ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

Distributed Neighbor Positioning In MANET with Protection against Adversarial Attacks

[1]Thummala Poojitha, [2]K. Bhargavi

[1]PG Scholar, Department Of Computer Science and Engineering, INTELL Engineering College, Anantapur, AndhraPradesh, India

[2]Assistant Professor, Department Of Computer Science and Engineering, INTELL Engineering College Anantapur, AndhraPradesh, India

ABSTRACT: The Mobile Ad-Hoc Networks, Routes may be disconnected due to dynamic movement of nodes. Such networks are more vulnerable to the 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 Neighbor nodes in a MANET. The Proposed Scheme Identifies a Neighbor nodes and Verifies Its Position Effectively.

KEYWORDS*:* wireless communication, algorithm/protocol design and analysis, routing protocols, Adversarial.

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multi hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for "Mobile Ad Hoc Network" A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Networking system such as Geographic routing in spontaneous networks, data gathering in sensor networks are the services that are designed on the availability of neighbor position information. Network topology is dependent on the position of the nodes, so identification of a node is necessary step in node-to-node communication. This kind of investigation of a neighbor node positions makes a door open for the adversaries, which may disturb the communication.

II. RELATED 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 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

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. For completeness, we also extend the above results to the 3-dimensional case. Experimental results demonstrate that our solution has very good localization accuracy and computational efficiency.

III. SCOPE OF RESEARCH

The existing approaches 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.

Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for handheld devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information. 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.

3.1 Discovery of neighbor nodes

Neighbor discovery deals with the identification of nodes with which a communication link can be established or that are within a given distance. An adversarial node could be securely discovered as neighbor and be indeed a neighbor (within some range), but it could still cheat about its position within the same range. In other words, SND lets a node assess whether another node is an actual neighbor but it does not verify the location it claims to be at .this is most often employed to counter wormhole attacks.

3.2 Verification of neighbor position

Neighbor verification schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic. Thus, a protocol is devised that is autonomous and does not require trustworthy neighbors.

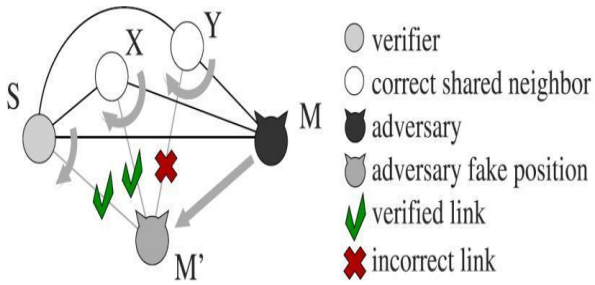


Figure1: Neighbor discovery in adversarial environment

Disadvantages of Existing System:

- Correctly establish their location in spite of attacks feeding false location information, and
- Verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

IV. PROPOSED SCHEME

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, k_X, and a public key, K_X, as well as a set of one-time use keys $\{k_{0X};K_{0X}\}$. Nodes are correct if they comply with the NPV protocol, and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

Adversarial if they deviate from it.

4.1 Distributed cooperative NPV scheme

A node S is called as a verifier, which discovers and verifies the position of its communicating Neighbors. A verifier, S, can initiate the protocol at any time instant, by triggering the 4-step message exchange. The aim of the message exchange is to let S 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: Node is in the claimed position.
Faulty: Node has announced an incorrect position.
Unverifiable: Insufficient information.
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. It also allows the verifier to independently classify its neighbors.

4.2 NPV Protocol

This protocol exchanges messages and verify the position of communicating nodes. Here four set of Messages are exchanged they are:

- POLL message
- REPLY message
- REVEAL message
- REPORT message

POLL message

A verifier S initiates this message. This message is anonymous. The identity of the verifier is kept hidden. Here software generated MAC addresses is used. This carries a public key K'_S chosen from a pool of onetime use keys of S'.

REPLY message

A communication neighbor X receiving the POLL message will broadcast REPLY message after a time interval with a freshly generated MAC address. This also internally saves the transmission time. This also contains some encrypted message with S public key (K'_S). This message is called as commitment of X C_X.

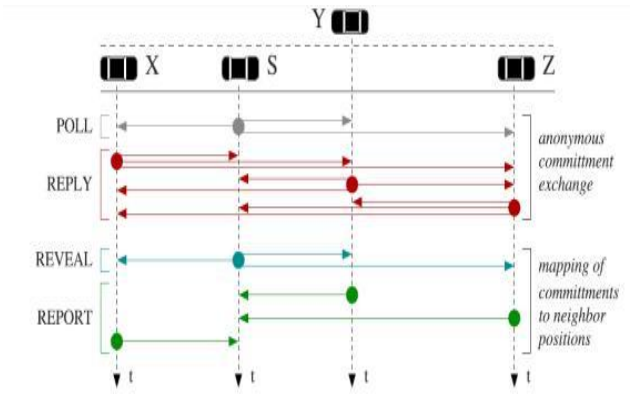


Figure 2: Message exchange

REVEAL message

The REVEAL message is broadcasted using Verifier's real MAC address. It contains A map MS, a proof that S is the author of the original POLL and the verifier identity, i.e., its certified public key and signature.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

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. The identifiers are obtained from the map M_S included in the REVEAL message. Also, X discloses its own identity by including in the message its digital signature and certified public key.

V. PSEUDO CODE

Step 1:--- Determine own location
Step 2:--- Secure Neighbor discovery with in some range
Step 3:--- Neighboring position verification
Step 4:--- protocol message exchange
Step 5:--- verify the current node position
Step 6:--- set of communication neighbors
Step 7:--- Time at which source node starts broadcast
Step 8:--- Time at which receiving node starts receiving
Step 9:--- To retrieve exact transmission and reception time instances avoid unpredictable latencies
Step 10:--- Find out position of all neighbors.

VI. ROBUSTNESS ANALYSIS OF THE PROPOSED SYSTEM

A single independent adversary cannot perform any successful attack against the NPV scheme. When the shared neighborhood increases in size, the probability that the adversary is tagged as faulty rapidly grows to 1. Multiple independent adversaries can only harm each other, thus reducing their probability of successfully announcing a fake position. In coordinated attacks, it is the nature of the neighborhood that determines the performance of the NPV scheme in presence of colluders. However, in realistic environments, our solution is very robust even to attacks launched by large groups of knowledgeable colluders. This system yields small advantage to the adversaries in terms of displacement. Finally, the overhead introduced by the NPV protocol is reasonable, as it does not exceed a few tens of Kbytes even in the most critical conditions.

VII. SIMULATION RESULTS

The The Simulations have been shown through the network simulator (NS2), and by using the TCL tool and Network Animator Window (NAM).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

Fig 1: Network topology is created so that the Nodes are present within the range and each Contain a unique id are shown In this figure.

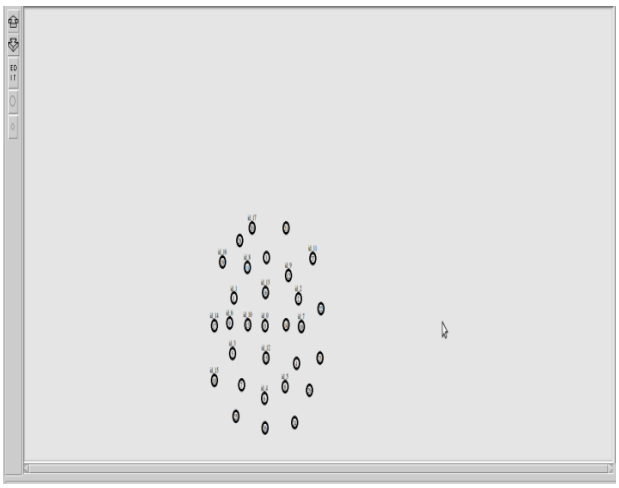
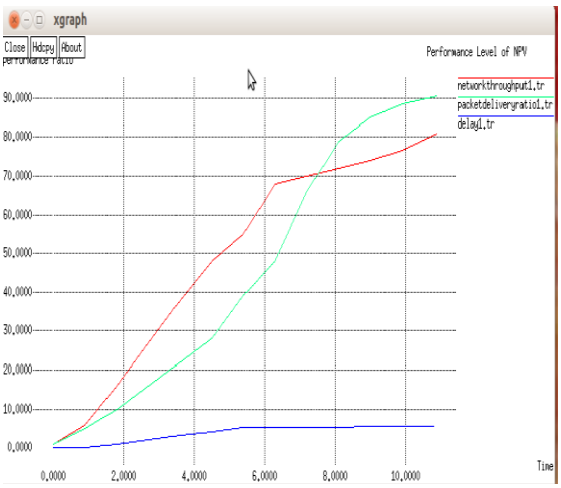


Fig**2**: the graph shows the increasing level of Network throughput, packet delivery and decreasing level of delay.



VIII. CONCLUSION

Techniques for finding neighbors effectively in a non priori trusted environment are identified. The proposed techniques will eventually provide security from malicious nodes. The protocol is robust to adversarial attacks. This scheme will continuously monitor the position of nodes. The performance of the proposed scheme will be effective one.

REFERENCES

1) Vora and M. Nesterenko, "Secure Location Verification Using Radio Broadcast," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 377-385, Oct.-Dec. 2006.
2) S. Capkun and J.-P. Hubaux, "Secure Positioning in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221-232, Feb. 2006.
3) T. Leinmu¨ ller, C. Maiho¨ fer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," Proc. ACM Third Int'l Workshop Vehicular Ad Hoc Networks (VANET), Sept. 2006.
4) J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," Proc. IEEE INFOCOM, May 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.
6) M. Poturalksi, P. Papadimitratos, and J.-P. Hubaux, "Towards Provable Secure Neighbor Discovery in Wireless Networks," Proc. Workshop Formal Methods in Security Eng., Oct. 2008.
7) E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp. 195-209, 2008
8) J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
9) M. Fiore, C. Casetti, C.-F. Chiasserini, and P. Papadimitratos,"Secure Neighbor Position Discovery in Vehicular Networks,"Proc. IEEE/IFIP 10th Ann. Mediterranean Ad Hoc NetworkingWorkshop (Med-Hoc-Net), June 2011.

BIOGRAPHY

THUMMALA POOJITHA is an M.Tech student in Department of Computer Science and Engineering in INTELL Engineering College Anantapur affiliated to Jawaharlal Nehru Technological University - Anantapur, Andhra Pradesh, India. Area of interest is Sensor Networks, Mobile Ad Hoc Networks and Network Security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 7, July 2014

K.BHARGAVI completed her M Tech in the Department of Computer Science and Engineering, and currently working as an Assistant professor in INTELL Engineering College Anantapur affiliated to Jawaharlal Nehru Technological University - Anantapur, Andhra Pradesh, India. Her Area of Interest is Networking, Internet Programming, and Network Security.