Discovery and Position Verification using AODV Protocol in Mobile Ad hoc Network

V. Devamanohari
M.E Computer Science and Engineering
Oxford Engineering College
Trichy, India

A. Karthikeyan
Assistant professor, Dept of CSE
Oxford Engineering College
Trichy, India

***Abstract*—The Ad hoc networking protocol and location aware services prerequisite the mobile nodes acquire the position of their neighbor. However, this process may be misused or disrupted by the adversary nodes. The discovery and position verifications are challenging process, due to absence of priori trusted nodes. This paper proposing the neighboring nodes are discovered using proactive through table driven methodology and AODV (Ad hoc on Demand Distance Vector Routing) with table driven methodology, preserve the table for finding the optimum path. Table driven methodology is foremost used for update the table at every 2 minutes without restoring the previous details and also preserving the fresh details in the table. The retransmission and by pass the lane is possible for using Ad hoc on Demand Distance Vector Routing Protocol with table drive methodology is easily ascertain the direct communication neighbor within the networks.**

Keywords—Route Discovery; Neighbor Position Verification; Proactive Protocol; AODV Protocol with Table Driven Methodology.

I. INTRODUCTION

The Mobile Ad hoc networking protocol, Neighbor discovery could deals with the identification of nodes with which a communication neighbor can be established, that the communication neighbors are within the certain distance. The process of an adversarial node could be securely discovered as neighbor and true neighbor, but it could still cheat about its position or location with some distance or same range.

Neighbor Discovery provides an essential functionality to discover other devices directly through the wireless medium. This is a basic building block for routing, the most essential in the context of wireless sensor network. Consider two nodes A and B, both are communication neighbor, and an adversary that controls two relay nodes V and M, within range of A and B, respectively. The adversarial node V receives packet from A, relays them to M, and then retransmits them to B [11]. The result is that, through a false link, A and B are misled to believe that they are neighbors, although they are not. It does not merely introduce an artificial wireless communication link between the victim (misled) nodes.

A neighbor verification protocol does not have to be complete, to discover and verify all actual neighbors. This is, most notably, due to the jamming attack that the adversary can always perform to prevent the discovery of legitimate neighbors [11]. Neighbor Discovery is simple and it is sufficient for the adversary to simply relay messages in the network, without any message modification, to stage what is often termed a wormhole attack. Wormhole attacks could detect based on the abnormal values of statistics of the connectivity graph. This requires assumptions about the expected values of these statistics. A distributed scheme relies on connectivity information detects wormhole attacks by checking for forbidden structure in the connectivity graph.

The correctness of node location is an important issue in mobile networks. It becomes challenging in the presence of adversaries aiming at harming the system. The verifier can decrypt the received data and acquire the position of all neighbors that participated. Since position dissemination is crucial for geographic routing forged position information has severe impact regarding both performance and security. Single path geographic routing protocol uses a number of different independent sensors to quickly give an estimation of the trustworthiness of other nodes position. Position verification system successfully discloses nodes disseminating false position and thereby widely prevents attacks using position cheating.

IJERT

II. RELATED WORKS

A. Geographic Routing Schemes

Routing scheme proposals for mobile ad hoc networks using various categories are restricted, directional flooding and greedy routing. Restricted approaches forward packets on multiple, previously undetermined paths that exist in a defined forwarding area. For example, Location Aided Routing (LAR) floods packets in a rectangular area spanned by the source to destination position at the diagonally opposite corners. Directional flooding of geographic routing protocols uses hierarchical approaches to forward packets [20]. Terminodes and grid routing are example. Greedy routing approach a packet is forwarded on a single path. At each node, next hop is selected among all neighbors closer to the packet destination position. This implies that a node has to know all its neighbors and their respective position, which is achieved by all nodes sending periodic broadcasts of their own position.

B. Location Verification using Broadcast

The location verification protocol relies on the broadcast nature of radio communication and cooperation of the sensor nodes. The prover issues a radio signal; sensors in its vicinity will receive the signal, while remote sensors will not. To ensure that the prover outside the zone does not compromise the protocol, sensors are placed outside this zone. If sensor receives the provers signal, it is rejected. The use of sensor nodes as rejecters has not been proposed before [18]. The protocol is resource effective, and it does not require extended sensor capabilities needed for Time-of-Flight location estimation approaches. The prover sends the radio signal with such strength that the verifiers within the distance x can receive it. If the prover does not obtain their decision, it extends the signal strength by x and rebroadcast the signal. This procedure repeats until the verifier respond.

C. Attacks on Global Positioning System (GPS)

In mobile devices are the global positioning system is outdoor positioning system. It is based on the set of satellites to provide a 3-D positioning with an accuracy of 3m. It provides devices an accurate time reference in a global positioning system. It cannot be used indoor positioning. Attacks on Ultrasound (US) positioning operate by determining Time of Flight sound signals measured between two nodes. In this system if used with radio frequency signals does not require any time synchronization between source and destination. Ultra sound systems are vulnerable to the distance reduction and distance enlargement attacks. To reduce the distance between two true nodes and two attacker can use radio link, it transmit the signal faster than the ultrasound. Attacks on Radio Frequency (RF) based on received signal strength (RSS), the distance can be calculated based on the transmitted and received signal strength. To cheat the measured distance an internal attacker needs to report a false power level to a true node. Malicious attacker can modify the measured distance between the two true nodes.

D. Position Verification with the Mobile Base Stations

The position verification protocol relies on the assumptions of the covert base station (CBS) is hidden; all communication between the node and the localization infrastructure is performed through the public base station (PBS). The position verification is performed through mobile base station (MBS). The base station sends a verification request to node from one location and wait for the response at a different location. The node does not know the positions of the mobile base station at the time of position verification. In this position verification protocol, the role of a public base station is thus replaced with base station mobility [16]. A set of covert base station and public base station forming a localization infrastructure, the both base stations are known the authority controlling the verification infrastructure. The node-centric position verification protocol is used for location verification.

In time difference of arrival (TDOA) system, at different times a signal can be sending to the base stations that the process can be cheated by the attacker. If the attacker will fake his position in a TDOA environment, he must also guess the direction in which he needs to point his directional antenna to send the delayed message to the correct base station. The TDOA-based location verification scheme is a low cost in which false location claims do not benefit the attacker and/or in which the attacker does not have the ability to perform the described wormhole attack. The advantage of TDOA is that node does not require communication base station to mobile station, the base station locate mobile nodes by determining the signal reception time at each base station.

E. Autonomous Position Verification

Greedy routing in vehicular ad hoc networks depends on reliable neighbor positions. Without verifying these positions, node may claim altered positions and run on several attacks. Some approaches to verify the node position use angle or distance calculation measurement like time of flight. The autonomous position verification threshold base, The Acceptance Range Threshold (ART) sensor is based on observation that radio networks. These sensor devices used in VANETs to achieve the maximal communication range, where the packet sent by a node B still received by a node A [20]. The Mobility Grade Threshold (MGT) sensor is based on assumption that node move at a well defined maximal speed. When receiving a beacon nodes record a timestamp, then the subsequent beacon nodes are in the same node. It checked between the two position whether it is average speed or exceeds mobility grade threshold. Maximum Density Threshold (MDT) is based on assumption that the restricted number of physical entities resides in a certain area.

III. PROPOSED SYSTEM

The wireless ad hoc network consists of two algorithms, proactive and reactive algorithm. One of the main technique or algorithm called proactive algorithm is to finding the routing path independently of the usage paths and another one is the reactive algorithm is establish a route to destination on demand only. In this paper using proactive algorithm for AODV protocol with table driven methodology.

In this architecture diagram, first analyzing the network to identify the positions of it neighbor nodes and it distance and then establish a route between two nodes then sender will fix the receiver and then finding the optimum path and finally implement the wakeup scheduling protocol, neighbor position verification scheme using Direct Symmetry Test algorithm and AODV with table driven methodology. For this table update fresh details without restoring the previous details and it automatically check the table at every 2 minutes.

IJERT

A. Network Analysis

The network analysis is fully monitoring the network and to identifying the position of the node. In a networks environment every node is sharing the resource from one node to another node or neighboring node. Every node is very much aware of neighboring node and all the node so every node known next hops and costs between the nodes. The node analysis is based on the node verification, it consists of two processes (i) every node is transferring the information about neighboring node to all the remaining nodes in the networks. (ii) Every node is transferring to the neighboring node information about member of the particular networks. In the network analysis using Link State Routing (LSR) algorithm, it consists of Flooding techniques concepts. Flooding is to spreading details to the neighboring nodes to all the other nodes in the networks.

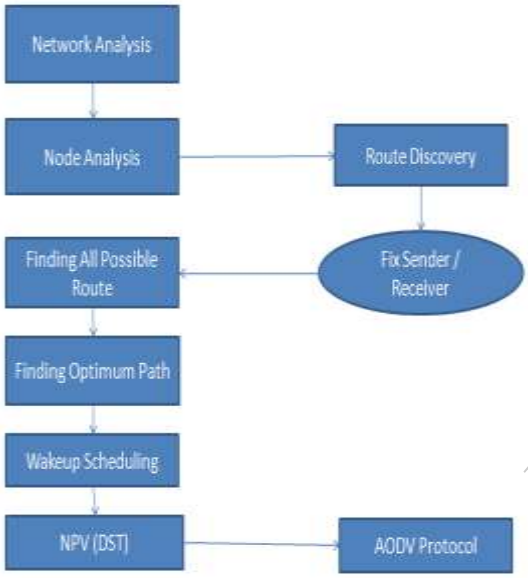

Fig 1: Architecture Diagram

B. Route Discovery

Route discovery is to establish a route between a sender and receiver. It means finding the path from starting node to ending node. It is a point to point communication. In this paper consists of two algorithms (i) Proactive through the table driven methodology, and (ii) AODV with the table driven methodology. A sender node tries to discover the route to send something to the destination and there are no known routes. The sender will fix the receiver and then implementing the two processes one if for finding the all possible route, finding the route for transferring the information. Another one if for finding the optimum path based on the four criteria (i) minimum cost and distance (ii) less intermediary node between the sender and receiver (iii) without congestion occur and (iv) at any cost my information should be reached at the destination. These four criteria are possible for select only one way between the sender and receiver.

C. Wakeup Scheduling Protocol

After the path selection is to changing the node from Hidden Terminal to Exposed Terminal then to turn the deactivation mode to activation mode. At the time of packet transformation to check the networks whether it is an activation mode or sleeping mode. If the nodes are activation mode transfer the data. Then the nodes are in sleeping to make the changes for hidden to exposed terminal. In a networks, normally the node are in a sleeping mode because to saving the power. When the nodes are in active mode it emits the signal fully based on the power consumption. Finally packet transformation is completed automatically changing the activation mode to sleeping mode.

D. Neighbour Position Verification Scheme

Neighbor position verification is a system to deals with a mobile ad hoc network, where a pervasive infrastructure is not display and the location of data must be acquired through node to node communication. This scheme is mainly used for to identifying the adversary node and then which adversary acts as an intermediate node using DST algorithm. Direct Symmetry Test (DST) is it verifies the direct links with its communication neighbors.

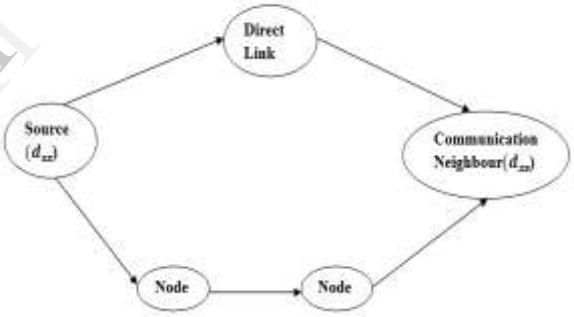

Fig 2: Direct Symmetry Test

In this diagram, the sender sends data to direct link with its communication neighbor or receiver. Here consider d_{sx} is a sender side d is a distance between sender and receiver, s is source or sender, and x is a direct link of source. Here d_{xs} is a receiver side d is a distance between sender and receiver, x is a communication neighbor and s is a source or sender. S verifies the direct link for communication neighbor and then checks the compromised neighbor nodes. These two things are right possible and then easily find out the adversary node. Who can act as an intermediary node, it is corresponding neighbor node or adversary node sender will identify that opponent node.

E. AODV Protocol with Table Driven Methodology

The Ad hoc on Demand Distance Vector Routing (AODV) protocol is an on demand routing algorithm. Ad hoc on Demand Distance Vector Routing allows mobile node to respond quickly and it using sequence number on route updates. Through the Ad hoc on Demand Distance Vector Routing protocol in ad hoc network possible for every node is very much aware of neighboring node. Every node is maintained the detailed table and every particular 2

IJERT

minutes to update the table and also automatically check the table. Here using the ad hoc network and Ad hoc on Demand Distance Vector Routing protocol it possible for the retransmission. The ad hoc network dynamically forming the temporary network without the use of existing network infrastructure after the process will be completed it fully erased the network. The details of the table for sender, receiver and time of data transmission, packet size, packet information and delivery report. Table Driven methodology is a scheme for allow to view the information in details at the time of whose sender and who will be communicate the neighbor and also current status reports are stored in the table.

IV. CONCLUSION

In this paper, I implement the Ad hoc on Demand Distance Vector Routing protocol (AODV) with Table Driven methodology. So it provides the better network analyzing methodology through the link state routing algorithm. And concentrates on establish the route between the sender and receiver through the route discovery based on the criteria for minimum cost and distance, less intermediary node between sender and receiver, the information will be reached as possible without any congestion. Route discovery used two algorithms for Proactive through the table driven methodology and Ad hoc on Demand Distance Vector routing with table driven methodology. Then identifying the neighbor position verification scheme is to find out the adversary node used on the Direct Symmetry Test (DST) algorithm. Finally, AODV protocol with table driven methodology is used by every node to maintain the detailed table and also every 2 minutes to update the table.

V. FUTURE ENHANCEMENT

In future the system may have the better security consideration with more number of systems and more distance. This particular work may be extended as providing security against some critical attack. These attacks are reply disregard attack, collinear attack and worm attack.

REFERENCES

1 609.2-2006: 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, Nov. 2008.
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, and 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, Apr. 2003.
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), Mar. 2009.
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), Mar. 2008.
13 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.
14 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.
15 J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
16 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.
17 S. _Capkun and J.-P. Hubaux, "Secure Positioning in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221- 232, Feb. 2006.
18 A. Vora and M. Nesterenko, "Secure Location Verification Using Radio Broadcast," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 377-385, Oct.-Dec. 2006.
19 J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," Proc. IEEE INFOCOM, May 2007.
20 T. Leinmu¨ ller, 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.
21 J.-H. Song, V. Wong, and V. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," Proc. IEEE Globecom, Dec. 2008.
22 M. Fiore, C. Casetti, C.-F. Chiasserini, and P. Papadimitratos, "Secure Neighbor Position Discovery in Vehicular Networks," Proc. IEEE/IFIP 10th Ann. Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), June 2011.

IJERT