DISCOVERY AND VERIFICATION OF NEIGHBOR POSITIONS IN MOBILE AD HOC NETWORKS

1P. Deepika, 2A. Ramesh,
1M.Tech. Student, Dept. of Computer Science and Engineering, SLC'S Institute of Engineering and Technology, Hyderabad.
2Associate Professor, Dept. of Computer Science and Engineering, SLC'S Institute of Engineering and Technology, Hyderabad.

Abstract: The position of their neighbors is required for all ad hoc networking protocols and location-aware services as their number is increasing day after day. However, adversarial nodes can be easily abused or disrupted by such a process. Verification of neighbor positions presents challenges in absence of a priori trusted nodes, the discovery have been scarcely investigated in the literature. In this paper, the open issues of fully distributed co-operative solution which is robust are proposed. This approach is robust and adversary to independent and colluding issues and could be only impaired by an overwhelming presence of adversaries. The results offered in this paper show that our protocol could frustrate more than 99 percent of the assail for the best possible conditions of the adversaries and have minimal false positive rates.


I. INTRODUCTION

For a wide range of protocols and applications where knowledge of the position of the participating nodes is required, location awareness has become an asset in mobile systems. In spontaneous networks, where geographic routing is used, the services that build on the availability of neighbor position information are data gathering in sensor networks, location-specific services for handheld devices, movement coordination among autonomous robotic nodes and traffic monitoring or danger warning in vehicular networks are examples.

Figure 1: Structure of MANET.

The important issue in mobile networks is the correctness of node locations and it becomes particularly challenging in the presence of adversaries aiming at harming the system. A solution is needed to overcome these cases. The solutions needed are something like to verify the positions of their neighbors and to detect adversarial nodes announcing false locations and to correctly establish their location in spite of attacks feeding false location information and so on. In this paper, we focused on the formal aspect, hereinafter referred to as neighbor position verification (NPV for short). We specifically dealt with a mobile ad hoc network, where the location data must be obtained through node-to node communication and an invasive infrastructure is not present. Since mobile ad hoc network leaves the door open for adversarial nodes to misuse or disrupt the location-based services this scenario is of particular interest. For instance, by marketing fake positions, attracting network traffic, adversaries can bias geographic routing or data gathering processes, and then eavesdropping or discarding it. Similarly, counterfeit positions can grant adversaries unauthorized access to location-reliant services, let vehicles give up road tolls, disrupt vehicular traffic or endanger drivers and passengers. In this framework, in absence of trusted nodes, the challenge is to perform a completely dispersed, lightweight NPV system that enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness. The following are the features of the NPV protocol that we proposed. It had been designed for impulsive ad hoc environments and as such, it does not rely on the occurrence of a trusted communications or of a priori reliable nodes; it leverages support but allows a node to perform all verification procedures separately. This approach has no need for lengthy communications, examples to arrive at consent among numerous nodes, making our scheme suitable for both high mobility and low environments; it is hasty, meaning that it can be performed by any node, at any point in time, without previous knowledge of the neighborhood. It is robust to independent and colluding adversaries; it is frivolous, as it creates low overhead traffic. In addition, our NPV scheme is well-suited with state of the art safety architectures, counting the ones that have been proposed for vehicular networks [1], [2], that represent a likely deployment environment for NPV. The rest of the paper is ordered as follows: In Section 2, we appraise previous works, prominence the novelty of our result. In Section 3, we describe the system model, the communication protocol, the purposes of the authentication procedure and our major results are outlined in Section 4. Finally, we provide a recital
evaluation of the protocol in a vehicular scenario and draw conclusions in Section 5.

II. PREVIOUS WORK
Significant developments took place over the past few years in the area of vehicular communication (VC) systems. Now, it is well-understood in the community that security and protection of private user information are a prerequisite for the deployment of the technology. This is so exactly because the benefits of VC systems, with the mission to enhance transportation safety and efficiency, are at stake. Without the integration of strong and practical security and privacy enhancing mechanisms, VC systems could be disrupted or disabled even by relatively unsophisticated attackers. We address this problem within the SeVeCom project, having developed a security architecture that provides a comprehensive and practical solution. We present our results in a set of two papers in this issue. In this first one, we analyze threats and types of adversaries; we identify security and privacy requirements, and present a spectrum of mechanisms to secure VC systems. We provide a solution that can be quickly adopted and deployed. Our progress towards implementation of our architecture, along with results on the performance of the secure VC system, is presented in the second paper. We conclude with an investigation, based on current results, of upcoming elements to be integrated in our secure VC architecture.

Increasing numbers of mobile computing devices, user-portable, or embedded in vehicles, cargo containers, or the physical space, need to be aware of their location in order to provide a wide range of commercial services. Most often, mobile devices obtain their own location with the help of Global Navigation Satellite Systems (GNSS), integrating, for example, a Global Positioning System (GPS) receiver. Nonetheless, an adversary can compromise location-aware applications by attacking the GNSS-based positioning: It can forge navigation messages and mislead the receiver into calculating a fake location. In this paper, we analyze this vulnerability and propose and evaluate the effectiveness of countermeasures. First, we consider replay attacks, which can be effective even in the presence of future cryptographic GNSS protection mechanisms. Then, we propose and analyze methods that allow GNSS receivers to detect the reception of signals generated by an adversary, and then reject fake locations calculated because of the attack. We consider three diverse defense mechanisms, all based on knowledge, in particular, own location, time, and Doppler shift, receivers can obtain prior to the onset of an attack. We find that inertial mechanisms that estimate location can be defeated relatively easy. This is equally true for the mechanism that relies on clock readings from off-the shelf devices; as a result, highly stable clocks could be needed. On the other hand, our Doppler Shift Test can be effective without any specialized hardware, and it can be applied to existing devices.

In this paper, we address the problem of robustly estimating the position of randomly deployed nodes of a wireless sensor network (WSN), in the presence of security threats. We propose a range-independent localization algorithm called high-resolution range-independent localization (HiRLoC) that allows sensors to passively determine their location with high resolution, without increasing the number of reference points, or the complexity of the hardware of each reference point. In HiRLoC, sensors determine their location based on the intersection of the areas covered by the beacons transmitted by multiple reference points. By combining the communication range constraints imposed by the physical medium with computationally efficient cryptographic primitives that secure the beacon transmissions, we show that HiRLoC is robust against known attacks on WSN, such as the wormhole attack, the Sybil attack, and compromise of network entities. Finally, our performance evaluation shows that HiRLoC leads to a significant improvement in localization accuracy compared with state-of-the-art range independent localization schemes, while requiring fewer reference points.

Wireless ad hoc networks are envisioned to be randomly deployed in versatile and potentially hostile environments. Hence, providing secure and uninterrupted communication between the un-tethered network nodes becomes a critical problem. In this paper, we investigate the wormhole attack in wireless ad hoc networks, an attack that can disrupt vital network functions such as routing. In the wormhole attack, the adversary establishes a low-latency unidirectional or bi-directional link, such as a wired or long-range wireless link, between two points in the network that are not within communication range of each other. The attacker then records one or more messages at one end of the link, tunnels them via the link to the other end, and replays them into the network in a timely manner. The wormhole attack is easily implemented and particularly challenging to detect, since it does not require breach of the authenticity and confidentiality of communication, or the compromise of any host. We present a graph theoretic framework for modeling wormhole links and derive the necessary and sufficient conditions for detecting and defending against wormhole attacks. Based on our framework, we show that any candidate solution preventing wormholes should construct a communication graph that is a sub graph of the geometric graph defined by the radio range of the network nodes. Making use of our framework, we propose a cryptographic mechanism based on local broadcast keys in order to prevent wormholes. Our solution does not need time synchronization or time measurement, requires only a small fraction of the nodes to know their location, and is decentralized.
Hence, it is suitable for networks with the most stringent constraints such as sensor networks. Finally, we believe our work is the first to provide an analytical evaluation in terms of probabilities of the extent to which a method prevents wormholes. Localization in the presence of malicious beacon nodes is an important problem in wireless networks. Although significant progress has been made on this problem, some fundamental theoretical questions still remain unanswered: in the presence of malicious beacon nodes, what are the necessary and sufficient conditions to guarantee a bounded error during 2-dimensional location estimation? Under these necessary and sufficient conditions, what class of localization algorithms can provide that error bound? In this paper, we try to answer these questions. Specifically, we show that, when the number of malicious beacons is greater than or equal to some threshold, there is no localization algorithm that can have a bounded error. Furthermore, when the number of malicious beacons is below that threshold, we identify a class of localization algorithms that can ensure that the localization error is bounded. We also outline two algorithms in this class, one of which is guaranteed to finish in polynomial time (in the number of beacons providing information) in the worst case, while the other is based on a heuristic and is practically efficient.

III. SYSTEM ANALYSIS
The correctness of node locations is therefore an all important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. In these cases, we need solutions that let nodes 1) correctly establish their location in spite of attacks feeding false location information, and 2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations. Secure neighbor discovery (SND) deals with the identification of nodes with which a communication link can be established or that are within a given distance. SND is only a step toward the solution we are after: simply put, an adversarial node could be securely discovered as neighbor and be indeed a neighbor (within some SND range), but it could still cheat about its position within the same range. RF signal doesn’t support for to discover the neighbor position.

Although the literature carries a multitude of ad hoc security protocols addressing a number of problems related to NPV, there are no lightweight, robust solutions to NPV that can operate autonomously in an open, ephemeral environment, without relying on trusted nodes. In this paper, we focus on the latter aspect, hereinafter referred to as neighbor position verification (NPV for short). Specifically, we deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication.
suitable for both low- and high mobility environments. It is reactive, meaning that it can be executed by any node, at any point in time, without prior knowledge of the neighborhood. It is robust against independent and colluding adversaries. It is lightweight, as it generates low overhead traffic.

IV. SYSTEM IMPLEMENTATION

In the POLL message Sending; the verifier starts the protocol by broadcasting a POLL whose transmission time is stores locally. The POLL is anonymous, since it does not carry the identity of the verifier, it is transmitted employing a fresh, software-generated MAC address, and it contains a public key K0S taken from S’s pool of anonymous one-time use keys that do not allow neighbors to map the key onto a specific node. We stress that keeping the identity of the verifier hidden is important in order to make our NPV robust to attacks. Since a source address has to be included in the MAC-layer header of the message, a fresh, software-generated MAC address is needed.

In Position Verification, once the message exchange is concluded, verifier can decrypt the received data and acquire the position of all neighbors that participated in the protocol. The verifier also knows the transmission time of its POLL and learns that of all subsequent REPLY messages, as well as the corresponding reception times recorded by the recipients of such broadcasts. Applying a ToF based technique; verifier thus computes its distance from each communication neighbor, as well as the distances between all neighbor pairs sharing a link.

In The Direct Symmetry Test (DST), verifier verifies the direct links with its communication neighbors. To this end, it checks whether reciprocal ToF-derived distances are consistent with each other, with the position advertised by the neighbor, and 3) with a proximity range. The latter corresponds to the maximum nominal transmission range, and upper bounds the distance at which two nodes can communicate.

In the Cross-Symmetry Test (CST), the CST ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, i.e., for which ToF-derived mutual distances are available. The CST verifies the symmetry of the reciprocal distances, their consistency with the positions declared by the nodes, and with the proximity range. For each neighbor, verifier maintains a link counter and a mismatch counts. The former is incremented at every new crosscheck on neighbor, and records the number of links between neighbors and other neighbors of verifier.

In the Multi Lateration Test (MLT), it ignores nodes already tagged as faulty or unverifiable and looks for suspect neighbors in WWS. For each neighbor that did not notify about a link reported by another node a curve is computed and added to the set ILX. Such a curve is the locus of points that can generate a transmission whose Time Difference of Arrival (TDoA) at verifier and neighbor matches that measured by the two nodes.

V. CONCLUSION

We presented a distributed solution for NPV, which allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes. Our analysis showed that our protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighborhood of the verifier. Simulation results confirm that our solution is effective in identifying nodes advertising false positions, while keeping the probability of false positives low. Only an overwhelming presence of colluding adversaries in the neighborhood of the verifier, or the unlikely presence of fully collinear network topologies, can degrade the effectiveness of our NPV. Future work will aim at integrating the NPV protocol in higher layer protocols, as well as at extending it to a proactive paradigm, useful in presence of applications that need each node to constantly verify the position of its neighbors.

VI. ACKNOWLEDGMENT

I would like to express my gratitude to all the people behind the screen who have helped me transform an idea into a real time application. I would like to express my heart-felt gratitude to my parents without whom I would not have been privileged to achieve and fulfill my dreams. A special thanks to the Secretary, T. Satyanarayana, for having founded such an esteemed institution.

I would like to thank Dr. C. Sri Ram, Principal, SLC’s IET, for his guidance and help. His insight during the course of my research and regular guidance were invaluable to me.

I profoundly thank Prof. T. Venkata Ramana, Head of the Department of Computer Science and Engineering (CSE), for providing right suggestions at every phase of the development of our project.

REFERENCES


