RESEARCH ARTICLE OPEN ACCESS

Route Discovery and Hop Node Verification to Ensure Authenticated Data Transmissions in Manet

Anitha.M[1] & Surya.R.M[2] [Asst. Prof]
Dept. Of Applied Electronics Jayam College of Engineering and Technology Nallanur, Dharmapuri.

ABSTRACT
In mobile ad hoc network, Position aided routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. As position information is broadcasted including the enemy to receive. 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 neighbours in MANET. The "Neighbor Position Verification" (NPV), is a routing protocol designed to protect the network from adversary nodes by verifying the position of neighbor nodes to improve security, efficiency and performance in MANET routing.

I. INTRODUCTION

MANET is an autonomous collection of mobile users that communicated over relatively bandwidth constrained wireless links, and the MANETs is to solve challenging real world problems. Since the nodes are mobile so it is dynamic in nature. The network topology may change rapidly and unpredictably over time. It is a unstructured network. It doesn't work constantly under any topology. The network is decentralized where all network activity including discovering and topology and delivering message must be executed by the nodes themselves. Neighbor discovery (ND) provides an essential functionality for wireless devices that is to discover other devices that they can communicate directly through the wireless networking. Routing begin the most essential in the context of wireless communication makes it easy to abuse ND.

The verification of node locations is an important issues in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system.

Finding the position of a neighbour

Neighbour discovery deals with the identification of nodes with which a communication link can established or that are within a given distance. An adversarial node could be securely discovered as neighbour and be indeed a neighbour (with in 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 neighbour but it does not verify the location it claims to be at. This is most often employed to counter wormhole attacks.

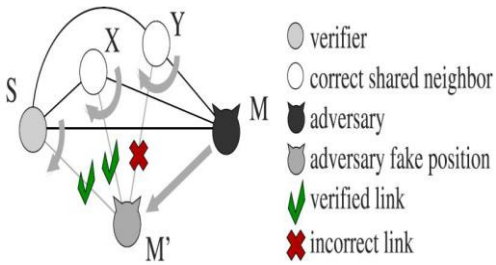


Figure1. Neighbor discovery in adversarial environment

Confirmation of claimed 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 neighbours.

Importance Of Neighbor Position Update

An ad hoc network is the collection of wireless mobile hosts forming a temporary without the aid of any established infrastructure or centralized administration. In such an environment , it is necessary for one mobile host to enlist the aid of other hosts in forwarding packet to its destination, due to the limited range of each mobile host'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 dynamic mobile node. This paper presents a protocol for updating the position of node in

dynamic ad hoc networks. The protocol adapts quickly to position changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

OVERVIEW

The presented a distributed solution for NPV, which allows any node in mobile ad hoc network to verify the position of its communication neighbor without relying on priori trust worthy nodes. The analysis showed that the protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighbourhood of the verifier. simulation results confirm that the solutions is effective in identifying nodes advertising false positions, while keeping the probability of false positions, while keeping the probability of false positives low. Only an overwhelming presence of colluding adversaries in the neighbourhood 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 protocols, as well as at extending it to proactive paradigm, useful in presence of applications that position of the neighbours.

PROBLEM STATEMENT

This 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.

II. EXISTING SYSTEM

In existing methodology, a fully distributed cooperative scheme for NPV, which enables a source node, to discover and verify the position of its communication neighbours. For clarity, here we summarize the principles of route discovery and position verification process. A source node, S can initiate the protocol at any time instant, by triggering the 4-step message exchange process [POLL, REPLY,REVEAL and REPORT], after completing the message exchange process, source node S has derives distance range of neighbour nodes to discover the shortest path to reach destination, after route discovery S runs several position verification tests in order to classify each candidate neighbour as either VERIFIED, FAULTY, UNVERFIABLE. Clearly , 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. we remark that our NPV scheme does not target the creation of a consistent "map" of neighbourhood relations throughout an ephemeral network: rather, it allows the verifier to independently classify its neighbours.

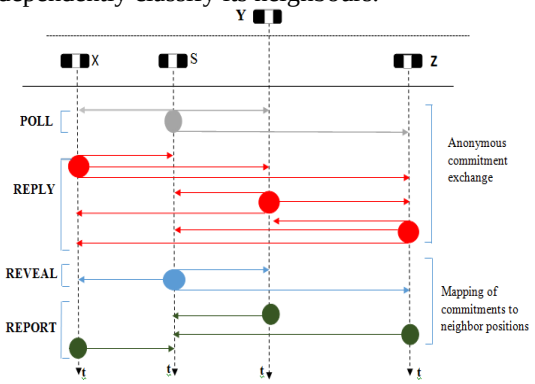


Figure2.Messages Exchange Process

EXISTING SYSTEM METHODOLOGY

POLL message A verifier S initiates this message. This message is anonymous. The identity of the verifier is kept hidden. Here software generated MAC address 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 XCX.

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.

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

The node position verification is not suitable for dynamic environment, since mobile nodes are in dynamic in nature, so each and every schedule the mobile nodes undergoes position verification test, thus results in delay time of packet delivery ratio.

III. PROPOSED SYSTEM

In proposed system the NPV protocol is extended to dynamic source configuration routing protocol, which results in mobile node verification

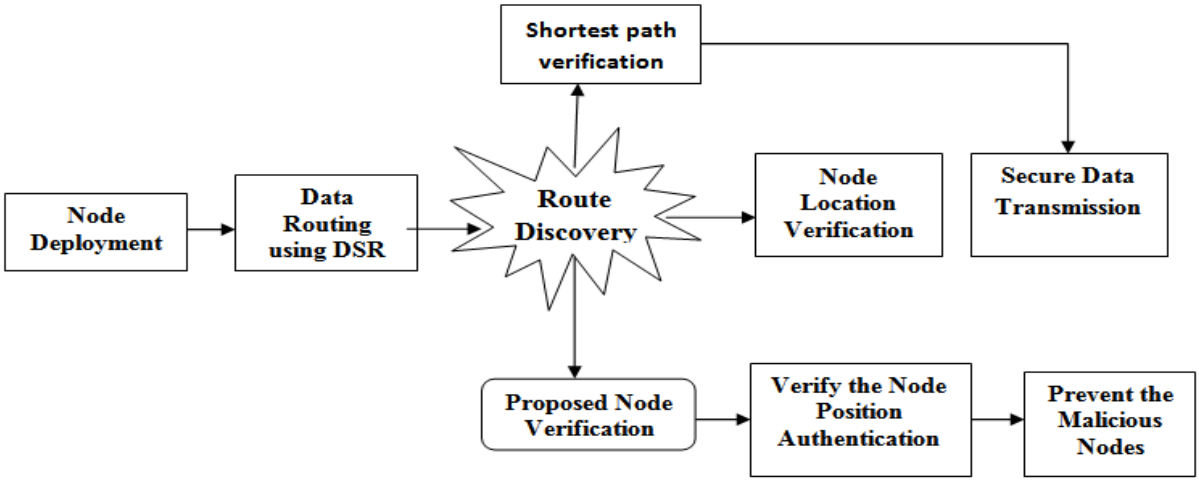
instead of node position verification. The node position verification achieved through hash function, which states that if source node wants to verify the neighbor nodes the source S generates a hash id through hash function H(n)=PUB_KEY/IDENTITY, the public key and id of source node generates hash id. In the same way the neighbor nodes generates hash id are same then the nodes are authenticated for data transmission through the minimum distance range discovered path to destination.

The proposed technique works in all kinds of environment and provides a secure data transmission and also decreases the time delay, improves the PDR, and throughput rate in network performance.

Proposed Algorithm Implementation

MD5 (MESSAGE-DIGEST ALGORITHM) 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.

IV. SYSTEM MODEL



Node Configuration Setting

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.

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.

Message exchange process for route discovery

This module states a 4 step message exchange 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, allowing nodes to record reciprocal timing information without disclosing their identities.

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. The source S uses such data to match timings and identities; then, it uses the timings to perform To F-based ranging and compute distances between all pairs of communicating nodes in its neighborhood.

Node Position Verification

Once Source node has derived such distances, it runs several position verification tests in order to classify each candidate neighbor as either: Verified node, i.e., a node the verifier deems to be at the claimed position or Faulty node, i.e., a node the verifier deems to have announced an incorrect position or Unverifiable node, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information. The position verification is performed by direct symmetric test, cross symmetry test and multilateration test.

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. In the same way the neighbor nodes generate the hash id, if the source node hash id and neighbor node hash id are same then the nodes are authenticated for data transmission through the minimum distance range discovered path to destination.

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). In the on-demand protocols, routes are discovered between a source and a destination only when the need arises to send data.

This provides a reduced overhead of communication and scalability. In the table-driven protocols, routing tables which contain routing information between all nodes are generated and maintained continuously regardless of the need of any given node to communicate at that time. With this approach, the latency for route acquisition is relatively small, which might be necessary for certain applications, but the cost of communications overhead incurred in the continued update of information for routes which might not be used for a long time if at all is too high.

DSR - Dynamic Source Routing Protocol

DSR is one of the most well known routing algorithms for ad hoc 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 that are either forwarding route discovery requests or overhearing packets through promiscuous listening mode to cache the routing information for future use.

DSR is also on demand, which reduces the bandwidth use especially in situations where the mobility is low. It is a simple and efficient routing protocol for use in ad hoc networks. It has two important phases, route discovery and route maintenance.

V. 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 protocol will also update the position of the nodes in an active environment. The performance of the proposed scheme will be effective one.

REFERENCES

[1] Marco Fiore,Claudio Ettore Casetti and Panagioties papadimitratos " Discovery And Verification Of Neighbor Position In Mobile Ad Hoc Networks", Members IEEE,feb 2013

[2] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.

[3] 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.

[4] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.

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

[6] 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.

[7] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux,"A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.

[8] 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.

[9] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm.Security (ASIACCS), Mar. 2008

[10] 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.

Anitha.M has obtained her BE degree in Electronics and Communication Engineering from Sengunthar college of Engineering, Tiruchencode in 2012. Currently she is doing her ME in Applied Electronics at Jayam College of Engineering and Technology, Dharmapuri. Presently she is involving in developing a advanced security method for data transmission in mobile ad hoc networks. She has published more than two research papers in national and international conferences. Her special areas of interest are networking, mobile computing and digital electronics.

Surya.R.M has obtained her BE degree in Electronics and Communication Engineering from Paavai Engineering College. She received her ME degree in Applied Electronics from Jayam College of Engineering and Technology. She published more than six research papers in various national and international conferences/journals. At present She is working as Assistant Professor in the department of Electronics and Communication Engineering in Jayam College of Engineering and Technology. She has participated in various national level workshops and seminars at various colleges.