobility provides new capabilities to attackers for various reasons. First of all, mobility allows a modification of the routing table of the victim node, simply by moving into the coverage range of it. The attacker may move away once it succeeds and without being traced. Moreover, the mobility of legitimate nodes may help attackers disperse malicious information (epidemic spreading). For example, a malicious node may transmit encrypted malicious data to a legitimate node, and the latter may keep sending this data to other legitimate nodes futher away, thus *spreading* the malicious information. Furthermore, the set of devices within the transmission range of a node keeps changing dynamically. Hence, it becomes harder to successfully authenticate all neighbors. Last but not least, mobile nodes have power and computation limitations. Thus, it becomes difficult for them to access a trusted third party, like a certification authority [11].

In general for securing an ad hoc network, a lot of work has been done towards algorithms that involve private/public key management and authentication. With mobility, new routing protocols have been proposed to protect the network from attacks that modify routing information. The description of these methods is beyond the scope of this paper. In this paper we focus on algorithms for secure location verification of devices within wireless ad hoc networks. We also describe in brief some efforts on verifying claimed positions in wireless networks that involve infrastructure coordinators. This is because some of those ideas are directly applicable to the ad hoc deployment.

2.3 Topology, Routing and Security

The network topology is related to the routing decisions that nodes perform; nodes exchange information to establish these routes, according to routing algorithms. Here we present attacks to routing protocols. Data exchange among nodes can be a potential target for attackers. Attackers can choose a lot of techniques: inject erroneous routing packets, replay old routing packets and distort routing packets. They can further partition or spy on the network, so as to decrease the throughput significantly.

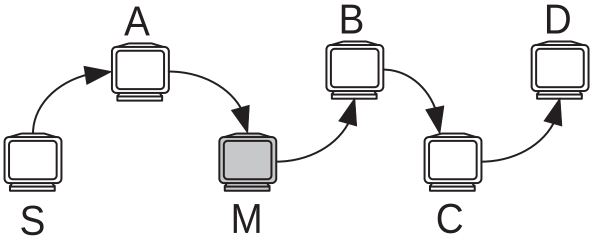

Figure 1: Modified source routes

To begin with, we consider the case of redirection with modified hop counts. This attack takes place when the hop count field of route discovery messages is changed. For example, AODV [12] uses the hop count field to determine the shortest path. In such a case, an attacker may set the hop count field of the RREQ to infinity; this would create routes that tend to not include the malicious node. This attack is most threatening when combined with spoofing [9]. More than that, DSR [13] utilizes routes without any integrity checks. Let's assume the scenario depicted in figure 1. A shortest path exists from S to D, S does not have a route towards D and nodes can hear only their 1-hop neighbors. Node M is the attacker. Node S sends a data packet towards D with the source route S -A - M - B - C - D. When M receives the packet, it may modify the route in the packet header, such as deleting C from it. As a result, when B receives the packet, it tries to send it to D directly; however this is not feasible, since D is not within the range of B. Hence, even though node C is topologically near node B, it cannot be used as a relay for this packet.

Another commonly known attack is the *tunneling* or *wormhole* attack, which we have described before. In figure 2 nodes M_1 and M_2 are the attackers. The dotted line denotes the path that M_1 and M_2 claim to have between them. Node S wants to send a packet to D. When M_1 receives the packet from S, it encapsulates the RREQ and sends it to M_2, through the existing route M_1 - A -B - C - M_2 [9]. When M_2 gets the packet it forwards it to D, as if it had only travelled using the route S - M_1 - M_2 - D. After the route discovery, node D finds out two routes from S; the first is S - A - B - C - D and the second is S - M_1 - M_2 - D, which is shorter. If the RREP is tunneled from M_2 to M_1, then node S will decide that the latter route is more efficient.

Besides the prior two attacks, spoofing can also be used. Assume the scenario of figure 3. Node A can hear B and D, B can hear A and C, D can hear A and C, C can hear B, D and E, M can hear A, B, C and D, and E can hear C and the next hop towards X. Again, M is the attacker. Node M can learn this topology by listening the RREQ/RREP packets. As depicted in figure 3, the attacker may create a routing loop so that none of

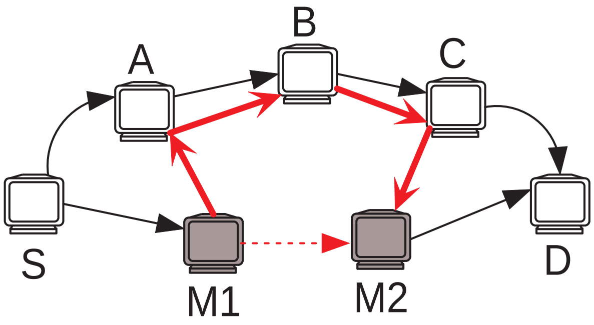

Figure 2: Tunneling or wormhole

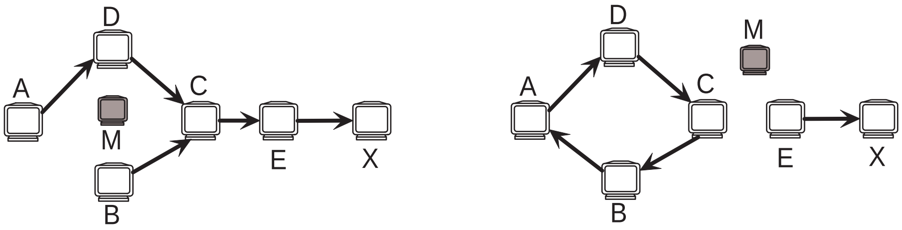

Figure 3: The spoofing attack

the four nodes can reach the destination. It first changes its MAC address to match A's, moves closer to B and out of A's range. It sends an RREP to B that contains a hop count to X that is less than the RREP sent by C. Thus, B will change its route towards X to go via A. Node M further changes its MAC address to match B's, moves closer to C and out of the range of B. It sends an RREP to C with the hop count to X lower than what was advertised by E. Node C then routes to X through B. A routing loop has now been created and node X is unreachable from the four nodes. From this example it becomes obvious that if an attacker knows the topology, it can severely affect the correct functionality of the network.

We described the most common attacks to routing protocols. There have been a number of efforts to address such attacks. Most of these efforts involve either a key management system or a secure routing design or both. In section 4 we present the most valuable of the latter ones. The rest of the efforts deal with secure verification of position claims. We analyze the location estimation techniques in section 3. We further present secure location verification solutions in more detail, in section 4.

3 Position Verification Techniques

In this section, we describe the four common location verification techniques. We discuss their security vulnerabilities and their relative merits.

3.1 Global Positioning System (GPS)

The Global Positioning System is the most widespread positioning system used nowadays. It is based on a set of satellites that provide a three-dimentional position. The accuracy of the system is within 3-5 m. GPS devices have accurate time reference; thus GPS is extensively used for navigation systems in open-air environment. In cannot be used indoor or in dense areas, because of the obstacles and the interference: satellite signals cannot reach the GPS devices.

GPS can provide a device with an estimation of its location. However it does not provide it with estimations for the positions or distances of other devices. As a result, neighbors still need to exchange their positions with each other. However, this is not safe if nodes do not trust each other. On the other hand, if nodes do trust their neighbors, GPS is a very helpful tool in determining their mutual positions. In a non-trusted environment, nodes may still use GPS, but they need to be authorized by a certification authority [7]. This, however, is not always feasible in wireless ad hoc networks.

The current design of the GPS was not intended for security purposes in the first place. As a consequence, it can suffer from many attacks, such as jamming, spoofing, blocking and physical attacks. The most serious attack on GPS is when a malicious attacker uses a GPS satellite simulator. The GPS simulator transmits signals that are stronger than those from the satellites. Using the GPS simulator, the malicious attacker can then feed a GPS receiver with fake GPS messages. In that case the receiver believes that it's physical position is different from the actual one. Since GPS does not have any security protection, the GPS receiver will automatically accept the simulator messages.

This position estimation technology is lightweight and thus it is quite preferable in many cases. However, it requires devices equipped with GPS receivers. Also, some sophisticated software changes could potentially protect the system from many attacks. However, due to the system design, intelligent intrusions will not be detectable.

3.2 Radio (RF)

In Radio Frequency schemes, the nodes may measure either the received RF signal strength, or the signal's *Time-of-Flight (ToF)*. When the fist method is used, the receiver is calculating the distance from the RF sender by measuring the signal strength it received and the strength of the signal that the sender transmitted. The sender declares the power level it used to transmit the packet. Thus, the receiver must trust the sender for the declared power at which the latter sent the RF signal.

This last observation implies that the RF method is vulnerable to attacks. An attacker may transmit the RF signal with higher or lower power than the advertised. In addition, another malicious node could potentially trick two devices into believing that they are closer or further than in reality: it may jam the nodes' communication, or replay their messages in with a different transmission power. Thus, such techniques are not appropriate for non-cooperative scenarios. However, because RF signals travel at the speed of light, attackers cannot decrease the ToF of the signal; they can only increase it. As a result, Radio-based positioning methods that measure the ToF exhibit better security properties than those that measure the signal strength.

3.3 Ultrasound (US)

The basic feature of such systems is that they measure the ToF of the sound signal between two nodes. This technology is often used together with the RF described above. In such cases, the ToF of the RF is ignored, because of the large difference between the speed of light and sound. Hence, the time at which the RF signal is sent and received is used by the pair of nodes as a reference time. In particular, both the US and RF signals are transmitted at the same time. The only action that the receiver has to do is to measure the difference it time of arrival between the two signals.

Ultrasound systems have two main limitations. First, they cannot be used outdoors due to the large amount of interference. Second, they are not animal-friendly. The most dangerous attack on US systems is when the attacker listens the US signal from the sender. It may then transmit this signal to the receiver faster than the original one. This can be accomplished if the attacker uses the RF link to send the US signal. As a consequence the attacker can make nodes think they are closer or further away than in reality. From that point and on, all the attacks examined in section 2 are possible. As we present in section 4, the authors of [3] have come up with a scheme that uses US signals to securely verify location claims.

3.4 Infrared (IR)

The ToF of the IR signal is also measured in such techniques. The sender measures the time needed for the light to propagate to the receiver and all the way back. The measured time denotes the distance between the pair of nodes.

The major disadvantage of this approach is that a direct line-of-sight between the nodes is necessary. Hence, the link between the nodes can be broken if an obstacle is placed. New links can be established by redirecting the existing light beams. This can be accomplished if the source redirects the beam to an intermediate node, which will further transmit the beam to the destination.

The advantage of IR-based methods is that the distance between the two nodes is derived by measuring the speed of light. As a consequence, the malicious node cannot speed-up the signal from one node to the other: it can only increase the measured ToF between the pair of nodes. In other words, the attacker can only enlarge its distance to the honest node, by simply delaying to transmit the IR signal.

3.5 Comparison of the four methods

From the above description, we find that the Radio Frequency methods are the least vulnerable to intrusions, especially in dynamic and heterogeneous environments. This is because with the use of RF it is possible to perform non-line-of-sight position verification. The precision can be very high, i.e. 15 cm with Ultra Wide Band systems at distances of 2 km [14], [15]. In addition, RF systems that use Time of Flight (ToF) are the most effective methods to counter malicious nodes in cooperative methods[1]. However, because they operate with the speed of light, the devices may require some fast-processing special hardware.

4 Location-based Security

In the previous sections, we described the currently known position estimation techniques, as well as their security problems. In this section, we present previous efforts on designing secure ad hoc routing protocols. We also describe the related studies on securing the location estimation of nodes within wireless networks.

4.1 Topology-Related Secure Ad Hoc Routing

During the last decade there has been some effort to provide routing security in wireless ad hoc networks. Some studies reveal and analyze the security vulnerabilities of the most prominant ad hoc routing protocols. Some studies propose security extensions to routing protocols, while others describe new protocols and comprehensive security architectures.

SRP: Papadimitratos and Haas [10] propose the *Secure Routing Protocol (SRP)*, which can discover *legitimate* routes, even in the presence of malicious nodes. However, they assume the existence of a prior security association

---

[1] In cooperative methods, more than one verifiers cooperate to estimate the claimant's location, as we describe later in subsection 4.2

between the communicating nodes. The authors present a number of attack scenarios and describe how their protocol detects those attacks.

SRP uses a route field in RREQ and RREP packets. Nodes in the path include their identifiers to the route field, as the routing packet travels towards its destination. However, a fatal vulnerability of this scheme is revealed in [19]. The author named this attack "Marshall attack": a malicious node M may forward an RREQ without appending its identifier or address to the SRP packet header. In that way, node M could trick the source to use the path that *appears* ideal, while it may not be. As we explained in section 2, the source node will probably decide to use the shortest path. In reality however the chosen path may not be the shortest one, and goes through node M.

From the topological point of view, one may observe that SRP does not *"protect"* the network topology. Route records are exchanged between neighbors, and thus expose the established routes. Revealing the topological information is a crucial disadvantage, especially in military applications.

SAR: Naldurg and Kravets [8] propose SAR, a Secure Aware ad hoc Routing protocol. Nodes are classified according to a trust hierarchy. The authors propose a generalized framework that allows the user to specify the level of routing security. Keys are used for each level of trust and data is routed only through trusted routes. The RREQ messages include security attributes and trust levels defined by the user. The route is built by only those nodes that satisfy the required trust level, while the rest drop the RREQ. Even though the presented ideas are quite interesting, the authors do not develop a specific protocol. They also do not give any details about how a node is assigned a trust value, or how the needed trust level is determined. As a result, it is not clear how SAR can be implemented in practice. In addition, SAR is also vulnerable to the Marshall attack [19]. As a consequence, SAR is not sufficient for high-risk environments, wherein demands on the level of security are more strict.

ARAN: The ARAN (Authenticated Routing for Ad hoc Networks) protocol is introduced in [9]. Sanzgiri et al. propose a pre-deployed security infrastructure; the protocol can be used in the *managed-open environment.* ARAN produces authentication and non-repudiation services using pre-determined cryptographic certificates. This guaranties end-to-end authentication. ARAN participants accept only packets that have been signed with a certified key; this key must be first issued by a trusted authority. However, the apriori deployed infrastructure is very limiting assumption. The protocol has two advantages:

1. It is as efficient as AODV in discovering and maintaining paths.
2. It employs small-size routing packets and small route discovery delays.

A drawback is that the trusted authority is a single point of failure and attack. The authors propose that multiple such authorities can be utilized to address this issue. This solution however probably complicates the whole mechanism, especially when mobility is present.

SPAAR: The Secure Position Aided Ad Hoc Routing Protocol is described in [5]. Carter and Yasinsac claim that SPAAR improves the security and performance, while maintaining location information. Every node maintains a neighbor table that contains the identity and position information of each verified neighbor. It also includes the cryptographic keys for every link with a neighbor. A node will only accept routing messages from a node in its neighbor table. This way, the wormhole and Marshall attacks can be easily detected. With the help of position information, a node may verify its one-hop neighbors before including them into the routing protocol. The disadvantage of this technique is that it assumes nodes with GPS receivers. As we explained in section 3, this introduces other types of attacks. The source must also know the geographic location of the destination. To participate in SPAAR, each node needs to be equipped with a public/private key pair. Nodes maintain a neighbor table, which contains the identity and position information of each verified neighbor. The location data is in the form of the neighbor's most recent position information. It is represented as latitude and longitude coordinates, along with the neighbor's coverage range. Each node periodically broadcasts a table update message to inform its neighbors of its new location coordinates and range. These messages are encrypted with a node group encryption key. The authors claim that their scheme *"provides all the necessary elements to secure routing: Authentication, non-repudiation, confidentiality and integrity"*. However, as we mentioned above, the GPS receivers introduce other vulnerabilities that are not considered by the authors.

Other related studies deal with intrusion detection mechanisms, analysis of cooperation approaches among wireless nodes, cluster-based security architectures, key management, malicious packet drop resistance and many more. Since these studies are not directly related to the network topology, it is beyond the scope of this paper to describe them.

4.2 Secure Location Verification

The previous work that we presented attempts to provide secure routing. There also exist approaches that attempt to secure the location verification of nodes. They try to securely verify the estimated position of nodes within a network. Even though there are numerous studies on node positioning, few of them address security aspects; we identified four related studies [3], [18], [17], [2].

Tao et. al [18] present a wireless indoor LAN location sensing system for security applications. Their system relies on measurements of the received signal strength. Appropriate algorithms are imported, which allow for the detection of malicious nodes. The basic problem is that the system needs to be trained and it seems to be vulnerable to position spoofing attacks.

Waters and Felten [17] describe a scheme for secure distance verification, based on ultrasound and radio signal propagation. They also import cryptography to secure messages against identity fraud. Users carry an external tamper-resistant trusted hardware device, i.e., *smart card.* Processing delay in the smart card is significant, but is assumed constant and publicly known to all participants. This latter assumption, together with their timing accuracy requirements, make their technique seem unrealistic.

In the remainder of this section we focus on two studies for secure location verification. In the first, Sastry et al. describe a technique based on ultrasound [3]. In the second, Capkun et al. [2] propose two novel mechanisms for position verification, called VM *(Verifiable Multilateration)* and VTDOA *(Verifiable Time Difference of Arrival).* They initially present their architecture for WLANs and they further extend it to support ad hoc networks. However, as we discuss later, we conclude that none of the above studies can guarantee total protection. There exist some serious vulnerabilities that these studies do not address.

A. The Echo Protocol: Sastry, Shankar and Wagner [3] focus on solving the in-region verification problem: a set of verifiers V wish to verify whether a claimant P is in a region R of interest. This area could be a stadium, a building or any other physical region. Their purpose is to control the access to resources that are not protected by some physical security, such as wireless networks. Two properties are required to ensure that the protocol is robust:

1. *Robustness:* If V accepts P's claim, then P, or a party colluding with P, has a physical presence in R.

2. *Completeness:* If P is in R then V will accept that P is in R.

The verifier and the claimant must both be able to communicate using RF and US techniques. In addition, the claimant must be able to bound its processing delay. Note that the authors assume that the verifiers are trusted nodes and that they can communicate securely amongst them. The "Echo" protocol has few resource demands and it does not require a setup phase.

If P's claimed location l is not within R, then V can reject the claim immediately. At the nominal start of the algorithm, V sends a nonce to P using RF and P immediately echoes the packet back using US. The verifier V can then calculate how long it should take to hear the echo. This amount consists of the time it takes to reach l using RF, plus the time for the return of the packet using US. If the elapsed time from the initial transmission to reception is more than this amount, V will reject the claim. Otherwise it will accept it. If P is able to return the packet in sufficient time then V is assured that P's distance is less or equal to l. There are two reasons that P does not send the nonce back in time. Either V is more than l units of distance

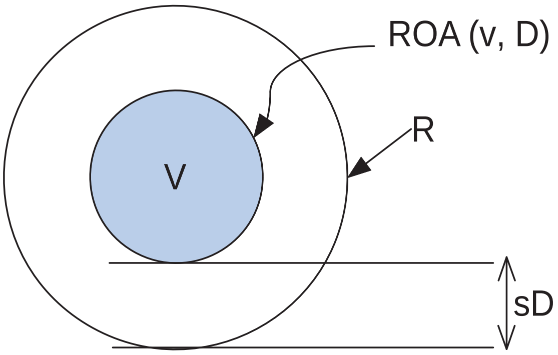

Figure 4: Region Of Acceptance for a verifier V. R is the area of interest, D is the processing delay and s is the speed of sound.

away or P has some processing delay between receiving the RF message and transmitting it back over US.

Ideally, P can receive the RF message and send it out over US instantly. However in reality this is impossible, due to the receiver's processing delay. Let us assume that P can bound its processing delay to some value D_p and make V aware of this value. In that case, V can compute the maximum time that has to wait for getting the response back. An attacker A could be a malicious claimant. A possible attack could be to submit a position claim l at the border of R. At the same time it could advertise an erroneous value for its processing delay to some very large value. However, if the actual value is very low, A could trick V into thinking that it was inside R when in fact it was not. A potential solution is for V to reduce the covered area in which is verifies claims. If P claims a processing delay of $D_p > 0$, then V should reject the claim when the claimed position l is within $D_p s$ of the outside brder, where s is the speed of sound. Hence the authors define the notion of ROA *(Region Of Acceptance)* to be the area where V is sure that it can correctly verify claims. This is depicted in figure 4. ROA(V, D_p) indicates the area where location claims are permitted by V. Node V should engage in the protocol only if l is within ROA(V, D_p).

So far, during the description we assumed that R is circular. However this may not always be true. In any case however, both V and P are assumed to know R. This information helps V compute the ROA(V, 0). In order to support arbitrary shapes of R, the prior procedure is slightly modified. Node P first broadcasts its claimed position l and processing delay D_p to V. If the claimed position is not within ROA(V, D_p), then V will reject the claim. Otherwise, V will broadcast a nonce to P. The latter will echo this packet back over US. V can again time the communication; if it equal or less than the time for the signal to travel out and back (and allowing for processing delay), V will accept the claim.

The authors also provide a security analysis of their protocol [3]. Even though their idea is interesting, they do not explain analytically how they actually address the cases of R having an arbitrary shape.

The main advantage of this approach is twofold. First, no key management or cryptography models are required. Therefore, no special software or hardware is needed for the verifier and the claimant. Second, the protocol does not require time synchronization between V and P. It only requires nodes to be able to compute the elapsed time between sending and receiving the nonce, using RF and US. Obviously, various intrusion detection difficulties arise from this observation, such as the ones mentioned in section 3.

B. Secure Positioning in Wireless Multi-hop Networks: Capkun et al. [2] present mechanisms for securing the position estimation of nodes within wireless networks. They address both cases of WLANs and Ad hoc (Multi-hop) networks. Here we focus only on the part of the work on ad hoc deployments. The proposed mechanisms aim to enable the network nodes to detect the modifications of the network topology. As mentioned earlier, the author makes use of Verifiable Multilateration[2] (VM) and of Verifiable Time Difference of Arrival (VTDOA). Nodes are not equipped with GPS receivers, however they have other distance-measuring capabilities.

Three major assumptions on this work can lead to prolonged discussions. First, the authors assume that besides the communicating nodes, in the same geographical region there *may* exist a number of landmarks. Nodes are assumed to be able to measure the distances with their neighbors, as well as their distances from potential landmarks. This assumption however is later relaxed. The distance computation can take place by measuring the round trip ToF of signal. Second, the network is assumed to be operated by a central authority. This authority can be online or offline - services of this authority can or cannot be reached by via the network respectively. In any case, the authority controls the network membership and assigns a unique identity to each node. Third, each node is capable of generating symmetric cryptographic keys *to accomplish any task required to secure its communications.* This latter assumption implies that a node can agree on cryptographic protocols with other nodes. The author claims that this method can address many of potential topology attacks described in section 2.

a. VM and VTDOA: Verifiable Multilateration is another technique for determining the position of a node from a set of a reference points, whose positions are known. Each reference point measures its distance from the node. The measured distances are then gathered by the authority. The position of the node is further calculated *(multilateration)* by computing the intersection point of the circles centered at the reference points. The radius of each circle is equal to the measured distances. In section 2, we described the main distance estimation mechanisms and their vulnerabilities. Multi-

---

[2] We explain them below

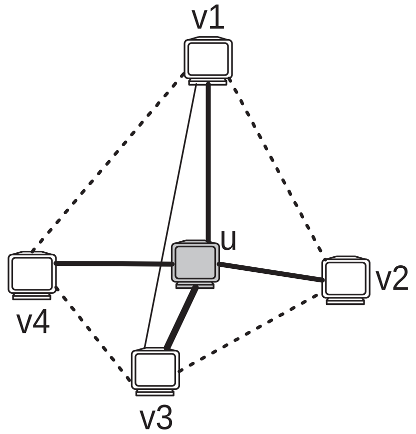

Figure 5: Verifiable Multilateration

lateration is as vulnerable as these methods, since it relies on those distance estimation techniques. The multilateration process is performed by a set of verifiers. The number of required verifiers depends on dimensionality: if we want the claimant's location in two dimensions, three verifiers are needed. For $3-D$ coordinates, we need four of them. Each verifier obtains an upper bound on its distance from the claimant. The verifiers further perform *multilateration* with the obtained bounds and calculate the claimant's location. A representative example is shown in figure 5. Verifiers v_1, v_2, v_3 and v_4 can verify the position of node u in three dimensions. Node u must be placed within the triangular pyramid formed by the verifiers. Similarly, verifiers u_2, u_5 and u_6 can verify the position of node z in two dimensions.

Similarly, VTDOA uses Time Difference Of Arrival to locate mobile devices. TDOA is the process of positioning a source of signal by finding the intersection of multiple hyperboloids. It is based on the time difference of arrival between the signal reception at multiple verifiers. VTDOA utilizes TDOA together with ToF distance estimation. The main advantage of this method is that the claimant cannot trick the verifiers easily about its location. This is because verifiers determine the location passively, by receiving a single signal sent by the claimant. This however is true when the claimant has an omni-directional antenna. Note that in the case of directional antennas, the claimant could send the signal to each of the verifiers separately, with a time shift. As a result, it could fool verifiers about its actual location.

b. Using landmarks: In this approach, node positions are determined by a set of landmark stations with known positions. This set is trusted by the central authority. Landmarks are placed in an organized manner and know their positions. Moreover, they can communicate mutually (one-hop) and they have access to the network authority. The number of landmarks needed to cover a region depends o their power range. Typically, if three landmarks

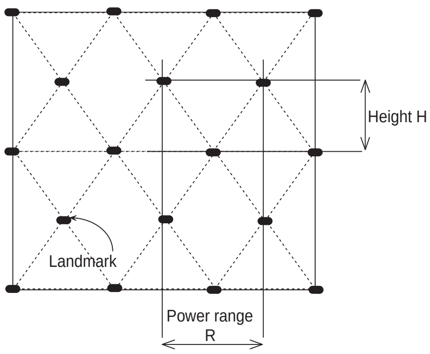

Figure 6: Secure positioning using landmark stations

are mutually reachable, they will be able to verify locations within their triangle. Hence, the optimal way is to place them so that they form regular triangles with sides equal to their power ranges. It is easy to prove that the number of landmarks needed in an $L * L$ region is $[2L/R + 3][L/H + 1]/2$, where R is the power range and H is the height of the triangle. This is clearly depicted in figure 6.

This scheme provides high security, if we assume landmarks to be intrusion-free. Actually, the security of this scheme is based on the security of Verifiable trilateration and VTDOA. Also, since the node positions are determined independently, the scheme is resistant from malicious and compromised intruders.

c. Secure Distributed Positioning: In many realistic cases, landmark stations will probably be absent in the region of consideration. For this reason, the Basic Distance Verification (BDV) mechanism is also proposed [2]. BDV is based on verifiable trilateration. The verifier V performs basic verification of the distance to the claimant P, by forming with its neighbors all verification triangles within P is present.

Node V calculates its distances to its neighbors and to P, and requests the distances measured by its neighbors. These distances are measured from each neighbor V, towards the neighbor V nodes and the claimant P. V further decides if P is present within the triangles. If all distance verifications result in the same distance, then V will accept the location of P. Otherwise it will assume that there is an attack. Upon detection of the attack, V will either report it to the central authority or will try to estimate locally which neighbor V will inform the authority.

The efficiency of BDV depends on the number of the formed triangles and on their mutual dependence. Obviously, if one of the verifiers is compromised and cooperates with P, then P will be able to trick other verifiers about its location. More specifically, if the claimant P is compromised, it may enlarge its distance to a claimant u. The claimant is aided by a malicious node, which enlarges one of the distances between the verifiers. As a consequence, the distances between verifiers are now consistent with the enlarged distance.

In a second scenario, an attacker controlling two malicious nodes can perform the same attack. It is sufficient to enlarge the distance between the verifier and the claimant, as well as the distance between two verifiers.

This work is very interesting, since it addresses the secure position verification through VM and VTDOA. The author shows through simulations that the network density is an important factor for the security of positioning systems. In particular, secure positioning in ad hoc networks requires higher node density. Some assumptions however could be relaxed. Specifically, since ad hoc network topologies are assumed, the notion of the central authority is not necessary. One can argue that the central authority will be absent in most distributed deployments. This assumption of course does not modify the importance and the validity of this work; as we described above, the central authority only contacts V nodes to gather intrusion detections and multilateration measurements. It does not perform any administrative roles. Perhaps replacing it with one amongst the verifiers would be beneficial. In addition, the proposed mechanism could potentially avoid including the landmarks. In most cases, landmark deployment is not feasible and probably more expensive to deploy and maintain. On the other hand, their existence can further increase the resistance of secure positioning algorithms to attacks.

5 Discussion and Conclusions

In this paper we showed how mobility enables attackers to intrude and harm a wireless ad hoc network. Mobility creates numerous security concerns, since moving attackers are much more difficult to identify. We presented the most important efforts to address topology-related attacks. After showing the vulnerabilities of each technique, we conclude that currently there is no complete solution for these problems. The methodologies that were presented in this paper are significant and can deal effectively with most of the currently known attacks. However, malicious users invent new intelligent mechanisms to attack the network. This is why making the location verification methods more secure is a hot research subject: more effort is needed to design better schemes, for detecting and containing such malicious actions.

References

[1] S. Capkun, J. P. Hubaux and M. Jakobsson, "Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks", EPFL-IC Technical report no. IC/2004/10.

[2] S. Capkun et. al, "Location Verification And Key Management In Wireless Networks", MSc thesis, University of Split, Croatia, EPFL 2004.

[3] N. Sastry, U. Shankar and D. Wagner, "Secure Verification of Location Claims", Report No. UCB//CSD-03-1245, EECS, University of California, Berkeley.

[4] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", Proceedings of the 1st ACM workshop on Security of Ad Hoc and Sensor Networks, 2003.

[5] S. Carter and A. Yasinsac, "Secure Position Aided Ad hoc Routing Protocol", In Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), November 2002.

[6] J. Y. Choi, "Security problems for ad hoc routing protocols", Technical report on security and cryptography, Dept. of Computer Science, Indiana University at Bloomington.

[7] G. Avoine and S. Vaudenay, "Fair Exchange with Guardian Angels" In Proceedings of the International Workshop on Information Security Applications (WISA), Lecture Notes in Computer Science, vol. 2908, pp.188-202, Springer-Verlag, August 2003.

[8] S. Yi, P. Naldurg, R.Kravets, "A security aware ad hoc routing protocol for wireless networks", 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), 2002.

[10] P. Papadimitratos, Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks", SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[11] M. Jakobsson, S. Wetzel, B. Yener, Stealth Attacks on Ad-Hoc Wireless Networks, IEEE VTC 03.

[12] Charles E. Perkins and Elizabeth M. Royer, "Ad hoc On-Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[13] D. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", in Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.

[14] R. S. Fontana, "Experimental Results from an Ultra Wideband Precision Geolocation System", in Ultra Wideband Short-Pulse Electromagnetics, May 2000.

[15] R. S. Fontana, E. Richley and J. Barney, "Commercialization of an Ultra Wideband Precision Asset Location System", in IEEE Conference on Ultra Wideband Systems and Technologies, November 2003.

[16] S. Brands and D. Chaum, "Distance-bounding protocols", in Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 344-359, Springer-Verlag, NY. 1994.

[17] B. Waters and E. Felten, "Proving the Location of Tamper-Resistant Devices", Technical report, Princeton University.

[18] P. Tao, A. Rudys, A.M. Ladd and D.S. Wallash, "Wireless LAN location-sensing for security applications", Proceedings of the ACM Workshop on Wireless Security (WiSe), pp.11-20, ACM Press, 2003.

[19] J. Marshall, "An Analysis of SRP for Mobile Ad Hoc Networks", in Proceedings og the 4th International Conference on Mobile Computing and Networking, Dallas, USA 1998.