DISCOVERY AND CERTIFICATION OF FOREIGNER POSITION PORTABLE AD HOC NETWORKS

[1]P.Ramalingam, [2]N.Tamizharasan
[1] Research Scholar, Department of Computer Science, SSM College of Arts and Science, Kumarapalayam
[2]Assistant professor, Department of Computer Science, SSM College of Arts and Science, Kumarapalayam
[1]ramalingamkavin@gmail.com, [2]nt.tamil11@gmail.com

Abstract: In mobile ad hoc, Position aided routing protocol can offer a significant performance increase over traditional ad hoc routing protocols. These routing protocols use geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. However, current position aided routing protocols were not designed for use in high-risk environments, as position information is broadcasted in the clear allowing anyone within range, including the enemy, to receive .In this paper, route detection and certification of neighbor's position information in MANET routing protocols, and ways to use the position information to enhance performance and security of MANET routing protocols. 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. These nodes affect the performance of routing protocol in ad-hoc networks.so, it is essential to identify the neighbors in a Manet. The proposed scheme identifies a neighbor and verifies its position effectively.

1. INTRODUCTION

A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves. The verification of node locations is an important issue in mobile networks. Neighbor discovery deals with the identification of nodes. A communication link can be established or those are within a given distance Verification of the positions announced by third parties. Thus, a protocol is devised that is autonomous and does not require trustworthy neighbors' packet to it's an adhoc network is a collection of wireless mobile hosts forming a temporary network. In such an environment, it is necessary for one mobile host to enlist the aid of other hosts in forwarding destination, due to the limited range of each mobile host's wireless transmissions. This paper presents a protocol for updating the position of a node in dynamic adhoc networks. The protocol adapts quickly to position changes when host movement is frequent.

2. Related work

Nodes carry a unique identity and can authenticate messages of other nodes through public key cryptography. In particular, it is assumed that each node X owns a private key,kX,and a public key, KX, as well as a set of one-time use keys {k0X;K0X }.Nodes are correct if they comply with the NPV protocol ,and adversarial if they deviate from it.

We propose a practical algorithm for worm whole detection. The algorithm is simple, localized, and is universal to node distributions and communication models. Our simulation results have confirmed a near perfect detection performance whenever the network is connected with a high enough probability, for common connectivity and node distribution models. We expect that this algorithm will have a practical use in real world deployments to enhance the robustness of Wireless networks against wormhole attacks.

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 progresses towards implementation of our architecture, along with results on the performance of the secure VC system, are 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. 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. 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 worm holes. 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 abroad 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. FINDING THE POSITION OF A NEIGHBOR

The aim of the message exchange is to lets collect information it can use to compute distances between any pair of its communication neighbors. After the distances are calculated the nodes are classified as:

Verified: N Fault; node has announced an in correct position

Unverifiable: insufficient information

3.1 NPV Protocol

3.1.1 POLL message

A verifier S initiates this message. This message is anonymous. The identity of the verifier is kept hidden.

3.1.2 REPLY Message

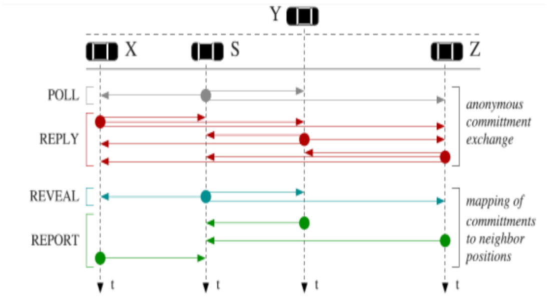
A communication neighbor X receiving the POLL message will broadcast REPLY message after a time Interval

3.1.3 REVEAL MESSAGE

The REVEAL message is Broadcasted using verifier real MAC address.

3.1.4 REPORT Message

The REPORT carries X’s position, the transmission time of X’s REPLY, and the list of pairs of reception times and temporary identifiers referring to the REPLY broadcasts X received.


Y
X
S
Z
POLL
REPLY
REVEAL
REPORT
anonymous committment exchange
mapping of committments to neighbor positions
t
t
t
t

4. System model

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

4.1 Nodes Unique Identity

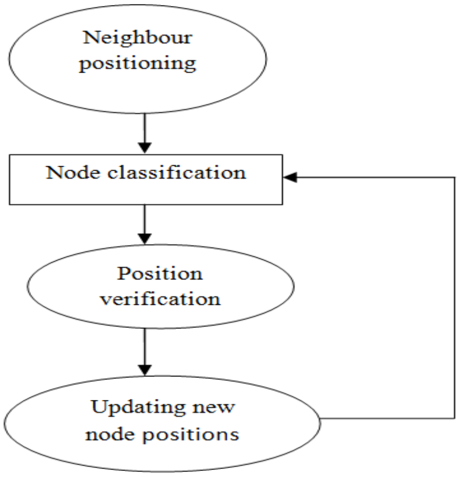
All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

4.2 Message exchange process for route discovery

This module states a 4 step message change process i.e. POLL, REPLY, REVEAL, and REPORT. As soon the protocol executed the, POLL and REPLY messages are first broadcasted by Source and its neighbors, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless medium.

4.3 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 neighbor. In cross symmetry test information mutually gathered by each pair of communication neighbors are checked.. In multi alteration test, the unmodified links are tested



System flow

4.4 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 S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected.

4.5 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

4.6 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.

4.7 Dynamically updating neighbor position

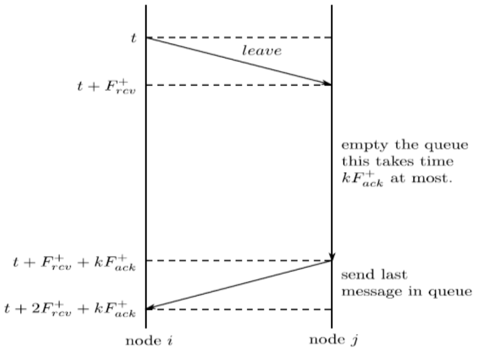
The neighbor discovery protocol is based on nodes sending notification messages tagged with ID and their current region whenever they enter or leave a region. In particular, there are three types of messages:

- Leave
- Join
- Join reply

Notation	Description
F+rcv	Upper bound on a specific Message being delivered
F+	Upper bound on an acknowledgment being received
k	Maximum size of the queue
t	Initial time

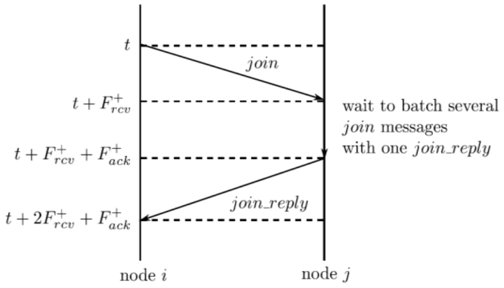
4.8 Summary of notations

When a node is a bottom move into a new region, it broadcasts a leave message some time before leaving. This message indicates to its neighboring nodes that they should begin tearing down the corresponding link if appropriate.


t
leave
$t + F^{+}_{rcv}$
empty the queue this takes time kF^{+}_{ack} at most.
$t + F^{+}_{rcv} + kF^{+}_{ack}$
send last message in queue
$t + 2F^{+}_{rcv} + kF^{+}_{ack}$
node i
node j

4.9 Leave message exchange

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


t
join
$t + F^{+}_{rcv}$
wait to batch several *join* messages with one *join_reply*
$t + F^{+}_{rcv} + F^{+}_{ack}$
join_reply
$t + 2F^{+}_{rcv} + F^{+}_{ack}$
node i
node j

4.10 Join and join reply message exchange:

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.

4.11 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).

4.12 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):

It 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. ROBUSTNESSANALYSIS 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

Techniques for finding neighbors effectively in a non priori trusted environment are identified. The Proposed techniques will eventually provide security from malicious n odes. The protocol is robust to adversarial attacks. This protocol will also update the position of the nodes in an active environment. The performance of the proposed scheme will be effective

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.