Discovery of Neighbor Nodes with Protection against Adversarial Attacks in MANETs

[1.]M. Sangeetha, [2.]R. Geetha, [3.]V. Aishwarya, [4.]R. Subash
[1,2,3,4.] Department of CSE,
Ranganathan Engineering College,
Coimbatore, India.

***Abstract*— Mobile Ad hoc Networks are configuring itself with the autonomous networks that do not require any central authority to control and coordinate the network. Neighborhood Discovery is the discovery process in that the mobile nodes or devices which are directly reachable for communication or within the transmission range. If the source and destination are within the transmission range there is no need for discovering the position of their neighbor nodes. Neighbor Discovery process can be disturbed by the adversarial nodes for harming the system and attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. For this problem, we provide a solution by introducing the Neighbor Position Discovery & Verification (NPDV) protocol for discover and verify the position of the neighbor nodes in MANET and also protect against the attacks caused by the adversarial nodes.**

Keywords*— *Mobile Ad hoc Networks; Neighborhood Discovery; Neighbor Position Discovery & Verification

I. INTRODUCTION

Neighbor discovery, as the name suggests, is the process of identifying the neighbor nodes within the transmission range. A neighbor of a node X is defined as one that is within the communication range of X. An adversary intending to disturb the neighbor discovery protocol, will try to make two non neighboring nodes believe that they are neighbors or will prevent two neighboring nodes from becoming neighbors.

Neighbor discovery is one of the first steps performed by a node upon deployment and disrupting it adversely affects a number of routing, MAC, topology discovery and intrusion detection protocols. It is especially harmful when an adversary can convince nodes that it is a legitimate neighbor, which it can do easily and without the use of cryptographic primitives.

Nodes found within the neighborhood are neighbors and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, sensing and localization. Neighbor discovery is especially important to the proper functioning of wireless networks.

When neighbor discovery fails, communications and protocols performance deteriorate. Neighbor discovery means determining whether a wireless device (node) is directly reachable without the assistance of any other device according to the predesigned rules of the network or not. Neighborhood can be unidirectional or bidirectional depending on whether only one side is able to deliver its messages to the other side or both sides are capable of doing so. A neighbor discovery attacker tries to deceivingly convince the nodes to believe that they are neighbors of a specific set of nodes (possibly including the adversary herself), when they are actually not. There are various types of attacks on neighbor discovery scenarios. The effectiveness level of an attack depends on whether the adversary is a part of the network or not.

Every neighbor discovery protocol is composed of a series of packet transmissions. In a weak protocol, these attacks can be launched to relay neighbor discovery packets to other areas of the network, in order to convince distant nodes to believe that they are true neighbors. 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, we focus on the aspect, hereinafter referred to as neighbor position discovery and verification (NPDV 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 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 NPDV procedure that

enables each node to acquire the locations advertised by its neighbors, and assess their truthfulness.

Nodes are correct if they comply with the NPDV protocol, and adversarial if they deviate from it. As authentication essentially thwarts external adversaries, we focus on the more powerful internal ones, i.e., nodes that possess the cryptographic material to participate in the NPDV and try to exploit it, by advertising arbitrarily erroneous own positions.

In mobile ad hoc network, Position aided routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. These routing protocols use geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. However, current position aided routing protocols were not designed for use in high-risk environments, as position information is broadcasted in the clear allowing anyone within range, including the enemy, to receive.

We study methods for route discovery and verification of neighbor's position information in MANET routing protocols, and ways to use the position information to enhance performance and security of MANET routing protocols. We introduce "Neighbor position discovery & verification" (NPDV), 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.

A. Attacks on Neighbor Discovery

To describe the current solutions for the neighbor verification problem categorize the attacks into two groups based on their resistance to internal (intrusive) or external (non-intrusive) attacks. In external attacks the adversary is not able to compromise the nodes and hence, does not have access to the private information like the cryptographic keys and communication codes stored in the memory of the nodes.

Usually, an external attacker is only able to overhear (eavesdrop), relay (replay) or block (jam) the packets. On the other side, an internal attacker is capable of masquerading himself as a legal node and thus can imitate all the behaviors of a healthy node. Having the private cryptographic keys, she can even generate fake (but authenticated) messages to obtain a higher number of neighbors to what a traditional healthy node does. It is rather obvious that the second type of adversary is much more powerful than the first one.

There are a few general attacks which have effects on neighbor discovery, and a few others which specifically address the neighbor-discovery-related issues. One of the oldest external passive attacks is eavesdropping. Regardless of the protocol architecture, an adversary is always able to overhear wireless communications. There is little chance for the designer to block eavesdropping. However keyed cryptographic operators (like the encryption ones) are quite useful in keeping the external adversaries from extracting sensitive information out of the transmitted signal.

Neighbor discovery protocols are no exception. The protocol designer must seal the places where the information might leak during wireless transmissions. The active invasions that target the availability of network services are called Denial of Service (DoS) attacks. DoS attacks can be planned to work on any layer of the network protocol stack depending on how much weak that layer is.

Jamming can be well categorized into the physical layer DoS attacks group. There are only a few non-perfect classic solutions like spread spectrum communication for this attack. Other types of DoS attack also exist among which some try to excessively overload a badly designed protocol run on a resource-limited machine. So, one can easily conclude that in sensor networks, designing a DoS-resilient neighbor discovery protocol is more complicated than in ad hoc networks. Ignoring the heuristic solutions, the classic countermeasures for protocol-related DoS attacks are easy-to-compute checksums and ciphers that reject massive fake messages.

Relaying and replaying are two other simple but powerful attacks. In the replay attack, an adversary uses an old packet which was previously generated by a healthy node in order to deceive another healthy node in the future. To overcome this problem researchers have suggested using timestamps (in clock-synchronized networks) and nonces.

II. EXISTING SYSTEM

In 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. The mobile networks become particularly challenging in the presence of adversaries aiming at harming the system.

Correctly establish their location inspite of attacks feeding false location information, and verify the positions of their neighbors, so as to detect adversarial nodes announcing false location is obtained by the proposed system. In the existing system, neighbor position verification protocol should not be used in. So there is no security is possible. Third parties (authorized person) should not be included so the correct information could not be forward.

Existing NPDV scheme is based 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. It is used that first lets nodes calculate distances to all neighbors and this scheme does not rely on trustworthy nodes, but it is designed for static sensor networks, and requires lengthy multiround computations involving several nodes that seek consensus on a common neighbor verification. It also allows nodes to validate the position of their neighbors through local observations only. This is performed by checking whether subsequent positions announced by one neighbor draw a movement over time that is physically possible. This approach forces a node to collect several data on its neighbor movements before a decision can be taken, making the solution unfit to situations where the location information is to be obtained and verified in a short time span. Moreover, an adversary can fool the protocol by simply announcing false positions that follow a realistic mobility pattern.

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[1]. 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 neighbor nodes to discover the shortest path to reach destination, after route discovery S runs several position verification tests in order to classify each candidate neighbor 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 NPDV 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.

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. 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 defence mechanisms [2]. Alternatively, terrestrial special purpose infrastructure could be used along with techniques to deal with nonhonest beacons [3].

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 [4]. 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.

Neighbor position verification was studied in the context of ad hoc and sensor networks; however, existing NPV schemes [5] 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.

III. PROPOSED SYSTEM

In proposed system the NPDV protocol is extended to dynamic source configuration routing protocol, which results in the mobile node verification instead of node position verification. The node verification is 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 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. By using the proposed NPDV protocol we can increase the transmission range and also there is no lengthy multi round calculations. It can prevent upto 99% of the adversarial attacks

Neighbor Position Discovery & Verification (NPDV) protocol has the following features:

- It is mainly designed for spontaneous ad hoc environments and it is rely on the absence of a trusted infrastructure or of a trustworthy nodes.
- It allows a node to perform all verification procedures simultaneously. This approach has no need for lengthy interactions. It is suitable for both low and high mobility environments.
- It can be executed by any node, at any point in time, without prior knowledge of the neighbourhood and also returns the result in time span.
- It is strong against independent and colluding adversaries.
- It is lightweight, as it generates low overhead traffic.

NPDV protocol is compatible with state of the art security architectures. In this we provide 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. NPDV protocol is reactive, as it can be executed at any instant by any node, returning a result in a short time span and robust to fake, yet realistic, mobility patterns announced by adversarial nodes over time.

The multitude of ad hoc security protocols addressing a number of problems related to NPDV, there are no lightweight, robust solutions to NPDV that can operate autonomously in an open, ephemeral environment, without relying on trusted nodes. It provides solutions to some NPDV related problems, such as secure positioning and secure discovery, and then we discuss solutions specifically addressing NPDV. Nodes are correct if they comply with the NPDV protocol, and adversarial if they deviate from it.

A fully distributed cooperative scheme for NPDV, which enables a node, hereinafter 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 four step message exchange within its one hop neighborhood.

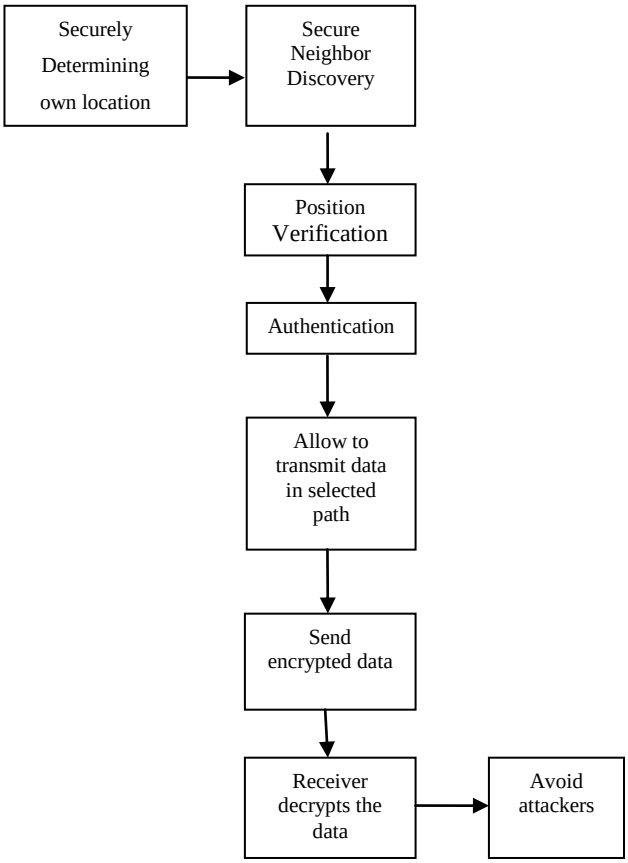

Fig.1. Architecture Diagram

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. The challenge is to perform, in absence of trusted nodes, a fully distributed and lightweight NPDV procedure that enables each node to acquire the locations advertised by their neighbors, and assess their truthfulness. NPDV protocol allows nodes to validate the positions of their neighbors through local observation only.

A. System Model

Consider a mobile network and define as communication neighbors of a node all the other nodes that it can reach directly with its transmissions. We assume that each node knows its own position with some maximum error and that it shares a common time reference with the other nodes: both requirements can be met by equipping communication nodes with GPS receivers. Each node owns private key, and a public key, as well as a set of one-time use keys as proposed in emerging architectures for secure and privacy-enhancing communication. Node can encrypt and decrypt data with its keys and the public keys of other nodes; also, it can produce digital signatures with its private key.

B. Neighbor Discovery

To discover and verify the position of its communication neighbors we enable a node called verifier (authorized person). Message exchange described in within its hop neighborhood. The aim of the message exchange is collect information it can use to compute distances between any pair of its communication neighbors. All information collected from authorized person. POLL and REPLY messages are first broadcasted by verifier (authorized person) and its neighbors, respectively. Verifier 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.

Fig.2. shows the network topology of the mobile nodes in the adversarial environment. Let S be the verifier which involves in discovery and verify the position of its neighbor and M be the adversary node announces a fake position M' for indicating the neighbor node to forge the messages.

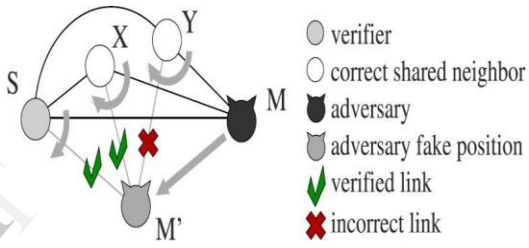

Fig.2. Network Topology of Mobile nodes

A fully distributed cooperative scheme for NPV, which enables a node, hereinafter 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 four step message exchange within its one hop neighbourhood.

C. Message Exchange

The message exchange is between the verifier and its communication neighbors followed by a description of the tests run by the verifier. Now, consider a verifier that initiates the NPV protocol. To retrieve the exact transmission and reception time instants avoiding the unpredictable latencies introduced by interrupt triggered at the drivers level, a solution such as that implementation is required.

Furthermore, the GPS receiver should be integrated in the 802.11 card; software defined radio solutions combining GPS and 802.11 capabilities are proposed. The message exchange procedure is outlined in Algorithm for verifier and in Algorithm for any of communication neighbors.

The aim of the message exchange is to let S collect information it can use to compute distance between any pair of its communication neighbors. POLL and REPLY messages are 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 timing information they collected.

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

IV. RESULT EVALUATION

To evaluate the performance of our NPDV, at every simulation second we randomly select 1 percent of the nodes as verifiers. Then, for each verifier, we compare the outcome of the verification tests with the actual nature of the neighbors.

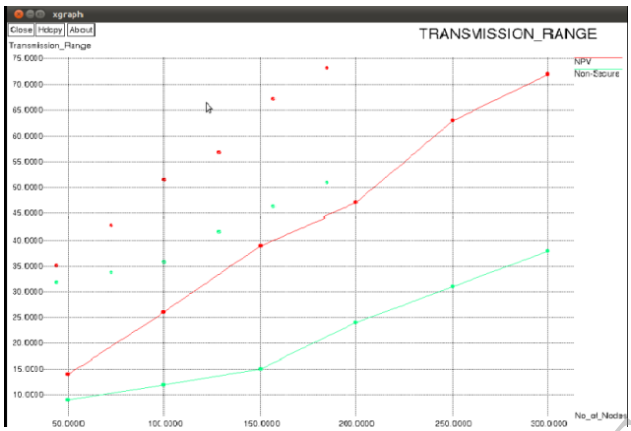

Fig.3. Transmission Range

The above figure shows the comparison of transmission range for the proposed system with the non secure protocol. This also represents the successful measure of our proposed protocol.

V. CONCLUSION

In this, we provide a solution for Neighbor Position Verification problem by using NPDV protocol in the presence of adversarial environment of mobile nodes. Our solution provides the protection against the adversarial attacks and involves secure communication between the source and destination. In this proposed system, transmission range increases and sends the message in single route. In future we enhances by sending the message by using multi path routing for efficient communication between the sender and the receiver.

REFERENCES

[1] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini, Panagiotis Papadimitratos. "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks". IEEE transactions on mobile computing, vol. 12, no. 2, February 2013.

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

[3] 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.

[4] 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.

[5] 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.