A LIGHT WEIGHT LOCATION VERIFICATION PROTOCOL BASED ON BEHAVIOR LEARNING PROCESS FOR MOBILE ADHOC NETWORKS

T.Buvaneswari[1], Dr.A.Antony Iruthayaraj[2]
Research Scholar[1], Senior professor –Research[2]
Computer Science and Engineering[1,2],
Vinayaka Missions University, Salem[1]. Aarupadai Veedu Institute of Technology, Paiyanoor[2]
tbuvaneswari@yahoo.com[1], anto_irud@hotmail.com[2]

Abstract— Fast changing and growing nature of mobile adhoc networks makes the accessibility of location aware services becoming difficult. With the presence of adversaries and attacking nodes, the location based service discovery becomes a challenging one. We propose a light weight location verification protocol for the verification of nodes which turns out to be a robust one and uses the behavior of nodes for the verification process. Here distributed one step Location Verification Protocol is being used and session based behavior learning process for the identification of adversary nodes has been adopted. The proposed method is indeed capable of preventing attack types such as node impersonation , Sybil, ddos attacks.

Index Terms— Neighbor Discovery, Location Verification, Location Based Services, vehicular networks

1 INTRODUCTION

The growing internet technology makes the mobile user to access all major services irrespective of their location. Nowadays Location based services are attaining popularity. For example in a road traffic network the mobile user can access few location based services to get know about the restaurants , hotels, hospitals etc which are nearer to them. Whatever the service they need the result is provided based on their locations only so that the location based services become more popular and used by many users on need basis. Here the focus is on mobile adhoc network where there are no standard topologies and neighbor nodes can serve as intermediate node and participate in routing process.

Location based services (LBS) has the ability to locate geographical position of the user to deliver area specific information. LBS can provide useful information regarding public transportation, route options, weather forecasts, and location of hospitals, restaurants, police stations, tourist attractions, landmarks, petrol pumps, ATMs etc. In a VANET traffic network the location based service can be accessed in many ways. The routing in VANET network becomes more complicated due to the increase in mobile nodes. A mobile node can access a service to know about the traffic and route to a desired destination by accessing the LBS. The LBS could send the knowledge about the traffic and possible set of routes to reach the destination. The mobile node could chose a path to reach destination. Alternatively, accessing the service need a request to be transferred, so that the neighboring nodes becomes participant in the transmission. In practice most of the times the neighbor node becomes adversary and introduces different kind of attacks, which in turn reduces the throughput rate of the network. Protocols for Neighborhood Discovery (ND) serve as fundamental building blocks in mobile wireless systems. Clearly, ND enables (multi-hop) communication, as it is essential for route discovery and data forwarding. ND can also support a wide range of system functionality: network access control, topology control, transmission scheduling, energy-efficient communication, as well as physical access control. Given the critical and multifaceted role of ND, its security and robustness must be ensured: ND protocols must identify the actual neighbors, even in hostile environments.

The location discovery of neighbor nodes and verification process becomes more complicated one, due to the increase in protocols of mobile adhoc networks. There are many protocols NPV, “Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks” [1], “Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multi lateration” [2] been addressed earlier for the verification of the mobile nodes location. Most of them

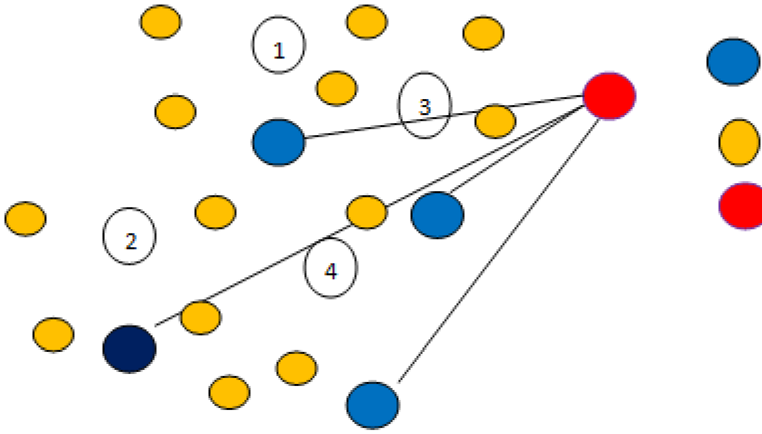


Fig1: Adversaries fake positions.

Fig1 shows that there are fake and adversary nodes and their positions. Yellow colored nodes are trusted ones, Red colored is the adversary node and blue colored is the false position of the adversary node. It is clear that the adversary node generates fake position for every neighbor node of it and sends false misleading location information to its neighbors. This false location information affects the process of routing in the mobile adhoc network, because each neighbor participates in the routing for mobile adhoc network. When an adversary sends fake position to its neighbor, and the neighbor selects the fake node to transmit a message, then the packet or information will not be transferred to the destination exactly. The fake node could take all the messages from the source node and may generate collinear or jamming attack to degrade the network performance

2 RELATED WORKS

Here we discuss various methods proposed for the verification of nodes position and node discovery. Secure services for application and management messages have proposed in [3], it uses secure message formats, and the processing of those secure messages, within the Dedicated Short-Range Communications (DSRC)/Wireless Access in Vehicular Environment (WAVE) system are defined. (Rewrite) The standard covers methods for securing WAVE management messages and application messages, with the exception of vehicle-originating safety messages. It also describes administrative functions necessary to support the core security functions.

For the discovery of mobile nodes [4], the author explored the possible types of attacks in the physical and communication medium of the mobile adhoc networks. Neighbor discovery is classified into physical and communication neighbor discovery. Protocols aiming at communication ND, which are based on physical ND protocols, often fail to achieve their objective. This is because these two types of discovery are not equivalent. At the same time, protocols for communication ND do not fully address the problem at hand. They are effective only under very specific operational conditions or they do not ensure correctness in all cases.

For the verification of Neighbor position [5][6], there are methods was dealt in the context of ad hoc and sensor networks; however, existing Neighbor Position Verification schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic.

For Secure Positioning in Wireless Networks [7], NPV protocol is proposed which calculate distances for 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. Furthermore, the resilience of the protocol in to colluding attackers has not been demonstrated. Static sensor networks [8] also require several nodes to exchange information on the signal emitted by the node whose location has to be verified. Moreover, it aims at assessing only whether the nodes are within a given region or not.

An Improved Security in Geographic Ad Hoc Routing throuh Autonomous Position Verification is discussed in [9]. The authors proposed an NPV protocol that 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 could draw a movement over a time in realistic sense. The approach [10] 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 mislead the protocol by simply announcing false positions that follow a realistic mobility pattern.

The scheme in Secure Location Verification for Vehicular Ad-Hoc Networks [8] exploits Time-of-Flight (ToF) distance bounding and node cooperation to mitigate the problems of the previous solutions. The cooperation is limited to couples of neighbor nodes, which renders the protocol ineffective against colluding attackers.

To the problems identified, there must be a protocol which is fully distributed and light weight to solve the verification of node position in mobile adhoc networks. It should not depend on trusted nodes and should be secure for various kinds of attacks.

3 OVERVIEW OF LIGHT WEIGHT LOCATION VERIFICATION SYSTEM

The proposed system verifies the node location using one step verification process utilizing session based behavior learning process. The node in the network receives their geometric and spatial metrics at the time of registration or entering in to the coverage of the base station. The nodes specify the location information and speed and displacement details at all time. At each time stamp the base station sends the notification to collect nodes behavior details. Upon receiving this message for certain time, if a node transmits a message it sends node and packet and forwarding node details to the base station. The base station maintains node details under its coverage and behavior matrix where it stores the transmission details of all nodes which could be used to identify the adversary nodes.

The proposed system has the following three phases. There are (i.)Registration, (ii.)Behavior Collection and (iii.)One step Location Verification.

3.1 Registration

When a mobile enters to a new coverage area, it needs to register in the base station about its latitude and longitude**.** The login message has the following parameters.

Message Id	Node Id	Location Details	Time Stamp(entry time)	Speed

Table1: Login Message format

In the login message it has Message-Id which is unique for the message sent by the node, Node-Id specifies the identification number of the node which sent the message, Location Details specifies the geometric location information and Time Stamp specifies that at what time the message generated and Speed

le is ge it ain- key sent vate

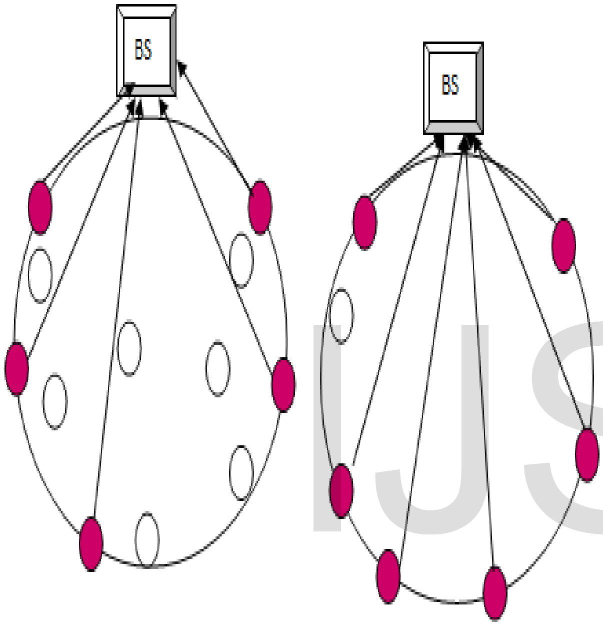


Figure2: Registration process with the base station

Algorithm:

Step1: start
Step2: Generate Node-ID nid.
Step3: Generate Message-ID mid.
Step4: compute Geometric metrics location values G_x, G_y.(Latitude/longitude?)
Step5: generate entry time stamp m_t.
Step6: compute speed n_s =ø(((G_x-G_{x-1})* (G_x-G_{x-1}))+((G_y-G_{y-1})* (G_y-G_{y-1})))/sec.
Step7: construct Login message L_m=nid+mid+(G_x,G_y)+m_t+n_s.
Step8: stop.

The base station maintains the following details in the node matrix.

MessID	NodeId	Location Details	Time Stamp	Speed
M1	N1	120,130	01.23.45.900	5m/sec
…	…	…	…	….
…	…	…	…	…
…	…	…	…	…

Table2: Base station node matrix

The node details are stored in the node matrix only if the node registers the base station at the time of handover process. So that the nodes location can be calculated using those parameters in the login message by the mobile base station at any point of time

3.2 Registration

The base station initiates Behavior Collection procedure periodically with specific time interval. Upon receiving this message each node either receives or transmits a message. It generates another control message which has the packet id received or transmitted, and node id from which it receives and also where to it transmits time stamp etc… The base station collects this information and updates the behavior matrix periodically. This procedure will be repeated periodically and the update time is set depend on the nodes movement to ana-

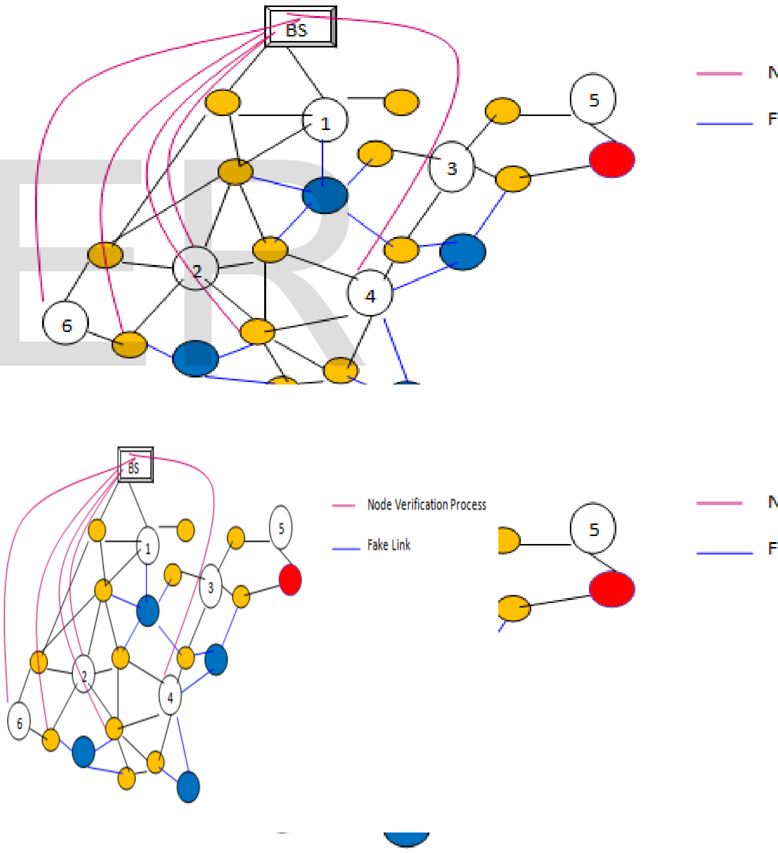


Figure3: Transmission of behavior message

From the figure 3 it is very clear that if the source 6 selects the path through 2 to reach 4 , then the base station receives the behavior message completely. The base station at every time slot analyses the behavior matrix and search for the completion of transmission with the packet id and source and destination id specified in the matrix. If the transmission is incomplete then it identifies the fake node with link and adversary node from the matrix and packet details. It updates all identified adversary details and records in adversary matrix.

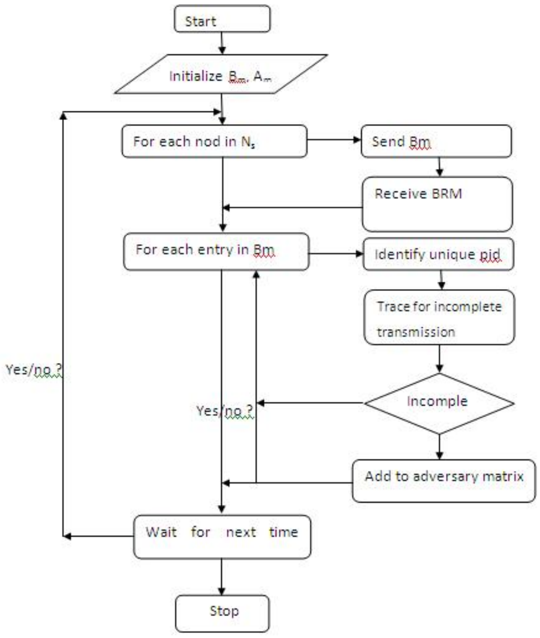
It is normally difficult to say a node as an adversary node with one single transmission. Sometimes the mobility of the node also can be the reason for incomplete transmission, because the node might have moved to some other location which is computed by the source node at the time of route selection. Here the behavior of adversary node helps us , by giving false locations to more than one neighbor, so that the adversary node could be identified by the base station by identifying the same node id present in various transmission which is incomplete from the behavior matrix stored in the base station.

Algorithm:

```
Step1: initialize behavior matrix $B_m$ and adversary matrix $A_{m,}$
initialize time stamp $B_{t.}$
Step2: for each node $Mn_i$ from the Node set $N_s$.
        Send Behavior message BM.
        Receive reply BRM.
        Extract packet id (Pid), source id (Sid), destination id
(Did) ,NodeId( Nid), Ts
        Store in $B_{m.}$
        End.

Step3: for each row in matrix $B_{m.}$
        Identify unique packet id pid.
        Search for the row for completion of transmission.
        If( incomplete)
        Add Nid in adversary matrix $A_{m.}$
        End.

Step4: wait for next time stamp and repeat step 3, 4 .
Step5: end.
```

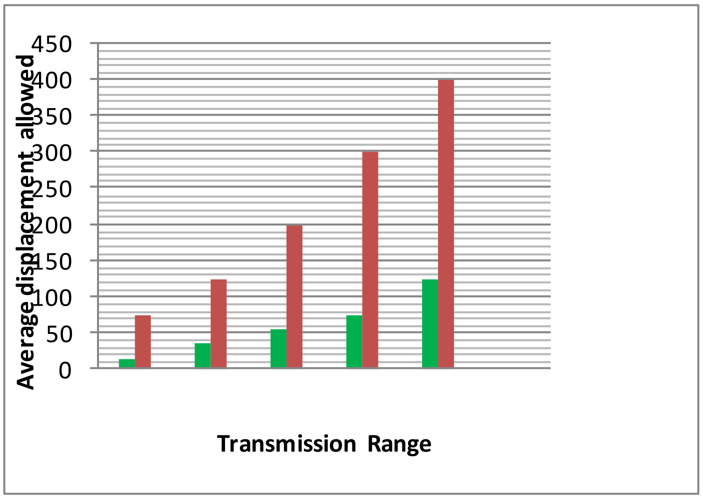


3.3 One step Location Verification

The mobile node initiates this verification process for each transmission. At the time of transmission it selects the path and the neighbors by broadcasting the message. On receiving a reply the source node collects the set of neighbors and updates its neighbor matrix. For every chosen path for destination, the neighbors are verified using procedure as given in the flow chart (Refer Fig 4). It sends the verification message V_m to the base station with the location details and geometric metric which is sent by the neighbor. The base station extracts the neighbor details and its geometric metric and computes the new location for the mobile node using the details in the node matrix. The neighbor details are kept stored in the node matrix when it enters within the coverage of the base station, it uses the location details of the mobile node and speed to compute the displacement of the neighbor node. It compares the location details sent by the source node and calculated location, if the difference between them is within a tolerance then it identify the neighbor as genuine node and also checks the entry of neighbor id in adversary matrix if the neighbor id is present in the adversary matrix they it assumes that the neighbor as adversary one. Based on the two comparison process it send reply as genuine node or adversary one for the source node to transmit the message to the neighbor in order to transmit the message else it discards the neighbor and select another neighbor to transmit. It repeats the verification process for all neighbors to transmit the message.

4 Results and Discussion:

The proposed system produces very good results and we have tested with large number of nodes and large number of adversary nodes.



Graph1: Displacement Allowed according to Range 1

The graph1 shows the result produced by the proposed system and the average displacement allowed with the proposed system according to the transmission range

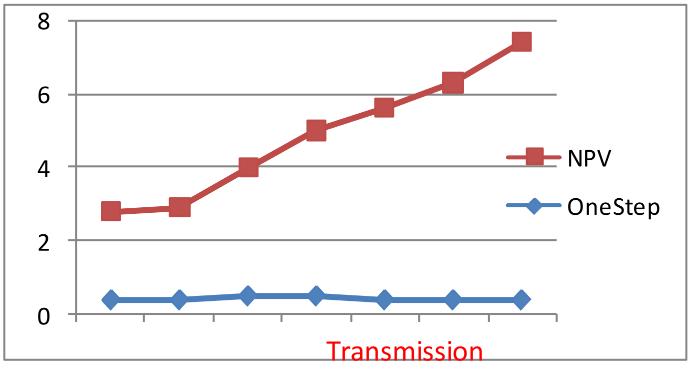


Figure 2: Traffic introduced by NPV and One step for verification process

The graph2 shows the traffic introduced by NodePositionVerification algorithm with our methodology. The results shows that our methodology introduces only little traffic compare to other systems.

5 Conclusion:

The proposed methodology is a secure one for all kind of attacks coming in mobile adhoc network. We used one step verification process, which is less time consuming and we collect behavior of the nodes periodically, so that even if there are many number of adversaries present in the network we could identify easily with the help of one step verification process. The behavior collection helps us to increase the performance and throughput of the overall network , because the forwarding node selection implies the performance of the overall system. Even though the behavior collection introduces little network overhead for 6%, it reduces the time of verification and heaviness of computing signature and using multiple keys for the identification and verification process, thus improves the efficiency of the overall network.

References

[1] 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.

[2] 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.

[3] 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[4] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. _Capkun, and J.-P. Hubaux, “Secure Neighborhood Discovery:A Fundamental Element for Mobile Ad Hoc Networks,” IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.

[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.

[6] 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.

[7] 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.

[8] 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

[9] J.-H. Song, V. Wong, and V. Leung, “Secure Location Verification for Vehicular Ad-Hoc Networks,” Proc. IEEE Globecom, Dec. 2008.

[10] Radha Poovendran and Loukas Lazos. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. volume 13, pages 27–59, Hingham, MA, USA, 2007.

[11] Lingxuan Hu and David Evans. Using directional antennas to prevent wormhole attacks. In Symposium on Network and Distributed Systems Security (NDSS), 2004.

[12] Kasper Bonne Rasmussen and Srdjan Cˇ apkun. Implications of radio fingerprinting on the security of sensor networks. In International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm), 2007.

[13] Ritesh Maheshwari, Jie Gao, and Samir R. Das. Detecting wormhole attacks in wireless networks using connectivity information. In IEEE Conference on Computer Communications INFOCOM, 2007.

[14] Levente Butty´an, L´aszl´o D´ora, and Istv´an Vajda. Statistical wormhole detection in sensor networks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, ESAS, volume 3813 of Lecture Notes in Computer Science, pages 128–141. Springer, 2005.

[15] Weichao Wang and Bharat Bhargava. Visualization of wormholes in sensor networks. In WiSe ’04: Proceedings of the 2004 ACM workshop on Wireless security, pages 51–60, New York, NY, USA, 2004. ACM Press.

[16] Alessandro Armando, et. al. The AVISPA tool for the automated validation of internet security protocols and applications. In Proceedings of CAV’2005, LNCS 3576, pages 281–285. Springer-Verlag, 2005.