Overcoming the Challenge of Security in a Mobile Environment

Ioannis Broustis, Michalis Faloutsos and Srikanth Krishnamurthy
Department of Computer Science and Engineering
University of California, Riverside, CA, 92521
{*broustis, michalis, krish*}@*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 security routing approaches. Although several of the current techniques are promising, we conclude that there does not exist a bulletproof approach as of yet.**

***Index Terms*—Wireless Ad Hoc Communications, Location Verification, Network Topology, Security.**

I. 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 can be categorized into 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 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 present how attacks are related to the network topology and routing. In section 3, we describe algorithmic solutions, which employ location verification techniques, so as to secure the claimed location of a node. Finally, in section 4 we conclude the paper.

1-4244-0198-4/06/$20.00 ©2006 IEEE

II. Topology-Related Attacks

Our definition of *attack* includes any behavior that causes anomalies to the network functionality. Our focus is to relate the nature of the attacks to the topology of the network. These attacks are possible as soon as malicious nodes penetrate the network, by misleading others about their location.

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.

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 the network, so as to decrease the throughput significantly.

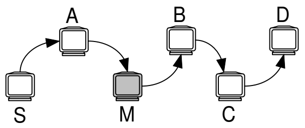

Fig. 1. Modified source routes

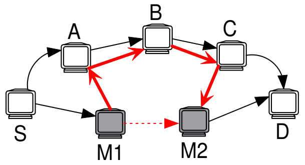

Fig. 2. Tunneling or wormhole

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. 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

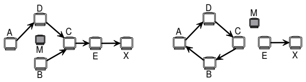

Fig. 3. The spoofing attack

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 to the RREQ/RREP packets. As depicted in figure 3, the attacker may create a routing loop so that none of 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.

III. Location-based Security

In this section, we describe the related studies on securing the location estimation of nodes within wireless networks. The following approaches attempt 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. If V accepts P's claim, then P, or a party colluding with P, has a physical presence in R. 2. 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 RadioFrequency (RF) and Ultrasound (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

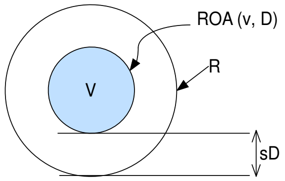

Fig. 4. Region Of Acceptance for a verifier V. R is the area of interest, D is the processing delay and s is the speed of sound.

the nonce back in time. Either V is more than l units of distance 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 border, 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.

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[1] (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 to 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 (*Time of Flight*) 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 may or may not be reached by via the network. 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.

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

[1] We explain these below

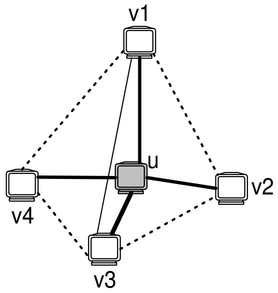

Fig. 5. Verifiable Multilateration

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. 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 on their power range. Typically, if three landmarks 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.

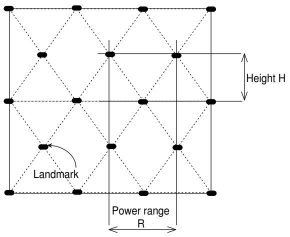

Fig. 6. Secure positioning using landmark stations

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.

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 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 detection and multilateration measurements. It does not perform any administrative role. Perhaps having one of the verifiers perform the central authority's duties 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.

IV. 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. 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 many 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”, Security of Ad Hoc and Sensor Networks, 2003.

[5] S. Carter and A. Yasinsac, ”Secure Position Aided Ad hoc Routing Protocol”, 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”, 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”, SCI 2002.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E.M. Belding-Royer, ”A secure routing protocol for ad hoc networks”, ICNP 2002.

[10] P. Papadimitratos, Z. J. Haas, ”Secure Routing for Mobile Ad hoc Networks”, CNDS 2002.

[11] M. Jakobsson, S. Wetzel, B. Yener, tealth Attacks on Ad-Hoc Wireless Networks IEEE VTC 3.

[12] Charles E. Perkins and Elizabeth M. Royer, ”Ad hoc On-Demand Distance Vector Routing”, 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”, WiSe 2003.

[19] J. Marshall, ”An Analysis of SRP for Mobile Ad Hoc Networks”, Mobile Computing and Networking, Dallas, USA 1998.