International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Efficient Route Discovery by Selecting Link Stability Neighbors in MANET

R. Maruthaveni[1], R. Latha[2]

[1]Dr. SNS Rajalakshmi College of Arts and Science, Saravanampatti, Coimbatore -49, India

[2]Dr. SNS Rajalakshmi College of Arts and Science, Saravanampatti, Coimbatore -49, India

Abstract: ***Energy awareness for computation and protocol management is becoming a crucial factor in the design of protocols and algorithms. On the other hand, in order to support node mobility, scalable routing strategies have been designed and these protocols try to consider the path duration in order to respect some QOS constraints and to reduce fake neighbor position for route discovery. Often energy saving and path duration and stability can be two contrasting efforts and trying to satisfy both of them can be very difficult because such a process can be easily abused or disrupted by adversarial nodes. Neighbor discovery is an important part of many protocols for mobile ad hoc networks, including localization and routing. When neighbor discovery fails, communications and protocols performance deteriorate. In this paper, we address this open issue by proposing mobile secure neighbor discovery with respect to select the most stable path so as to reduce the latency and the overhead due to route reconstruction, which offers a measure of protection against fake positions by allowing participating mobile nodes to securely determine if they are neighbors. We prove security properties of our protocol, and demonstrate its effectiveness through GLOMOSIM simulations.***

Keywords: *Mobile adhoc networks Security and Classifications, Highly Dynamic networks.*

1. 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 1) correctly establish their location in spite of attacks feeding false location information, and 2) 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. 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.
- 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 lightweight, as it generates low Overhead traffic.

2. 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.

Securely determining own location. 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. Secure neighbor discovery (SND) deals with the identification of nodes with which a communication link can be established. 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.

NPV schemes often rely on fixed 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. 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. 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.

3. Literature Survey

Mobile Ad Hoc Network

Ad hoc networks are emerging as the next generation of networks and defined as a collection of mobile nodes forming a temporary (spontaneous) network without the aid of any centralized administration or standard support services. An ad hoc network is usually thought of as a network with nodes that are relatively mobile compared to a wired network.

A Community Based Mobility Model for Ad Hoc Network Research

Validation of mobile ad hoc network protocols relies almost exclusively on simulation. The value of the validation is, therefore, highly dependent on how realistic the movement models used in the simulations are. Since there are a very limited number of available real traces in the public domain, synthetic models for movement pattern generation must be used. The model allows collections of hosts to be grouped together in a way that is based on social relationships among the individuals. This grouping is then mapped to a topographical space, with movements influenced by the strength of social ties that may also change in time.

The definition of realistic mobility models is one of the most critical and, at the same time, difficult aspects of the simulation of applications and systems designed for mobile environments. Currently, there are very few and very recent public data banks capturing node movement in real large-scale mobile ad hoc environments.

Protocol with Stability Link for MANETS

In recent years' mobile ad hoc networks (MANETs), a group oriented services has one of the primary application classes. It supports such services that use multicast routing. Therefore it is required to design stable and an efficient routing protocol for MANETs to support better packet delivery ratio, minimum delays and decreased overheads. In this paper, a multicast routing protocol based mesh networks that finds stable multicast path from source to receivers is proposed. This model enhances link stability with contention delay and queuing system. The stable routes are found based on selection of stable forwarding nodes that have high stability of link connectivity. The link stability is calculated by using parameters link received power, distance between neighboring nodes and link quality. The performance of the proposed model is simulated over a large number of MANET nodes with wide range of mobility with two well known mesh based multicast routing protocol. It is observed that the proposed model produces better throughput and reduced overheads. It is the extension of AODV routing protocol where the multicast groups are identified by a unique address and group sequence number. When a node wants to join a multicast group(Perkins et al), it checks whether or not it is the first multicast receiver by checking the multicast announcement data.

LSLP: Link Stability and Lifetime Prediction Based Qos Aware Routing for MANET

As mobile ad hoc network is burgeoning, different applications are developing with different service requirement. In particular multimedia applications and other real time applications e.g. voice transmission requires very stringent and inflexible quality of service (QoS). A great magnitude of attention has been paid against cost and energy consumption and mobility for non-QoS-aware routing protocols. While QoS-aware routing protocols put emphasis on QoS matrices and mobility individually. Unrestricted mobility of nodes invalidates old paths, causing the packets of the flow to wait until the routing protocol is able to get information about the new paths. This degrades the performance of the network, reducing the throughput and increasing the delay and packet loss. In this paper, we mingled the idea of link stability and energy consumption to uncover better path in terms of both stability and cost along with QoS support.

A mobile ad hoc network is envisaged as a collection of mobile nodes with no fixed infrastructure and with no central authority. Extensive use of portable mobile devices and the increasing demand of connectivity among the devices have made mobile ad hoc network as one of the flourishing frontier of wireless research. Mobile ad hoc network is a self-configured and self-maintained network with no centralized authority. Other remarkable features of MANET include quick and inexpensive deployment and network with unrestricted mobility. Every node in MANET acts as both a host and a router and must perform some network function.

As a consequence MANET faces routing challenges for its dynamic nature. With the development of the MANET, people pay more and more attention to the power aware routing strategy and QoS routing strategy. Because mobile hosts in the network such as PDA, notebook are mostly power constrained, saving their power and consequently prolonging the lifetime of the network is the focus of the power aware routing strategy. However, there is little research work has been done to combine these two strategies.

Single-Copy Routing In Intermittently Connected Mobile Networks

Intermittently connected mobile networks are wireless networks where most of the time there does not exist a complete path from source to destination, or such a path is highly unstable and may break soon after it has been discovered. In this context, conventional routing schemes would fail. To deal with such networks an opportunistic hop-by-hop routing model is used. According to the model, a series of independent, local forwarding decisions are made based on current connectivity and predictions of future connectivity information diffused through nodes' mobility.

The important issue here is how to choose an appropriate next hop.

There are two major categories of hop-by-hop routing schemes, single-copy routing schemes and multiple-copy routing schemes. In single-copy routing schemes there's only a single custodian for each message. Multiple-copy routing schemes may generate multiple copies of the same message which can be routed independently for increased efficiency and robustness.

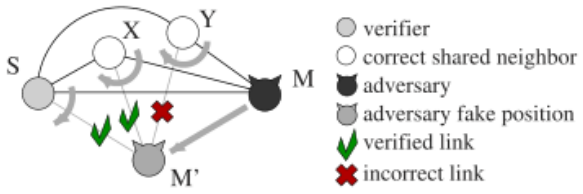
A number of different single-copy routing algorithms are proposed, and their performance is evaluated using both simulation and analysis. Finally, a hybrid single-copy routing algorithm is shown to achieve the best performance among all existing and proposed single-copy schemes.

Some of the single copy routing strategies are,
- Direct Transmission
- Randomized Routing Algorithm
- Utility-based Routing

4. Systems and Adversary Model

We consider a mobile network and define as communication neighbors of a node all the other nodes that it can reach directly with its transmissions.

Neighbor discovery is the process by which a node in a network determines the total number and identity of other nodes in its vicinity. It is a fundamental building block of many protocols including localization, routing, leader election, and group management. In wireless networks, neighbors are usually defined as nodes that lie within radio range of each other. Attackers have the freedom to perform malicious activities ranging from simple denial of service to sophisticated deception. 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.



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 attacks.

Neighbor position verification was studied in the context of ad hoc and sensor networks; however, existing NPV schemes often rely on or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. Thus, we devise a protocol that is autonomous and does not require trustworthy neighbors.
- 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.

5. Methodology

To our knowledge, our protocol is the first to provide a fully distributed, lightweight solution to the NPV problem that does not require any infrastructure or a priori trusted neighbors and is robust to several different attacks, including coordinated attacks by colluding adversaries.

We propose a fully distributed cooperative scheme for NPV, which enables a node, here in after called the verifier, to discover and verify the position of its communication neighbors. A verifier, S, can initiate the protocol at any time instant, by triggering the 4-step message exchange called POLL, REPLY, REVEAL and REPORT, within its 1-hop neighborhood. The aim of the message exchange is to let S as source collect information it can use to compute distances between any pair of its communication neighbors. To that end, POLL and REPLY messages are first broadcasted by S 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. Then, after a REVEAL broadcast by the verifier, nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected. The verifier S uses such data to match timings and identities; then, it uses the timings to perform ranging and compute distances between all pairs of communicating nodes in its neighborhood. Once S has derived such distances, it runs several position verification tests in order to classify each candidate neighbor as either:
1) Verified, i.e., a node the verifier deems to be at the claimed position;
2) Faulty, i.e., a node the verifier deems to have announced an incorrect position;
3) Unverifiable, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information.
4) We remark that our NPV scheme does not target the creation of a consistent "map" of neighborhood relations throughout an ephemeral network: rather, it allows the verifier to independently classify its neighbors.

- Our NPV scheme is compatible with state-of the-art security architectures, including the ones that have been proposed for vehicular networks.
- It is lightweight, as it generates low overhead traffic.
- It is robust against independent and colluding adversaries
- It leverages cooperation but allows a node to perform all verification procedures autonomously

6. Results of MANET

Finally, based on our findings, as future work we focus on an approach to find and select routes, which accounts for the

expected data transfer time over the path and allows to reduce the overhead of reactive routing protocols. In future, present the design, implementation, and evaluation of the Adaptive Routing protocol for delay-tolerant unicast communication in intermittently connected sensor networks. In the evaluation of protocol, the performance is compared with regard to the following metrics.

1) Message delivery ability
2) Message delivery delay
3) Message exchanges

7. Conclusion

We studied the duration and availability probabilities of routing paths in MANETs—a fundamental issue to provide reliable routes and short route disruption times. We focused on the Random Direction mobility model and derived both exact and approximate (but simple) expressions for the probability of path duration and availability. We used these results to determine the optimal path in terms of route stability; in particular, we showed some properties of the optimal path and we provided an approximate yet accurate expression for the optimal number of hops.

8. Scope of Future Enhancement

A fundamental issue arising in mobile ad hoc networks (MANETs) is the selection of the optimal path between any two nodes. Ensuring a data path to be valid for sufficiently longer period of time is a very difficult problem in MANET due to its highly dynamic nature. A method that has been advocated to improve routing efficiency is to select the most stable path so as to reduce the latency and the overhead due to route reconstruction.

As per Distributed cooperative scheme for NPV technique, solves the neighbor verification and this scheme does not concentrate on link failures which is more often in MANET network so neighbor position verification is not get optimized results thus provide solution to link breakages through path quality technique and enhance neighbor position verification technique as per path quality technique which delivers results in efficient manner.

This routing technique applies the following three metrics for path quality neighbor coverage selection:

1) The estimated total energy to transmit and process a data packet
2) The residual energy
3) The path stability. Route maintenance and route discovery procedures are similar to the DSR protocol, but with the route selection based on the three aforementioned metrics. Delivery probabilities are synthesized locally from context information's like value describes the above metrics. A delivery probability of each node is used to select link stability path over dynamic route discovery.

The process of prediction and evaluation of the context information in proposed technique can be summarized as follows:

1) Each node calculates its delivery probabilities for a given set of nodes.
2) This process is based on the calculation of utilities for each attribute describing the context.
3) The calculated delivery probabilities under current status are periodically sent to the route request neighbor with its positions as part of the update of routing information like current position information.
4) Each node maintains a logical forwarding table of tuples describing the next logical hop and its associated delivery probability and predicted position information for all known destinations.
5) Each node uses local prediction of delivery probabilities with respect to neighbors between updates of information.
6) Each node selects the best forwarding node among list of neighbor's on the basis of highest stability value and position verified node.

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 1) correctly establish their location in spite of attacks feeding false location information, and 2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations. 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.

References

[1] 1609.2 - 2006 : IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.
[2] 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,
[3] P. Papadimitratos and A. Jovanovic, "GNSS- Based Positioning : Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.
[4] 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.
[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. Zhong, M. Jadliwala, S. Upadhyaya, a nd C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes," Proc. IEEE INFOCOM, Apr. 2008.
[7] 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.
[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, " Proc. IEEE INFOCOM,
[9] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "TrueLink: A Practical Countermeasure to the

Wormhole Attack in Wireless Networks," Proc. IEEE 14th Int'l Conf. Network Protocols (ICNP), Nov. 2006.
[10] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information, " Proc . IEEE INFOCOM, Apr. 2007.
[11] 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),
[12] 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),