AENSI Journals
Australian Journal of Basic and Applied Sciences
ISSN:1991-8178
Journal home page: www.ajbasweb.com

Secure Discovery Scheme and Minimum Span Verification of Neighbor Locations in Mobile Ad-hoc Networks

[1] T. Buvaneswari and [2] Dr. A. Antony Iruthayaraj

[1]Research Scholar, Computer Science and Engineering, Vinayaka Missions University, Salem. India.
[2]Senior professor Research Aarupadai Veedu Institute of Technology, Paiyanoor. India.

ARTICLE INFO
Article history:
Received 23 December 2013
Received in revised form 25 February 2014
Accepted 26 February 2014
Available online 15 March 2014

Keywords:
Neighbor Discovery, Location Verification, Manet, Location Based Services, Vanet.

ABSTRACT

The development of mobile technology brings service accessibility of location aware service an important criteria in mobile ad-hoc networks where challenging metric is the dynamic changing topology of Manet. This dynamic topology welcomes the huge network threats in different forms like Hyperbola and collinear attacks. Generally the adversaries responds to the route discovery procedure of any routing protocol with fake positions, so that to be get selected as a forwarding node in the routing process , subsequently to affect the routing process and degrade the throughput of the network by simply discarding the message or by generating modification attacks. We propose a secure neighbor discovery scheme, which uses proactive and reactive details of the neighbor nodes to compute a group G, where set of nodes get selected according to the location details. From the group of nodes G, a single node will be selected for the forwarding phase whose location will be verified with the base station using some simple verification protocol. The verification protocol uses the proactive and reactive details to verify the location of the mobile node. The proposed method has more advantages that the neighbor discovery is done with little overhead by the source node and only the verification process engage with the base station.

To Cite This Article: T. Buvaneswari and Dr. A. Antony Iruthayaraj., Secure Discovery Scheme and Minimum Span Verification of Neighbor Locations in Mobile Ad-hoc Networks. ***Aust. J. Basic & Appl. Sci.,*** *8(2): 30-36, 2014*

INTRODUCTION

Mobile adhoc networks (Manet), popular technology the world society speaks about due to the technology development. The modern world uses internet technology for everything as a part of their life, and now a day they use mobile technology in place of IT to get access to the location based service. The kind of sophisticated service grows with the risk rate in accessing the service. The service providers have more challenges in providing services and maintaining the quality of service parameters. As like in other networks like wired and wireless networks, the Manet also prone to different type of network attacks.

Mobile adhoc network, another kind of wireless network where you can find number of base stations which supports the communication of mobile nodes. The mobile node supports the routing process of the communication to improve the throughput of the network. The mobile nodes are moving at some speed and towards a direction, which makes the topology of the network gets changing at every fraction of time. Due to this reason there will be number of nodes comes into the coverage perimeter of a base station and leaves, which cannot be trusted for service handling. What the adversary does here is, it replies with the route discovery phase using fake location information with the intension to get participate in routing process. After gets selected it simply discard the packet, or manipulate the packet, or else it will never receive the packet because of false location. This makes the transmission as a failure one and service throughput degrades.

Location Based Services are one, which is provided and accessed based on the location information. In a road traffic network the location based service can be accessed in many ways. The routing in road 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 reach a destination by accessing the location based service. The Lbs could reply the knowledge about the traffic and set of routes to reach the destination. The mobile node can chose a path to reach destination. In another way, accessing the service need a request to be transferred, so that the neighboring nodes becomes participant in the transmission. Most of the times the neighbor node becomes adversary and introduces different kind of attacks, which reduces the throughput of the network.

Corresponding Author: T. Buvaneswari, Research Scholar, Computer Science and Engineering, Vinayaka Missions University, Salem. India.
E-mail: tbuvaneswari@yahoo.com

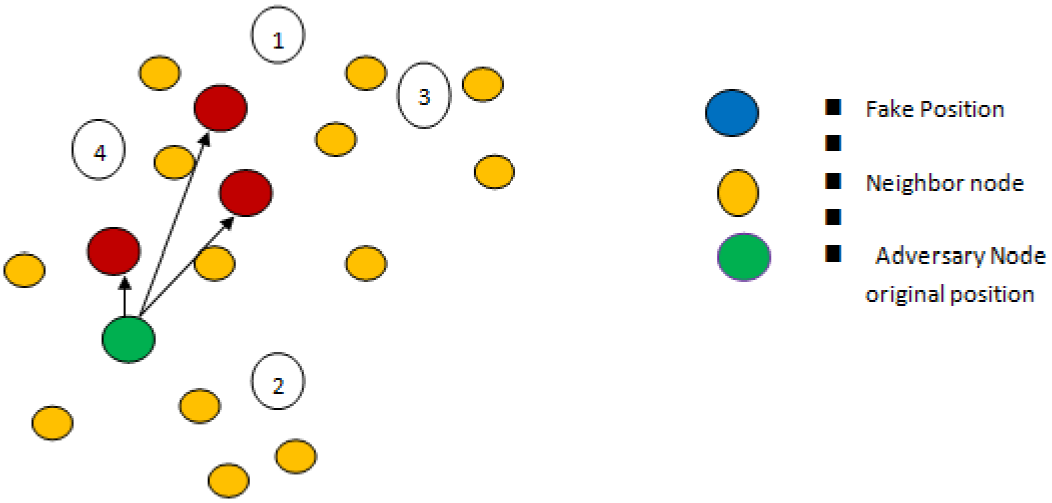


Fig. 1: Shows the example scenario of the fake location.

Protocols for Neighborhood Discovery 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 as neighbors only those devices that actually are 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 been discussed earlier for the verification of the mobile nodes location. Most of them based on the distance and time taken for the request and reply process. The adversaries are giving fake locations for the request when it receives from a source node and dilutes the routing protocol and reduces the network performance.

From figure 1: we can see the adversary node with the green color and the red color node shows the fake positions generated by the adversary nodes and nodes colored with yellow are the neighbor nodes. Support if the node 4 , plans to transmit a packet to any node from the list (2-3-1) then what the adversary does is it generates three different fake locations around node-4 in order to get selected. From this scenario it is clear that, whatever be the destination , the fake node will be selected in all the case.

So that there must be a protocol which verifies the location of the nodes gets selected in the routing phase of the transmission with little overhead in time and space and power ratio.

Related Works:

There are different approach has been proposed for the problem identified using different parameters like proactive and reactive details of the nodes in the transmission range. Here we discuss few of them according to the problem identified.

An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols (Seon Yeong Han, 2013), proposes an adaptive Hello messaging scheme to suppress unnecessary Hello messages without reduced detectability of broken links. Simulation results show that the proposed scheme reduces energy consumption and network overhead without any explicit difference in throughput.

Dynamic Neighbor Positioning In Manet with Protection against Adversarial Attacks (Priyadarshani, K., 2013), propose techniques for finding neighbours effectively in a non priori trusted environment are identified. These techniques will eventually provide security from malicious nodes. The protocol is robust to adversarial attacks. This protocol will also update the position of the nodes in an active environment. The performance of the proposed scheme will be effective one.

Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks (Fiore, M., 2013), address the problem of a priori trusted nodes, the discovery and verification of neighbor positions presents challenges that have been scarcely investigated in the literature. This open issue is addressed 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.

Neighbor node discovery and Trust prediction in manets (Thilagavathy, S., 2013), gate this vulnerability and secure ND is crucial. This paper uses the directional antenna algorithm called as scanning based direct discovery algorithm to discover the neighbors. To enable cooperative working of the various distributed protocols we use trust system to provide the trust level of various nodes, thereby enhancing the cooperation among the nodes. This paper uses distributed hybrid trust algorithm and also uses relationship maturity concept to compute the trust of the nodes. This paper demonstrates that Trust systems are better than already existing cryptographic techniques.

For the discovery of mobile nodes in (Poturalksi, M., 2008), they explored the various attacks possible in the physical and communication medium of the mobile adhoc networks. They classified the neighbor discovery as 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 (Chiang, J., 2009; Capkun, S., 2008), there are methods was studied 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.

Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks, 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.

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.

Proposed Method:

The proposed method uses proactive details about the nodes which have learned at the time of registration process when the node first comes into the transmission range of the base station. With the proactive details, it uses reactive information received from the verifying node, in order to verify the location of the selected node. In the proposed method the Base station Bs uses a different addressing scheme as follows:

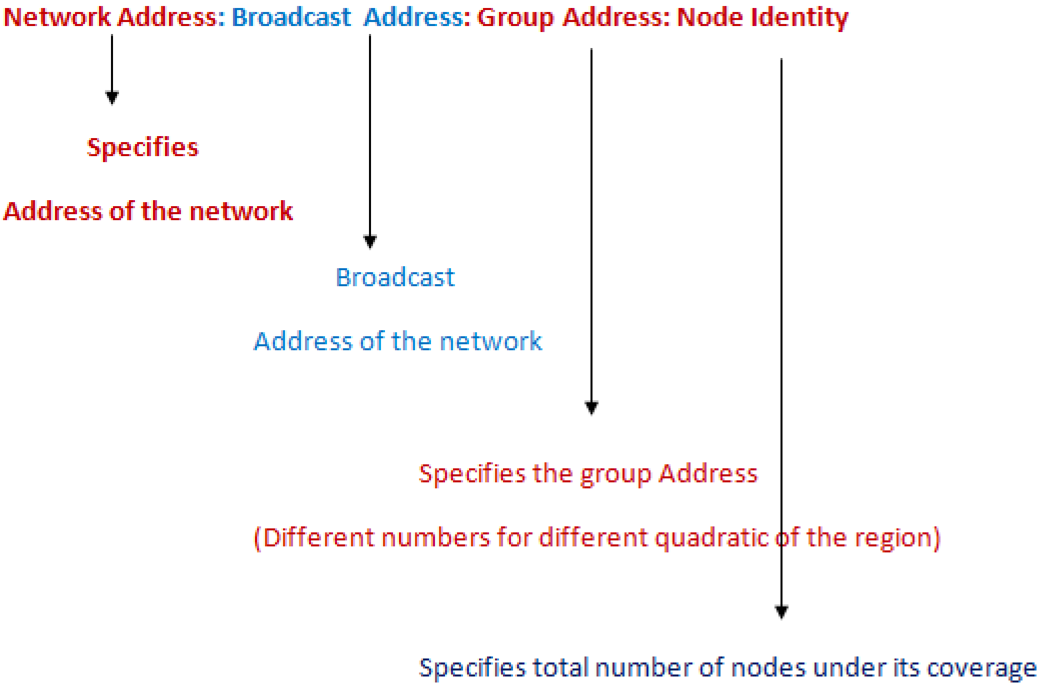

Network Address: Broadcast Address: Group Address: Node Identity
Specifies
Address of the network
Broadcast
Address of the network
Specifies the group Address
(Different numbers for different quadratic of the region)
Specifies total number of nodes under its coverage

Fig. 2: Proposed addressing Scheme.

The proposed method has the following three phases:

Group Join:

The group join mechanism is invoked by the mobile node when it switches it location from the transmission range of a base station from another. The group join message has the following details.

Table 1: Shows the Group join Message format.

Req. ID	Node-Address	Location Details	Time Stamp	Speed	Private Key

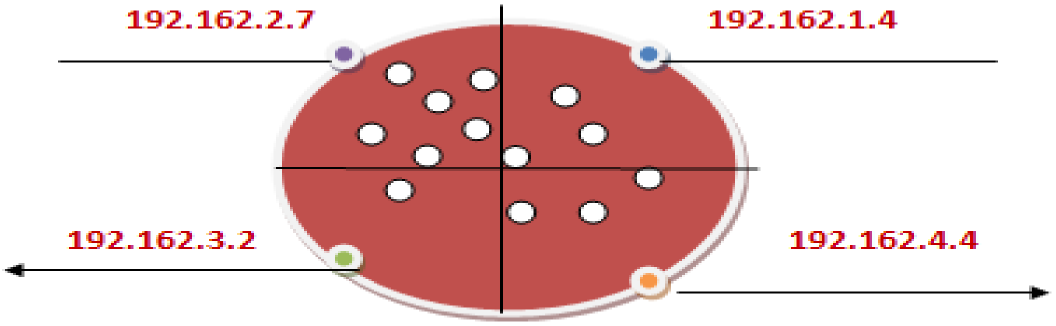


Fig. 3: Address allocation scenario.

The group join message has the following fields namely: Req.ID – specifies the unique identification of the group join request, Node-Address – specifies the unique address of the mobile node, Location Details – has the geographic location details of the mobile node and the time stamp – specifies the time at which the message sent by the node, and Speed tells the displacement or at what speed the mobile node is moving, finally the private key – mentions the private key to be used to communicate with the node. Whenever the base station receives the message it updates the node details in the matrix what it is maintaining. This message is authenticated with the private key p_k generated by the node and here after whatever the message sent by the node will be authenticated with that particular private key. Also the base station uses a different addressing scheme which restricts the adversaries to generate fake locations. The base station also sends the addressing scheme and range of addresses allocated details and adversaries list with the acknowledgement to the source node.

Algorithm:

```
Step1: start
Step2: initialize neighbor matrix Nb, addressing scheme As, Allocation range Al, Adversaries Adl.
Step3: Generate group join Request message GJR.
    GJR(Req.ID)= Generate random number.
    GJR(Node.Address) = Broadcast Address of the mobile node.
    GJR(Location Details)= { Longitude, Latitude, $G_x$, $G_y$};
    GJR(TimeStamp) = {Current Time};
    GJR(Speed)= $\$((( G_x-G_{x-1})*( G_x-G_{x-1}))+(( G_y-G_{y-1})*( G_y-G_{y-1})))/sec.;$
    GJR(Pk) = {Private key }
Step4: Send to the base station Bs.
Step4: Receive reply GJRep.
    Nb=extract Neighbor details from GJRep.
    As= GJRep(Addressing Scheme).
    Al = GJRep(Allocation Range).
    Adl = GJRep(Adversaries List).
Step5: stop.
```

Neighbor Discovery Scheme:

The source node constructs a broadcast message to discover the neighbors around the node. On receiving the broadcast message the nodes under the transmission range of the node replies with the acknowledgement with the location information. The source node initialize a timer to receive the acknowledgement, after the timer expires it stops receiving the acknowledgment. With the set of nodes from which it receives the acknowledgement. After receiving the acknowledgement it check with the addressing of each node with the addressing scheme of the base station and adversaries list. If any malicious address found with the list then it removes the address of node from which it has to select a route to the destination. After checking the addressing scheme it generates a group of node id's which are very close to the source node and checks with the last update of the adversary notification. If the adversary notification time expires then it forward the group constructed to the base station for verification otherwise it simply selects a node from the group and starts forwarding. Unlike other verification mechanisms, the proposed method uses base station just to verify the location of the nodes and return a list of nodes. From the list returned the source node can select closer node to forward the data packet. Here the overhead generated at base station due to verification process is minimized by broadcasting the identified adversary to the other nodes in the transmission range of the base station.

Algorithm:

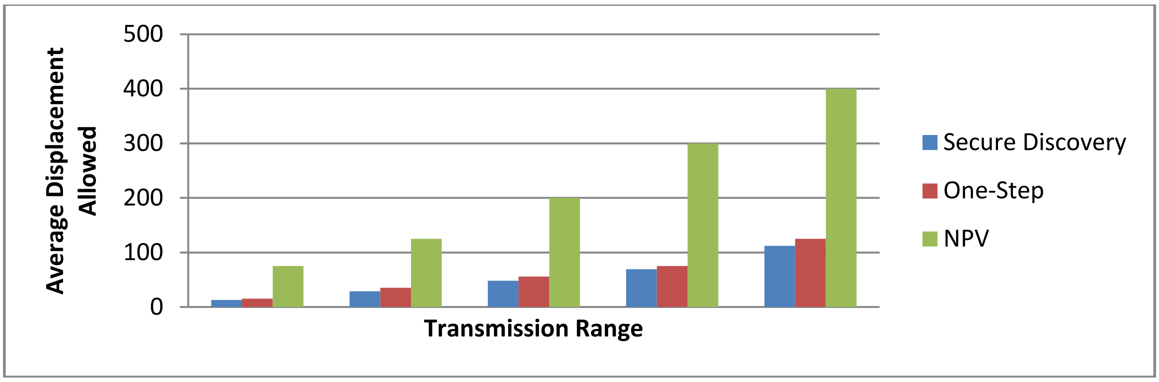
```
Step1: start
Step2: initialize transmission group TG, broadcast timer Bt..
Step3: read Neighbor matrix Nb, Adversary list Adl, Addressing scheme As, allocation range
Al, adversary notification time Ant.
Step4: compute Hello Broadcast message –Hello.
Step5: broadcast to all its neighbors Nb.
Step6: start broadcast timer Bt.
    Receive acknowledgement until Bt expires.
        TG(i) = ack{Node-Address}.
    End.
Step7: for each entry in TG
        Verify adversary list Adl.
                If  TG(i)@Adl then
                        TG=TG-TG(i).
                End
        Verify addressing scheme and range.
        If TG(i)> addressing range then
                TG=TG-TG(i).
        End
        If Addressing Scheme( TG(i))  != addressing scheme then
                TG=TG-TG(i).
        End
    End.
Step8:  check the adversary notification time Ant.
        If Ant is active then
                Forwarding node Fn =Select a node from the group TG.
                Start transmitting through Fn.
        Else
                Send TG to Base station.
                Approved TG = verified list from BS.
                 Select a node from the group TG.
                Start transmitting through Fn.
        End.
Step9: stop.
```

Location verification Process:

The location verification process uses the proactive details which are available from the time of node group join process. Upon receiving request from the source node it checks the set of addresses assigned from the address list and if there is any address unfound then it removes the address from the transmission group TG and add to the adversary list Al. From the location details available with the request, it compares the location of each node from the group TG. It computes the possible displacement for each node according to its speed to verify with the new location. Adversaries are identified and removed based on the computed locations and the new transmission group will be sent to the source node. If there is any new adversary found then it will be broadcasted to all the nodes in the network which will be get updated at the adversaries list of the nodes.

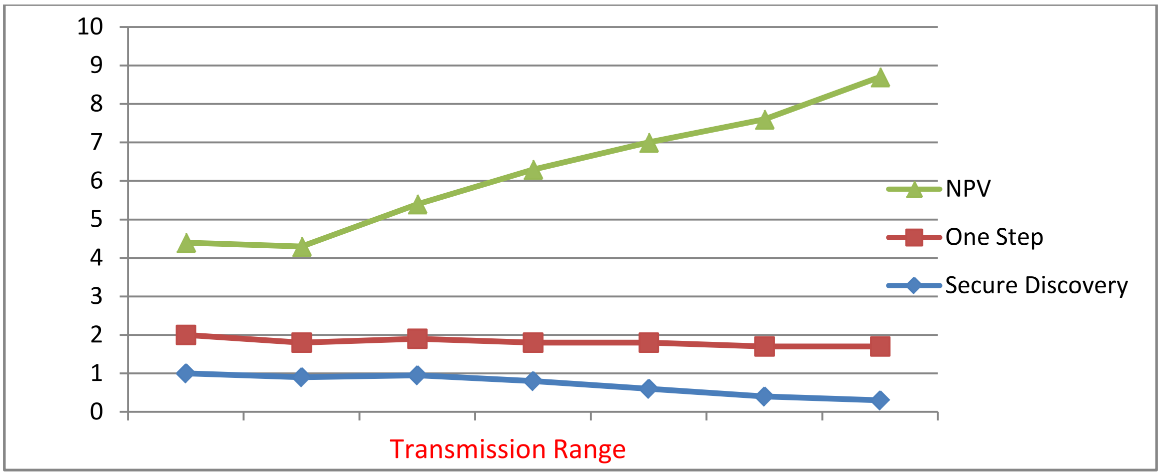
RESULTS AND DISCUSSION

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



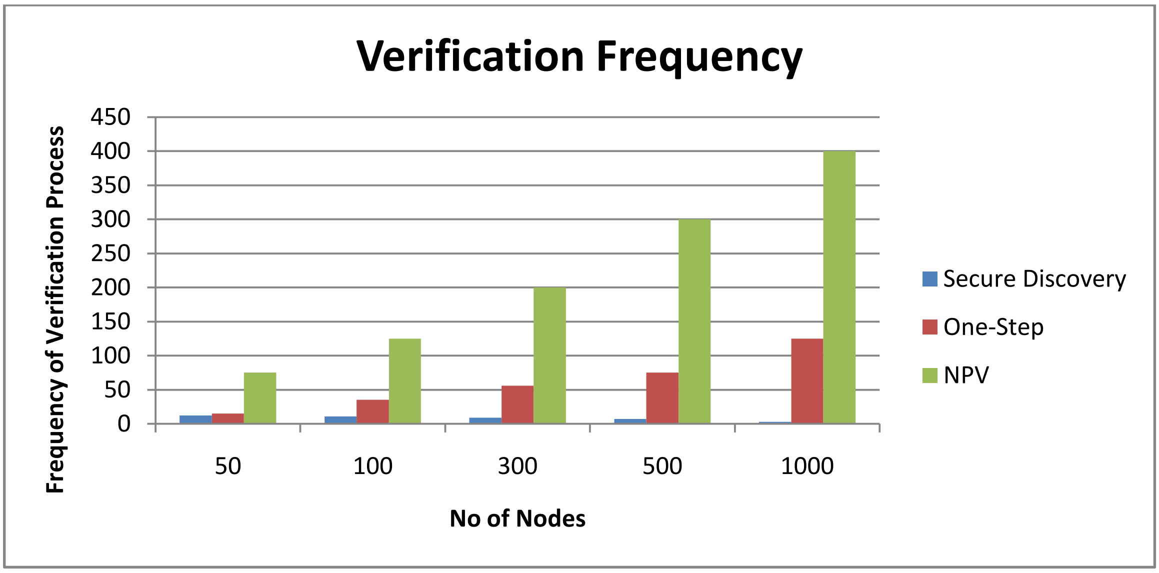
Graph 1: Displacement Allowed according to Range 1.

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



Graph 2: Shows the Traffic introduced by different methods for verification process.

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



Graph 3: Verification Frequency.

The graph 3: shows the frequency of verification process invoked to the base station or in some other form in different approaches. It shows clearly that the proposed approach has minimized the frequency of verification and overhead generated by the process of verification.

Conclusion:

The proposed methodology is a secure one for all kind of attacks coming in mobile adhoc network. We used secure node discovery procedure and location verification process, which is less time consuming and we use proactive and reactive node details , so that even if there are many number of adversaries present in the network we could identify easily with the help of verification process. The proactive details with the reactive information about the nodes help us to increase the performance and throughput of the overall network. Even though the discovery phase introduces little network overhead, it reduces the frequency of verification and overhead generated by earlier methods. The verification process will be asked to the base station only if the adversary notification timer gets expired, which reduces the communication with the base station. Ultimately this discovery and verification scheme increases the throughput and reduces the latency of the network.

REFERENCES

Calandriello, G., P. Papadimitratos, A. Lioy and J.P. Hubaux, 2011. “On the Performance of Secure Vehicular Communication Systems,” IEEE Trans. Dependable and Secure Computing, 8(6): 898-912.

Capkun, S., K. Rasmussen, M. Cagalj and M. Srivastava, 2008. “Secure Location Verification with Hidden and Mobile Base Stations,” IEEE Trans. Mobile Computing, 7(4): 470-483.

Chiang, J., J. Haas and Y. Hu, 2009. “Secure and PreciseLocation Verification Using Distance Bounding and Simultaneous Multilateration,” Proc. Second ACM Conf. Wireless Network Security (WiSec).

Del, E., L.S. Re, L. Ronga, L. Vettori, E. Lo Presti, Falletti and M. Pini, 2009. “Software Defined Radio Terminal for Assisted Localization in Emergency Situations,” Proc. First Int’l Conf. Wireless Comm., Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (CTIF Wireless Vitae).

Ekici, E., S. Vural, J. McNair and D. Al-Abri, 2008. “Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks,” Elsevier Ad Hoc Networks, 6(2): 195-209.

Fiore, M., 2013. Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks , IEEE Transactions on Mobile Computing, 12(2): 289-303.

Fiore, M., C. Casetti, C.F. Chiasserini and P. Papadimitratos, 2011. “Secure Neighbor Position Discovery in Vehicular Networks,” Proc. IEEE/IFIP 10th Ann. Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net).

Ha¨rri, J., M. Fiore, F. Filali and C. Bonnet, 2009. “Vehicular Mobility Simulation with Vanet Mobi Sim,” Trans. Soc. Modeling & Simulation.

Marco Fiore, Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks, IEEE transactions on mobile computing, 12(2).

Poturalksi, M., P. Papadimitratos and J.P. Hubaux, 2008. “Towards Provable Secure Neighbor Discovery in Wireless Networks,” Proc. Workshop Formal Methods in Security Eng.

Poturalski, M., 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),.

PRECIOSA: Privacy Enabled Capability in Co-Operative Systems and Safety Applications, http://www.preciosa-project.org, 2012.

Priyadarshani, K., 2013. Dynamic Neighbor Positioning In Manet with Protection against Adversarial Attacks, IJCER, 3(4).

Seon Yeong Han, 2013. An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols, IEEE Transactions on communication, 17(5): 1040-1043.

Shokri, R., M. Poturalski, G. Ravot, P. Papadimitratos and J.P. Hubaux, 2009. “A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks,” Proc. Second ACM Conf. Wireless Network Security (WiSec).

Thilagavathy, S., 2013. Neighbor node discovery and Trust prediction in manets, International Journal of Science, Engineering and Technology Research (IJSETR), 2(1).