ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

An Authenticated Neighbour Location In Mobile Ad Hoc Networks

S. Bhuvaneswari[1], P. Sivakamasundari, M.E[2]

M.E Computer Science & Engineering, Adhiparasakthi Engineering College, Melmaruvathur, India[1]

Assistant Professor, Adhiparasakthi Engineering College, Melmaruvathur, India[2]

Abstract - The 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 priority trusted nodes, the discovery and verification of neighbor positions presents challenges that have been scarcely investigated in the literature. Identifying a trusted neighbor location is one of the major tasks in the mobile ad hoc network. This can be done by the signal passed by the nearby node. An issue is the signal get by the nearer node is a trusted one or not. In this paper is creating a secure protocol for finding the nearby node in an ad-hoc network. Finally the result gives with verification and robust whether the neighbor node position is a valid one or not.

Terms and Abbreviations -

QOS Quality Of Service

DOS Denial Of Service

Denial Of Service attack, is an explicit attempt to make a computer resource unavailable by either injecting a computer virus or flooding the network with useless traffic. There are two types of DOS attacks such as computer attack and network attack.

Quality Of Service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, grade of service, etc.

Web Service Web service is a software system designed to support interoperable machine-to-machine interaction over a network

Application Computer Software designed to help the user to perform specific tasks.

Server Computer program running to serve the needs or requests of other programs which may or may not be running on the same computer.

I. INTRODUCTION

Location awareness has become an asset in mobile systems, where a wide range of protocols and applications require knowledge of the position of the participating nodes. 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. In these cases, we need solutions that let nodes 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.

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. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. For example, by advertising forged positions, adversaries could bias geographic routing or data gathering processes, attracting network traffic and then eavesdropping or discarding it. Similarly, counterfeit positions could grant adversaries unauthorized access to location dependent services, let

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers.

In this context, the challenge is to perform, in absence of trusted nodes, a fully distributed, lightweight NPV procedure that enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness. We therefore propose an NPV protocol that has the following features:

It is designed for spontaneous ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes. It leverages cooperation but allows a node to perform all verification procedures autonomously.

This approach has no need for lengthy interactions, e.g., to reach a consensus among multiple nodes, making our scheme 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.

Mobile computing is the ability to use computing capability without a pre-defined location by connection to a network. Ubiquitous computing cannot be realized unless mobile computing matures. This has enabled user to work from anywhere as long as there is a connection established. A user can work without being in a fixed position. Their mobility ensures that they are able to carry out numerous tasks at the same time perform their stated jobs.

One can now access all the important documents and files over a secure channel or portal and work as if they were on their computer. A worker can simply work efficiently and effectively from which ever location they see comfortable and suitable. Users are able to work with comfortable environments.

II. PROPOSED SYSTEM

The architecture involves the transferring the information one node to another node. Information transferred as packet using QOS (Quality of Service).

Node creation is forming a new wireless networks. Get the number of nodes and range value. Finally forming a wireless network and establishing the communication for all nodes.

Identifying a trusted neighbor location is one of the major tasks in the mobile ad hoc network. This can be done by the signal passed by the nearby node. An issue is the signal get by the nearer node is a trusted one or not.

It is creating a secure protocol for finding the nearby node in an ad-hoc network.

Finally the result gives with verification and robust whether the neighbor node position is a valid one or not.

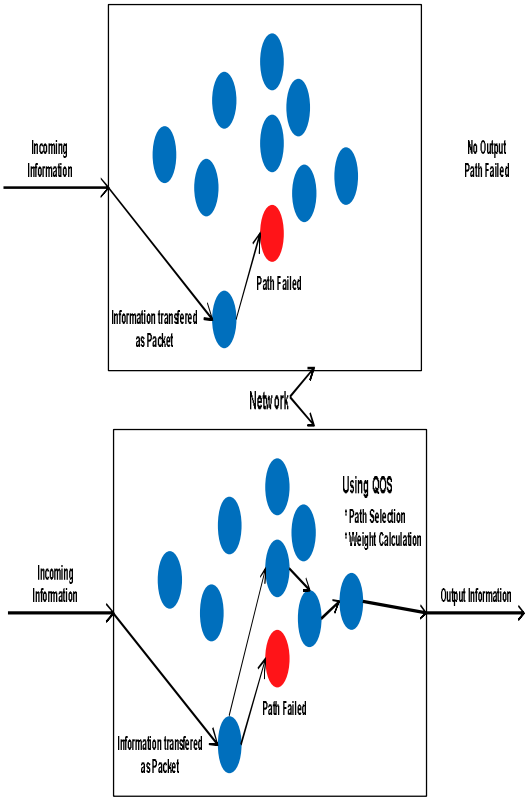

Fig. 1.System Architecture

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

III. MODULES WITH DESCRIPTION

A. NODE CREATION

In this module is forming a new wireless network. Get the number of nodes for adding into wireless network from the users. Get the radius level which is being covered by each node.

Finally forming a wireless network and establishing the communication for all nodes. I have formed a Initial topology structure.

B. TRUSTING TOPOLOGY PROCESS

In this module is forming a trusted topology. Choose a Node For that want to join trusted topology. Requested Node must be Submit a policy which is requiring a trusted node. Choose a Node for grant Permission for requested node which is already joined the trusted topology.

Accept Node must be check the require policy which is submitted by Requested node. From this process we can filter the outsider attack into our topology. Now our topology keeps safe from the outsider attack.

C. INSTRUDE PROCESS

In this module is eliminating an intruder for keep trusted topology structure. After joined into topology the node may become a intruder. Which node change their kernel level information that node will be consider as intruder.

Which node makes DOS Attack that will consider as intrudes. The intruder will be sent out from our topology. From this process we can filter the insider attack into our topology. Now our topology keeps safe from the insider attack.

D. STATE OF EACH NODE

Meta protocol have many states that is Begin state, Sleep state, Awake state, Rest state, Working state and halt state. Begin state is initial state for all the nodes which is joined into topology. All the nodes should be shift from begin state to sleep state. The node which is stay into sleep state that can shift to awake state.

The Awake state nodes may shift to either working state or back to sleep state. Working state nodes only can transfer the files between them. Working state nodes may be shift to either rest state or back to awake state. The rest state nodes can move to either sleep state or return to working state.

E. SECURE FILE TRANSFER

Trusted topology network nodes can transform files between them because our topology network gives a full trustworthy. Working state node can only transfer files between them. Remaining node cannot transfer files between them. Which node wants to be communicating to other node those two nodes must come to working state. So that we can increase the network life time. Our topology include many states for each node from this process we can achieve the lifetime increase of each network.

F. DATA VERIFICATION

In data verification module, receiver verifies the path. Suppose data come with malicious node means placed in malicious packet. Otherwise data placed in honest packet. This way user verifies the data's.

IV. RELATED WORK

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. Below, we list relevant works and highlight the novelty of our contribution. For clarity of presentation, we first review solutions to some NPV-related problems, such as secure positioning and secure discovery, and then we discuss solutions specifically addressing NPV.

Securely determining own location

In mobile environments, self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and non cryptographic. Alternatively, terrestrial special purpose infrastructure could be used along with techniques to deal with non honest beacons. We remark that this problem is orthogonal to the problem of NPV. In the rest of this paper, we will assume that devices employ one of the techniques above to securely determine their own position and time reference.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Secure neighbor discovery

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. In other words, SND is a subset of the NPV problem, since it lets a node assess whether another node is an actual neighbor but it does not verify the location it claims to be at. SND is most often employed to counter wormhole attacks practical solutions to the SND problem have been proposed in while properties of SND protocols.

Neighbor position verification

Neighbor position verification was studied in the context of ad hoc and sensor networks; however, existing NPV 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, we devise a protocol that is autonomous and does not require trustworthy neighbors. NPV protocol is proposed that first lets nodes calculate distances to all neighbors, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions. This scheme does not rely on trustworthy nodes, but it is designed for static sensor networks, and requires lengthy multi round computations involving several nodes that seek consensus on a common neighbor verification. Furthermore, the resilience of the protocol to colluding attackers has not been demonstrated. The scheme in suits static sensor networks too, and it requires several nodes to exchange information on the signal emitted by the node whose location has to be verified. Moreover, it aims at assessing not the position but whether the node is within a given region or not. Our NPV solution, instead, allows any node to validate the position of all of its neighbors through a fast, one-time message exchange, which makes it suitable to both static and mobile environments. Additionally, we show that our NPV scheme is robust against several different colluding attacks.

NPV Protocol, The Cross Symmetry Test and The Direct Symmetry Test algorithms used in An authenticated neighbor location in mobile ad hoc networks.

A. NPV PROTOCOL ALGORITHM

The proposed an NPV protocol is designed for spontaneous ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes.

It leverages cooperation but allows a node to perform all verification procedures autonomously. This approach has no need for lengthy interactions, e.g., to reach a consensus among multiple nodes, making our scheme 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.

ALGORITHM

node S do

S ->* : (POLL, K's)

S : store ts

When receive REPLY from X E

S : store txs, cx

after Tmax + Tjitter do

S : ms={(cx, ix)/txs)}

B. THE CROSS-SYMMETRY TEST

The cross symmetry test ignores nodes already declared as faulty by the DS and only considers nodes that proved to be communication neighbors between each other, i.e., for which ToF-derived mutual distances are available. However, pairs of neighbors declaring collinear positions with respect

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

to S are not taken into account. This choice makes our NPV robust to attacks in particular situations.

For all other pair the CST verifies the symmetry of the reciprocal distances and their consistency with the positions declared by the nodes and with the proximity range. For each neighbor maintains a link counter and a mismatch counter. The former is incremented at every new crosscheck on X, and records the number of links between neighbor and other neighbors. The latter is incremented every time at least one of the cross-checks on distance and position fails and identifies the potential for neighbor being faulty.

ALGORITHM

node S do
S:Us←0, Ws←0
forall X E Ns, X E Fs do
if dxy , dyx and
Ps E line(px , py)
S:lx=lx+1, ly=ly+1
If dxy-dyx > 2x+e or
dxy > R then
S: mx=mx+1,

C. THE DIRECT SYMMETRY TEST

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

ALGORITHM

node S do

S: Fs←0

forall X E Ns do

If dsx – dxs > 2 or

ps – px / - dxs > 2 or

dsx > R then

S:Fs←X

V. CONLUSION

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 neighbour 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 neighbour 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.

REFERENCES

[1]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.

[2] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

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

[4] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes," Proc. IEEE INFOCOM, Apr. 2008.

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