A NEW AUTHENTICATION MECHANISM FOR NPV IN MOBILE AD HOC NETWORKS

[1]S.Radhika, [2]M.Sumathi
[1]Research Scholar, Department of Computer Science, Mahendra Arts and Science College, Kalippatti
[2]Assistant professor, Department of Computer Science, Mahendra Arts and Science College, Kalippatti

Abstract: In a mobile ad hoc network without knowing neighbor node position which makes a chance to attackers to easily enter into the network. A growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbors. However, such a process can be easily abused or disrupted by adversarial nodes. In absence of a priori trusted nodes, the discovery and verification of neighbor positions presents challenges that have been scarcely investigated in the literature.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, First Correctly establish their location in spite of attacks feeding false location information, and Second Verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations. Routes may be disconnected due to dynamic movement of nodes.such networks are more vulnerable to both internal and external attacks due to presence of adversarial nodes.We introduce "Neighbor position verification"(NPV), a routing protocol designed to protect the network from adversary nodes by verifying the position of neighbor nodes to improve security, efficiency, and performance in MANET routing.

1. INTRODUCTION

Opposed to the infrastructure wireless networks where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET is a kind of wireless ad hoc network. It is a self-configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move haphazardly and organize themselves arbitrarily. In other words, ad hoc network do not rely on any fixed infrastructure (i.e. the mobile ad hoc network is infrastructure less wireless network. The Communication in MANET is take place by using multi-hop paths. Including the ones that have been proposed for vehicular networks which represent a likely deployment environment for NPV. The details of the NPV protocol and of verification tests are then presented and the resilience of our solution to different attacks is analyzed. Finally, we provide a performance evaluation of the protocol in a vehicular scenario. Finally show that our protocol can thwart more than 99 percent of the attacks under the best possible conditions for the adversaries, with minimal false positive rates.

2. RELATED WORK

We studied the problem of sensor localization in the presence of malicious adversaries and proposed a high-resolution range-independent localization scheme called HiRLoc. We showed that HiRLoc localizes sensors with significantly higher accuracy than previously proposed methods, while requiring fewer hardware resources. Furthermore, we showed that HiRLoc allows the robust location computation even in the presence of security threats in WSN, such as the wormhole attack, the Sybil attack and compromise of network entities. Our simulation studies confirmed that variation of the transmission parameters at the reference points leads to high-resolution location estimation. We have designed a secure neighbor verification protocol tailored for wireless sensor networks.

To demonstrate its applicability to WSN, we have provided a proof-of-concept implementation on existing off-the-shelf hardware (Cricket motes). We have proved that the protocol is secure against the classic 2-end wormhole attack. Yet, our scheme is also effective against more complex relay attacks, as we have demonstrated with simulations in the associated technical report This scheme can be extended. For example, the scheme can be relatively easy augmentable to 3D networks by replacing the quadrilateral test with its equivalent in the new setting.

Moreover, other distance estimation techniques are worthy of being implemented as (probably better) alternatives for US-based measurement.

We investigate the problem of secure neighbor discovery (ND) in wireless networks. We build a formal framework, and provide a specification of neighbor discovery or, more precisely, its most basic variant: two-party ND. We consider two general classes of protocols: time-based protocols (T-protocols) and time- and location-based protocols (TL protocols). For the T-protocol class, we identify a fundamental limitation governed by a threshold value depending on the ND range: We prove that no T-protocol can solve the ND problem if and only if adversarial nodes can relay messages faster than this threshold. This result is a useful measure of the ND security achieved by T-protocols and leads us to investigate other classes of protocols. In particular, we prove that no such limitation exists for the class of TL-protocols: They can solve the ND problem for any adversary, as long as the time and location measurements are accurate enough, and line-of-sight signal propagation is assumed. The protocols we analyze are very simple if not the simplest possible to allow positive results.

We investigate how to analyze and design provably secure ND protocols, building on top of the framework introduced in We contribute a number of extensions that enable us to model and reason about more elaborate ND protocols (CR-protocols) than those previously considered (B-protocols). Basically, our revised framework(i) models additional practical aspects of wireless communications,(ii) caters to the co-existence and interoperability of secure ND protocols with other wireless security protocols, and (iii) focuses more than our work in on sought properties that are of practical relevance, in particular, pertaining to the ND protocol availability. We see this work as a step towards provably secure neighbor discovery. We outline a number of possible extensions to our framework, and open problems in the Discussion section. Among those, the seemingly most interesting one is to reason on secure ND protocols in the presence of internal adversaries. The nature of protocols that could deal with this type of adversarial behavior, as well as some recently discovered attacks mandate, in our opinion, a shift from message-oriented to models that explicitly consider symbol sat the physical communication layer.

We conclude with an investigation, based on current results, of upcoming elements to be integrated in our secure VC architecture. We have developed security architecture for VC systems, aiming at a solution that is both comprehensive and practical. We have studied the problem at hand systematically, identifying threats and models of adversarial behavior as well as security and privacy requirements that are relevant to the VC context. We introduced a range of mechanisms, to handle identity and credential management, and to secure communication while enhancing privacy. In the second paper of this contribution, we discuss implementation and performance aspects, present a gamut of research investigations and results towards further strengthening secure VC systems and addressing remaining research challenges towards further development and deployment of our 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 counter measures. 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. We qualitatively and quantitatively analyze those in this paper, and identify memory based mechanisms that can help in securing GNNS signals. In

particular, we realize that location based inertial mechanisms and a clock offset test can be relatively easily defeated, with the adversary causing (through jamming) a sufficiently long period of unavailability. In the latter case, only specialized highly stable clock hardware could enable detection of fraudulent GNSS signals. Our Doppler Shift Test provides resilience to long unavailability periods without specialized equipment. Our results are the first, to the best of our knowledge, to provide tangible demonstration of effective mechanisms to secure mobile systems from location information manipulation via attacks against the GNSS systems. As part of on-going and future work, we intent to further refine and generalize the simulation framework we utilized here, to consider precisely the effect of counter-measures that only partially limit the attack impact. Moreover, we will consider more closely the cost of mounting attacks of differing sophistication levels, especially through proof of concept implementations. Wireless ad hoc networks are envisioned to be randomly deployed in versatile and potentially hostile environments.

The Probabilistic Location Verification (PLV) algorithm for dense sensor networks is presented. Assuming that the compromised nodes make up a small percentage of the total sensor node population, a small number of verifier nodes was used to conclude whether or not the claimed location is a plausible one. It is assumed that the average density of the sensor nodes in the sensing field and the communication range of sensor nodes are known. Using a new set of probabilistic tools, PLV compares the node's Euclidean distance with the hop count of the verification packet. Simulation results confirm the accuracy and effectiveness of this light-weight location verification system. In our future work, the PLV algorithm will be improved to with built-in measures against wormhole attacks and cooperative attacks of multiple malicious nodes. New methods to ensure the hop count and content integrity will also be investigated to reduce the computational burden on sensor and verifier 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 providean analytical evaluation in terms of probabilities of the extent to which a method prevents wormholes.We presented a graph theoretic framework for characterizing the wormhole attack in wireless ad hoc networks. We showed that any candidate prevention mechanism should construct a communication graph that is a connected sub graph of the geometric graph of the network. We then proposed a cryptography-based solution to the wormhole attack that makes use of local broadcast keys. We provided a distributed mechanism for establishing local broadcast keys in randomly deployed networks and provided an analytical evaluation of the probability of wormhole detection based on spatial statistics theory. We analytically related network parameters such as deployment density and communication range with the probability of detecting and eliminating wormholes, thus providing a design choice for preventing wormholes with any desired probability. Finally, we also illustrated the validity of our results with extensive simulations.

In this work, we propose and analyze a new approach for securing localization and location verification in wireless networks based on hidden and mobile base stations. Our approach enables secure localization with a broad spectrum of localization techniques, ultrasonic or radio, based on the received signal strength or signal time of flight. Through several examples, we show how this approach can be used to secure node-centric and infrastructure-centric localization schemes. We further show how this approach can be applied to secure localization in mobile ad hoc and sensor networks**.** In this work, we proposed a novel approach to secure localization based on CBSs (hidden base stations and MBSs). This approach enables secure localization with a broad spectrum of localization technique ultrasonic or RF based on the received signal strength or the time of signal flight. We have demonstrated that this approach can be easily integrated with several existing node-centric and infrastructure-centric localization schemes. We have shown how the security of this approach depends on the precision of the localization systems and on the number of CBSs. Our future work includes implementations of our schemes and their evaluation in various indoor and outdoor scenarios. We also intend to investigate in more detail the privacy implications of our approach.

3. DISCOVER AND VERIFY THE POSITION OF ITS COMMUNICATION NEIGHBOURS:

To our knowledge, our protocol is the first to provide a fully distributed, lightweight solution to the NPV problem that does not require any infrastructure or a priori trusted neighbors and is robust to several different attacks, include-ing coordinated attacks by colluding adversaries.

Also, unlike previous works, our solution is suitable for both low and high mobile environments. File transmission in mobile ad hoc network is through node to node communication. In here using the NPV its allowed to free the attackers in this mobile ad hoc network.

Once NPV has derived, it runs several position verification tests in order to classify each candidate neighbor as either: 1. Verified, i.e., a node the verifier deems to be at the claimed position; 2. Faulty, i.e., a node the verifier deems to have announced an incorrect position; 3. Unverifiable, i.e.a node the verifier cannot prove to be either correct or faulty, due to insufficient information. Clearly, the verification tests aim at avoiding false negatives (i.e., adversaries announcing fake positions that are deemed verified) and false positives (i.e., correct nodes whose positions are deemed faulty), as well as at minimizing the number of unverifiable nodes. We remark that our NPV scheme does not target the creation of a consistent "map" of neighborhood relations throughout an ephemeral network: rather, it allows the verifier to independently classify its neighbors.

4. NPV in MANET

4.1 User registration and login for ad hoc usage:

Every application needs to allow authorized user through authentication process. In this stage it's used to create the ad hoc user for this application using both registration and login for ad hoc user screen. To avoid attackers in mobile ad hoc network this login and registration process is preliminary task to provide security. Ad hoc user registers their account in this application. Those who are already registered their account in this application; they can access their account through login. In this ad hoc user login and registration provide authentication check in this paper.

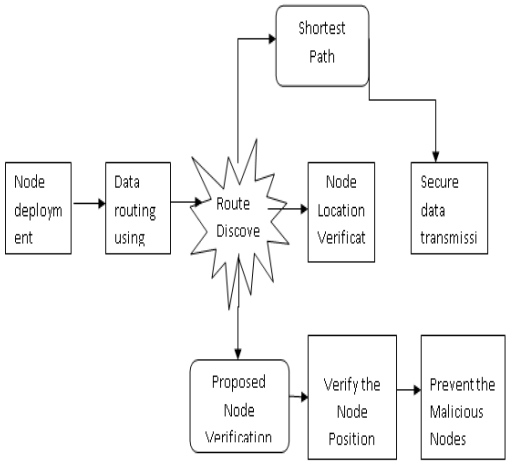


Figure 1: Architecture Diagram

4.2 Discover own location and neighbour location

Discovering own location and neighbour location is tedious task in mobile ad hoc network. In this stage of process it's used to find the own location and Neighbour location through the Wi-Fi integrated service. These findings are used to involve in the neighbour position verification. This verification is done through the NPV algorithm. Secure transmission in mobile ad hoc network is complex and it's achieved by NPV algorithm..

4.3 Connection between neighbour nodes:

Connection establishment with neighbour and accept connection by their neighbors' made a connection more secure. In this stage it's used to follow initial security mechanism through the cryptography techniques.

Connections with their neighbours are established here using AES cryptography technique. Connection need to be accepted in both ends then only source can sent secure message transaction. Neighbour position verification algorithm used to check all with their neighbour through above mentioned steps to verify their neighbours.

4.4 Secure content transaction

In final stage of this application implementation is secure content transaction to secure discovered neighbour destination. Position verification done through NPV algorithm and the message and attachments, whatever I need to send to the secure neighbour are happened to be here. Use send option after attachments and secure neighbour node selected.

4.5 Distance Computation

In order to compute the distance range, after a POLL and REPLY message a REVEAL message broadcast by the source nodes disclose to Through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected.

4.6 Position verification

To verify the position of a node following three tests is done, they are: In the Direct Symmetry Test,S verifies the direct links with its communication neighbour. In cross symmetry test information mutually gathered by each pair of communication neighbors are checked. In multilateration test, the unmodified links are tested.

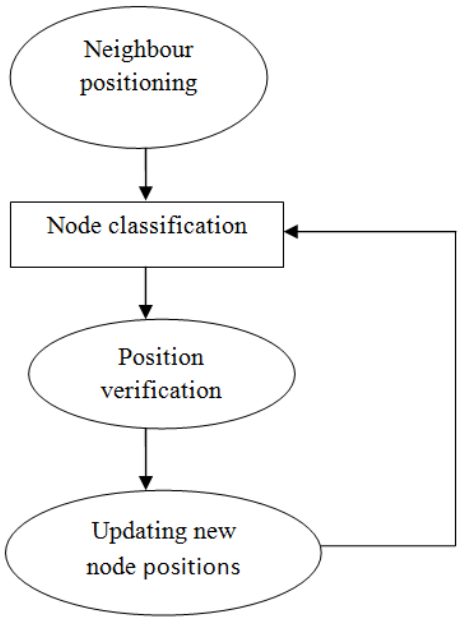


Figure 2: System flow

4.7 Node Position Verification

Once Source node has derived such distances, it runs several position verification tests in order to classify each candidate neighbor .The position verification is performed by direct symmetric test, cross symmetry test and multilateration test.

4.8 Node Verification Process

In this module a proposed work of node verification technique is introduced to detect the adversary nodes in the network. The node verification is done by hash function technique the public key and id of source node generates hash id.

4.9 Result analysis

We analyze the robustness of our scheme against different types of internal adversaries. Here classify the conceivable attacks into two classes, depending on the goal of the adversaries ToF-based ranging; we analyze the entire space of attacks against NPV. The effects of combinations of attacks of the first type are then investigated in our performance evaluation. Attacks where the adversaries aim at letting the verifier validate their own fake position; Attacks where the adversaries aim at disrupting the verification of correct node positions Attacks.

4.10 Jamming

This is the only external attack that can harm the system. Any adversary (internal or external) can jam the channel and erase REPLY or REPORT messages. However, to succeed, M should jam the medium continuously for a long time, since it cannot know when exactly a node will transmit its REPLY or REPORT. Or, M could erase the REVEAL, but, again, jamming should cover the entire Titter time. Overall, there is no easy point to target: a jammer has to act throughout the NPV execution, which implies a high energy consumption and is a disruptive action possible against any wireless protocol. In addition, mobility makes it harder to repeatedly jam different instances of the NPV protocol run by the same verifier.

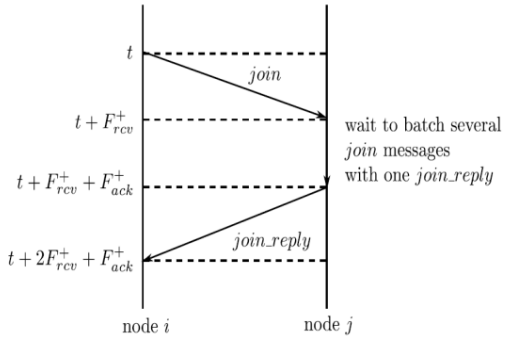
4.11 Clogging

An adversary could initiate the NPV protocol multiple times in a short period and get repeated REPLY and REPORT messages from other nodes, so as to congest the channel. In particular, REPORTs are larger in size, thus likely cause the most damage. However, NPV has a way of preventing that: the initiator must unveil its identity before such messages are transmitted by neighbors. An exceedingly frequent initiator can be identified, and it's REVEALs ignored, thanks to the use of certified keys. REPLYs instead are small in size and are broadcast messages (thus require no ACK): their damage is limited, but their unnecessary transmission is much harder to thwart. Indeed, REPLY messages are sent after an anonymous POLL; such anonymity is a hard-to dismiss requirement, since it is instrumental for keeping the identity of the verifier hidden. As a general rule, correct nodes can reasonably self-limit their responses if POLLs arrive at excessive rates.

4.12 Sybil and Relay (Wormhole) Attacks:

An adversary can assume several trusted identities, M ¼ fM1; . . .;MIg, if 1) it owns several certificated pairs of public/private keys (Sybil attack), or 2) it impersonates colluding adversaries at the end of wormholes. The availability of several identities could be used by an adversary to acquire its neighbor positions, i.e., to become knowledgeable. However, attacks launched by independent, knowledgeable adversaries have no chance of success. When a node enters a new region and determines that it is going to remain there for sufficiently long,it broadcasts a join message.This message indicates to the neighbors that they should start position verification for the corresponding link.It also serves as a request to learn the ids of neighbors.

Nodes that receive a join messages end a join reply message in response so that the original node can learn their ids.The timing of these messages ensures that the proper semantics of the corresponding links are maintained.This means that the overhead for setting up and tearing downlinks is taken into account,and reliable message delivery is guaranteed.



Join and join reply message exchange

4.13 Routing Algorithms

Most QoS routing algorithms represent an extension of existing classic best-effort routing algorithms. Many routing protocols have been developed which support establishing and maintaining multi-hop routes between nodes in MANETs. These algorithms can be classified into two different categories: on-demand (reactive) such as DSR, AODV, and TORA, and table-driven (proactive) such as Destination Sequenced Distance Vector protocol (DSDV).

4.14 DSR- Dynamic Source Routing Protocol:

DSR is one of the most well-known routing algorithms for adhoc wireless networks. It was originally developed by Johnson, Maltz, and Broch. DSR uses source routing, which allows packet routing to be loop free.It increases its efficiency by allowing nodes.

5. ALGORITHM IMPLEMENTATION MD5 (MESSAGE-DIGEST ALGORITHM):

Is a widely used cryptographic function with a 128- bit hash value? MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

6. ROBUSTNESS ANALYSIS OF THE PROPOSED SYSTEM:

A single cannot perform any successful attack against the NPV scheme.Multiple independent adversaries can only harm each other, thus reducing their probability of successfully announcing a fake position. .Finally, the overhead introduced by the NPV protocol is reasonable, as it does not exceed a few tens of K bytes even in the most critical condition.

7. SECURITY

Security critical conditions, wireless network is becoming more and more important while the using of mobile equipment's such as cellular phones or laptops is tremendously increasing. Like all kinds of networks,passive attack and active attack are two kinds of attacks which can be launched against adhoc networks. The secure adhoc routing protocols enhance the existing adhoc routing protocols, such as DSR and AODV with security extensions.

8. CONCLUSION

In this proposed system presented a distributed solution for NPV, which allows any node in a mobile ad hoc network to verify the position of its communication neighbours 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. Future work will aim at integrating the NPV protocol in higher layer protocols and that each node to constantly verify the position of its neighbour.

REFERENCES

[1] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[3] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.

[4] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13,pp. 27-59, 2007.

[5] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations," IEEE Trans. Mobile Computing, vol. 7, no. 4, pp. 470-483, Apr. 2008.