IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 131-137
www.iosrjournals.org

Discovery and Verification of Neighbor Positions in MANETs using Extended NPV Protocol

Sherimol Hameed,Deepu S
PG Scholar,Department of ECE,University College of Engineering,Muttom,India
Lecturer Department of ECE,University College of Engineering,Muttom,India

ABSTRACT*: MANET is an autonomous collection of mobile nodes that communicated over relatively bandwidth constrained wireless links.In such communication these networks are highly vulnerable to internal and external attacks due to the presence of adversarial nodes.In this research work, we first analyze the problems that may arise from falsified position data. Then inorder to lessen these problems we propose a detection mechanism that are capable of recognizing nodes cheating about their location. In contrast to other position verification approaches our solution does not rely on special hardware. It involves verification of nodes position by different tests and thereby widely prevents attacks using position cheating and communication is achieved through the successful nodes in the case of proactive enviornment.The results show that our proposed system improves the network security and performance.*

Keywords*- Neighbor Position Verification Protocol(NPV);Mobile AdHoc Networks(MANET); Vehicular AdHoc Network(VANET); Routing Protocols.*

I . INTRODUCTION

During the recent years ,Mobile Ad hoc networks (MANETs) have attracted a lot of attention in the research community. Inter-vehicle communication is regarded as one of the major applications of mobile ad hoc networks (MANETs). A 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. The existing system address this open issue by proposing a fully distributed cooperative solution that is robust against independent and colluding adversaries, and can be impaired only by an overwhelming presence of adversaries. Results show that our protocol can thwart more than 99 percent of the attacks under the best possible conditions for the adversaries, with minimal false positive rates even in the mobile environment.

The existing systems have proposed a number of positioning and distance estimation techniques for mobile ad hoc networks. But the majority of distance estimation and positioning techniques are highly vulnerable to attackers like internal and external attacks. The most obvious threat to sensor network is the physical displacement of the nodes and such type of attacks are called node displacement attack. The current system is not dealing with such type of attacks. Finally factors such as small and large scale fading, diffraction and scattering cause the signal to be disrupted in certain areas. In such cases nodes correctly establish their location in spite of attacks feeding false location information.

The basic needs of the study is to Achieve Intelligent Transportation System which avoid collision and route vehicle properly to improve safety,Movement co-ordination among autonomous robotic networks,Data gathering in MANETs,Can be used in military applications to send confidential data. .In this study, we focus on Mobile ad hoc networks where a pervasive infrastructure is not present and we analyze the reactive protocol such as neighbor position verification (NPV).Finally we propose a modified algorithm that can be applied to mobile environment and then btain a simulation model of this algorithm in network Simulator. The main objective of this is to study about the mobile and vehicular ad hoc networks,to identify location verification and distance estimation techniques,to understand different geographic routing protocols like PLV,RLV,NPV, to analyze different types of attackers and their effect on the communication network,finally how to protect our communication network from these attacks.

II. EXISTING SYSTEM

Location awareness is becoming an important capability for mobile computing devices, where many protocols need knowledge of the position of the participating nodes. For example, knowledge about neighboring nodes can be used to route, cluster and broadcast in an efficient manner. Whenever a node needs to send data to

another node on a network, it must first know where to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a proper route to the destination node.In such cases it is essential to provide the availability of neighbor information. The described NPV procedure that enables each node to attain the locations advertised by its neighbors, and evaluate their truthfulness.But the main drawback it is used to verify the position of the neighbors that the nodes declare[1].

The progress in the area of efficient localization algorithms, the problem of malicious beacon nodes has not received sufficient attention. In this paper, we study the robust localization problem in the presence of such nodes. In particular, we establish necessary and sufficient conditions for distributed distance-based localization in the presence of a given number of malicious nodes. To prove the sufficient condition, we propose LOCOMO, a novel and efficient distance-based localization framework that can provide a guaranteed degree of localization accuracy.[2].Pervasive computing systems will likely be deployed in the near future, with the proliferation of wireless devices and the emergence of ad hoc networking as key enablers. Coping with mobility and the volatility of wireless communications in such systems is critical. Neighborhood Discovery (ND), namely, the discovery of devices directly reachable for communication or in physical proximity, becomes a fundamental requirement and a building block for various applications. However, the vary nature of wireless mobile networks makes it easy to abuse ND and thereby compromise the overlying protocols and applications. Thus, providing methods to mitigate this vulnerability and to secure ND is crucial. Securing ND is indeed a difficult and largely open problem. Moreover, given the severity of the problem, we advocate the need to formally model neighborhood and to analyze ND schemes.[3] The main drawbacks are message length grows as more and more nodes are discovered and the presence of physical obstacles may cause nodes to incorrectly infer another node as its neighbor.

NPV protocol is used to exchange the messages and verifies the position of communicating nodes. In this protocol four sets of messages are exchanged.They are

- POLL message
- REPLY message
- REVEAL message
- REPORT message

POLL message
A verifier S initiates this message. This message is anonymous. The verifier identity is kept hidden.

REPLY message
A communication neighbor X receiving the POLL message will broadcast REPLY message after a time interval.

REVEAL message
The REVEAL message broadcasting is done by using Verifier's real MAC address. It contains a proof that S is the author of the original POLL and the verifier identity.

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 the REPLY broadcasts X received.[4].

In the recent years, mobile *ad hoc* networks (MANETs) have attracted a lot of attention in the research community. Still, there are very few real application scenarios where the wide deployment of MANETs is really foreseeable in the near future. It describes the summary of knowledge for security issues in Mobile ad hoc Networks (MANEt). Even though there are papers that approach certain aspects of the security field, risks and threats are still there.We propose solutions to the current state in respect to the network security.[5].

The mobile ad hoc network has the following typical features .

1.Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

2.Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

3.Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.[6].

Mobile devices obtain their own location with the help of Global Navigation Satellite Systems (GNSS), integrating, for example, a Global Positioning System (GPS) receiver. Nonetheless, an adversary can compromise location-aware applications by attacking the GNSS-based positioning: It can forge navigation messages and mislead the receiver intocalculating a fake location.[7].

Location verification is a technique which is used to ensure that information about the location of vehicles being disclosed is correct. There are a few strategies of discovering a vehicle's current position to choose from. Some basic ones are looked at in some detail before an in-depth analysis of current schemes and protocols is presented. Most solutions found in the literature concerned with location verification are designed for wireless sensor ad hoc networks. [8].

A Vehicular Ad Hoc Network (VANET) is a system which provides collision avoidance and general traffic information. Vehicles are able to collect real-time data, and relay the information to other vehicles, in order to assist the drivers to reach the destination safely and efficiently. When one vehicle suddenly slows down, or there is a collision, a message is passed on to the vehicles behind it to warn them a collision will be avoided if they too slow down.[9].

Traditional security goals, such as authentication, secrecy, and non repudiation, require reasoning about message contents. In contrast, secure neighborhood discovery relates primarily to the properties of the signals through which messages are exchanged. ND protocols operate essentially with respect to two layers: (i) an abstract layer that describes (benign and adversarial) message content handling, and (ii) a physical layer that describes (benign and adversarial) handling of signals sent across the communication medium (e.g., signal strength or time of arrival)[10].

III. PROPOSED SYSTEM METHODOLOGY

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 . We assume that each node knows its own position and its neighbor node position. The verification of 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 the neighbor nodes and verify them various techniques are proposed.

An ad hoc network is a 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 host to enlist the aid of other hosts in forwarding a 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 a dynamic mobile node. This paper presents a protocol for updating the position of a 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.

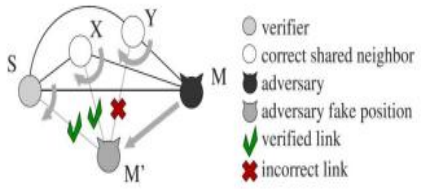

Fig 3.1 Neighbor discovery in adversarial environment

M is a malicious node announcing a false location M′, so as to fraudulently gain some advantage over other nodes. The figure portrays the actual network topology with black edges,while the modified topology, induced by the fake position announced by M, is shown with gray edges. It is evident that the displacement of M

to M′ causes its edges with the other nodes to rotate, which, in turn, forces edge lengths to change as well. The tests thus look for discrepancies in the node distance information to identify incorrect node positions.

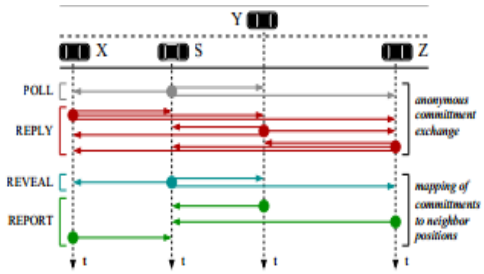

Fig. 3.2 Message exchange overview, during one instance of the NPV protocol

We propose a fully-distributed cooperative scheme for NPV,which enables a node hereinafter called the verifier to discover and verify the positions of its communication neighbors.

A verifier, S, can initiate the protocol at any time instant,by triggering the 4-step message exchange depicted in Fig.3.2 within its 1-hop neighborhood. The aim of the message exchange is to let S 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 ToF-based 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.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.

A. POSITION VERIFICATION

To verify the position of a node following two tests is done, they are:

- Direct symmetry test
- Cross symmetry test

In the Direct Symmetry Test, S verifies the direct links with its communication neighbors. To this end, it checks whether reciprocal Time of Flight-derived distances are consistent with each other, with the position advertised by the neighbor, and with a proximity range R.In cross symmetry test information mutually gathered by each pair of communication neighbors are checked. This ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, i.e., for which ToF-derived mutual distances are available.In multilateration test, the unnotified links are tested. For each neighbor X that did not notify about a link reported by another node Y, with X, Y € WS range. Once all couples of nodes have been checked, each node X for which two or more unnotified links exist is considered as suspect.

The Cross-Symmetry Test (CST), implements cross-verifications, i.e., it checks on the information mutually gathered by each pair of communication neighbors. The CST ignores nodes already declared as faulty by the DST and only considers nodes that are 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 to S are not taken into account.

In proposed system the NPV protocol is extended to dynamic source configuration routing protocol, which results both mobile node verification and node position verification. For clarity, here we summarize the steps of npv algorithm.

B.PROPOSED ALGORITHM

1.Start moving nodes.
2.Source broadcast the message.
3.Nodes accept the messages and assign their IDs.
4.Nodes check each other if the node position is out of region.
5.If it happens neglect the node otherwise continue consider.
6.Confuse the malicious nodes by self retransmitting mechanism.
7. Apply different test to each node.
8.Once all tests are completed then never consider the unverified & faulty nodes.
9. Track the movement of malicious nodes.
10.If more malicious nodes are together then change the wall topology to isolate malicious node.

A single independent adversary cannot perform any successful attack against the NPV scheme. When the shared neighborhood increases in size, the probability that the adversary is tagged as faulty rapidly grows to 1. Multiple independent adversaries can only harm each other, thus reducing their probability of successfully announcing a fake position. . In coordinated attacks, it is the nature of the neighborhood that determines the performance of the NPV scheme in presence of colluders. However, in realistic environments, our solution is very robust even to attacks launched by large groups of knowledgeable colluders. This system yields small advantage to the adversaries in terms of displacement. Finally, the overhead introduced by the NPV protocol is reasonable, as it does not exceed a few tens of Kbytes even in the most critical conditions.

IV. RESULTS AND DISCUSSIONS

Our experiments verify that the proposed protocol can, indeed, successfully cope with a high number of adversaries, while operating in an adversarial environment. The simulation is done by using network simulator (NS-2) software, with different number of mobile nodes ranging from 0-100 . The simulation time period is 500 seconds, pause time 20sec, and the simulated mobility network area is 500m × 500m square. To represent ad hoc network we 100 mobile nodes.One chosen as the source(node 22) and one as destination(node 6).

The following performance metrics are evaluated for the number of nodes and compare with the existing system.

The graph represent a worst case analysis of the proposed NPV, are shown in terms of the probability that the tests return false positives and false negatives as well as of the probability that a (correct or adversary) node is tagged as unverifiable. In addition, we plot the average difference between the true position of a successful adversary and the fake position it advertises,in terms of positioning error.The probability of a node is tagged as faulty becomes highest is only for the 50m variation in the positioning error.

The probability that adversaries are verified increases ever so slightly with their density. The highest effect is on the probability of correct nodes being tagged as faulty, which however reaches its highest value (4.2) only for 40 percent of adversaries in the network.

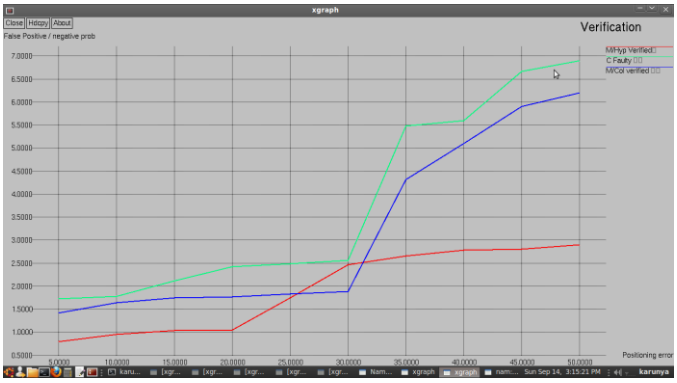

Fig 4.1: Probability that a neighbor is tagged incorrectly versus the positioning error

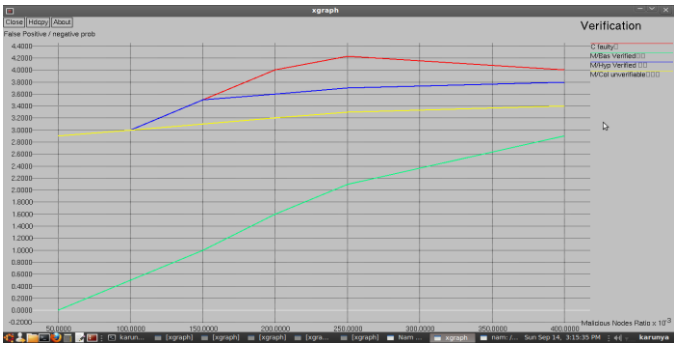

Fig 4.2: Probability that a neighbor is tagged incorrectly versus the ratio of adversaries

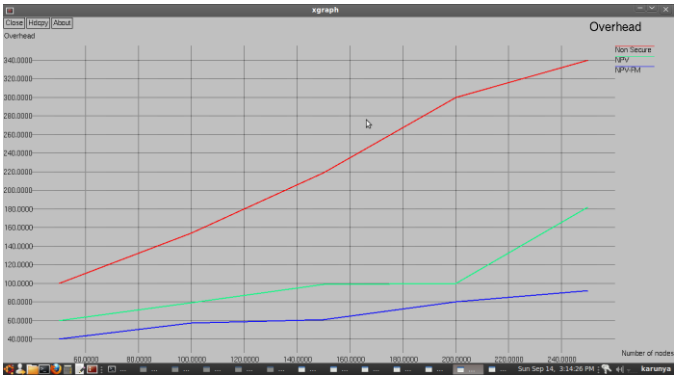

Fig 4.3 Graph showing overhead versus number of nodes

Overhead refers to the time it takes to transmit data on a packet-switched network. Each packet requires extra bytes of format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces the overall transmission speed of the raw data. The overhead is very high for the non secure system while comparing with the NPV and modified NPV schemes.The overhead is very less for the modified NPV scheme.

Fig. 4.4 portrays the traffic induced on the network by one instance of the NPV protocol. The plot only accounts for transmission range variations since, once more, the other parameters do not have an impact on the overhead.We can

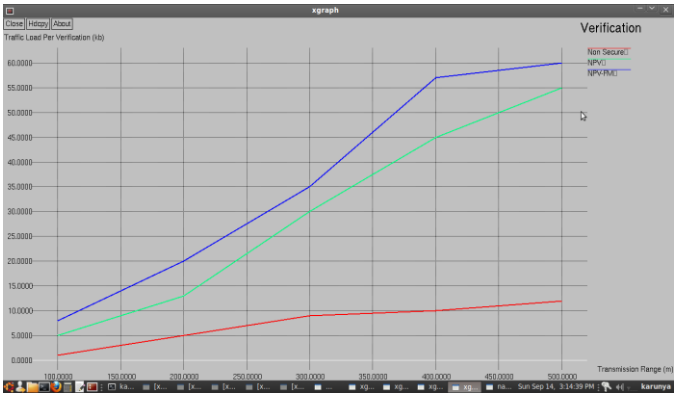

Fig 4.4 Traffic load induced by one instance of the Protocol vs Transmission range

observe that security comes at a cost, since the traffic load of the NPV protocol is higher than that of a basic nonsecure neighbor position discovery, consisting of only one poll and associated position replies from neighbors. More precisely, themodified NPV protocol overhead,NPV protocol overheads are comparable to that of the nonsecure discovery for smaller transmission ranges, while the difference tends to increase for larger

ranges. However, the cost of the NPV protocol is affordable in absolute terms, since one run requires just a few tens of kbytes to be exchanged among nodes, even in presence of dense networks and large transmission ranges.

Given that we assumed the best possible conditions for the adversaries, the above results prove our NPV to be highly resilient to attacks. Indeed, we observed typical probabilities of false positives/negatives below very few percent, while that of a node being tagged as unverifiable is below 5 percent. Moreover, we showed that a significant portion of the successful attacks yields small advantage to the adversaries in terms of displacement. Finally, the overhead introduced by the NPV protocol is reasonable, as it does not exceed a few tens of kbytes even in the most critical conditions.

V. CONCLUSION

Constantly changing topology of the network makes ad hoc routing protocols incapable of providing satisfactory performance and providing security in MANETs became a great deal.In this paper presented 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 neighborhood of the verifier in a proactive paeadigm.Future work will aim at each node to constantly verify the position of its neighbor even if the adversaries in the network are majority and providing security without altering the topology.

REFERENCES

[1] Padmavathi K,Jaganraj L "*A Study on Secure Spontaneous Ad Hoc Network Protocol for Neighbor Position Verification*" Oct 2013
[2] T. Leinmuller, C. Maiho¨ fer, E. Schoch, and F. Kargl,"*Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification*," Proc. ACM Third Int'l Workshop Vehicular Ad Hoc Networks (VANET), Sept. 2006.
[3] P. Papadimitratos and A. Jovanovic, "*GNSS-Based Positioning: Attacks and Countermeasures*," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.
[4] Marco Fiore, Claudio Ettore Casetti,Carla-Fabiana Chiasserini, Senior Member, Panagiotis Papadimitratos, "*Discovery and Verification of NeighborPositions in Mobile Ad Hoc Networks*"Feb 2013
[5] Tim Leinm¨uller, Elmar Schoch, Frank Kargl *"Position Verification Approaches for Vehicular Ad Hoc Networks*"2008
[6] Wenjia Li and Anupam Joshi, "*Security Issues in Mobile Ad Hoc Networks- A Survey"*
[7] Amel LTIFI, Ahmed ZOUINKHI , Mohamed Salim BOUHLEL" *A Cooperative Trust Management System for VANET Integrating WSN Technology*"Oct 2013
[8] Farhan Ahammed and Albert Zomaya, "*Location verification in vehicular ad hoc networks"* May 2009.
[9] Max Ott "*Secure Positioning in Wireless Networks"* May 2009.
[10] Sheng Zhong Murtuza Jadliwala Shambhu Upadhyaya Chunming Qiao "*LOCOMO: Distance-based Localization against Malicious Beacon Nodes"*