OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

A Distributed Approach for Neighbor Position Verification in MANETs

Mahendranath Chowdry Kundla[1], Kancharla Kalpana[2]
[1] *M. Tech (CSE), MVR College of Engineering and Technology, A.P., India.*
[2]*Asst. Professor, Dept. of Computer Science & Engineering, MVR College of Engineering and Technology, A.P., India.*

Abstract: *Mobile Ad Hoc Network(MANET) is a kind of wireless network where you can find number of base stations which supports the communication of mobile nodes. The mobile node supports the routing process of the communication to improve the throughput of the overall network. The mobile nodes are moving at some speed and towards the direction, which makes the topology of the wireless network gets changing at every fraction of time. Due to this reason there will be number of nodes comes into the coverage area of a base station and leaves, which cannot be trusted for service handling. What the adversary does here is that it replies with the route discovery phase using fake location information with the intension to get participate in the routing process. After gets selected it simply discard the packets received, or manipulate the packets, or else it will never receive the packets because of the false location. This makes the transmission as a failure one and service throughput degrades automatically. Location Based Services are one, which is provided and accessed based on the location content. In a road traffic network the location based service can be accessed in various ways. The routing in the road network becomes more complicated due to the increase in mobile nodes. A mobile node can access a service to know about the traffic and the route to reach a destination by accessing the location based service. The correctness of the 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. This paper presents a protocol for updating the position of the node in dynamic mobile ad hoc networks. The protocol adapts quickly to position changes when node movement is frequent, yet requires little or no overhead during the periods in which hosts move less frequently.*

Keywords: *CST, DST, MANET, Neighbor discovery, NPV.*

I. INTRODUCTION

Mobile adhoc networks (MANET) [1] is a popular technology the world society speaks about due to the technology development. The modern world uses internet technology for everything as a part of their life, and now a day they use mobile technology in place of information technology to get access to the location based service. The kind of sophisticated service increases with the risk rate in accessing the service. The service providers have more challenges in providing the services and maintaining the quality of service parameters. A mobile network is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the wireless network topology may change rapidly and unpredictably over time. The MANET network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves. The verification of the node locations is an important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. In order to find out the neighbor nodes and verify them various techniques are proposed.

Neighbour discovery deals with the identification of neighboring nodes with which a communication link can be established or that are within a given distance. An adversarial node could be securely discovered as neighbour node and be indeed a neighbour (within some range), but it could still cheat about its position within the same range. In other words, secure neighbor discovery lets a node assess whether another node is an actual neighbour but it does not verify the location it claims to be at .this is most often employed to counter wormhole attacks. Figure1 shows an example of topological information stored by verifier S at the end of the message exchange and effect of a fake position announcement by M.

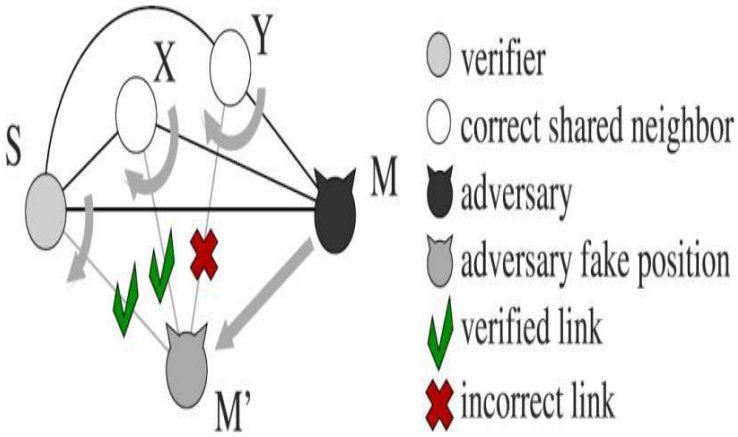

Fig.1: Neighbor discovery in adversarial environment

Neighbor verification [2] schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the neighbor positions announced by third parties. In mobile ad hoc environments, however, the pervasive presence of either infrastructure or neighbour nodes that can be aprioristically trusted is quite unrealistic. Thus, a protocol is devised that is autonomous and does not require the trustworthy neighbours. A mobile ad hoc network is the collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it is necessary for one mobile node to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile node's wireless transmissions. In order to procure the position of other nodes while moving, an approach is proposed such a way that it helps in obtaining the position of a dynamic mobile node. This paper presents a protocol for updating the position of the node in dynamic mobile ad hoc networks. The protocol adapts quickly to position changes when node movement is frequent, yet requires little or no overhead during the periods in which hosts move less frequently.

II. RELATED WORK

In [3] , the authors propose an Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols. The authors present an adaptive Hello messaging scheme to suppress unnecessary Hello messages without reduced detectability of the broken links. Simulation results show that the proposed method reduces energy consumption and the network overhead without any explicit difference in throughput. In [4], the authors propose Dynamic Neighbor Positioning In Manet with Protection against Adversarial Attacks. The authors present techniques for finding neighbours effectively in a non priori trusted environment are identified. These techniques will eventually provide security from attacker nodes. The protocol is robust to malicious attacks. This protocol will also update the position of the mobile nodes in an active environment. The performance of the proposed method will be effective one.

In [5], the authors propose Neighbor node discovery and Trust prediction in MANETs. This paper uses the directional antenna algorithm known as scanning based direct discovery algorithm to discover the neighbour nodes. To enable the cooperative working of the various distributed protocols we use trust system to provide the trust level of various mobile nodes, thereby enhancing the cooperation among the nodes. This paper uses the distributed hybrid trust algorithm and also uses relationship maturity concept to compute the trust of the mobile nodes. This paper demonstrates that Trust systems are better than already existing encryption techniques. For the discovery of mobile nodes [6], the authors explored the various attacks possible in the physical and communication medium of the MANETs. The authors classified the neighbor discovery as physical and communication neighbor discovery. Protocols aiming at communication neighbour discovery, which are based on physical discovery protocols, often fail to achieve their objective. This is because that these two types of discovery are not equivalent. At the same time, the protocols for communication neighbour discovery do not fully address the problem at hand. They are very effective only under very specific operational conditions or they do not ensure correctness in all cases.

For the verification of Neighbor position [7] [8], there are techniques that was studied in the context of mobile ad hoc and sensor networks; however, existing Neighbor Position Verification schemes often rely on traditional or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In mobile ad hoc environments, however, the pervasive presence of either infrastructure or neighbour nodes that can be aprioristically trusted is quite unrealistic.

III. PROPOSED WORK

In this paper we propose a fully distributed cooperative scheme for neighbor position verification (NPV), which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors.

1. NPV Protocol

The proposed NPV protocol is designed for spontaneous mobile ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes. This protocol leverages cooperation but allows a node to perform all verification procedures autonomously. This method has no need for lengthy interactions, e.g., to reach a consensus among multiple mobile nodes, making our scheme suitable for both low and high mobility environments. It is reactive, meaning that it can be executed by any mobile node, at any point in time, without prior knowledge of the neighborhood. It is robust against independent and colluding attacks. It is lightweight, as it generates low overhead routing traffic.

Algorithm 1:
Step 1: node S do
Step 2: S ->* : (POLL, K's)
Step 3: S : store ts
Step 4: When receive REPLY from X E
Step 5: S : store txs, cx
Step 6: after Tmax + Tjitter do
Step 7: S : ms={(cx, ix)/txs)}

2. Direct Symmetry Test

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

Algorithm 2:
Step 1: node S do
Step 2: S: Fs<-0
Step 3: For all X E Ns do
Step 4: If dsx – dxs > 2 or
Step 5: ps – px / - dxs > 2 or
Step 6: dsx > R then
Step 7: S:Fs<-X

3. Cross Symmetry Test

The cross symmetry test(CST) ignores nodes already declared as faulty by the DST and only considers mobile nodes that proved to be communication neighbor nodes between each other, i.e., for which To F derived mutual distances are available. However, pairs of neighbor nodes declaring collinear positions with respect to S are not taken into account. This choice makes our NPV robust to attacks in many particular situations. For all other pair the cross test verifies the symmetry of the reciprocal distances and their consistency with the positions declared by the neighbor 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 communication links between neighbor and other neighbors. The latter is incremented every time at least one of the cross-checks on distance and the position fails and identifies the potential for neighbor being faulty.

Algorithm 3:
Step 1: node S do
Step 2: S:Us<- 0, Ws<- 0
Step 3: For all X E Ns, X E Fs do
Step 4: if dxy , dyx and
Step 5: Ps E line(px , py)
Step 6: S:lx=lx+1, ly=ly+1
Step 7: If dxy-dyx > 2x+e or
Step 8: dxy > R then
Step 9: S: mx=mx+1.

IV. CONCLUSION

In mobile ad hoc networks(MANETs), position aided routing protocols can offer a significant performance increase over fixed ad hoc routing protocols. As position information is broadcasted including the attacker to receive. Routes may be disconnected due to the dynamic movement of mobile nodes. Such mobile networks are more vulnerable to both internal and external attacks due to presence of the attacker nodes. These mobile nodes affect the performance of the routing protocol in ad hoc networks. So it is essential to identify the neighbor nodes in MANET. The Neighbor Position Verification (NPV) is a routing protocol designed to protect the wireless network from adversary nodes by verifying the position of neighbor nodes to improve security, efficiency and performance in ad hoc network routing.

REFERENCES

[1] Chansu Yu, y Ben Lee , Hee Yong Youn, ”Energy Efficient routing protocols for mobile ad hoc networks”, Wireless Communications and Mobile Computing, John Wiley & Sons, Ltd, PP-959–973, 2003.
[2] 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.
[3] Seon Yeong Han, 2013. An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols, IEEE Transactions on communication, 17(5): 1040-1043.
[4] Priyadarshani, K., 2013. Dynamic Neighbor Positioning In Manet with Protection against Adversarial Attacks, IJCER, 3(4).
[5] Thilagavathy, S., 2013. Neighbor node discovery and Trust prediction in manets, International Journal of Science, Engineering and Technology Research (IJSETR), 2(1).
[6] Poturalksi, M., P. Papadimitratos and J.P. Hubaux, 2008. “Towards Provable Secure Neighbor Discovery in Wireless Networks,” Proc. Workshop Formal Methods in Security Eng.
[7] Chiang, J., J. Haas and Y. Hu, 2009. “Secure and PreciseLocation Verification Using Distance Bounding and Simultaneous Multilateration,” Proc. Second ACM Conf. Wireless Network Security (WiSec).
[8] Capkun, S., K. Rasmussen, M. Cagalj and M. Srivastava, 2008. “Secure Location Verification with Hidden and Mobile Base Stations,” IEEE Trans. Mobile Computing, 7(4): 470-483.