ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Secure Neighbor Position Verification for Mobile Ad Hoc Network

Balaji P[1], Gopinathan B[2]

PG scholar, Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[1]

Assoc Prof., Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India[2]

Abstract: Routes in mobile ad hoc networks can be disconnected due to the movement of nodes. By this issue the transmission of data is not secure and the adversarial nodes can easily attack the other nodes. These adversarial nodes affect the performance in networks and so, it is more important to identify the neighbor node in mobile ad hoc networks. To secure data and to minimize adversary attacks, the mobile node is required to learn the discovery and neighbor's position which is more challenging in mobile ad hoc networks. In this paper, the fully distributed Enhanced NPV (ENPV) scheme is proposed and it is robust against colluding adversaries. This ENPV protocol can prevent maximum number of adversaries attack.

Keywords: Adversary nodes, Colluding Adversaries, Enhanced NPV, MANET, Neighbor Discovery

I. INTRODUCTION

Mobile ad hoc network is a self configuring network of mobile routers connected by wireless links. It is an infrastructure-less network. In mobile ad hoc network each device is free to move in any direction.

This type of network changes its links frequently to other devices and data must be routed via intermediate nodes. A mobile ad-hoc network is an ad-hoc network but an ad-hoc network is not necessarily a mobile ad hoc network.

It has no base station and the nodes can only transmit to other nodes within link coverage. MANET is mainly used in Military environments, Emergency operations, and in Personal area application.

The node location verification is an important issue in mobile ad hoc networks and it becomes challenging in the presence of adversaries aims at harming the system.

The solution for these cases is that the nodes should verify the neighbor's position and detects the adversarial nodes which announce false locations. The neighbor nodes should be trusted nodes or else the adversarial nodes can easily attack the network.

In order to overcome this challenge Enhanced Neighbor Position Verification (ENPV) protocol is proposed which is fully distributed, lightweight and robust against colluding adversaries.

It does not rely on the trustworthy node. Enhanced NPV protocol can be executed at any time, by any node, without the knowledge of neighborhood.

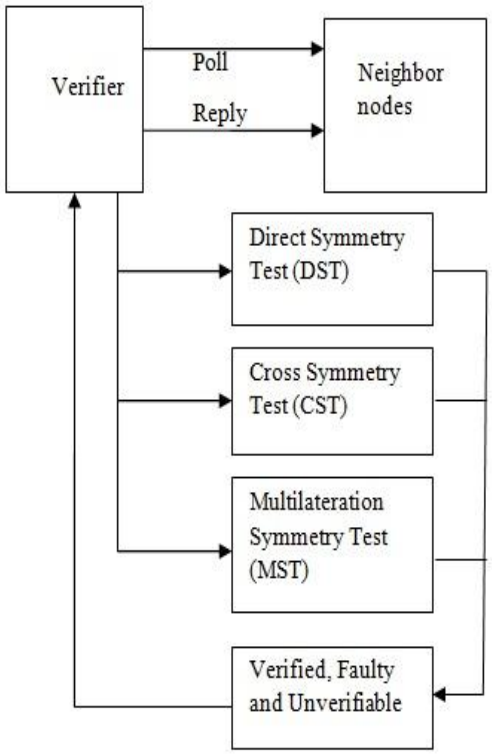

Fig. 1. Overview of ENPV Protocol

The Fig. 1 represents the overview of ENPV protocol. The description of this diagram is given in section IV.

II. RELATED WORK

A. Neighbor Discovery

Neighbor discovery is a fundamental building block of networking protocols, determines which devices are within direct radio communication. It deals with the identification of nodes in which the communication link can be established within a given range. If the neighbor discovery fails, the communication and performance degrades.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Neighborhood discovery protocol [1] is used to determine the neighbors of a given node. The main role of this protocol is to identify the nodes, which is the actual neighbors, to prevent from the adversaries. Neighborhood discovery protocol is partial it may fail to verify all neighbors. Attacker can jam communication, so it is hard to guarantee the message delivery.

B. Neighbor Position Verification

1) Probabilistic Location Verification (PLV): PLV algorithm is used for secured location verification. The PLV algorithm is mainly applicable in wireless sensor networks [2]. In PLV algorithm only a small number of specialized verifiers are needed and it is flexible against attacks and provides graceful degradation in performance. It leverages the probabilistic dependence of the number of hops a packet traverses to reach a destination and the Euclidean distance between the source and the destination. To determine the plausibility of the claimed location a small number of verifier nodes are used, which is represented by a real number between zero and one. By using the calculated plausibility metric, it is possible to create arbitrary number of trust levels in the location claimed. By simulating this algorithm it provides high performance in face of various attacks.

2) Multilateration and Distance bounding protocol: This protocol is used for secured verification. Multilateration scheme [3] is used to verify the prover's location. In this scheme verifier and prover is mainly used. Here the prover proves his location. Multilateration must be performed simultaneously by modifying the distance bounding protocol so that the prover responds to simultaneous challenges from each verifier. Distance bounding protocol should prove that the prover is within a certain distance from a verifier. Here the multilateration protocol is based on time-of-flight scheme and it achieves the minimum security in location verification.

3) Verifiable Multilateration (VM): VM algorithm [4] is used to secure positioning. This mechanism is based on the measurements of the time of radio signal propagation. Secure Positioning In Sensor Networks (SPINE) scheme is used in this mechanism. It secures from two types of attackers 1. Internal attackers and 2. External attackers. Internal attackers report the false position and external attackers modifies the calculated position. The positioning is done by two types a) node-centric and b) Infrastructure-centric. In node-centric positioning system, node computes its positions by observing radio signals with known locations. In infrastructure-centric positioning system, infrastructure computes its positions of nodes based on their mutual communications. SPINE secures the positioning in networks based on VM.

4) Secure Neighbor Position Discovery (SNPD): SNPD protocol [5] is used for secure discovery and verification of neighbor nodes. This protocol is lightweight, distributed and efficient which enables each node to discover and verify the position of its neighbors. This protocol can be executed at any time, at any node, without prior knowledge of other nodes. Without trustworthy neighbor nodes it can be easily enabled. This protocol is used in vehicular ad hoc networks. Here the verifier is used to verify the nodes. The Verifier does the message exchange with the nodes and it verifies the position by some tests.

III. EXISTING WORK

A. Secure Neighbor Discovery

For neighbor discovery, secure neighbor discovery (SND) protocol is mainly used. SND identifies the nodes. In this protocol the adversaries can able to cheat its position within the same range. SND does not verify the node location. It is most often attacked by wormhole attacks [6].

B. NPV Protocol

The NPV protocol [6] is used here to verify the neighbor position. NPV protocol enables a node, called verifier to discover and verify the position of the neighbor nodes. Every node does the message exchange protocol with the neighbor nodes. Message exchange protocol contains following messages: poll, reply, reveal and report messages. Verifier calculates the transmission time and reception time when the poll message is exchanged. By this the exact distance between the nodes can be calculated easily. And verifier does the verification tests to verify whether the node is verified, faulty or unverifiable. The tests are direct symmetry test, cross symmetry test and multilateration test. Only one verifier is used to verify the neighbor position so there is a possible of adversaries attack.

IV. PROPOSED WORK

In the proposed approach, the existing secure neighbor discovery (SND) is mainly attacked by wormhole attacks. We propose a Mobile Secure Neighbor Discovery (MSND) protocol, which protects the nodes against wormhole. MSDN uses the graph rigidity concept for wormhole detection [7].

For neighbor position verification, Enhanced NPV protocol is proposed which is lightweight and it does not rely on presence of trustworthy nodes. Here each and every node acts as a verifier. Every node does the message exchange protocol and position verification with the neighbor nodes.

A. Message Exchange Protocol

Every node does message exchange protocol with the neighbor nodes. Message exchange protocol contains various types of messages like Poll and Reply messages. The verifier broadcasts the poll message to all the neighbor nodes. Poll message consist the Mac address of the verifier and the verifier stores the transmission time of the poll message. In poll message the verifier will shows its identity to the neighbor nodes by its digital signature. Now the verifier is known to all the neighbor nodes, so the neighbor nodes will unicast the reply message to the verifier. The reply message consist the identity of the neighbor nodes and the position of that node. After this message exchange protocol only the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

verifier knows all the neighbor nodes position. The verifier notes the transmission time and reception time of poll message, so that it calculates the distance between the nodes. The distance can be calculated by, consider two nodes x and y, the distance between the nodes x and y is,

$$d_{XY} = (t_{XY} - t_X) \cdot c$$

where, d_{XY} is the distance between the nodes X and Y, t_{XY} is the actual reception time at y of a message by X, t_X is the actual transmission time of a message by X and c is the speed of the message transmission. The distance between y and x is,

$$d_{YX} = (t_{YX} - t_Y) \cdot c$$

where, d_{YX} is the distance between the nodes Y and X, t_{YX} is the actual reception time at y of a message by Y, t_Y is the actual transmission time of a message by Y and c is the speed of the message transmission.

B. *Position Verification*

After calculating the distance between nodes, the verifier does some of the tests to verify whether the node is verified, faulty, or unverifiable. Verified means the node is in current position, faulty means the node is in incorrect position so it may be an adversarial node and unverifiable means the node may be correct or unverifiable. The tests are Direct symmetry test (DST), Cross symmetry test (CST) and Multilateration test (MST). In Direct symmetry test (DST), the distance between the verifier node and other nodes should not exceed twice the ranging error ε_m, and should be within the error margin $2\varepsilon_p + \varepsilon_r$ and finally it should not be larger than proximity range R. If the value exceeds, it is noted as faulty. In Cross symmetry test, the verifier node will cross check the information between other two nodes, it will not test the nodes which is ignored in the DST. In CST, two nodes should be in the collinear position. If there is less than two non-collinear neighbors then the node is unverifiable, if there is more than two non-collinear neighbors, then it is faulty. In Multilateration symmetry test, the faulty and unverifiable nodes will be avoided, the verifier node links with all the neighbors. It calculates the transmission time between the verifier node and other neighbors. The points will be noted in the graph and it gives a hyperbolic curve. Now the node is considered as verified node.

All the nodes verify the neighbor node so it is easy to verify the verified node. By this approach the Enhanced NPV protocol is robust against the colluding adversaries it prevents more than 99 percent of the attacks from the adversaries.

V. IMPLEMENTATION AND RESULT

To evaluate the performance of ENPV protocol, we randomly select 1 percent of the nodes as verifiers for every simulation second. For each verifier, compare the outcome of the verification tests with the neighbors. Consider colluding adversaries acts in groups, which is referred as clusters. Note that a colluding cluster size is equal to 1 corresponds to independent attacks. Also, adversaries perfectly know the identity and location of all colluding and non colluding neighbors.

The cluster size does not cause more correct nodes to be unverifiable, because there is a lack of non collinear neighbors that can verify them. Collinear attacks yield small advantage for adversaries, which forced to announce positions quite close to their real locations. Collinear attacks results the smallest gain for adversaries. Values of various parameters used in the simulations are listed in Table I.

TABLE I
VALUES OF VARIOUS PARAMETERS USED IN SIMULATIONS

Parameter	value
R	225 [m]
ε_p	8 [m]
ε_r	6.5 [m]
ε_m	4 [m]
Length of signature	20 [bytes]
Poll message size	30 [bytes]
Reply message size	80 [bytes]

The performance of the ENPV protocol is more effective than NPV protocol.

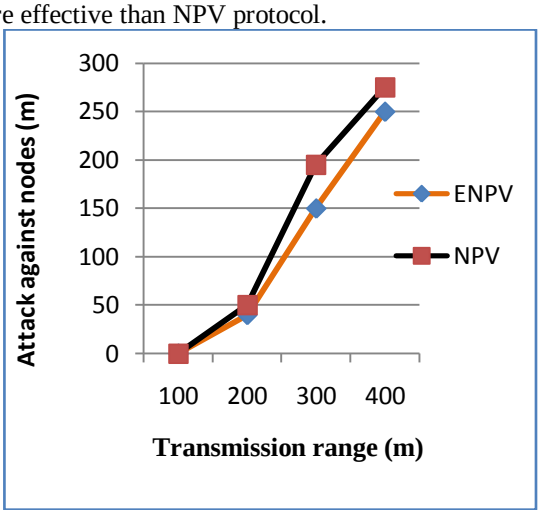

Fig. 2. Adversaries Running a Successful Attack Against Nodes

VI. CONCLUSION

The proposed fully distributed Enhanced NPV allows every node to verify the position of its neighbor without relying on the trustworthy nodes. Enhanced NPV technique will provide security from adversary nodes. This protocol is robust against adversaries. It allows all the nodes to perform all verification procedures. The performance of the proposed ENPV scheme will be effective.

REFERENCES

[1] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.

[2] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp. 195-209, 2008.

[3] J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multi-lateration," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.

[4] 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.

[5] 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 Networking Workshop (Med-Hoc-Net), June 2011.

[6] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos, "Discovery and Verificaion of Neighbor Positions in Mobile Ad Hoc Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.

[7] R. Stoleru, H. Wu, H. Chenji, "Secure Neighbor Discover in Mobile Ad Hoc Networks," proc. Eighth IEEE Int'l conf. Mobile Ad-Hoc and Sensor Systems, Oct. 2011.

BIOGRAPHIES

Mr. P. Balaji obtained his bachelor's degree in Computer Science and Engineering from Adhiyamaan College of Engineering affiliated to Anna University, Chennai. Currently he is pursuing his Master degree in Computer Science and Engineering from Adhiyamaan College of Engineering, Hosur, Tamilnadu.

Prof. B. Gopinathan obtained his bachelor's degree in Information Technology from M.I.E.T Engineering College, Trichy-7 and he received his Master degree in Computer Science and Engineering from Arunai Engineering College, Tiruvannamalai. Currently he is pursuing his Ph.D at Anna University, Chennai in the field of Ad hoc Networks. He has 8 years of teaching experience and currently, he is working as a Associate Professor in CSE department at Adhiyamaan College of Engineering, Hosur, Tamilnadu.